

PROYECTO FINAL
Tienda Minishop
Grupo 3

Realizado por:

CRISTIAN CAMILO OROZCO OSPINA
JUAN SEBASTIAN JIMENEZ SEPULVEDA
JAIDER ROJAS ALVAREZ
MATEO CORRALES VINASCO

Pruebas de Software

JEISSON IBARGUEN MATURANA

Institución Universitaria Pascual Bravo

TABLA DE CONTENIDO

1. INTRODUCCIÓN.....	2
2. ROLES DEL EQUIPO.....	2
3. CHECKLIST OWASP.....	3
4. MATRIZ DE TRAZABILIDAD.....	6
5. PRUEBAS FUNCIONALES.....	8
6. PRUEBAS DE RENDIMIENTO.....	12
7. PRUEBAS DE SEGURIDAD.....	19
8. RECOMENDACIONES.....	27
9. CONCLUSIÓN.....	28

INTRODUCCIÓN

El presente documento documenta la evaluación completa de la plataforma Tienda Minishop (<https://pascualbravo.ingejei.com/>), basada en WordPress/WooCommerce. El objetivo principal es aplicar metodologías, herramientas y pruebas funcionales, de rendimiento y de seguridad para asegurar que la tienda Minishop cumpla con estándares de calidad, de funcionalidad y de datos. Basado en ello, se realizaron las siguientes pruebas:

1. Pruebas funcionales: Se validaron las funciones más importantes como: registro, búsqueda de productos, carrito de compras, checkout y notificaciones, utilizando casos de prueba bien definidos y scripts automatizados en Selenium.
2. Pruebas de rendimiento: Se utilizó JMeter para simular escenarios de carga, incluyendo usuarios simultáneos, procesos de compra concurrentes, subida masiva de imágenes y estrés sobre la base de datos. Se midieron tiempos de respuesta y estabilidad bajo diferentes condiciones.
3. Pruebas de seguridad: Se realizó una auditoría basada en OWASP Top 10, apoyada por herramientas como Burp Suite, SQLMap e Hydra. Se identificaron posibles vulnerabilidades como inyección SQL, XSS, ataques de fuerza bruta, fallos en control de acceso, CSRF, encabezados HTTP mal configurados y componentes desactualizados.

ROLES DEL EQUIPO

Rol	Funciones	Nombres
<i>Auditor de Pruebas</i>	Aprueba estrategia, vigila cobertura, firma el informe.	Jaider Rojas Alvarez
<i>Equipo de Pruebas</i>	Crea y corre los scripts de Selenium/JMeter/Kali.	Juan Sebastian Jimenez
<i>Documentador</i>	Redacta el PDF y recopila evidencias.	Mateo Corrales Vinasco
<i>Presentador</i>	Sintetiza hallazgos y lidera la defensa oral.	Cristian Camilo Orozco

CHECKLIST OWASP

Item	Categoría	Checklist (¿Qué se verifica?)	¿Cómo se verifica?
A1	Inyección	<p>¿Es posible inyectar código malicioso en campos de entrada o URLs?</p> <p>¿La aplicación valida y limpia correctamente los datos antes de ejecutar consultas SQL u otros comandos?</p>	<p>Ubica campos que envíen datos al servidor, como formularios de login o búsqueda, e ingresa cargas como 'OR '1'='1 o similares. Observa si se alteran valores, aparecen errores del sistema o se muestra información que importante. También se puede usar herramientas como SQLMap o BurpSuite para detectar posibles lugares de inyección.</p> <p>Después, prueba si los datos ingresados son validados o escapados correctamente. Si las cargas no se ejecutan y no afectan la aplicación, significa que las solicitudes y consultas son limpiadas y aseguradas correctamente.</p>
A2	Pérdida de autenticación y gestión de sesiones	<p>¿Se puede acceder a secciones protegidas sin iniciar sesión?</p> <p>¿Las sesiones expiran de manera adecuada?</p>	<p>Inicia sesión desde el login y accede a alguna sección de la página que solo sea accesible si has iniciado sesión (por ejemplo: tu carrito de compras, el checkout de un producto o el panel de administrador para agregar productos). Luego, copia la URL de esa página y cierra sesión. Después, pega esa URL en el navegador para verificar si puedes acceder sin haber iniciado sesión o si te redirige al login u otra sección que impida el acceso. Esta prueba se puede hacer de forma manual o utilizando Selenium.</p> <p>Iniciar sesión normalmente en la aplicación y permanecer inactivo por un tiempo (10 a 30 minutos). Verificar que el sistema detecta la inactividad y que, al momento de ejecutar una acción que requiera una sesión activa o que esté restringida por sesión (como entrar a mi perfil, preferencias, etc.), se dirija efectivamente a una página de login o que indique un mensaje de sesión terminada. Se puede realizar o automatizar con Selenium.</p>

A3	Datos sensibles accesibles	<p>¿Los datos que se mandan en los formularios se mandan de manera segura y encriptada?</p> <p>¿Los datos de un usuario pueden ser vistos por otros usuarios que no deberían?</p>	<p>Verificar el tipo de protocolo de la página, viendo que esta tenga protocolo de encriptación de datos HTTPS y que estos no se envíen en texto plano, para que nadie pueda ver los datos enviados. También se puede usar BurpSuite para ver la forma en que se envían los datos y asegurarse de que estos vayan cifrados.</p> <p>Primero, inicia sesión con una cuenta de usuario y entra a la sección donde aparezca información sensible, como los datos de la cuenta. Copia la URL de esa página y luego cierra sesión. Después, inicia sesión con otra cuenta diferente, pega la URL que copiaste y fíjate si te permite ver la información del primer usuario o si te redirige para que no puedas acceder a esos datos.</p>
A4	Entidad externa de XML (XXE)	¿Se permite la carga de XML en algún formulario de la aplicación?	Revisar en todos los formularios de la aplicación si en alguno de ellos se necesita la carga de archivos XML. En aquellos que utilicen cargas XML, ejecutar cargas (payloads) modificadas para intentar inyectar código, recursos o estructuras de documento maliciosas.
A5	Control de acceso inseguro	<p>Se prohíbe correctamente el acceso a recursos o funcionalidades según el rol o nivel de acceso del usuario?</p> <p>¿Se previene la escalación de privilegios?</p>	<p>Iniciar sesión con un usuario con un rol o nivel de acceso bajo (por ejemplo, un cliente) e intentar acceder a URLs o funcionalidades que requieren un rol o nivel de acceso superior. Repetir el paso anterior, pero con un rol o nivel de acceso alto (por ejemplo, un administrador).</p> <p>Enviar con herramientas como Selenium o Postman, peticiones y llamadas a Endpoints o APIs para comprobar sus respuestas HTTP (403, 401, etc.), según las claves de acceso o la falta de estas.</p>
A6	Configuración de seguridad incorrecta	<p>¿Existen headers de seguridad HTTP faltantes o una mala configuración (CORS, CSP, X-Frame-Options, etc.)?</p> <p>¿Hay directorios expuestos que no deberían ser públicos?</p>	<p>Utilizar herramientas online como securityheaders.com o Mozilla HTTP Observer para escanear los headers de la página web.</p> <p>Asegurarse de que en la configuración de Apache/NGINX los directorios y puertos expuestos sean los mínimos y necesarios. También se pueden utilizar escáneres de vulnerabilidades como OWASP ZAP o Nikto para verificar endpoints o directorios expuestos.</p>

A7	Cross site scripting (XSS)	¿Existen entradas donde se puedan inyectar scripts o código malicioso?	<p>Inyectar cargas (payloads) que alerten sobre la ejecución inadecuada de código (por ejemplo, <code><script>alert(1)</script></code>) en los campos de entrada y endpoints, es decir, búsquedas, comentarios, formularios, etc., y observar las respuestas en el navegador o en BurpSuite.</p> <p>Verificar que el contenido ingresado por el usuario sea escapado, sanitizado y limpiado correctamente para evitar la ejecución inesperada de código.</p>
A8	Decodificación insegura	¿Se decodifican los datos o cargas externas de forma insegura (JSON, XML, etc.)?	<p>Encontrar los endpoints que reciben datos codificados (JSON, XML, etc.) y enviar cargas (payloads) modificadas que intenten ejecutar, acceder o mostrar recursos sensibles que no deberían estar expuestos al momento de decodificar estas cargas.</p> <p>Verificar con Burp Intruder la decodificación con diferentes cargas y formatos para asegurarse de que la decodificación se ejecuta de manera segura.</p>
A9	Componentes con vulnerabilidades	¿Se usan librerías, componentes o recursos externos desactualizados y obsoletos?	<p>Verificar la lista de dependencias y plugins para confirmar que las versiones instaladas (chequeando package.json y wp plugin list) son las últimas o no están obsoletas. Estas verificaciones de vulnerabilidades se pueden realizar mediante herramientas como WPScan y Patchstack, además de consultar las bases de datos públicas de vulnerabilidades CVE.</p>
A10	Insuficiente monitorización y registro	<p>¿Se registra de forma correcta la actividad o el tráfico sospechoso, o eventos de seguridad importantes?</p> <p>¿Los logs están activados, guardados y protegidos correctamente?</p>	<p>Realizar acciones de seguridad importantes, como logins exitosos y fallidos, cambios de contraseñas, cambios de correo, eliminación de datos, etc., y comprobar que el log posea la información correspondiente, documentando la fecha y hora, la cuenta e IP, la acción y el resultado como información adicional. Esta información específica se obtiene codificando el logger propiamente, o a través de herramientas como Wordfence o los logs del panel de control. Se puede acceder a los logs básicos técnicos activando el modo DEBUG de WordPress.</p> <p>Verificar que la configuración de la herramienta o código logger es correcta y que evita que los logs sean eliminados accidentalmente, o que solo sean eliminados después de mucho tiempo (se recomienda que esté configurado a que permanezcan mínimo 90 días) además, que solo se pueda acceder a ellos por usuarios o cuentas con roles o niveles de acceso correctos.</p>

