



Práctica Final Bootcamp Ciberseguridad
<Pentesting Web – Mundonipon.com>

Auditores: Tomás Auñón Hernández y Mónica Durán Alfonso

Fecha de Entrega: 13/02/2025



KEEP CODING
Tech School

ÍNDICE

Declaración de Confidencialidad	4
Disclaimer	4
Información de Contacto	4
Descripción General de la Evaluación	5
Componentes de la evaluación	6
Prueba de Penetración Web	6
Clasificación de Gravedad	6
Factores de Riesgo	7
Probabilidad	7
Impacto	7
Alcance	7
Exclusiones por Alcance	7
Permisos del cliente	7
Resumen Ejecutivo	8
Alcance y limitaciones de tiempo	8
Resumen de Pruebas	8
Reconocimiento	8
Subdominios	8
Escaneo de Puertos	8
Tecnologías Utilizadas	9
Explotación	9
Resumen de Vulnerabilidades y Calificaciones	10
Descubrimientos del Test Interno de Penetración	10
Metodología	11
OWASP TOP 10	11
1. Broken Access Control:	11
2. Cryptographic Failures:	13
3. Injection:	14
Recomendaciones	15
4. Insecure Design:	15
Recomendaciones	16
5. Security Misconfiguration:	17
6. Vulnerable and Outdated Components:	17
7. Identification and Authentication Failures:	17
Recomendaciones	18

8. Software and Data Integrity Failures:.....	18
Recomendaciones	18
9. Security Logging and Monitoring Failures:.....	19
Recomendaciones	19
10. Server Side Request Forgery:	20
Otras Vulnerabilidades.....	22
Full Path Disclosure:	22
Conclusión	23
Resumen de Resultados	23
Recomendaciones.....	23

Declaración de Confidencialidad

Este documento es propiedad exclusiva del cliente Mundo Nipón y la empresa auditora Keep-Pentesting. Este documento contiene información confidencial y de propiedad exclusiva. La duplicación, redistribución o uso, total o parcial, en cualquier forma, requiere el consentimiento tanto de la parte del cliente (Mundo Nipón) como de la empresa auditora (Keep-Pentesting).

El cliente Mundo Nipón puede compartir este documento con auditores bajo acuerdos de confidencialidad para demostrar el cumplimiento de los requisitos de prueba de penetración.

Disclaimer

Una prueba de penetración se considera una instantánea en el tiempo. Los hallazgos y recomendaciones reflejan la información recopilada durante la evaluación y no los cambios o modificaciones realizados fuera de ese período.

Los compromisos con límite de tiempo no permiten una evaluación completa de todos los controles de seguridad. Keep-Pentesting priorizó la evaluación para identificar los controles de seguridad más débiles que un atacante podría explotar. Keep-Pentesting recomienda realizar evaluaciones similares anualmente por parte de evaluadores internos o externos para garantizar el éxito continuo de los controles.

Información de Contacto

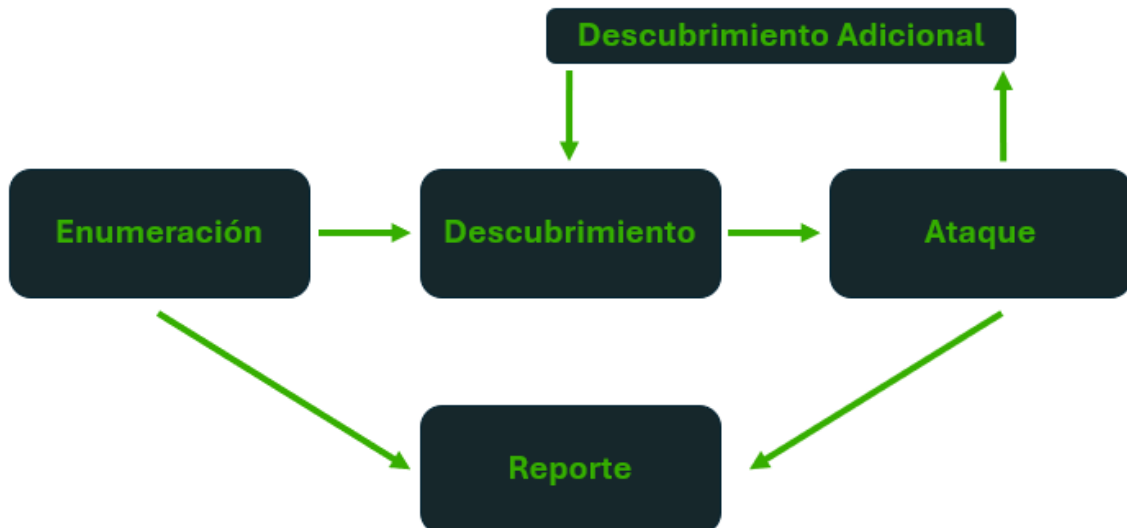
Name	Title	Contact Information
www.mundonipon.com		
Carlos Cilleruelo	Global Information Security Manager	Email: info@mundonipon.com
Keep-Pentesting Cybersecurity		
Tomás Auñón	Lead Penetration Tester	Email: tomasauñon@gmail.com
Mónica Durán	Lead Penetration Tester	Email: monicadual1915@gmail.com

Descripción General de la Evaluación

Del 27 de enero de 2025 al 13 de febrero de 2025, Mundo Nipón contrató a **Keep-Pentesting** para evaluar la postura de seguridad de su infraestructura en comparación con las mejores prácticas actuales de la industria, que incluyeron una prueba de penetración de red interna. Todas las pruebas realizadas se basan en la Guía técnica NIST SP 800-115 *Technical Guide to Information Security Testing and Assessment*, OWASP *Testing Guide (v4)*, and customized testing frameworks.

Las fases de las actividades de prueba de penetración son las siguientes.

- **Enumeración:** se recopilan los objetivos del cliente y se obtienen las reglas de interacción
- **Descubrimiento:** se realiza un escaneo y una enumeración para identificar posibles vulnerabilidades, áreas débiles y explotaciones.
- **Ataque:** se confirman las posibles vulnerabilidades a través de la explotación y se realiza un descubrimiento adicional en caso de un nuevo acceso.
- **Reporte:** se documentan todas las vulnerabilidades y explotaciones encontradas, los intentos fallidos, y las fortalezas y debilidades de la compañía.



Componentes de la evaluación

Prueba de Penetración Web

Una prueba de penetración interna emula el rol de un atacante desde un puesto remoto. Un ingeniero escaneará la web para identificar posibles vulnerabilidades del host y realizará ataques de red comunes y avanzados.

Clasificación de Gravedad

La siguiente tabla define los niveles de gravedad y el rango de puntuación CVSS correspondiente que se utilizan en todo el documento para evaluar la vulnerabilidad y el impacto del riesgo.

