Reporte técnico

Pentester: Federico Leandro Cañellas
Fecha: 17-08-2025
Hora: 19:05:15

Sumario ejecutivo

Este trabajo consiste en el diseño, implementación y validación de un conjunto de scripts en Python orientados a la automatización del reconocimiento, escaneo y explotación ética de aplicaciones web en entornos controlados. El objetivo principal es la confección de un informe técnico generado de forma automatizada, que documenta rutas ocultas, puntos de entrada, cabeceras HTTP, servicios expuestos y vulnerabilidades comunes como SQL Injection y Cross-Site Scripting.
La metodología aplicada integra fases de reconocimiento automatizado, escaneo de puertos y servicios, explotación controlada, validación de resultados y generación automatizada del informe profesional.
El resultado del proyecto incluye scripts funcionales, un flujo automatizado de recopilación y análisis de datos, y un informe final con evidencias, tablas de hallazgos, recomendaciones y niveles de criticidad, siguiendo estándares de redacción profesional y principios de ética en ciberseguridad.
Este trabajo refuerza competencias en automatización ofensiva, análisis técnico de vulnerabilidades y documentación profesional, enfatizando la importancia de aplicar criterios de legalidad, responsabilidad y buenas prácticas en todo el proceso.

Hallazgos

#	Hallazgo / Vulnerabilidad	Descripción	Nivel de criticidad	Impacto	Recomendación
URL: http://testphp.vulnweb.com/.bash_history					
1	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	Media	Permite a un atacante conocer exactamente qué software corre y buscar exploits específicos de esa versión.	• Eliminar header **Server** de la respuesta.
2	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	Baja	Aumento en el riesgo de inyeccion XSS.	• Implementar header **Content-Security-Policy** con dominios de confianza.
3	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	Media	Su ausencia permite a los atacantes realizar **Man in the Middle**.	• Configurar header **Strict-Transport-Security** en URL. • Incluir flag IncludeSubDomains en configuración.

URL: http://testphp.vulnweb.com/					
4	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	Media	Permite a un atacante conocer exactamente qué software corre y buscar exploits específicos de esa versión.	• Eliminar header **Server** de la respuesta.
5	Exposición de información en header **X-Powered-By**	Se detectó **PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1** en el header **X-Powered-By**.	Media	Facilita ataques dirigidos, como exploits de vulnerabilidades conocidas del lenguaje o framework.	• Eliminar header **X-Powered-By** de la respuesta.
6	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	Baja	Aumento en el riesgo de inyeccion XSS.	• Implementar header **Content-Security-Policy** con dominios de confianza.
7	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	Media	Su ausencia permite a los atacantes realizar **Man in the Middle**.	• Configurar header **Strict-Transport-Security** en URL. • Incluir flag IncludeSubDomains en configuración.
URL: http://testphp.vulnweb.com/.bashrc					
8	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	Media	Permite a un atacante conocer exactamente qué software corre y buscar exploits específicos de esa versión.	• Eliminar header **Server** de la respuesta.
9	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	Baja	Aumento en el riesgo de inyeccion XSS.	• Implementar header **Content-Security-Policy** con dominios de confianza.
10	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	Media	Su ausencia permite a los atacantes realizar **Man in the Middle**.	• Configurar header **Strict-Transport-Security** en URL. • Incluir flag IncludeSubDomains en configuración.
URL: http://testphp.vulnweb.com/.config					
11	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	Media	Permite a un atacante conocer exactamente qué software corre y buscar exploits específicos de esa versión.	• Eliminar header **Server** de la respuesta.
12	Ausencia de header **Content-Security-**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	Baja	Aumento en el riesgo de inyeccion XSS.	• Implementar header **Content-Security-Policy** con dominios de confianza.