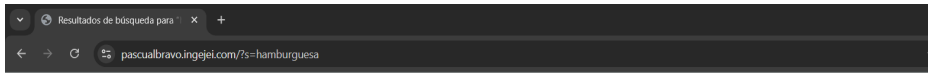
MATRIZ DE TRAZABILIDAD

ID	Categoría	Prioridad	Fuente	Objetivo	Herramienta
1	Funcionalidad	Alta	https://pascualbravo.ingejei.com/wp-login.php?action=register	Verificar el registro de usuarios y que se puedan crear cuentas sin errores.	Selenium
2	Funcionalidad	Alta	https://pascualbravo.ingejei.com/wp-login.php	Comprobar el correcto funcionamiento del login según credenciales inválidas y válidas y la muestra de mensajes de error adecuados	Selenium
3	Funcionalidad	Baja	https://pascualbravo.ingejei.com/registro-y-busqueda/	Verificar que el filtro por palabra clave funcione de manera correcta, pasando resultados	Selenium
5	Funcionalidad	Media	https://pascualbravo.ingejei.com/shop/	Comprobar que funcione de manera correcta la opción de agregar productos al carrito	Selenium
6	Funcionalidad	Alta	https://pascualbravo.ingejei.com/checkout/	Probar el flujo de pago con tarjeta comprobando que se complete sin que haya fallos	Selenium
7	Funcionalidad	Media	https://pascualbravo.ingejei.com/wp-login.php?action=lostpassword	Validar el envío de correos transaccionales y ver si se reciben las notificaciones	Selenium
8	Rendimiento	Media	pascualbravo.ingejei.com	Simular 500 usuarios concurrentes navegando por la pagina principal, y medir los tiempos de respuesta y su demanda	JMeter

9	Rendimiento	Media	https://pascualbravo.ingejei.com/checkout/	Medir los tiempos de respuesta en el checkout probandolo con 100 usuarios simultáneos y encontrar errores de timeout	JMeter
10	Rendimiento	Media	http://pascualbravo.ingejei.com/wp-admin/media-new.php	Subir archivos grandes a través de un test para medir el estrés de la página con cargas masivas sin que haya caídas	JMeter
11	Rendimiento	Media	https://pascualbravo.ingejei.com/?s=hamburguesa	Medir los tiempos de respuesta, carga, velocidad y % de error sobre una carga de 200 usuarios/llamadas concurrentes	JMeter
12	Rendimiento	Media	pascualbravo.ingejei.com/shop	Realizar test de resistencia durante 2 horas usando 100 usuarios, esto para detectar fugas de memoria o ver si hay degradación del servicio	JMeter
13	Seguridad	Alta	https://pascualbravo.ingejei.com/wp-login.php	Escanear vulnerabilidades SQL injection con todos los formularios de entrada	Burpsuite - Curl
14	Seguridad	Alta	https://pascualbravo.ingejei.com/wp-login.php	Probar el inicio de sesión por fuerza bruta	Hydra
15	Seguridad	Alta	https://pascualbravo.ingejei.com/wp-login.php	Auditar la gestión de roles y permisos intentando accesos no autorizados	Burpsuite - Curl
16	Seguridad	Media	https://pascualbravo.ingejei.com/	Revisar los encabezados de seguridad HTTP para mitigar ataques de inyección y clickjacking	Burpsuite - SQLMap
17	Seguridad	Media	https://pascualbravo.ingejei.com/wp-login.php	Envíos de formularios de peticiones con y sin el token CSRF válido	Nmap - Kali Linux

PRUEBAS FUNCIONALES

ID	Descripción	Precondición	Entrada	Resultado esperado	Responsable	Resultado
1	Quiero verificar que el flujo de registro de usuario funcione correctamente, para que los nuevos usuarios puedan crear su cuenta sin errores ni validaciones faltantes.	El usuario no debe de tener una cuenta registrada previamente (no puede usar el mismo correo), la base de datos debe de estar conectada con la página.	Correo electrónico y contraseña	Un mensaje debe de ser visible indicando que su registro ha sido completado.	Juan Sebastian Jimenez	Exitoso
 <p>Running 'LoginyRegister'</p> <ol style="list-style-type: none"> 1. open on /wp-login.php?action=register OK 2. type on id=user_login with value persona2 OK 3. type on id=user_email with value persona2@gmail.com OK 4. click on id=wp-submit OK <p>'LoginyRegister' completed successfully</p>						
2	Quiero validar la búsqueda de productos por palabra clave, para que los resultados sean relevantes y muestren la información completa (imagen, precio, stock).	Debe estar respectivamente logueado el usuario y el sistema tiene productos registrados en la base de datos con títulos, descripciones, imágenes, precios y stock	La palabra Clave deseada (por ejemplo Hamburguesa)	El sistema muestra el producto buscado con toda su respectiva información	Juan Sebastian Jimenez	Exitoso



PASCUALBRAVO (PRUEBAS SOFTWARE)

Inicio Equipo Aplicación Contacto Shop

Latest posts

Hamburguesa Rica



mayo 27, 2025

Running 'FiltroyProductos'

1. open on /wp-login.php OK
2. type on id=user_login with value JEISIM18@GMAIL.COM OK
3. type on id=user_pass with value |wAVKAaeW6\n OK
4. open on /registro-y-busqueda/ OK
5. type on id=wp-block-search__input-2 with value hamburguesa OK
6. click on css=button.wp-block-search__button OK

'FiltroyProductos' completed successfully

3

Quiero probar el proceso de añadir y eliminar productos del carrito, **para que** el total de la compra se actualice correctamente y no queden residuos de artículos.

El usuario debe estar logueado con su respectiva cuenta y hay productos disponibles para agregar al carrito


Añadir el producto deseado, estar en el apartado de Cart

El carrito debe mostrar solo el producto deseado, con su respectivo total dependiendo de la cantidad de productos a comprar y al dar click en la opción eliminar este desaparece del carrito

Juan
Sebastián
Jimenez

Exitoso

Cart

PRODUCTO	TOTAL	TOTAL DEL CARRITO
 <p>Hamburguesa Rica</p> <p>\$30,000.00 \$25,000.00</p> <p>GUARDAR \$5,000.00</p> <p>Experimenta una Explosión de Sabor Presentamos la Hamburguesa Rica, una delicia que te hará agua la...</p> <p>- 1 +</p> <p>Eliminar artículo</p>	\$25,000.00	<p>Añade un cupón</p> <hr/> <p>Subtotal \$25,000.00</p> <hr/> <p>Total \$25,000.00</p> <p>Proceder al pago</p>

Cart



Your cart is currently empty!

New in store

Running 'AgregarEliminarProductosCarrito'

- open on /wp-login.php OK
- type on id=user_login with value JEISIM18@GMAIL.COM OK
- type on id=user_pass with value jwAVKAaeW6 OK
- open on /shop OK
- click on css=button.add_to_cart_button[data-product_id="24"] OK
- open on /cart OK
- click on css=button.wc-block-cart-item__remove-link[aria-label="Hamburguesa Rica"] OK

'AgregarEliminarProductosCarrito' completed successfully

4

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.

El usuario tiene productos en el carrito, debe de existir la pasarela de pago con tarjeta y el stock del producto está disponible

Producto con su respectiva información, método de pago y datos de la tarjeta.

El pago se procesa sin errores mostrando un mensaje de pago exitoso y el usuario recibe un correo con todos los detalles de la compra

Juan Sebastian Jimenez

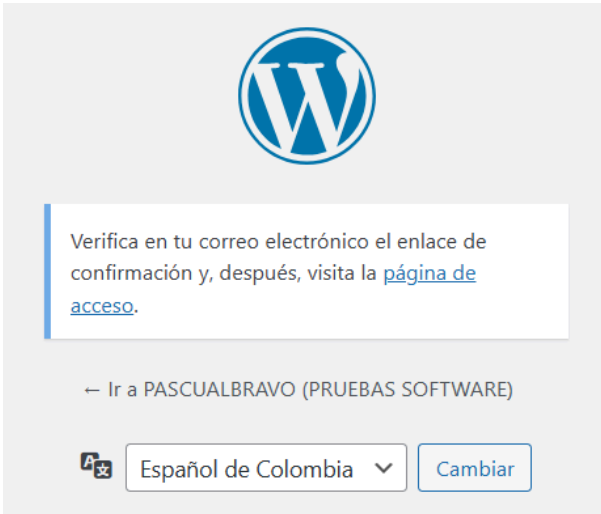
Fallido

Opciones de pago



No hay ningún método de pago disponible. Esto puede ser error nuestro. Por favor, contáctanos si necesitas ayuda para realizar tu pedido.