Gravedad	CVSS V3 Rango Puntuación	Definición
Crítico	9.0-10.0	La explotación es sencilla y, por lo general, da como resultado un compromiso a nivel del sistema. Se recomienda elaborar un plan de acción y aplicar el parche de inmediato.
Alto	7.0-8.9	La explotación es más difícil, pero podría provocar privilegios elevados y, potencialmente, una pérdida de datos o tiempo de inactividad. Se recomienda elaborar un plan de acción y aplicar el parche lo antes posible.
Medio	4.0-6.9	Existen vulnerabilidades, pero no son explotables o requieren pasos adicionales, como ingeniería social. Se recomienda elaborar un plan de acción y aplicar el parche después de que se hayan resuelto los problemas de alta prioridad.
Bajo	0.1-3.9	Las vulnerabilidades no son explotables, pero reducirían la superficie de ataque de una organización. Se recomienda elaborar un plan de acción y aplicar el parche durante la próxima ventana de mantenimiento.
Info	N/A	No existe ninguna vulnerabilidad. Se proporciona información adicional sobre los elementos detectados durante las pruebas, los controles estrictos y la documentación adicional.

Factores de Riesgo

El riesgo se mide por dos factores: **probabilidad** e **impacto**.

Probabilidad

La probabilidad mide la posibilidad de que se explote una vulnerabilidad. Las calificaciones se otorgan en función de la dificultad del ataque, las herramientas disponibles, el nivel de habilidad del atacante y el entorno del cliente.

Impacto

El impacto mide el efecto potencial de la vulnerabilidad en las operaciones, incluida la confidencialidad, la integridad y la disponibilidad de los sistemas y/o datos del cliente, el daño a la reputación y la pérdida financiera.

Alcance

Evaluación	Detalles
Test interno de penetración	En el escaneo muestra estas IPs: 104.21.46.230 172.67.142.185 51.210.97.55

Exclusiones por Alcance

Por solicitud del cliente, **Keep-Pentesting** no realizó ninguno de los siguientes ataques durante las pruebas:

- Denegación de servicio (DDoS)
- Suplantación de identidad/ingeniería social

Mundo Nipón permitió todos los demás ataques no especificados anteriormente.

Permisos del cliente

Mundo Nipón proporcionó a **Keep-Pentesting** los siguientes permisos:

- Evaluar la seguridad de la aplicación web mundonipon.com en remoto utilizando técnicas pasivas y activas.

Resumen Ejecutivo

Keep-Pentesting evaluó la postura de seguridad interna de Mundo Nipon a través de pruebas de penetración del 27 de enero de 2025 al 12 de febrero de 2025. En estas secciones se describen las vulnerabilidades descubiertas, los intentos exitosos y fallidos y las fortalezas y debilidades.

Alcance y limitaciones de tiempo

El alcance durante el compromiso no permitió la denegación de servicio o la ingeniería social en todos los componentes de prueba.

Se establecieron limitaciones de tiempo para las pruebas. Se permitió la prueba de penetración de la red interna durante nueve (17) días naturales.

Resumen de Pruebas

Durante la auditoría de seguridad realizada en el sitio web **mundonipon.com**, se llevó a cabo un escaneo de puertos con el objetivo de identificar posibles vulnerabilidades en los servicios expuestos. Sin embargo, es importante destacar que la presencia de Cloudflare como proveedor de protección y distribución de contenido (CDN) ha introducido ciertas limitaciones en la cantidad de información recopilada.

Reconocimiento

Subdominios

Se han encontrado los siguientes subdominios válidos:

- beta.mundonipon.com
- mail.mundonipon.com
- dev.mundonipon.com
- colaboradores.mundonipon.com
- smtp.mundonipon.com
- pop3.mundonipon.com
- correo.mundonipon.com

Escaneo de Puertos

- **Objetivo:** Identificar puertos abiertos y servicios asociados que pudieran presentar vulnerabilidades.
- **Herramientas Utilizadas:** Nmap, Zenmap.
- **Resultados:** La mayor parte del tráfico y la infraestructura del sitio web se encuentra flanqueada por **Cloudflare** que actúa como un intermediario entre los usuarios y el servidor, optimizando el rendimiento y asegurando el sitio web contra ataques y vulnerabilidades. Como resultado, el escaneo de puertos reveló únicamente información relacionada con los servidores de Cloudflare, sin acceso directo a los servidores de origen del sitio web.

Las IPs analizadas son las siguientes:

172.67.142.185	104.21.46.230	51.210.97.55
80: http cloudflare 443: https cloudflare 8080: http cloudflare 8443: https cloudflare	80: http cloudflare 443: https cloudflare 8080: http cloudflare 8443: https cloudflare	22755: OpenSSH 7.9p1 Debian 10+deb10u2

Tecnologías Utilizadas

- osCommerce: CMS de tienda online
- Google Analytics
- PHP
- Cloudflare: Como CDN, WAF.
- MySQL
- SweetAlert2: Librería JS para animaciones
- jQuery

No se han podido obtener las versiones de las tecnologías ya que Cloudflare impide poder listarlas.

Explotación

Se han realizado pruebas en base al OWASP TOP 10.

- **Broken Access Control:** Se han realizado pruebas de escalada vertical y horizontal de privilegios para intentar acceder a información no autorizada con el usuario inicial.
- **Cryptography Failures:** Se han revisado certificados y conexiones seguras.
- **Injection:** Se han realizado pruebas de inyección como SQL injection, XSS, Inyección de comandos, Remote File Inclusion, etc.
- **Insecure Design:** Se ha revisado el código fuente y diseño de la página buscando vulnerabilidades explotables y partes inseguras.
- **Security Misconfiguration:** Se han revisado la web en busca de cambios en el software que permitan una explotación.
- **Vulnerable and Outdated Components:** Se han buscado las versiones de las tecnologías utilizadas en la web, aunque ha sido realmente difícil debido a que utiliza Cloudflare.
- **Identification and Authentication Failures:** Se han comprobado los tipos de autenticación de la página así como la manera en que viajan los datos de autenticación de los distintos paneles de login. Se ha detectado posibilidad de fuerza bruta en algunos paneles.
- **Software and Data Integrity Failures:** Se han revisado posibles fallos en la integridad de los datos y exposición de url privadas.
- **Security Logging and Monitoring Failures:** Se ha comprobado la integridad de los paneles de login así como la posibilidad de enumerar usuarios analizando las respuestas del servidor.
- **Server Side Request Forgery:** Se ha comprobado la posible explotación de esta vulnerabilidad basada en la utilización de URL que modifican datos utilizando autenticaciones previas.
- **Full Path Disclosure:** Se ha comprobado que con ciertas url's el servidor responde con directorios que sensibles que deberían mantenerse privados ya que permiten la enumeración de directorios reales del servidor.