	Policy				
13	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	Media	Su ausencia permite a los atacantes realizar **Man in the Middle**.	• Configurar header **Strict-Transport-Security** en URL. • Incluir flag IncludeSubDomains en configuración.
URL: http://testphp.vulnweb.com/.cvs					
14	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	Media	Permite a un atacante conocer exactamente qué software corre y buscar exploits específicos de esa versión.	• Eliminar header **Server** de la respuesta.
15	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	Baja	Aumento en el riesgo de inyeccion XSS.	• Implementar header **Content-Security-Policy** con dominios de confianza.
16	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	Media	Su ausencia permite a los atacantes realizar **Man in the Middle**.	• Configurar header **Strict-Transport-Security** en URL. • Incluir flag IncludeSubDomains en configuración.
URL: http://testphp.vulnweb.com/.cvsignore					
17	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	Media	Permite a un atacante conocer exactamente qué software corre y buscar exploits específicos de esa versión.	• Eliminar header **Server** de la respuesta.
18	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	Baja	Aumento en el riesgo de inyeccion XSS.	• Implementar header **Content-Security-Policy** con dominios de confianza.
19	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	Media	Su ausencia permite a los atacantes realizar **Man in the Middle**.	• Configurar header **Strict-Transport-Security** en URL. • Incluir flag IncludeSubDomains en configuración.
URL: http://testphp.vulnweb.com/.env					
20	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	Media	Permite a un atacante conocer exactamente qué software corre y buscar exploits específicos de esa versión.	• Eliminar header **Server** de la respuesta.
	Ausencia de				• Implementar header **Content-**

21	header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	Baja	Aumento en el riesgo de inyeccion XSS.	**Security-Policy** con dominios de confianza.
22	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	Media	Su ausencia permite a los atacantes realizar **Man in the Middle**.	• Configurar header **Strict-Transport-Security** en URL. • Incluir flag IncludeSubDomains en configuración.
URL: http://testphp.vulnweb.com/.forward					
23	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	Media	Permite a un atacante conocer exactamente qué software corre y buscar exploits específicos de esa versión.	• Eliminar header **Server** de la respuesta.
24	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	Baja	Aumento en el riesgo de inyeccion XSS.	• Implementar header **Content-Security-Policy** con dominios de confianza.
25	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	Media	Su ausencia permite a los atacantes realizar **Man in the Middle**.	• Configurar header **Strict-Transport-Security** en URL. • Incluir flag IncludeSubDomains en configuración.
URL: http://testphp.vulnweb.com/#/login					
26	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	Media	Permite a un atacante conocer exactamente qué software corre y buscar exploits específicos de esa versión.	• Eliminar header **Server** de la respuesta.
27	Exposición de información en header **X-Powered-By**	Se detectó **PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1** en el header **X-Powered-By**.	Media	Facilita ataques dirigidos, como exploits de vulnerabilidades conocidas del lenguaje o framework.	• Eliminar header **X-Powered-By** de la respuesta.
28	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	Baja	Aumento en el riesgo de inyeccion XSS.	• Implementar header **Content-Security-Policy** con dominios de confianza.
29	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	Media	Su ausencia permite a los atacantes realizar **Man in the Middle**.	• Configurar header **Strict-Transport-Security** en URL. • Incluir flag IncludeSubDomains en configuración.