5	Quiero validar el envío de correos transaccionales (confirmación de pedido, restablecer contraseña), para que los usuarios reciban siempre la notificación adecuada.	El usuario tiene una dirección de correo válida y accesible	Usuario hace clic en restablecer contraseña e introduce su correo	El sistema automáticamente envía un correo al usuario con un respectivo asunto y un enlace para cambiar la contraseña	Juan Sebastian Jimenez	Exitoso
---	---	---	---	---	------------------------	---------



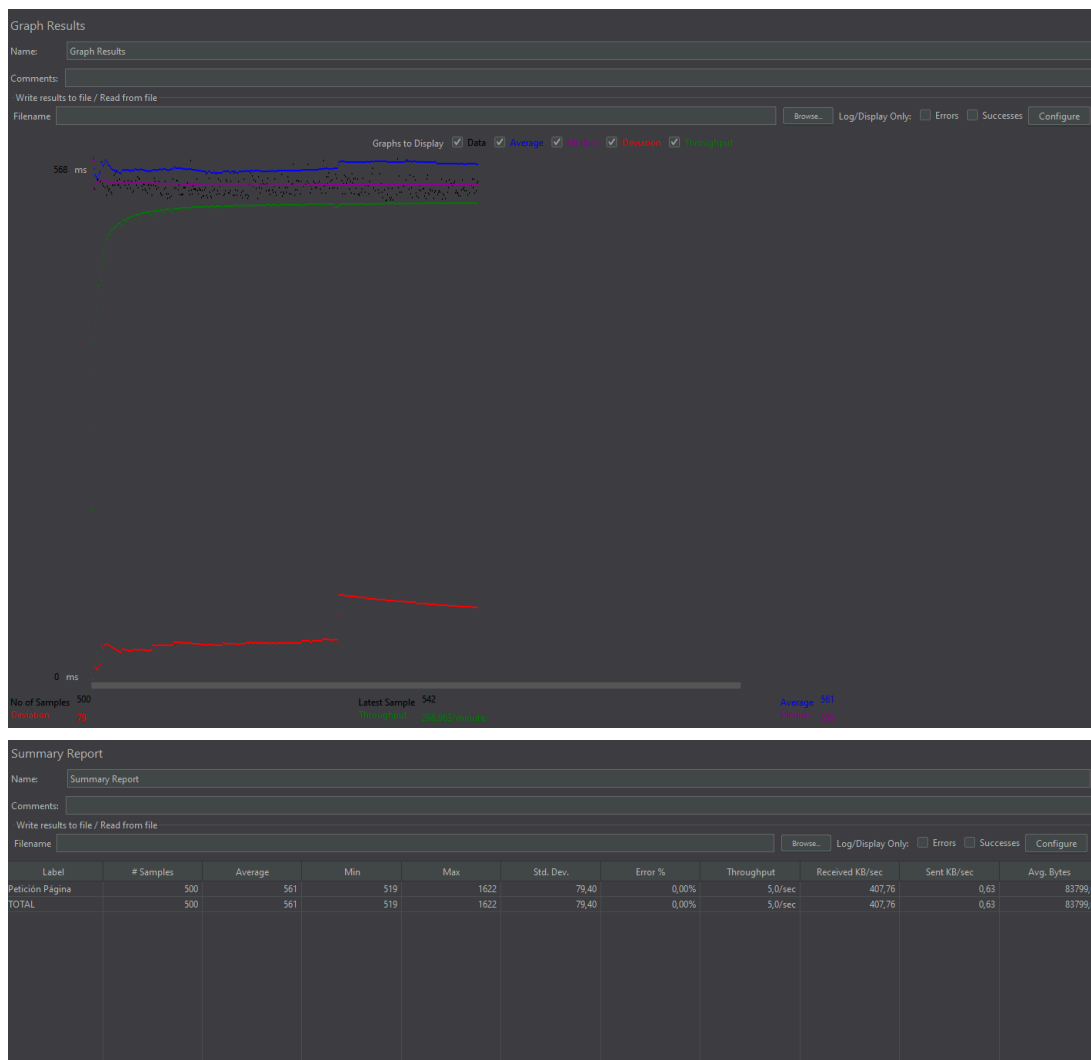
Running 'OlvidarContraseña'

1. open on /wp-login.php OK
2. type on id=user_login with value JEISIM18@GMAIL.COM OK
3. type on id=user_pass with value klos OK
4. click on linkText=¿Olvidaste tu contraseña? OK
5. open on /wp-login.php?action=lostpassword OK
6. type on id=user_login with value JEISIM18@GMAIL.COM OK
7. click on id=wp-submit OK

'OlvidarContraseña' completed successfully

PRUEBAS DE RENDIMIENTO

ID	Descripción	Precondición	Entrada	Resultado esperado	Responsable	Resultado
1	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.	El servidor debe estar activo y en funcionamiento junto con la url accesible y la respectiva configuración de Jmeter.	Solicitud http get a la página de inicio por cada uno de los 500 usuarios simultáneos	El servidor debe mantenerse estable, sin caídas ni mensajes de error.	Juan Sebastian Jimenez	Exitoso



Aggregate Report													
Name:		Aggregate Report											
Comments:													
Write results to file / Read from file													
Filename												Browse...	
												Log/Display Only:	
												<input type="checkbox"/> Errors	
												<input type="checkbox"/> Successes	
												Configure	
Label	# Samples	Average	Median	90% Line	95% Line	99% Line	Min	Maximum	Error %	Throughput	Received KB/sec	Sent KB/sec	
Petición Página	500	561	539	634	648	738	519	1622	0,00%	5,0/sec	407,76	0,63	
TOTAL	500	561	539	634	648	738	519	1622	0,00%	5,0/sec	407,76	0,63	

2	<p>Quiero medir el tiempo de respuesta al procesar un checkout con 100 usuarios simultáneos, para que el sistema escale adecuadamente sin errores de timeout.</p>	<p>La funcionalidad del checkout debe estar activa, el servidor debe estar corriendo y sin errores previos y la respectiva configuración del Jmeter</p>	<p>100 usuarios realizando solicitudes de checkout simultánea mente.</p>	<p>El tiempo de respuesta promedio debe estar por debajo de 2 segundos y el error debe ser 0% o cercano a 0%.</p>	<p>Juan Sebastian Jimenez</p>
---	--	---	--	---	-------------------------------

Exitoso

Summary Report

Name:Summary Report

Comments:

Write results to file / Read from file

Filename

Browse...

Log/Display Only

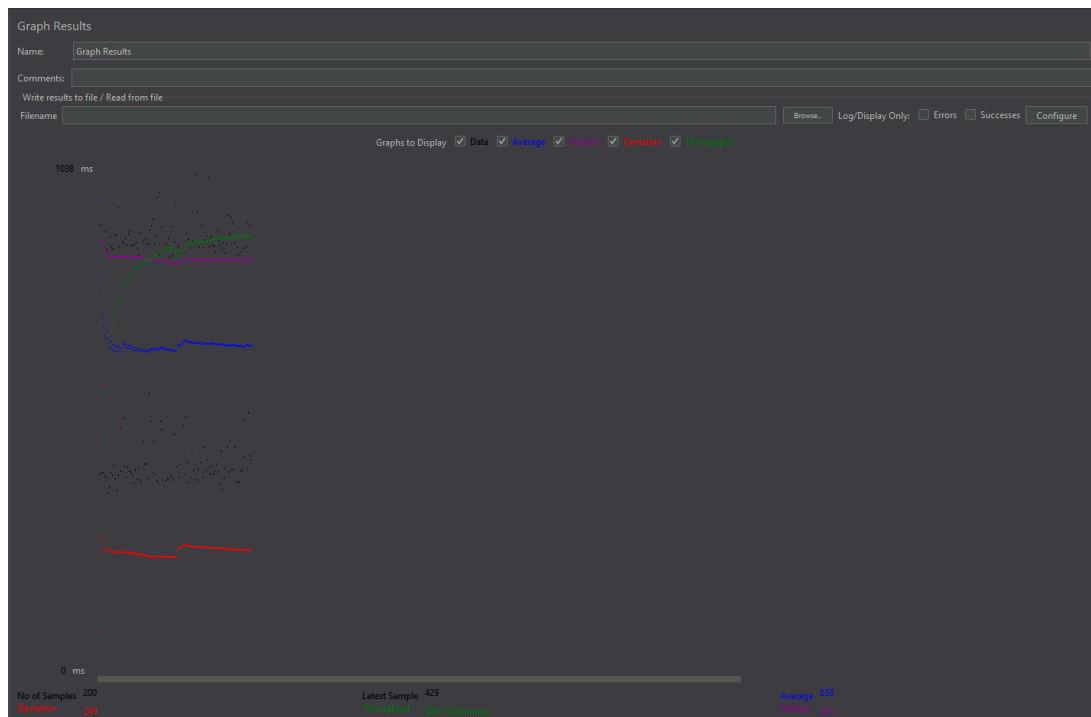
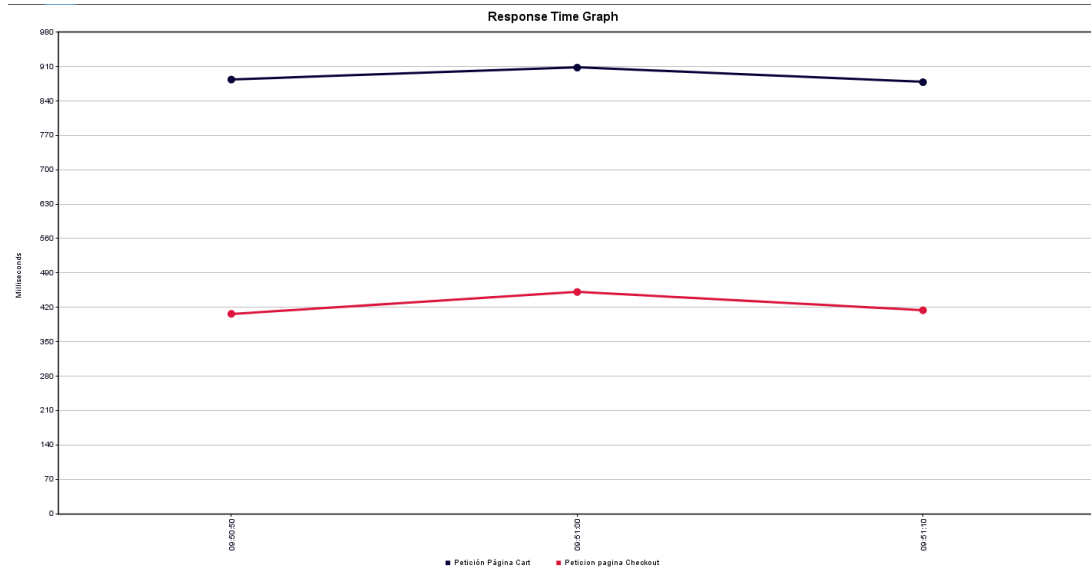
Errors