Resumen de Vulnerabilidades y Calificaciones

Las siguientes tablas muestran las vulnerabilidades encontradas por impacto así como recomendaciones para su mitigación.

Descubrimientos del Test Interno de Penetración

0	0	0	4	2
Crítico	Alto	Medio	Bajo	Info

VULNERABILIDAD	GRAVEDAD	CVSS V3 RANGO DE PUNTUACIÓN	DESCRIPCIÓN
Cryptographic Failures	Bajo	0.1-3.9	Soporte para versiones TLS desactualizadas. Recomendable deshabilitar esta opción en el servidor para TLS 1.0 Y 1.1
Insecure Desing	Bajo	0.1-3.9	Comentarios en código fuente innecesarios que indican la presencia de algún Malware. Recomendación eliminar dichos comentarios si no hay un objetivo claro. Gestión de errores con <code>windows.onerror()</code> . Este manejo de errores enviando un reporte a la página <code>ajax_error_js.php</code> puede dar lugar a secuestro de cookies en caso de lograr un XSS efectivo.
Identification and Authentication Failures	Bajo	0.1-3.9	Se ha detectado Basic Authentication en paneles de login en las páginas www.mundonipon.com/paneldecontrol y beta.mundonipon.com . Este tipo de autenticación no tiene límite de intentos y se puede realizar un ataque por fuerza bruta.
Full Path Disclosure	Bajo	0.1-3.9	Se ha detectado que el servidor devuelve rutas sensibles al mostrar errores de memoria en las rutas https://mundonipon.com/includes/application_top.php https://mundonipon.com/includes/configure.php lo que da lugar a un mapeo de la estructura de directorios.
Software and Data Integrity Failures	Info	N/A	Se ha encontrado información sensible filtrada a través de las reseñas de Google debido a URL privadas impresas en las facturas. Esto ha dado lugar a poder enumerar el directorio <code>/paneldecontrol</code> que muestra un panel de login.
Security Loggin and Monitorinf Failures	Info	N/A	Enumeración de usuarios en los formularios de registro y recuperación de contraseña. Puede dar lugar a ataques de fuerza bruta solo en el campo del password, mermando la seguridad.

Metodología

Para llevar a cabo la auditoría de seguridad se utilizó la metodología OWASP TOP 10, un estándar reconocido a nivel mundial que identifica las diez principales amenazas de seguridad en aplicaciones web.

OWASP TOP 10

La metodología OWASP TOP 10 se enfoca en la identificación y mitigación de las vulnerabilidades críticas, se realizaron pruebas con cada una de ellas que pasamos a detallar:

1. Broken Access Control:

No fué posible realizar una intrusión a través de Broken Access Control.

Se han realizado pruebas de manera vertical no obteniendo un parámetro en el usuario que nos permita cambiar el rol, por lo que los usuarios dependen de cómo la cookie oScid esté grabada en el sistema y del rol del usuario que esté grabada.

Como se observa en la siguiente captura, los únicos parámetros que viajan en el login son el usuario y la contraseña. Hay que remarcar que la contraseña aparece en texto plano en la solicitud.

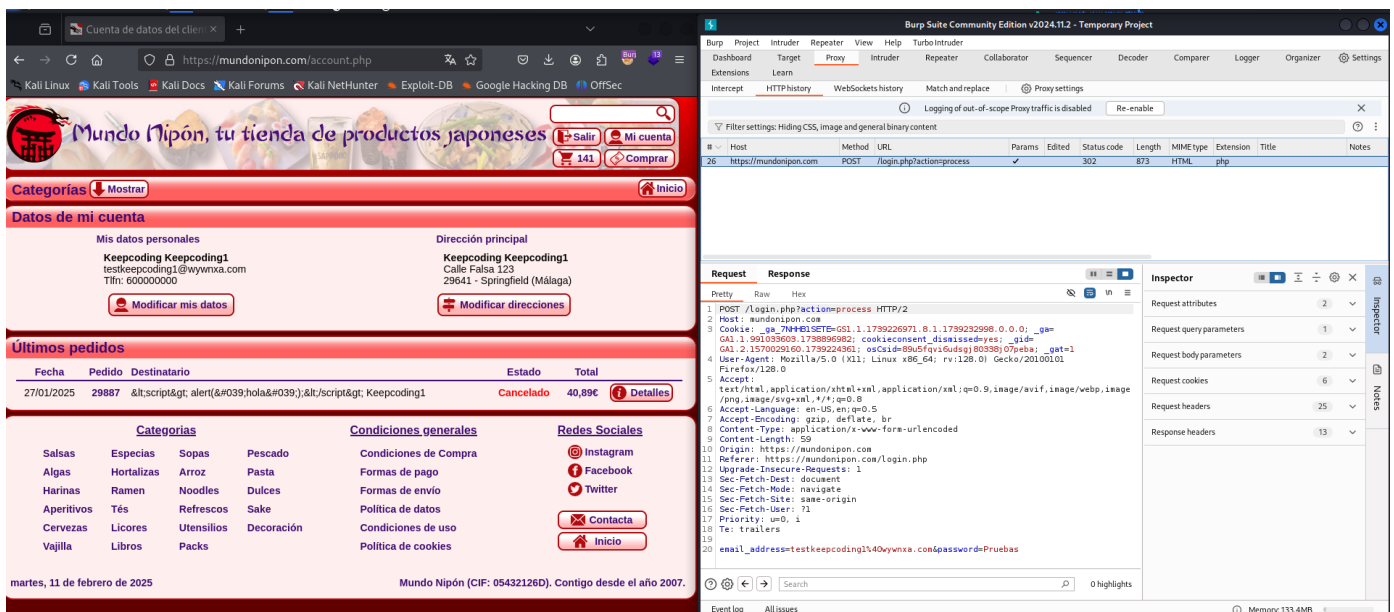


Imagen 1. Solicitud interceptada con contraseña en texto plano.

Por otro lado, también se han realizado pruebas para realizar un Broken Access Control de manera horizontal intentando acceder a datos de otros usuarios, pero tampoco fue posible.

Para ello hemos utilizado un pedido de prueba con id 29887, ya que este id se envía en método GET.