URL: http://testphp.vulnweb.com/.cache					
30	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	Media	Permite a un atacante conocer exactamente qué software corre y buscar exploits específicos de esa versión.	• Eliminar header **Server** de la respuesta.
31	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	Baja	Aumento en el riesgo de inyeccion XSS.	• Implementar header **Content-Security-Policy** con dominios de confianza.
32	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	Media	Su ausencia permite a los atacantes realizar **Man in the Middle**.	• Configurar header **Strict-Transport-Security** en URL. • Incluir flag IncludeSubDomains en configuración.
URL: http://testphp.vulnweb.com/					
33	Falta de protección CSRF en formulario	El formulario no implementa un token CSRF, lo que permite a un atacante realizar solicitudes maliciosas en nombre de un usuario autenticado.	Alto	Posible ejecución de acciones no autorizadas, comprometiendo la integridad de la cuenta del usuario y de los datos del sistema.	• Implementar un token CSRF único por sesión o por formulario, validando su presencia en cada solicitud POST. • Alternativamente, usar cabeceras SameSite y técnicas de doble cookie para protección adicional.
URL: http://testphp.vulnweb.com/#/login					
34	Falta de protección CSRF en formulario	El formulario no implementa un token CSRF, lo que permite a un atacante realizar solicitudes maliciosas en nombre de un usuario autenticado.	Alto	Posible ejecución de acciones no autorizadas, comprometiendo la integridad de la cuenta del usuario y de los datos del sistema.	• Implementar un token CSRF único por sesión o por formulario, validando su presencia en cada solicitud POST. • Alternativamente, usar cabeceras SameSite y técnicas de doble cookie para protección adicional.
Host: 192.168.1.1					
35	Puerto expuesto **22**	**Servicio:** Shell Seguro (SSH), inicios de sesión seguros, transferencias de archivos (scp, sftp) y reenvío de puertos.	Alta	Acceso administrativo remoto; compromiso del servidor si existen credenciales débiles o exploits	• Mantener actualizado; usar claves en lugar de contraseñas; restringir acceso por IP mediante firewall.
				Exposición de aplicaciones web	• Migrar a HTTPS con TLS; aplicar

36	Puerto expuesto **80**	**Servicio:** Protocolo de Transferencia de Hipertexto (HTTP) usa TCP en las versiones 1.x y 2. HTTP/3 usa QUIC, un protocolo de transporte sobre UDP.	Alta	que pueden contener vulnerabilidades (XSS, SQLi, RCE, etc.); transmisión de datos sin cifrado	hardening en el servidor web; implementar WAF y prácticas de desarrollo seguro.
37	Puerto expuesto **443**	**Servicio:** Protocolo Seguro de Transferencia de Hipertexto (HTTPS) usa TCP en versiones 1.x y 2. HTTP/3 usa QUIC, un protocolo de transporte sobre UDP.	Alta	Ataques SSL/TLS débiles o mal configurados pueden exponer datos sensibles.	• Usar TLS 1.2/1.3; deshabilitar protocolos inseguros; aplicar certificados válidos y monitoreo continuo.
38	URL vulnerable a SQLi.	URL **http://localhost:4000/login.php** permite ejecutar consultas maliciosas contra la base de datos, exponiendo o alterando información sensible.	Crítico	Acceso no autorizado a la base de datos, robo de credenciales, modificación o eliminación de datos, escalamiento de privilegios.	• Implementar consultas parametrizadas(preparadas) en todas las interacciones con la base de datos para mitigar SQLi.
39	URL vulnerable a SQLi.	URL **http://localhost:4000/message.php** permite ejecutar consultas maliciosas contra la base de datos, exponiendo o alterando información sensible.	Crítico	Acceso no autorizado a la base de datos, robo de credenciales, modificación o eliminación de datos, escalamiento de privilegios.	• Implementar consultas parametrizadas(preparadas) en todas las interacciones con la base de datos para mitigar SQLi.
40	URL vulnerable a XSS.	URL **http://localhost:4000/get-message.php** permite inyectar y ejecutar código JavaScript en el navegador de los usuarios, comprometiendo su sesión o datos personales.	Crítico	Robo de cookies de sesión, redirección a sitios maliciosos, manipulación de la interfaz, phishing interno.	• Aplicar validación estricta y codificación de salida (output encoding) en todos los parámetros que se muestran en la interfaz para evitar XSS.

Evidencias

#	Hallazgo / Vulnerabilidad	Descripción	Evidencia	URL
1	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	nginx/1.19.0	http://testphp.vulnweb.com/.bash_history
2	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	**Headers:** Server, Date, Content-Type	http://testphp.vulnweb.com/.bash_history
3	Ausencia de header **Strict-Transport-**	No se está forzando la comunicación HTTPS debido a la ausencia del header	**Headers:** Server, Date, Content-Type	http://testphp.vulnweb.com/.bash_history