Successes

Configure

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
Peticion Página Cart	100	891	825	1618	90,76	0,00%	3,3/sec	428,87	0,86	134384,0
Peticion pagina Che...	100	426	363	1238	90,30	0,00%	3,3/sec	436,97	0,89	134198,0
TOTAL	200	658	363	1618	249,36	0,00%	6,4/sec	845,30	1,71	134291,0

Aggregate Report													
Name:		Aggregate Report											
Comments:													
Write results to file / Read from file													
Filename												Browse...	
												Log/Display Only:	
												<input type="checkbox"/> Errors	
												<input type="checkbox"/> Successes	
												Configure	
Label	# Samples	Average	Median	90% Line	95% Line	99% Line	Min	Maximum	Error %	Throughput	Received KB/sec	Sent KB/sec	
Petición Página ...	100	891	866	942	1038	1148	825	1618	0,00%	3,3/sec	428,87	0,86	
Petición pagina ...	100	426	406	490	510	563	363	1238	0,00%	3,3/sec	436,97	0,89	
TOTAL	200	658	825	900	956	1148	363	1618	0,00%	6,4/sec	845,30	1,71	



3	Quiero ejecutar un test de estrés subiendo archivos grandes (imágenes de producto) en paralelo, para que la aplicación soporta cargas masivas sin caídas.	La funcionalidad de carga imagen debe estar activa y funcionando correctamente y el Jmeter debe estar configurado correctamente	20 usuarios concurrentes subiendo archivos grandes de manera paralela	El sistema no debe colapsar ni presentar caídas el tiempo de respuesta promedio debe ser menor o igual a 2 segundos	Juan Sebastian Jimenez	Exitoso
---	--	---	---	---	------------------------	---------

Summary Report

Name:Summary Report

Comments:

Write results to file / Read from file

Filename

Browse...

Log/Display Only:

☐ Errors

☐ Successes

Configure

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
GET Login Page	20	341	316	424	32,63	0,00%	2,0/sec	19,38	0,59	9743,0
POST Login	20	750	685	1064	79,71	0,00%	2,0/sec	231,08	2,49	120217,0
post subida de archi...	20	727	685	787	31,10	0,00%	2,0/sec	289,13	108,95	145340,0
Debug Sampler	20	0	0	1	0,43	0,00%	2,2/sec	0,68	0,00	314,4
TOTAL	80	454	0	1064	312,14	0,00%	7,1/sec	477,39	97,62	68903,6

Aggregate Report

Name:Aggregate Report

Comments:

Write results to file / Read from file

Filename

Browse...

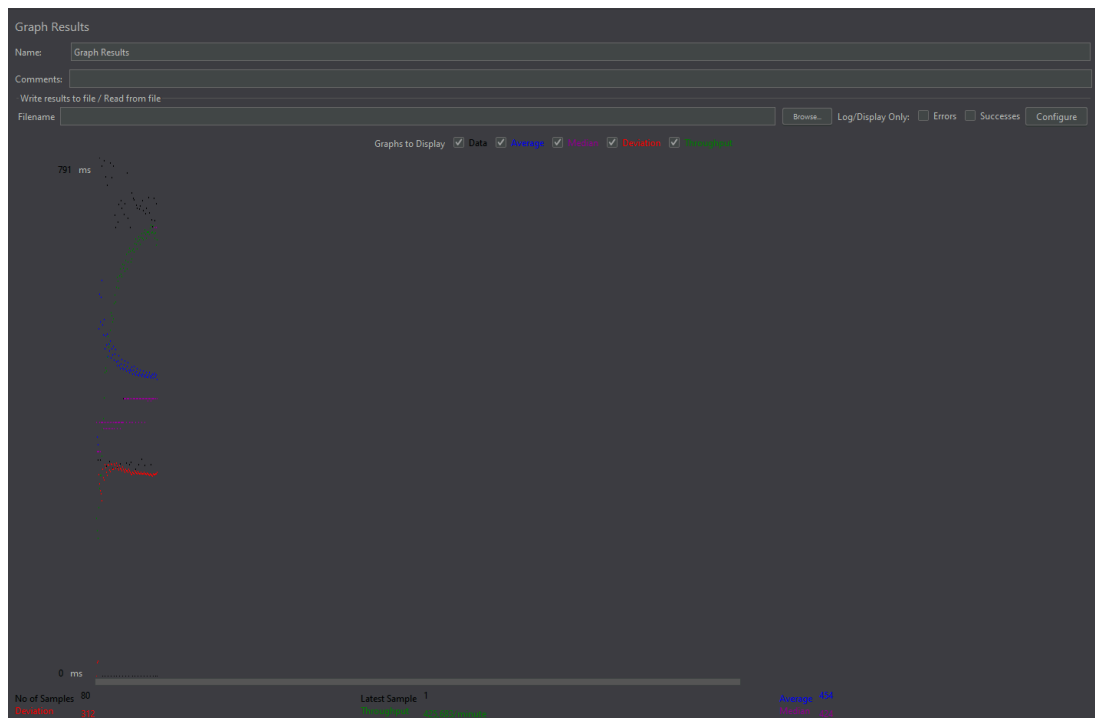
Log/Display Only:

☐ Errors

☐ Successes

Configure

Label	# Samples	Average	Median	90% Line	95% Line	99% Line	Min	Maximum	Error %	Throughput	Received KB/sec	Sent KB/sec
GET Login Page	20	341	326	388	421	424	316	424	0,00%	2,0/sec	19,38	0,59
POST Login	20	750	726	794	807	1064	685	1064	0,00%	2,0/sec	231,08	2,49
post subida de a...	20	727	718	779	783	787	685	787	0,00%	2,0/sec	289,13	108,95
Debug Sampler	20	0	0	1	1	1	0	1	0,00%	2,2/sec	0,68	0,00
Total	80	454	424	768	787	807	0	1064	0,00%	7,1/sec	477,39	97,62



Aggregate Graph

Name: /Aggregate Graph

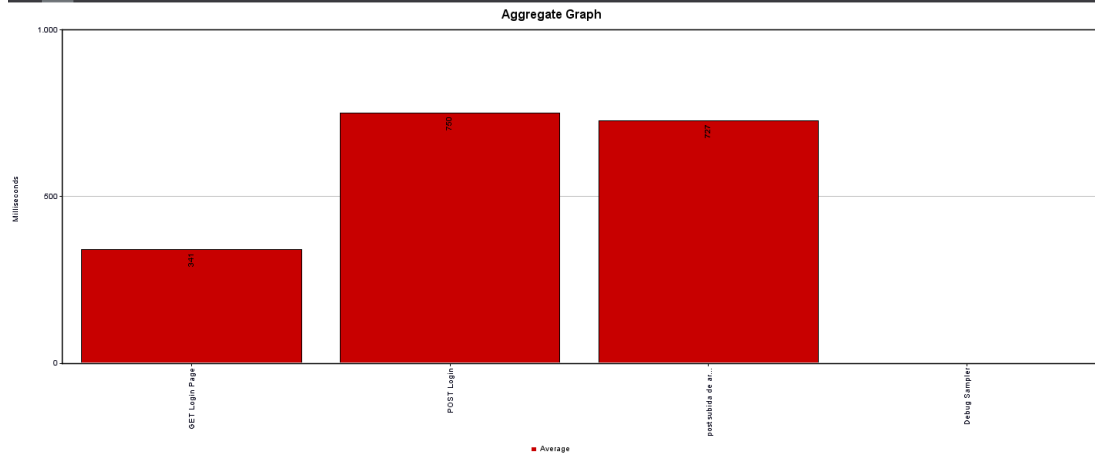
Comments:

Write results to file / Read from file

Filename: Browse... Log/Display Only: ☐ Errors ☐ Successes

Label	# Samples	Average	Median	90% Line	95% Line	99% Line	Min	Maximum	Error %	Throughput	Received KB/sec	Sent KB/sec
GET Login Page	20	341	326	388	421	424	316	424	0,00%	2,0/sec	19,38	0,59
POST Login	20	750	726	794	807	1064	685	1064	0,00%	2,0/sec	231,08	2,49
post subida de a...	20	727	718	779	783	787	685	787	0,00%	2,0/sec	288,13	108,95
Debug Sampler	20	0	0	1	1	1	0	1	0,00%	2,2/sec	0,68	0,00
Total	80	454	424	768	787	807	0	1064	0,00%	7,1/sec	477,39	97,62

Settings: Graph



4

Quiero analizar el rendimiento de la base de datos bajo 200 consultas/sqs, **para que** no haya cuellos de botella en la capa de datos.