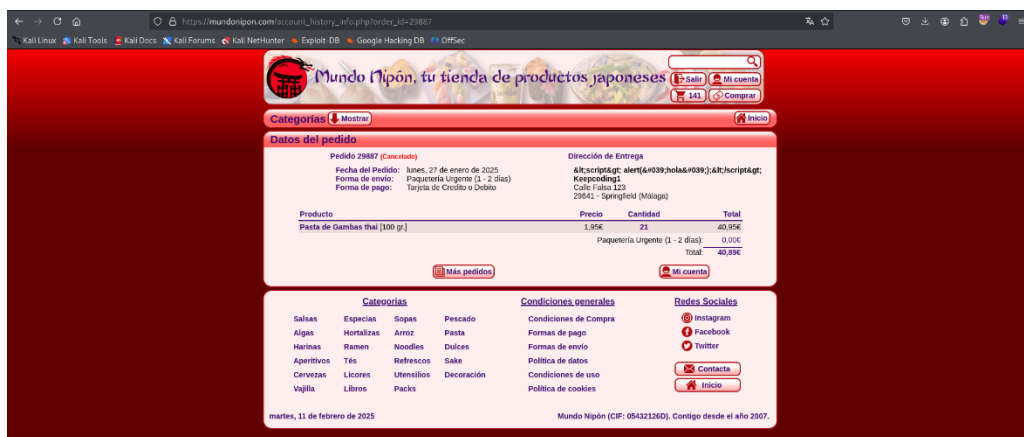


Imagen 2. Pedido realizado con ID29887.

Lo hemos sustituido por el id 26385 que nos consta que existe debido a una reseña de la que hablaremos más adelante. La página nos redirige a nuestra cuenta, por lo que es un vector que no podemos explotar.

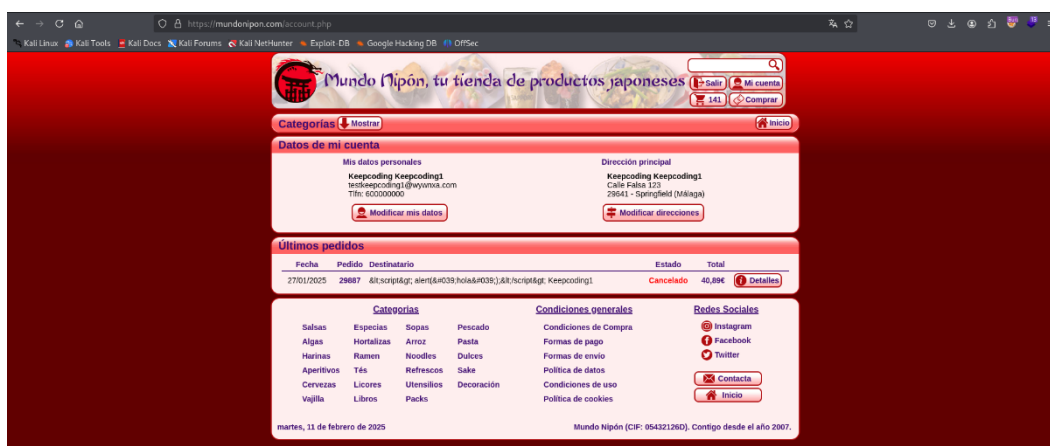


Imagen 3. Se sustituye el ID 29887 por el ID 26385.

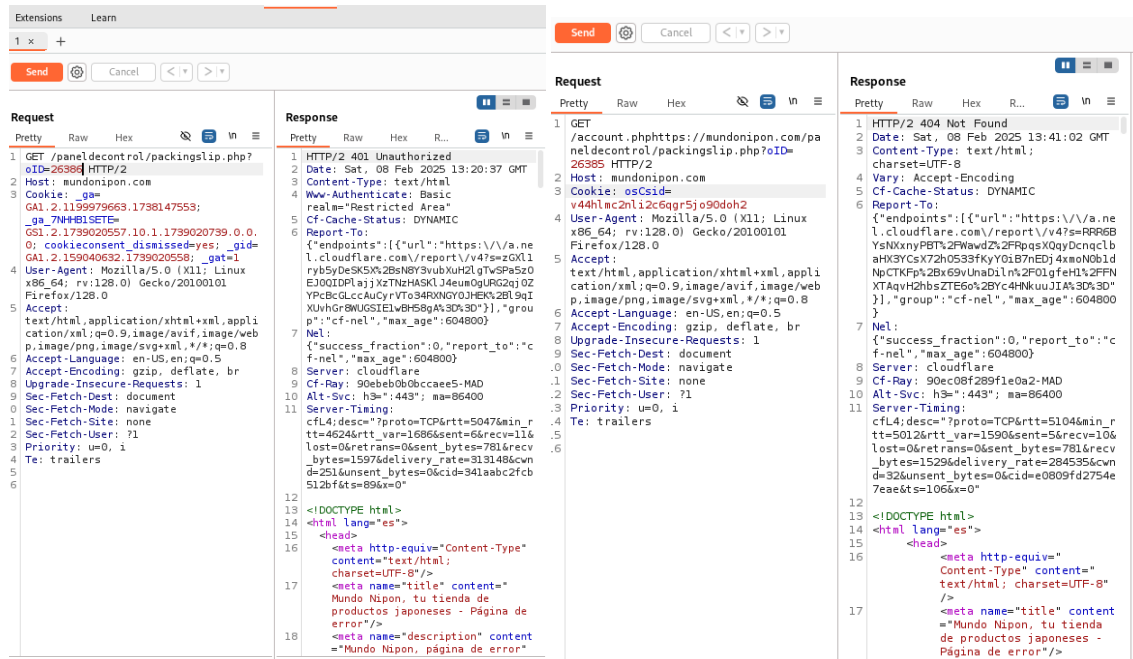


Imagen 4. Acceso no autorizado con error 401.

Imagen 5. Acceso no autorizado con error 404.

A pesar de los intentos realizados, no se logró explotar ninguna vulnerabilidad de Broken Access Control. Los resultados de las pruebas fueron los siguientes:

- **Acceso No Autorizado:** Todos los intentos de acceder a áreas restringidas utilizando manipulación de parámetros en la URL resultaron en errores de acceso, incluyendo códigos de estado HTTP 401 (Unauthorized) y 404 (Not Found).
- **Cookies de Sesión:** Las pruebas que utilizaron cookies de sesión no permitieron eludir los controles de acceso existentes. La aplicación correctamente verificó la validez y los permisos asociados a las cookies de sesión.
- **Autenticación Adicional:** Las páginas críticas requirieron autenticación adicional, impidiendo el acceso no autorizado incluso con credenciales válidas.

2. Cryptographic Failures:

Se han encontrado soporte para versiones de TLS desactualizadas. Aunque la web cuenta con certificado SSL TLS 1.3, se recomienda deshabilitar el soporte para versiones 1.0 y 1.1.