	Security	**Strict-Transport-Security**.		
4	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	nginx/1.19.0	http://testphp.vulnweb.com/
5	Exposición de información en header **X-Powered-By**	Se detectó **PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1** en el header **X-Powered-By**.	PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1	http://testphp.vulnweb.com/
6	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	**Headers:** Server, Date, Content-Type, X-Powered-By	http://testphp.vulnweb.com/
7	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	**Headers:** Server, Date, Content-Type, X-Powered-By	http://testphp.vulnweb.com/
8	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	nginx/1.19.0	http://testphp.vulnweb.com/.bashrc
9	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	**Headers:** Server, Date, Content-Type	http://testphp.vulnweb.com/.bashrc
10	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	**Headers:** Server, Date, Content-Type	http://testphp.vulnweb.com/.bashrc
11	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	nginx/1.19.0	http://testphp.vulnweb.com/.config
12	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	**Headers:** Server, Date, Content-Type	http://testphp.vulnweb.com/.config
13	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	**Headers:** Server, Date, Content-Type	http://testphp.vulnweb.com/.config
	Exposición de			

14	información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	nginx/1.19.0	http://testphp.vulnweb.com/.cvs
15	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	**Headers:** Server, Date, Content-Type	http://testphp.vulnweb.com/.cvs
16	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	**Headers:** Server, Date, Content-Type	http://testphp.vulnweb.com/.cvs
17	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	nginx/1.19.0	http://testphp.vulnweb.com/.cvsignore
18	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	**Headers:** Server, Date, Content-Type	http://testphp.vulnweb.com/.cvsignore
19	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	**Headers:** Server, Date, Content-Type	http://testphp.vulnweb.com/.cvsignore
20	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	nginx/1.19.0	http://testphp.vulnweb.com/.env
21	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	**Headers:** Server, Date, Content-Type	http://testphp.vulnweb.com/.env
22	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	**Headers:** Server, Date, Content-Type	http://testphp.vulnweb.com/.env
23	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	nginx/1.19.0	http://testphp.vulnweb.com/.forward
24	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	**Headers:** Server, Date, Content-Type	http://testphp.vulnweb.com/.forward

25	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	**Headers:** Server, Date, Content-Type	http://testphp.vulnweb.com/.forward
26	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	nginx/1.19.0	http://testphp.vulnweb.com/#/login
27	Exposición de información en header **X-Powered-By**	Se detectó **PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1** en el header **X-Powered-By**.	PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1	http://testphp.vulnweb.com/#/login
28	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	**Headers:** Server, Date, Content-Type, X-Powered-By	http://testphp.vulnweb.com/#/login
29	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	**Headers:** Server, Date, Content-Type, X-Powered-By	http://testphp.vulnweb.com/#/login
30	Exposición de información en header **Server**	Se detectó **nginx/1.19.0** en el header **Server**.	nginx/1.19.0	http://testphp.vulnweb.com/.cache
31	Ausencia de header **Content-Security-Policy**	No hay restricciones para cargar scripts de terceros, inline scripts, llamado a funciones como **eval** o URLs **javascript:**	**Headers:** Server, Date, Content-Type	http://testphp.vulnweb.com/.cache
32	Ausencia de header **Strict-Transport-Security**	No se está forzando la comunicación HTTPS debido a la ausencia del header **Strict-Transport-Security**.	**Headers:** Server, Date, Content-Type	http://testphp.vulnweb.com/.cache
33	Falta de protección CSRF en formulario	El formulario no implementa un token CSRF, lo que permite a un atacante realizar solicitudes maliciosas en nombre de un usuario autenticado.	Elementos del form: searchFor, goButton	http://testphp.vulnweb.com/
34	Falta de protección CSRF en formulario	El formulario no implementa un token CSRF, lo que permite a un atacante realizar solicitudes maliciosas en nombre de un usuario autenticado.	Elementos del form: searchFor, goButton	http://testphp.vulnweb.com/#/login
35	Puerto expuesto **22**	**Servicio:** Shell Seguro (SSH), inicios de sesión seguros, transferencias de archivos (scp, sftp) y reenvío de	**Detección nmap**: Dropbear sshd 2019.78 protocol 2.0	IP: 192.168.1.1