El servidor de base de datos debe estar operativo y corriendo sin ningún inconveniente

200 usuarios generando consultas hacia la base de datos a través del endpoint correspondiente

Tiempo de respuesta promedio menor o igual a 2 segundos y la base de datos no debe presentar sobrecargas

Juan Sebastian Jimenez

Exitoso

Summary Report

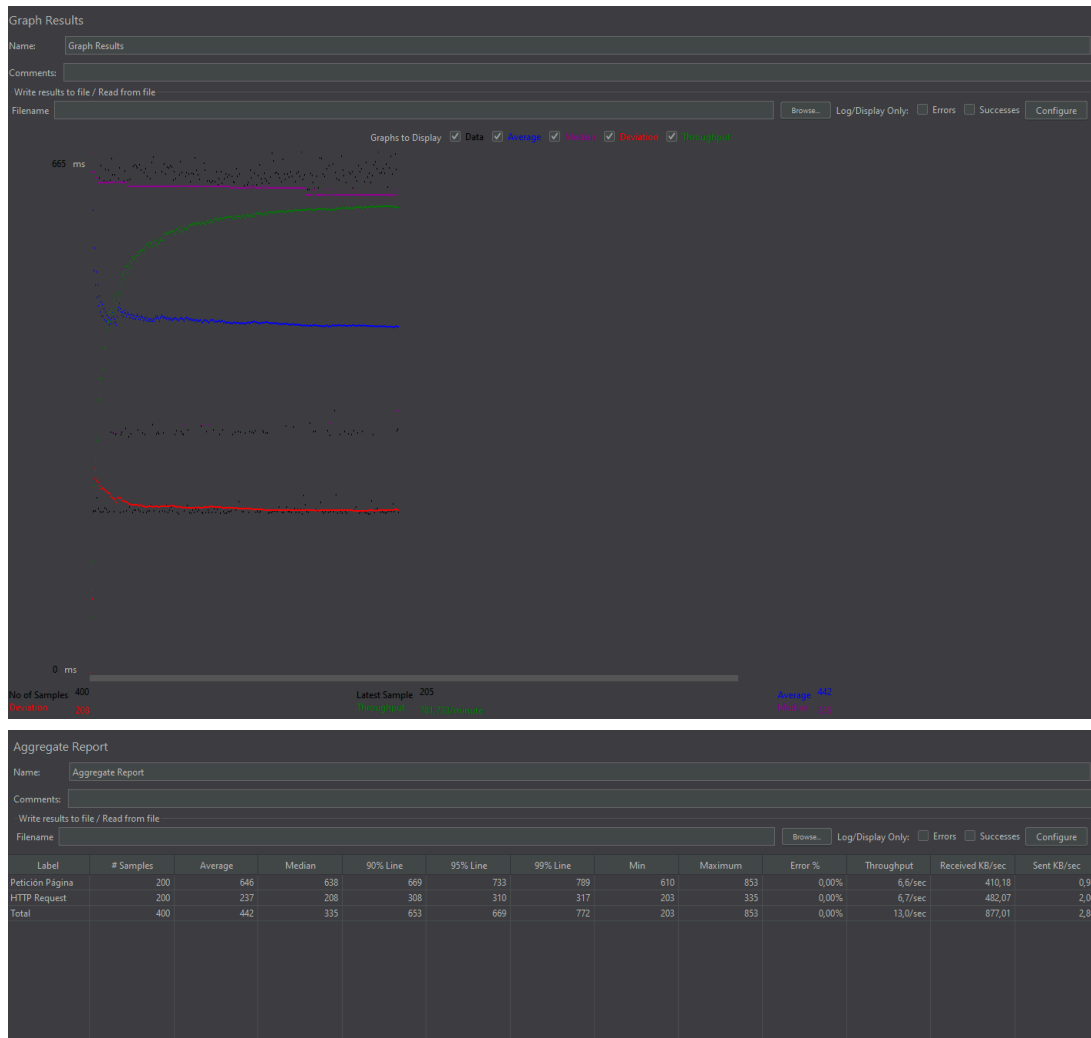
Name: Summary Report

Comments:

Write results to file / Read from file

Filename: Browse... Log/Display Only: ☐ Errors ☐ Successes

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
Petición Página	200	645	610	853	34,01	0,00%	6,6/sec	410,18	0,92	64042,6
HTTP Request	200	237	203	335	46,08	0,00%	6,7/sec	482,07	2,00	73814,0
TOTAL	400	442	203	853	208,93	0,00%	13,0/sec	877,01	2,86	68928,3



5 Quiero realizar un test de resistencia continuo durante 2 horas con 100 usuarios, **para que** detectar fugas de memoria o degradación progresiva del servicio.

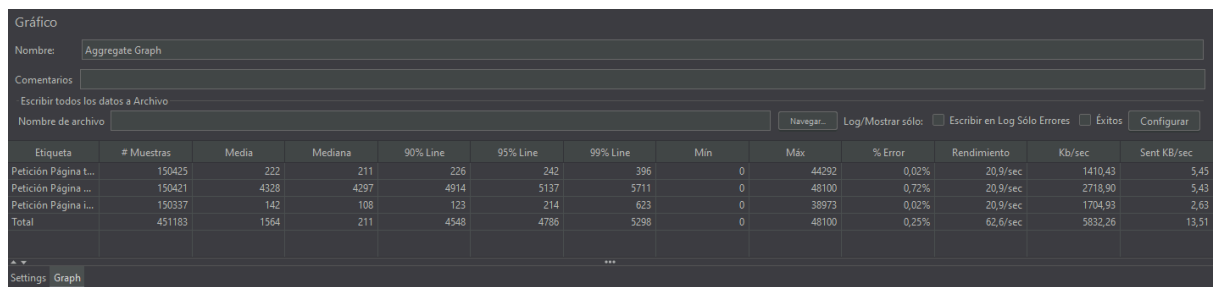
El servidor está en pleno funcionamiento y la base de datos debe estar sin ningún problema

Se simula tráfico continuo de 100 usuarios concurrentes durante 2 horas que envían solicitudes a inicio, tienda y carrito.

El servidor debe mantener el rendimiento estable, sin errores graves y sin caídas por parte del servidor.

Juan Sebastian Jimenez

Exitoso Parcialmente



PRUEBAS DE SEGURIDAD

ID	Descripción	Precondición	Entrada	Resultado esperado	Responsable	Resultado
1	Quiero ejecutar escaneos de vulnerabilidades (SQL Injection) en todos los formularios de entrada, para que la aplicación esté protegida contra inyecciones maliciosas.	El servidor debe de estar en funcionamiento y las herramientas de análisis deben de estar previamente configuradas (Burp Suite y SQLmap)	Petición HTTP interceptada desde el login /wp-login.php y la inyección SQL	La herramienta no debe encontrar parámetros vulnerables a inyección SQL y los formularios deben de estar protegidos	Juan Sebastian Jimenez	Exitoso

Dashboard	Target	Proxy	Intruder	Repeater	Collaborator	Sequencer	Decoder
Intercept	HTTP history	WebSockets history	Match and replace			Proxy settings	
Filter settings: Hiding CSS, image and general binary content							
#	Host	Method	URL	Params	Edited	Status	
21	https://pascualbravo.ingejei.com	GET	/favicon.ico			404	
22	https://pascualbravo.ingejei.com	GET	/wp-includes/js/zxcvbn.min.js			200	
23	https://pascualbravo.ingejei.com	POST	/wp-login.php	✓		200	
24	https://firefox.settings.services...	GET	/v1/			200	
25	https://contile.services.mozilla....	GET	/v1/tiles			204	
26	https://pascualbravo.ingejei.com	GET	/wp-login.php			200	
27	https://firefox-settings-attach...	GET	/main-workspace/search-config-icons...			200	
28	https://pascualbravo.ingejei.com	POST	/wp-login.php	✓		200	
29	https://contile.services.mozilla....	GET	/v1/tiles			204	
30	https://firefox.settings.services...	GET	/v1/buckets/monitor/collections/chang...	✓		200	
31	https://firefox.settings.services...	GET	/v1/buckets/security-state/collections/...	✓		200	
32	https://content-signature-2.cd...	GET	/g/chains/202402/onecr1.content-sign...			200	
33	https://firefox.settings.services...	GET	/v1/buckets/security-state/collections/...	✓		200	