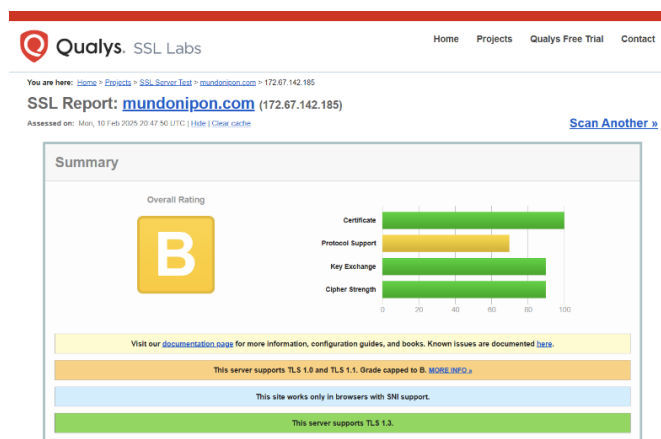


Imagen 6. Versión TLS desactualizada en IP 172.67.142.185

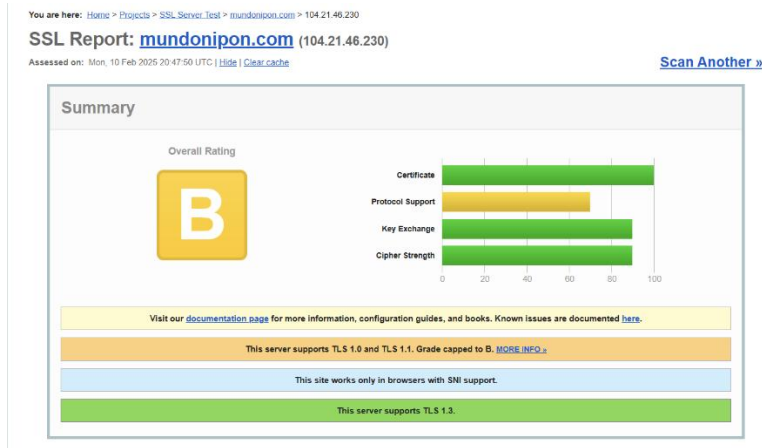


Imagen 7. Versión TLS desactualizada en IP 104.21.46.230

3. Injection:

Durante la auditoría de seguridad realizada para el sitio web **mundonipon.com**, se llevaron a cabo diversas pruebas de inyección con el objetivo de identificar posibles vulnerabilidades en la aplicación. **La aplicación no es aparentemente vulnerable a inyección.**

Estas pruebas incluyen:

Inyección SQL: Pruebas para detectar posibles puntos de inyección en las consultas SQL.

Inyección de comandos: Pruebas para identificar la posibilidad de ejecutar comandos del sistema a través de entradas no sanitizadas.

Inyección de script: Pruebas para detectar inyecciones de script (XSS) en diferentes puntos de la aplicación.

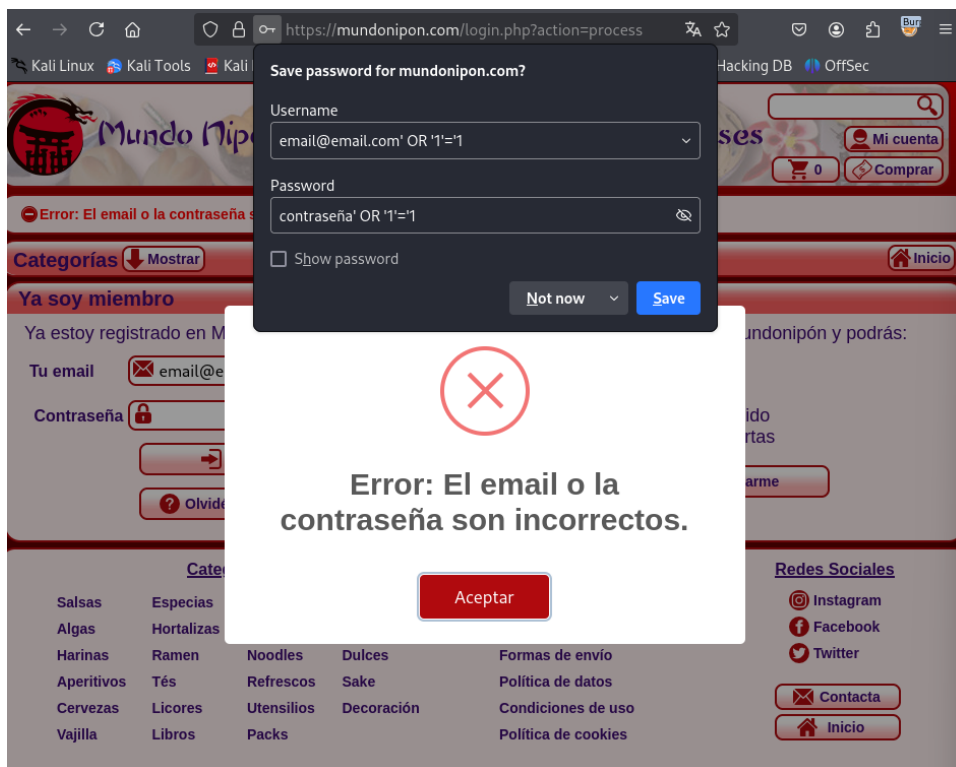


Imagen 8. Ataque con Inyección SQL.

Dirección de Entrega

<script> alert('hola');</script>
Keepcoding1
 Calle Falsa 123
 29641 - Springfield (Málaga)

Imagen 9. Ataque con inyección SQL.

Recomendaciones

- **Pruebas Internas Complementarias:** Se recomienda realizar pruebas internas directamente en los servidores de origen para obtener una visión más realista de las posibles vulnerabilidades directamente sobre la aplicación sin que intervenga Cloudflare.
- **Monitoreo Continuo:** Continuar utilizando servicios de protección como Cloudflare es crucial para mitigar ataques comunes, pero debe complementarse con auditorías internas regulares y evaluaciones de seguridad.

4. Insecure Design:

En el proceso de auditoría de seguridad realizado en el sitio web **mundonipon.com**, se identificaron comentarios en el código HTML que sugieren una gestión inadecuada de errores y la omisión de problemas de seguridad conocidos.

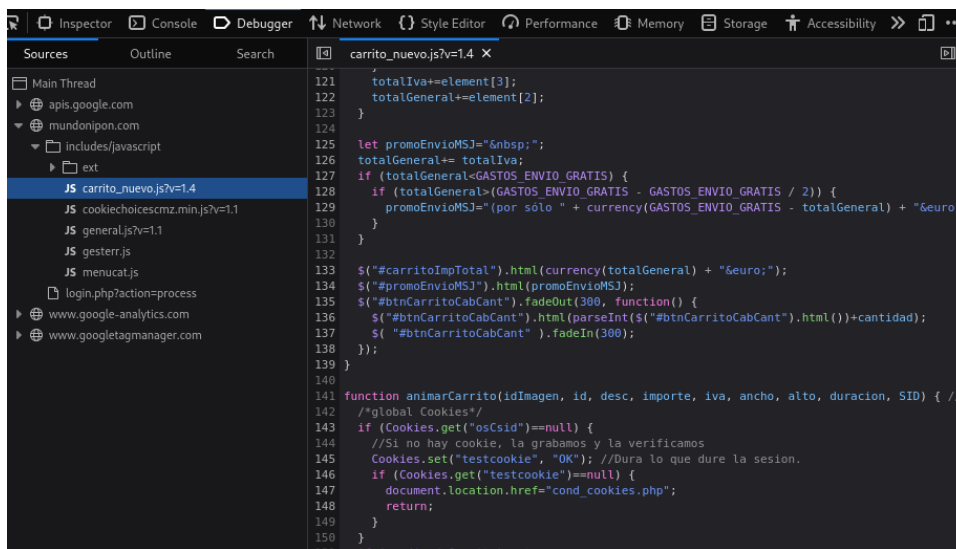


Imagen 10. Comentarios sensibles dentro del código.