		puertos.		
36	Puerto expuesto **80**	**Servicio:** Protocolo de Transferencia de Hipertexto (HTTP) usa TCP en las versiones 1.x y 2. HTTP/3 usa QUIC, un protocolo de transporte sobre UDP.	**Detección nmap**: micro_httpd	IP: 192.168.1.1
37	Puerto expuesto **443**	**Servicio:** Protocolo Seguro de Transferencia de Hipertexto (HTTPS) usa TCP en versiones 1.x y 2. HTTP/3 usa QUIC, un protocolo de transporte sobre UDP.	**Detección nmap**: micro_httpd	IP: 192.168.1.1
38	URL vulnerable a SQLi.	URL **http://localhost:4000/login.php** permite ejecutar consultas maliciosas contra la base de datos, exponiendo o alterando información sensible.	Payloads testeados: **SQL error**, **' or 1=1; --**, **' or `1`=`1`; --**	http://localhost:4000/login.php
39	URL vulnerable a SQLi.	URL **http://localhost:4000/message.php** permite ejecutar consultas maliciosas contra la base de datos, exponiendo o alterando información sensible.	Payloads testeados: **SQL error**, **' or 1=1; --**, **' or `1`=`1`; --**, **[Error] Cannot connect to host localhost:4000 ssl:default [Connect call failed ('127.0.0.1', 4000)]**, **[Error] Cannot connect to host localhost:4000 ssl:default [Connect call failed ('127.0.0.1', 4000)]**, **[Error] Cannot connect to host localhost:4000 ssl:default [Connect call failed ('127.0.0.1', 4000)]**, **[Error] Cannot connect to host localhost:4000 ssl:default [Connect call failed ('127.0.0.1', 4000)]**, **[Error] Cannot connect to host localhost:4000 ssl:default [Connect call failed ('127.0.0.1', 4000)]**	http://localhost:4000/message.php
40	URL vulnerable a XSS.	URL **http://localhost:4000/get-message.php** permite inyectar y ejecutar código JavaScript en el navegador de los usuarios, comprometiendo su sesión o datos personales.	Payloads testeados: **Básico <script>alert(1)</script>**, **HTML image with onerror**, **SVG with onload**, **Atributo con evento JS**, **Tag cerrado malicioso**, **JS URI en iframe**, **[Error] Cannot connect to host localhost:4000 ssl:default [Connect call failed ('127.0.0.1', 4000)]**, **[Error] Cannot connect to host localhost:4000 ssl:default [Connect call failed ('127.0.0.1', 4000)]**, **[Error] Cannot connect to host localhost:4000 ssl:default [Connect call failed ('127.0.0.1', 4000)]**, **[Error] Cannot connect to host localhost:4000 ssl:default [Connect call failed ('127.0.0.1', 4000)]**, **[Error] Cannot connect to host**	http://localhost:4000/get-message.php

			localhost:4000 ssl:default [Connect call failed ('127.0.0.1', 4000)], [Error] Cannot connect to host localhost:4000 ssl:default [Connect call failed ('127.0.0.1', 4000)]	