Request

Pretty Raw Hex

```

1 POST /wp-login.php HTTP/2
2 Host: pascualbravo.ingejei.com
3 Cookie: wordpress_test_cookie=WP%20Cookie%20check
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
  Firefox/128.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
  /png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://pascualbravo.ingejei.com/wp-login.php
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 122
11 Origin: https://pascualbravo.ingejei.com
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i
18 Te: trailers
19
20 log=%27+0R+1%3D1--&pwd=abc&wp-submit=Acceder&redirect_to=
  https%3A%2F%2Fpascualbravo.ingejei.com%2Fwp-admin%2F&testcookie=1
  
```

```

(kali@kali)~/.Seguridad/Historia11
$ sqlmap -r BurpLoginPeticion.txt \
--batch --level=5 --risk=3 --dbs \
--output-dir=Historia11reporte_sqlmap

[+] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applica-
ble local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting @ 20:06:21 /2025-06-02/

[20:06:21] [INFO] parsing HTTP request from 'BurpLoginPeticion.txt'
[20:06:21] [WARNING] using '/home/kali/Seguridad/Historia11/Historia11reporte_
sqlmap' as the output directory
[20:06:21] [INFO] testing connection to the target URL
got a 301 redirect to 'https://pascualbravo.ingeji.com/wp-login.php'. Do you
want to follow? [Y/n] Y
redirect is a result of a POST request. Do you want to resend original POST d
ata to a new location? [Y/n] Y
you have not declared cookie(s), while server wants to set its own ('wordpres
s_test_cookie=WP%20Cookie%20check'). Do you want to use those [Y/n] Y
[20:06:22] [INFO] checking if the target is protected by some kind of WAF/IPS
[20:06:22] [INFO] testing if the target URL content is stable
[20:06:23] [WARNING] POST parameter 'log' does not appear to be dynamic
[20:06:23] [WARNING] heuristic (basic) test shows that POST parameter 'log' m
ight not be injectable
[20:06:23] [INFO] testing for SQL injection on POST parameter 'log'
[20:06:23] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[20:06:24] [WARNING] reflective value(s) found and filtering out
[20:06:29] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[20:07:36] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (N
OT)'
[20:08:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (
subquery - comment)'
[20:09:02] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (s
ubquery - comment)'
[20:09:27] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (
comment)'
[20:09:36] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (c
omment)'

[23:28:39] [INFO] testing 'MySQL OR time-based blind (ELT)'
[23:29:04] [INFO] testing 'MySQL AND time-based blind (ELT - comment)'
[23:29:21] [INFO] testing 'MySQL OR time-based blind (ELT - comment)'
[23:29:38] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:30:04] [INFO] testing 'PostgreSQL > 8.1 OR time-based blind'
[23:30:30] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind (comment)'
[23:30:48] [INFO] testing 'PostgreSQL > 8.1 OR time-based blind (comment)'
[23:31:05] [INFO] testing 'PostgreSQL AND time-based blind (heavy query)'
[23:31:32] [INFO] testing 'PostgreSQL OR time-based blind (heavy query)'
[23:31:57] [INFO] testing 'PostgreSQL AND time-based blind (heavy query - com
ment)'
[23:32:15] [INFO] testing 'PostgreSQL OR time-based blind (heavy query - comm
ent)'
[23:32:33] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[23:33:00] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF -
comment)'
[23:33:19] [INFO] testing 'Microsoft SQL Server/Sybase AND time-based blind (
heavy query)'
[23:33:46] [INFO] testing 'Microsoft SQL Server/Sybase OR time-based blind (h
eavy query)'
[23:34:11] [INFO] testing 'Microsoft SQL Server/Sybase AND time-based blind (
heavy query - comment)'
[23:34:28] [INFO] testing 'Microsoft SQL Server/Sybase OR time-based blind (h
eavy query - comment)'
[23:34:46] [INFO] testing 'Oracle AND time-based blind'
[23:35:11] [INFO] testing 'Oracle OR time-based blind'
[23:35:36] [INFO] testing 'Oracle AND time-based blind (comment)'
[23:35:53] [INFO] testing 'Oracle OR time-based blind (comment)'
[23:36:11] [INFO] testing 'Oracle AND time-based blind (heavy query)'
[23:36:35] [INFO] testing 'Oracle OR time-based blind (heavy query)'
[23:37:01] [INFO] testing 'Oracle AND time-based blind (heavy query - comment
)'
[23:37:18] [INFO] testing 'Oracle OR time-based blind (heavy query - comment
)'
[23:37:36] [INFO] testing 'IBM DB2 AND time-based blind (heavy query)'
[23:38:01] [INFO] testing 'IBM DB2 OR time-based blind (heavy query)'
[23:38:26] [INFO] testing 'IBM DB2 AND time-based blind (heavy query - commen
t)'
[23:38:43] [INFO] testing 'IBM DB2 OR time-based blind (heavy query - comment
)'
[23:39:01] [INFO] testing 'SQLite > 2.0 AND time-based blind (heavy query)'
[23:39:27] [INFO] testing 'SQLite > 2.0 OR time-based blind (heavy query)'
[23:39:53] [INFO] testing 'SQLite > 2.0 AND time-based blind (heavy query - c
omment)'
[23:40:10] [INFO] testing 'SQLite > 2.0 OR time-based blind (heavy query - co
mment)'
[23:40:27] [INFO] testing 'Firebird >= 2.0 AND time-based blind (heavy query)'
[23:40:53] [INFO] testing 'Firebird >= 2.0 OR time-based blind (heavy query)'

```

2	<p>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.</p>	<p>El formulario de autenticación se encuentra accesible en el dominio, el formulario utiliza el método de HTTP POST y se dispone de un diccionario de usuarios y contraseñas</p>	<p>Host, puerto, la ruta del login el diccionario de usuarios y contraseñas</p>	<p>El sistema debería bloquear los intentos tras múltiples fallos, o mostrar mensaje de cuenta bloqueada temporalmente</p>	<p>Juan Sebastian Jimenez</p>	<p>Fallido</p>
<pre> word: contraseña123 [443][http-post-form] host: pascualbravo.ingejei.com login: -e admin pass word: lwAVKAaeW6 [443][http-post-form] host: pascualbravo.ingejei.com login: @gmail.com pa ssword: -e 123456 [443][http-post-form] host: pascualbravo.ingejei.com login: @gmail.com pa ssword: pascual2025 [443][http-post-form] host: pascualbravo.ingejei.com login: @gmail.com pa ssword: lwAVKAaeW6 [443][http-post-form] host: pascualbravo.ingejei.com login: @gmail.com pa ssword: contraseña123 [443][http-post-form] host: pascualbravo.ingejei.com login: jeisim18@gmail. com password: -e 123456 [443][http-post-form] host: pascualbravo.ingejei.com login: jeisim18@gmail. com password: contraseña123 [443][http-post-form] host: pascualbravo.ingejei.com login: jeisim18@gmail. com password: admin123 [443][http-post-form] host: pascualbravo.ingejei.com login: jeisim18@gmail. com password: pascual2025 [443][http-post-form] host: pascualbravo.ingejei.com login: jeisim18@gmail. com password: lwAVKAaeW6 1 of 1 target successfully completed, 15 valid passwords found Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-02 21: 37:49 </pre>						
3	<p>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.</p>	<p>Usuario autenticado con el rol de cliente, existe una ruta sensible (/wp/admin/.users.php) destinado a gestión de los usuarios.</p>	<p>Solicitud de HTTP interceptada y enviada manualmente por Burp Suite y la respectiva cookie con el rol del cliente.</p>	<p>El servidor debe de redirigir o denegar el acceso al cliente y ninguna información del endpoint privilegiada debe exponerse</p>	<p>Juan Sebastian Jimenez</p>	<p>Exitoso</p>