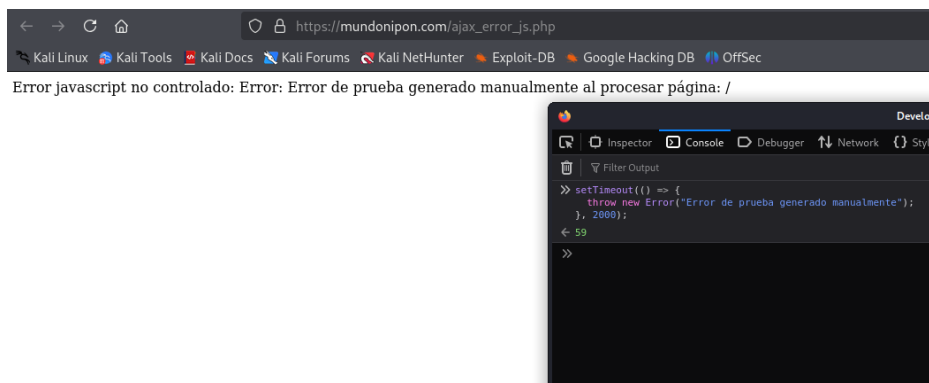
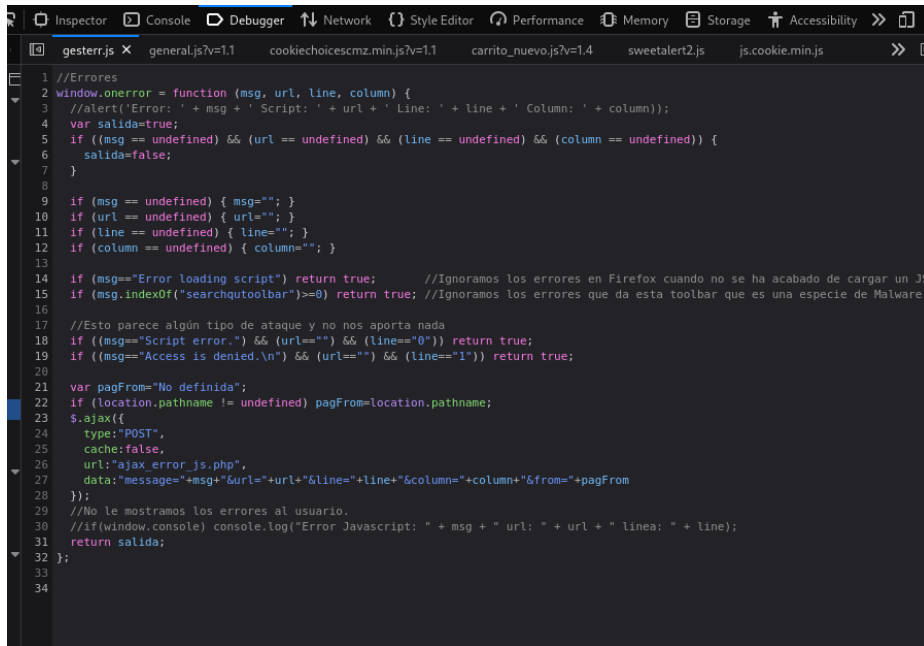


Imagen 11. Inyección de error de prueba.



```
1 //Errores
2 window.onerror = function (msg, url, line, column) {
3   //alert('Error: ' + msg + ' Script: ' + url + ' Line: ' + line + ' Column: ' + column);
4   var salida=true;
5   if ((msg == undefined) && (url == undefined) && (line == undefined) && (column == undefined)) {
6     salida=false;
7   }
8
9   if (msg == undefined) { msg=""; }
10  if (url == undefined) { url=""; }
11  if (line == undefined) { line=""; }
12  if (column == undefined) { column=""; }
13
14  if (msg=="Error loading script") return true; //Ignoramos los errores en Firefox cuando no se ha acabado de cargar un JS
15  if (msg.indexOf("searchquotoolbar")>=0) return true; //Ignoramos los errores que da esta toolbar que es una especie de Malware
16
17  //Esto parece algún tipo de ataque y no nos aporta nada
18  if ((msg=="Script error.") && (url=="") && (line=="0")) return true;
19  if ((msg=="Access is denied.\n") && (url=="") && (line=="1")) return true;
20
21  var pagFrom="No definida";
22  if (location.pathname != undefined) pagFrom=location.pathname;
23  $.ajax({
24    type:"POST",
25    cache:false,
26    url:"ajax_error_js.php",
27    data:"message="+msg+"&url="+url+"&line="+line+"&column="+column+"&from="+pagFrom
28  });
29  //No le mostramos los errores al usuario.
30  //if(window.console) console.log("Error Javascript: " + msg + " url: " + url + " linea: " + line);
31  return salida;
32 };
33
34
```

Imagen 12. Comentarios sobre manejo de errores.

Recomendaciones

1. Eliminar Comentarios Sensibles:

- Remover todos los comentarios que puedan revelar información sensible o prácticas inseguras.

2. Gestión de Errores Adecuada:

- Implementar una gestión de errores adecuada que maneje los errores de manera segura y eficiente.
- Asegurarse de que todos los errores se registren correctamente y se aborden, en lugar de ser ignorados.