Recomendaciones técnicas

#	Hallazgo / Vulnerabilidad	Recomendación	Responsable	Prioridad
URL: http://testphp.vulnweb.com/.bash_history				
1	Exposición de información en header **Server**	Eliminar header **Server** de larespuesta.	DevOps/Backend	Media
2	Ausencia de header **Content-Security-Policy**	Implementar header **Content-Security-Policy** con dominios de confianza.	Devops/Frontend	Alta
3	Ausencia de header **Strict-Transport-Security**	Incluir flag IncludeSubDomains en configuración.	Devops	Alta
URL: http://testphp.vulnweb.com/				
4	Exposición de información en header **Server**	Eliminar header **Server** de larespuesta.	DevOps/Backend	Media
5	Exposición de información en header **X-Powered-By**	Eliminar header **X-Powered-By** de larespuesta.	DevOps/Backend	Media
6	Ausencia de header **Content-Security-Policy**	Implementar header **Content-Security-Policy** con dominios de confianza.	Devops/Frontend	Alta
7	Ausencia de header **Strict-Transport-Security**	Incluir flag IncludeSubDomains en configuración.	Devops	Alta
URL: http://testphp.vulnweb.com/.bashrc				
8	Exposición de información en header **Server**	Eliminar header **Server** de larespuesta.	DevOps/Backend	Media
9	Ausencia de header **Content-Security-Policy**	Implementar header **Content-Security-Policy** con dominios de confianza.	Devops/Frontend	Alta
10	Ausencia de header **Strict-Transport-Security**	Incluir flag IncludeSubDomains en configuración.	Devops	Alta
URL: http://testphp.vulnweb.com/.config				
11	Exposición de información en header **Server**	Eliminar header **Server** de larespuesta.	DevOps/Backend	Media
12	Ausencia de header **Content-Security-Policy**	Implementar header **Content-Security-Policy** con dominios de confianza.	Devops/Frontend	Alta

13	Ausencia de header **Strict-Transport-Security**	Incluir flag IncludeSubDomains en configuración.	Devops	Alta
URL: http://testphp.vulnweb.com/.cvs				
14	Exposición de información en header **Server**	Eliminar header **Server** de larespuesta.	DevOps/Backend	Media
15	Ausencia de header **Content-Security-Policy**	Implementar header **Content-Security-Policy** con dominios de confianza.	Devops/Frontend	Alta
16	Ausencia de header **Strict-Transport-Security**	Incluir flag IncludeSubDomains en configuración.	Devops	Alta
URL: http://testphp.vulnweb.com/.cvsignore				
17	Exposición de información en header **Server**	Eliminar header **Server** de larespuesta.	DevOps/Backend	Media
18	Ausencia de header **Content-Security-Policy**	Implementar header **Content-Security-Policy** con dominios de confianza.	Devops/Frontend	Alta
19	Ausencia de header **Strict-Transport-Security**	Incluir flag IncludeSubDomains en configuración.	Devops	Alta
URL: http://testphp.vulnweb.com/.env				
20	Exposición de información en header **Server**	Eliminar header **Server** de larespuesta.	DevOps/Backend	Media
21	Ausencia de header **Content-Security-Policy**	Implementar header **Content-Security-Policy** con dominios de confianza.	Devops/Frontend	Alta
22	Ausencia de header **Strict-Transport-Security**	Incluir flag IncludeSubDomains en configuración.	Devops	Alta
URL: http://testphp.vulnweb.com/.forward				
23	Exposición de información en header **Server**	Eliminar header **Server** de larespuesta.	DevOps/Backend	Media
24	Ausencia de header **Content-Security-Policy**	Implementar header **Content-Security-Policy** con dominios de confianza.	Devops/Frontend	Alta
25	Ausencia de header **Strict-Transport-Security**	Incluir flag IncludeSubDomains en configuración.	Devops	Alta
URL: http://testphp.vulnweb.com/#/login				
26	Exposición de información en header **Server**	Eliminar header **Server** de larespuesta.	DevOps/Backend	Media
27	Exposición de información en header **X-Powered-By**	Eliminar header **X-Powered-By** de larespuesta.	DevOps/Backend	Media
	Ausencia de header **Content-**			