<div><div><div>Request</div><div><div>PrettyRawHex</div><div><div>1GET /wp-admin/users.php HTTP/2</div><div>2Host: pascualbravo.ingejei.com</div><div>3Cookie: wordpress_sec_c02428a877ffeelfa567b91e0426d92b=cuentaprueba%7C1749085609%7COW9wqEWru0mPxQsISxSdaWyeLliug0SgVeEqB9Iibvq%7C7e01b962e17f8634ab01e3c84b1de1d71472c4b49d8b5862fb10370f6589d58a; wordpress_test_cookie=WP%20Cookie%20check; _lscache_vary=7e8ffc8549ac625ce6e7871d5eb007c1; wordpress_logged_in_c02428a877ffeelfa567b91e0426d92b=cuentaprueba%7C1749085609%7COW9wqEWru0mPxQsISxSdaWyeLliug0SgVeEqB9Iibvq%7C3e95ef9419489a8ff21bd6cd1469a4b24f232a8a6d06a72432317c009aca743a; wp-settings-l=libraryContent%3Dbrowse%26mfold%3Do; wp-settings-time-l=1748911049; woocommerce_items_in_cart=1; woocommerce_cart_hash=ae8cb223914a3dc90cab2ab7525e4f20; wp_woocommerce_session_c02428a877ffeelfa567b91e0426d92b=1%7C%7C1749083912%7C%7C1749080312%7C%7C85884cbed14a6775edb66cce8599791; trigger-hosting-status-daily-shown-event=1</div><div>4User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0</div><div>5Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8</div><div>6Accept-Language: en-US,en;q=0.5</div><div>7Accept-Encoding: gzip, deflate, br</div><div>8Referer: https://pascualbravo.ingejei.com/wp-login.php</div><div>9Upgrade-Insecure-Requests: 1</div><div>10Sec-Fetch-Dest: document</div><div>11Sec-Fetch-Mode: navigate</div><div>12Sec-Fetch-Site: same-origin</div><div>13Sec-Fetch-User: ?1</div><div>14Priority: u=0, i</div><div>15Te: trailers</div><div>16</div><div>17</div></div></div></div><div><div>Response</div><div><div>PrettyRawHexRender</div><div><div>1HTTP/2 302 Found</div><div>2X-Powered-By: PHP/8.2.28</div><div>3Expires: Wed, 11 Jan 1984 05:00:00 GMT</div><div>4X-Redirect-By: WordPress</div><div>5Location: https://pascualbravo.ingejei.com/</div><div>6Set-Cookie: _lscache_vary=d8664661084360fe52025 01:10:09 GMT; Max-Age=172800; path=/;</div><div>7X-Litespeed-Cache-Control: no-cache</div><div>8Cache-Control: no-cache, no-store, must-rev</div><div>9Content-Type: text/html; charset=UTF-8</div><div>10Content-Length: 0</div><div>11Date: Tue, 03 Jun 2025 01:10:09 GMT</div><div>12Server: LiteSpeed</div><div>13Platform: hostinger</div><div>14Panel: hpanel</div><div>15Content-Security-Policy: upgrade-insecure-r</div><div>16</div><div>17</div></div></div></div><div><div>(kali@kali)-[~/Seguridad/Historia13]</div><div>\$ cat evidencia_rol_cliente.txt</div><div>HTTP/2 302</div><div>x-powered-by: PHP/8.2.28</div><div>expires: Wed, 11 Jan 1984 05:00:00 GMT</div><div>x-redirect-by: WordPress</div><div>location: https://pascualbravo.ingejei.com/my-account/</div><div>x-litespeed-cache-control: no-cache</div><div>cache-control: no-cache, no-store, must-revalidate, max-age=0</div><div>content-type: text/html; charset=UTF-8</div><div>content-length: 0</div><div>date: Tue, 03 Jun 2025 01:21:57 GMT</div><div>server: LiteSpeed</div><div>platform: hostinger</div><div>panel: hpanel</div><div>content-security-policy: upgrade-insecure-requests</div><div>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"</div></div></div> <tr><td>4</td><td>Quiero revisar los encabezados HTTP de seguridad (CSP, HSTS, X-Frame-Options), para que esté mitigada la mayoría de ataques de inyección y clickjacking.</td><td>El servidor web debe estar activo y disponible en la URL objetivo, y se debe poder acceder vía HTTPS</td><td>Se realiza una petición HTTP GET al recurso /wp-login.php del servidor a través de la herramienta Burp Suite</td><td>El servidor debe devolver encabezados HTTP de seguridad correctamente configurados al acceder a la ruta.</td><td>Juan Sebastian Jimenez</td><td>Exitoso</td></tr>						4	Quiero revisar los encabezados HTTP de seguridad (CSP, HSTS, X-Frame-Options), para que esté mitigada la mayoría de ataques de inyección y clickjacking.	El servidor web debe estar activo y disponible en la URL objetivo, y se debe poder acceder vía HTTPS	Se realiza una petición HTTP GET al recurso /wp-login.php del servidor a través de la herramienta Burp Suite	El servidor debe devolver encabezados HTTP de seguridad correctamente configurados al acceder a la ruta.	Juan Sebastian Jimenez	Exitoso
4	Quiero revisar los encabezados HTTP de seguridad (CSP, HSTS, X-Frame-Options), para que esté mitigada la mayoría de ataques de inyección y clickjacking.	El servidor web debe estar activo y disponible en la URL objetivo, y se debe poder acceder vía HTTPS	Se realiza una petición HTTP GET al recurso /wp-login.php del servidor a través de la herramienta Burp Suite	El servidor debe devolver encabezados HTTP de seguridad correctamente configurados al acceder a la ruta.	Juan Sebastian Jimenez	Exitoso						

Name	Value	
X-Powered-By	PHP/8.2.28	>
Expires	Wed, 11 Jan 1984 05:0...	>
Cache-Control	no-cache, must-revali...	>
Content-Type	text/html; charset=UT...	>
Set-Cookie	wordpress_test_cooki...	>
Set-Cookie	wordpress_test_cooki...	>
X-Frame-Options	SAMEORIGIN	>
Referrer-Policy	strict-origin-when-cro...	>
X-Litespeed-Cache-C...	public,max-age=6048...	>
X-Litespeed-Tag	407_L,407_default,4...	>
Etag	"569-1748920134;br"	>
X-Litespeed-Cache	miss	>
Vary	Accept-Encoding	>
Date	Tue, 03 Jun 2025 03:0...	>
Server	LiteSpeed	>
Platform	hostinger	>
Panel	hpanel	>
Content-Security-Policy	upgrade-insecure-req...	>
Alt-Svc	h3=":443"; ma=25920...	>

```
HITP/2 200
HITP/2 200
x-powered-by: PHP/8.2.28
x-powered-by: PHP/8.2.28
expires: Wed, 11 Jan 1984 05:00:00 GMT
expires: Wed, 11 Jan 1984 05:00:00 GMT
cache-control: no-cache, must-revalidate, max-age=0, no-store, private
cache-control: no-cache, must-revalidate, max-age=0, no-store, private
content-type: text/html; charset=UTF-8
content-type: text/html; charset=UTF-8
set-cookie: wordpress_test_cookie=WP%20Cookie%20check; path=/; secure; HttpOnly
set-cookie: wordpress_test_cookie=WP%20Cookie%20check; path=/; secure; HttpOnly
x-frame-options: SAMEORIGIN
x-frame-options: SAMEORIGIN
referrer-policy: strict-origin-when-cross-origin
referrer-policy: strict-origin-when-cross-origin
etag: "569-1748920134;;;,"
etag: "569-1748920134;;;,"
x-litespeed-cache: hit
x-litespeed-cache: hit
date: Tue, 03 Jun 2025 03:38:53 GMT
date: Tue, 03 Jun 2025 03:38:53 GMT
server: LiteSpeed
server: LiteSpeed
platform: hostinger
platform: hostinger
panel: hpanel
panel: hpanel
content-security-policy: upgrade-insecure-requests
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, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000
```


5	Quiero probar la protección contra CSRF enviando formularios y peticiones con y sin el token CSRF válido, para que se evite que atacantes realicen acciones no autorizadas en nombre de un usuario autenticado.	Usuario autenticado en el sistema de administración de Wordpress	Se envían solicitudes POST hacia /wp-admin/profile.php con y sin token CSRF	Solo se deben aceptar las solicitudes que contengan token CSRF válido; las que no lo tengan deberán de ser rechazadas	Juan Sebastian Jimenez	Exitoso
---	--	--	---	---	------------------------	---------