3. Revisión y Eliminación de Malware:

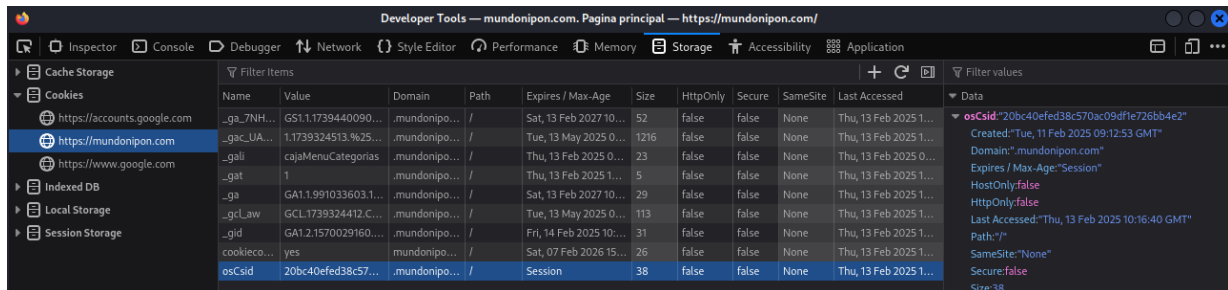
- Investigar y eliminar cualquier software malicioso mencionado en los comentarios.
- Implementar medidas para prevenir la instalación de malware en el futuro.

4. Capacitación del Equipo de Desarrollo:

- Proporcionar capacitación continua sobre las mejores prácticas de seguridad y la importancia de una gestión adecuada de errores.
- Posible fuga de datos al enviar la información a Ajax_error_js.php a través de \$.ajax. Esto puede dar lugar a que un atacante consiga inyectar código malicioso ya que al parecer se envían los datos al servidor sin autenticación.
- También se puede utilizar la función declarada para conseguir exfiltrar cookies de sesión junto con un vector de entrada XSS a través del manejador de errores que se utiliza. En este caso las entradas parecen estar bien sanitizadas y no ha sido posible, pero si en algún momento se consigue una inyección, este vector podría dar lugar a un secuestro de cookies.

5. Security Misconfiguration:

Se llevó a cabo una evaluación de la configuración de seguridad. Sin embargo, debido a la implementación de Cloudflare como proveedor de protección y distribución de contenido, no se tuvo acceso directo a los servidores de origen. Se han revisado parámetros de cookies y deberían tener el parámetro http only en true y está en false.



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
_ga_7NH...	GS11.1739440090...	.mundoipon...	/	Sat, 13 Feb 2027 10...	52	false	false	None	Thu, 13 Feb 2025 1...
_gac_UA...	1.1739324513.%25...	.mundoipon...	/	Tue, 13 May 2025 0...	1216	false	false	None	Thu, 13 Feb 2025 1...
_gali	cajaMenuCategorias	.mundoipon...	/	Thu, 13 Feb 2025 0...	23	false	false	None	Thu, 13 Feb 2025 0...
_gat	1	.mundoipon...	/	Thu, 13 Feb 2025 1...	5	false	false	None	Thu, 13 Feb 2025 1...
_ga	GA1.1.991033603.1...	.mundoipon...	/	Sat, 13 Feb 2027 10...	29	false	false	None	Thu, 13 Feb 2025 1...
_gcl_aw	GCL1739324412.C...	.mundoipon...	/	Tue, 13 May 2025 0...	113	false	false	None	Thu, 13 Feb 2025 1...
_gid	GA1.2.1570029160...	.mundoipon...	/	Fri, 14 Feb 2025 10...	31	false	false	None	Thu, 13 Feb 2025 1...
cookiec...	yes	.mundoipon...	/	Sat, 07 Feb 2026 15...	26	false	false	None	Thu, 13 Feb 2025 1...
osCsid	20bc40efed38c57...	.mundoipon...	/	Session	38	false	false	None	Thu, 13 Feb 2025 1...

Imagen 13. Parámetro httponly false.

6. Vulnerable and Outdated Components:

Se intentó identificar posibles componentes de software vulnerables y desactualizados, pero con la protección implementada por Cloudflare no se pudo acceder a información detallada sobre las versiones de software en los servidores de origen.

Se han probado vulnerabilidades genéricas para las tecnologías encontradas sin encontrar vulnerabilidades explotables asociadas.

- Oscommerce
- MySQL
- PHP

De los que fue posible identificar, no se obtuvieron vulnerabilidades explotables.

- OpenSSH 7.9p1

7. Identification and Authentication Failures:

Se ha revisado el panel de administración descubierto a través de una reseña de Google en la url <http://mundoipon.com/paneldecontrol>.

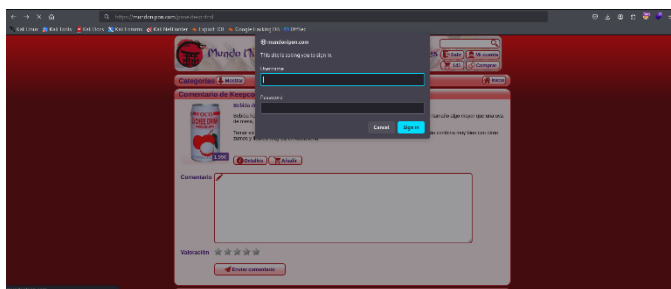


Imagen 14. Panel de control.

Este panel utiliza Authorization Basic, lo que significa que el usuario y contraseña van prácticamente en texto plano por la red. Se codifican en base64 pero es fácilmente decodificable. Por otra parte, para este tipo de autenticación no se implementan máximo número de intentos por lo que es posible realizar una fuerza bruta.

Se ha intentado una fuerza bruta a los usuarios admin, administrator e info@mundoipon.com sin éxito. Éste último se consiguió enumerar a través del formulario de registro.

De igual manera ocurre con beta.mundoipon.com, el cual tiene otro panel de login similar.

Recomendaciones

- Limitar el número de intentos y solicitudes en los paneles de autenticación.

8. Software and Data Integrity Failures:

Se identificaron posibles vulnerabilidades relacionadas con la exposición de datos sensibles. Específicamente, se observó que un cliente había subido una foto en una reseña de internet que contenía una URL privada del panel de control, junto con un ID que puede permitir acceder a información específica.

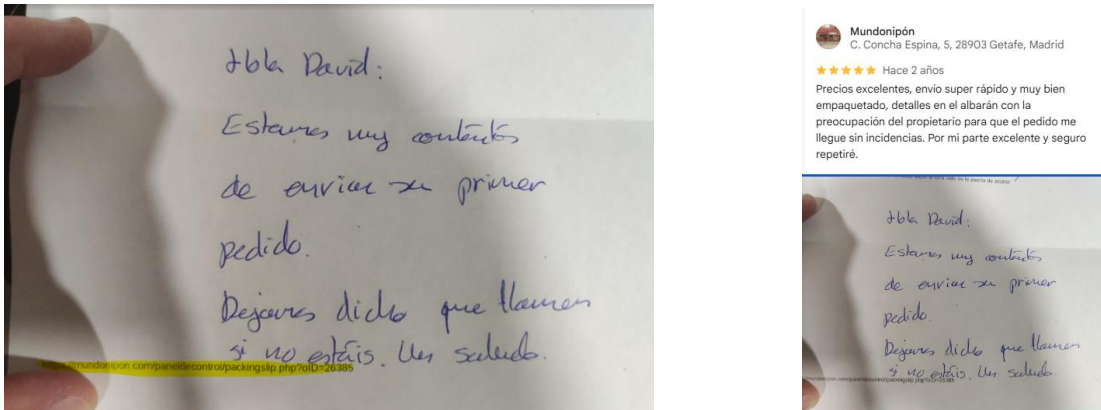


Imagen 15. Reseña de un cliente con URL del panel de control con el ID.