28	Ausencia de header **Content-Security-Policy**	Implementar header **Content-Security-Policy** con dominios de confianza.	Devops/Frontend	Alta
29	Ausencia de header **Strict-Transport-Security**	Incluir flag IncludeSubDomains en configuración.	Devops	Alta
URL: http://testphp.vulnweb.com/.cache				
30	Exposición de información en header **Server**	Eliminar header **Server** de larespuesta.	DevOps/Backend	Media
31	Ausencia de header **Content-Security-Policy**	Implementar header **Content-Security-Policy** con dominios de confianza.	Devops/Frontend	Alta
32	Ausencia de header **Strict-Transport-Security**	Incluir flag IncludeSubDomains en configuración.	Devops	Alta
URL: http://testphp.vulnweb.com/				
33	Falta de protección CSRF en formulario	Implementar token CSRF único por formulario, validando su presencia en cada solicitud.	Backend	Alta
URL: http://testphp.vulnweb.com/#/login				
34	Falta de protección CSRF en formulario	Implementar token CSRF único por formulario, validando su presencia en cada solicitud.	Backend	Alta
Host: 192.168.1.1				
35	Puerto expuesto **22**	Mantener actualizado; usar claves en lugar de contraseñas; restringir acceso por IP mediante firewall.	SysAdmin/DevOps	Alta
36	Puerto expuesto **80**	Migrar a HTTPS con TLS; aplicar hardening en el servidor web; implementar WAF y prácticas de desarrollo seguro.	SysAdmin/DevOps	Alta
37	Puerto expuesto **443**	Usar TLS 1.2/1.3; deshabilitar protocolos inseguros; aplicar certificados válidos y monitoreo continuo.	SysAdmin/DevOps	Alta
38	URL vulnerable a SQLi.	Implementar consultas parametrizadas(preparadas) en todas las interacciones con la base de datos para mitigar SQLi.	Backend	Crítica
39	URL vulnerable a SQLi.	Implementar consultas parametrizadas(preparadas) en todas las interacciones con la base de datos para mitigar SQLi.	Backend	Crítica
40	URL vulnerable a XSS.	Aplicar validación estricta y codificación de salida (output encoding) en todos los parámetros que se muestran en la interfaz para evitar XSS.	Backend	Crítica

Nivel de Criticidad

Nivel	Descripción	Número de Hallazgos	Ejemplos comunes
	Compromete de forma inmediata la confidencialidad, integridad		Ejecución remota de código (RCE), inyección SQL sin

Crítico	o disponibilidad de sistemas y datos.	2	autenticación, fuga masiva de datos sensibles.
Alto	Puede ser explotado con relativa facilidad y causar impacto significativo.	6	XSS almacenado, CSRF que permite acciones críticas, credenciales hardcodeadas.
Medio	Impacto moderado o requiere condiciones específicas para explotarse.	22	XSS reflejado, exposición de rutas internas, uso de cifrado obsoleto (MD5, SHA1).
Bajo	Bajo impacto, sin riesgo directo inmediato.	10	Información de versión del servidor, mensajes de error detallados, encabezados de seguridad ausentes.

Reflexión Ética y Profesional

¿Cómo garantizaste que tus pruebas fueron éticas y controladas?

Trabajé siempre en entornos controlados o de laboratorio, evitando afectar datos reales o la disponibilidad de servicios en producción.
Documenté cada paso para poder justificar las acciones y resultados, y me aseguré de detener cualquier prueba que pudiera generar un impacto no previsto.

¿Qué aprendiste sobre el poder y los límites de la automatización ofensiva?

Aprendí que la automatización ofensiva es muy poderosa para acelerar y escalar pruebas, porque me permite lanzar miles de requests, payloads o análisis en muy poco tiempo y con consistencia, cubriendo superficies de ataque enormes sin saltarme pasos. También facilita integrar pruebas en pipelines y encontrar patrones que manualmente me costaría mucho detectar.
Pero también entendí que tiene límites claros: puede generar falsos positivos o falsos negativos, no interpreta la lógica de negocio, no se adapta bien a defensas o validaciones poco comunes, y no reemplaza la creatividad ni el criterio humano para encadenar vulnerabilidades y evaluar su impacto real.
En el fondo, la veo como una herramienta que potencia mi trabajo, pero no lo sustituye; necesito estar encima para guiarla, interpretarla y decidir el siguiente paso.

¿Qué decisiones tomaste que reflejan responsabilidad profesional en ciberseguridad?

Simulé servicios vulnerables para evitar afectar la disponibilidad de sitios que son efectivamente vulnerables para propósitos de estudio. De ésta manera, tambien evité realizar pruebas sin autorización previa.