<div> <div>Request</div> <div> <div>Pretty</div> <div>Raw</div> <div>Hex</div> </div> <div> <div>1</div> <div>POST /wp-admin/profile.php HTTP/2</div> <div>2</div> <div>Host: pascualbravo.ingejei.com</div> <div>3</div> <div>Cookie: wordpress_sec_c02428a877ffeel567b91e0426d92b=jeisim18%40gmail.com%7C1749171765%7CubaxiuQNRuBgYE9umoKZ3ZxWuuf2bydWyMVHPTzIMLw%7C4bla1e9b81d6c8e03f9b25ff0e29597e8f39ec4da31014df2723c124ebed322; wp-settings-1=libraryContent%3Dupload%26fold%3D0; wp-settings-time-1=1748998965; wordpress_test_cookie=WP%20Cookie%20check; _lscache_vary=7e8ffc8549ac625ce6e7871d5eb007c1; wordpress_logged_in_c02428a877ffeel567b91e0426d92b=jeisim18%40gmail.com%7C1749171765%7CubaxiuQNRuBgYE9umoKZ3ZxWuuf2bydWyMVHPTzIMLw%7C42a24b3206f9ad05948f4aa77b%224f4a7ad26bd5a0bd5a9e19d988e036f2fd; woocommerce_items_in_cart=1; woocommerce_cart_hash=c82886a509d3bb4eb56e5d0031df4687; wp_woocommerce_session_c02428a877ffeel567b91e0426d92b=1%7C%7C174917176%7C%7C1749168167%7C%7Ca2c97de5e7c47d15d6729dcfb6414db5</div> <div>4</div> <div>User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0</div> <div>5</div> <div>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8</div> <div>6</div> <div>Accept-Language: en-US,en;q=0.5</div> <div>7</div> <div>Accept-Encoding: gzip, deflate, br</div> <div>8</div> <div>Referer: https://pascualbravo.ingejei.com/wp-admin/profile.php</div> <div>9</div> <div>Content-Type: application/x-www-form-urlencoded</div> <div>10</div> <div>Content-Length: 800</div> <div>11</div> <div>Origin: https://pascualbravo.ingejei.com</div> <div>12</div> <div>Upgrade-Insecure-Requests: 1</div> <div>13</div> <div>Sec-Fetch-Dest: document</div> <div>14</div> <div>Sec-Fetch-Mode: navigate</div> <div>15</div> <div>Sec-Fetch-Site: same-origin</div> <div>16</div> <div>Sec-Fetch-User: ?1</div> <div>17</div> <div>Priority: u=0, i</div> <div>18</div> <div>Te: trailers</div> <div>19</div> <div></div> <div>20</div> <div>_wpnonce=abc123&wp_http_referer=%2Fwp-admin%2Fprofile.php&from=profile&checkuser_id=1&color_nonce=d5cf28a716&admin_color=ocean&admin_bar_front=1&locale=site-default&user_login=jeisim18%40gmail.com&first_name=&last_name=&nickname=jeisim18%40gmail.com&display_name=&email=jeisim18%40gmail.com&url=http%3A%2F%2Fpascualbravo.ingejei.com&description=&pass1=&pass2=&billing_first_name=&billing_last_name=&billing_company=&billing_address_1=&billing_address_2=&billing_city=&billing_postcode=&billing_country=&billing_state=&billing_phone=&billing_email=jeisim18%40gmail.com&bionnino_first_name=&bionnino_last_name=f</div> </div> </div> <div> <div>Response</div> <div> <div>Pretty</div> <div>Raw</div> <div>Hex</div> <div>Render</div> </div> <div> <div>1</div> <div>HTTP/2 403 Forbidden</div> <div>2</div> <div>X-Powered-By: PHP/8.2.28</div> <div>3</div> <div>Referrer-Policy: strict-origin-when-cross-</div> <div>4</div> <div>X-Frame-Options: SAMEORIGIN</div> <div>5</div> <div>Content-Type: text/html; charset=UTF-8</div> <div>6</div> <div>X-Litespeed-Tag: 407_tag_priv,public:407_H</div> <div>7</div> <div>Expires: Wed, 11 Jan 1984 05:00:00 GMT</div> <div>8</div> <div>X-Litespeed-Cache-Control: no-cache</div> <div>9</div> <div>Cache-Control: no-cache, no-store, must-re</div> <div>10</div> <div>Content-Length: 2504</div> <div>11</div> <div>Vary: Accept-Encoding</div> <div>12</div> <div>Date: Wed, 04 Jun 2025 01:37:30 GMT</div> <div>13</div> <div>Server: LiteSpeed</div> <div>14</div> <div>Platform: hostingner</div> <div>15</div> <div>Panel: hpanel</div> <div>16</div> <div>Content-Security-Policy: upgrade-insecure-</div> <div>17</div> <div>Alt-Svc: h3=":443"; ma=2592000, h3-29=":44</div> <div>18</div> <div>ma=2592000, h3-0046=":443"; ma=2592000, h3</div> <div>19</div> <div>ma=2592000; v="43,46"</div> <div>20</div> <div><!DOCTYPE html></div> <div>21</div> <div><html lang="es-CO"></div> <div>22</div> <div><head></div> <div>23</div> <div><meta http-equiv="Content-Type"</div> <div>24</div> <div><meta name="viewport" content="v</div> <div>25</div> <div><meta name="robots" content="max</div> <div>26</div> <div></title></div> <div>27</div> <div>Ha ocurrido un error.</div> <div>28</div> <div></title></div> <div>29</div> <div><style type="text/css"></div> <div>30</div> <div>html{</div> <div>31</div> <div>background:#f1f1f1;</div> <div>32</div> <div>}</div> <div>33</div> <div>body{</div> <div>34</div> <div>background:#fff;</div> <div>border:1pxsolid#ccc0d4</div> <div>color:#444;</div> <div>font-family:-apple-sys</div> <div>font-size:14px;</div> <div>font-weight:normal;</div> <div>font-style:normal;</div> <div>font-variant:normal;</div> <div>font-variant-ligatures:normal;</div> <div>font-variant-caps:normal;</div> <div>font-variant-east-asian:normal;</div> <div>font-variant-numeric:normal;</div> <div>font-variant-variant:normal;</div> <div>font-variant-x-english:normal;</div> <div>font-variant-x-english-ligatures:normal;</div> <div>font-variant-x-english-variant:normal;</div> <div>font-variant-x-english-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant:normal;</div> <div>font-variant-x-english-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-variant-ligatures:normal;</div> <div>font-variant-x-english-variant:normal;</div> <div>font-variant-x-english-variant-ligatures:normal;</div> <div>font-variant-x-english-variant:normal;</div> <div>font-variant-x-english-variant-ligatures:normal;</div> <div>font-variant-x-english-variant:normal;</div> <div>font-variant-x-english-variant-ligatures:normal;</div> <div>font-variant-x-english-variant:normal;</div> <div>font-variant-x-english-variant-ligatures:normal;</div> <div>font-variant-x-english-variant:normal;</div> <div>font-variant-x-english-variant-ligatures:normal;</div> <div>font-variant-x-english-variant:normal;</div> <div>font-variant-x-english-variant-ligatures:normal;</div> <div>font-variant-x-english-variant:normal;</div> <div>font-variant-x-english-variant-ligatures:normal;</div> <div>font-variant-x-english-variant:normal;</div> <div>font-variant-x-english-variant-ligatures:normal;</div> <div>font-variant-x-english-variant:normal;</div> <div>font-variant-x-english-variant-ligatures:normal;</div> <div>font-variant-x-english-variant:normal;</div> <div>font-variant-x-english-variant-ligatures:normal;</div> <div>font-variant-x-english-variant:normal;</div> <div>font-variant-x-english-variant-ligatures:normal;</div> <div>font-variant-x-english-variant:normal;</div> <div>font-variant-x-english-variant-ligatures:normal;</div> <div>font-variant-x-english-variant-normal;</div> </div> </div>
--

RECOMENDACIONES

Después de realizar los análisis y pruebas, se puede identificar ciertos puntos de mejora respecto a los procedimientos y evidencias resultantes. Estas recomendaciones buscan optimizar la estructura, consistencia y resiliencia de las pruebas.

1. Protección contra ataques de fuerza bruta
 - a. Implementar un limitador de intentos por IP o cuenta (por ejemplo, 5 intentos provocaría un bloqueo temporal) para bloquear herramientas como Hydra.
 - b. Registrar en logs cada intento de ingreso y generar alertas de tráfico y actividades sospechosas (por ejemplo, más de 10 intentos en 2 minutos).
2. Pruebas de rendimiento:
 - a. Añadir métricas de tiempo respuesta promedio (por ejemplo, medianas y percentiles) simulando una variedad de dispositivos y tipos de conexión para reflejar condiciones reales de uso.
 - b. Incluir porcentajes de error y solicitudes rechazadas para aquellas respuestas que sean de un código HTTP mayor a 400 y de peticiones sin respuesta (timeout).
3. Flujo de pago:
 - a. Implementar las funciones restantes del flujo de pago, como lo es el checkout con tarjeta.
 - b. Agregar el método de pago por tarjeta y verificar que este correctamente configurado y habilitado en WooCommerce.
 - c. Agregar seguros de formulario para que valide correctamente los datos antes de enviarlos.f
4. Test de resistencia:
 - a. Durante la prueba continua de 2 horas con 100 usuarios, se detectaron errores menores en el manejo del carrito, revisar el flujo del carrito y reforzar su estabilidad bajo carga prolongada.
 - b. Optimizar la gestión de sesiones y el uso de almacenamiento en caché para reducir carga innecesaria.
 - c. Revisar configuraciones del servidor, como la asignación de memoria y el manejo de procesos concurrentes.
 - d. Utilizar herramientas de monitoreo en tiempo real para identificar posibles fugas de memoria o degradación progresiva.

CONCLUSIÓN

Durante el proceso de evaluación de la tienda Minishop, se realizaron pruebas funcionales, de rendimiento y de seguridad en los principales componentes y funcionalidades de la plataforma. Los resultados muestran que el sistema cumple adecuadamente en la mayoría de los aspectos evaluados, demostrando así:

- ❖ Pruebas funcionales: Pruebas funcionales: Las funciones básicas como registro, búsqueda de productos, uso del carrito y envío de correos transaccionales se ejecutaron correctamente. Sin embargo, el flujo de checkout con tarjeta falló por una configuración incompleta en la pasarela de pago, lo cual impidió finalizar transacciones.
- ❖ Pruebas de rendimiento: El sitio mantuvo tiempos de respuesta aceptables (< 2 s) con hasta 500 usuarios concurrentes, incluyendo operaciones de búsqueda, navegación y carga de imágenes. En la prueba de resistencia (2 horas con 100 usuarios), se detectaron fallos menores en el manejo del carrito que sugieren la necesidad de optimizar sesiones y cacheo.
- ❖ Pruebas de seguridad: Se validaron correctamente protecciones contra CSRF, control de accesos y presencia de encabezados HTTP de seguridad. No se identificaron vulnerabilidades por inyección SQL. Sin embargo, el formulario de login carece de protección contra ataques de fuerza bruta: no cuenta con límites de intentos, bloqueo temporal ni CAPTCHA, permitiendo múltiples accesos automatizados sin restricción.

Aunque la plataforma cumple con gran parte de los requisitos funcionales y técnicos, las fallas en el flujo de pago y la ausencia de defensa contra fuerza bruta son problemas importantes. Aparte, ciertos detalles menores en el rendimiento prolongado deben ajustarse para garantizar una mayor estabilidad.