Recomendaciones

- **Revisión y Filtrado de Contenidos:** Implementar procesos de revisión y filtrado de fotos y otros contenidos subidos por los usuarios para detectar y eliminar información sensible.
- **Educación del Usuario:** Proporcionar directrices y educar a los usuarios sobre la importancia de no compartir información sensible.
- **Ocultación de Identificadores Sensibles:** Evitar mostrar identificadores sensibles en las interfaces de usuario.

9. Security Logging and Monitoring Failures:

Se realizaron intentos de enumeración de usuarios a través de los paneles de login. No fué posible ya que sea cual sea el campo incorrecto siempre dice "Email o Password incorrectos".

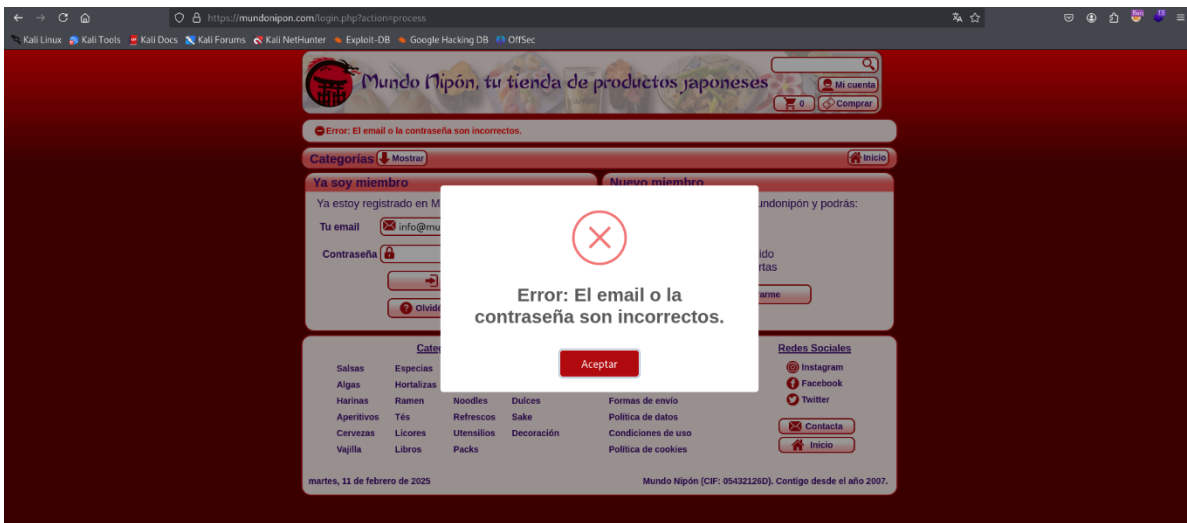


Imagen 16. Intento de enumeración de usuarios.

En cambio sí que fue posible realizarlos a través de la edición de datos de usuario y del formulario de recuperación de contraseña ya que indican claramente que el email ya está registrado, en caso de estarlo, lo que permite enumerar usuarios y posteriormente realizar un ataque de fuerza bruta solo al password, lo que merma gran parte de la seguridad.

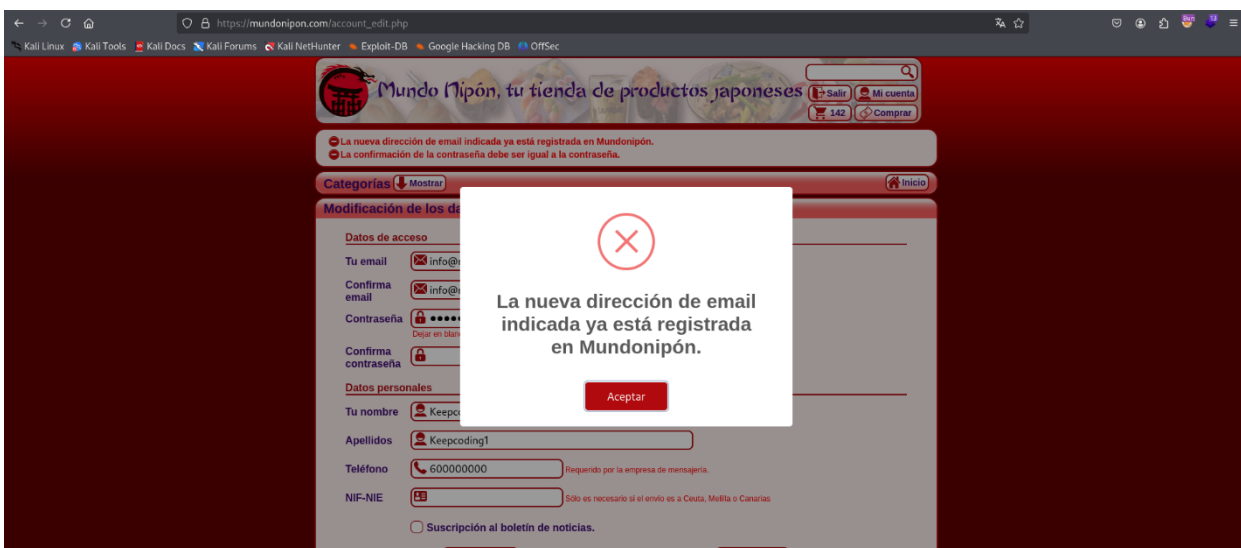


Imagen 17. Enumeración de usuarios en panel de modificación de datos.

Recomendaciones

Sería recomendable utilizar Usuarios como inicio de sesión ya que resulta mas complejo de enumerar y de esta manera aunque se modificara el correo, el usuario de acceso no quedaría expuesto.

10. Server Side Request Forgery:

Este sistema no es vulnerable a SSRF ya que no utiliza una API para listar los productos, sino una base de datos dividida en categorías y productos a través de un CMS.

Se intenta ejecutar un ataque de **Server-Side Request Forgery (SSRF)** interceptando y modificando una solicitud HTTP que utilizaba el campo de búsqueda de productos en la aplicación web de mundonipon.com. Se procede a cambiar el parámetro de búsqueda para apuntar a un recurso interno del servidor (<http://localhost:8080/privado>). La página web devolvió un mensaje indicando "no se ha encontrado ningún producto", lo que demuestra que la solicitud fue procesada pero no produjo el resultado esperado, indicando una posible mitigación efectiva del ataque.

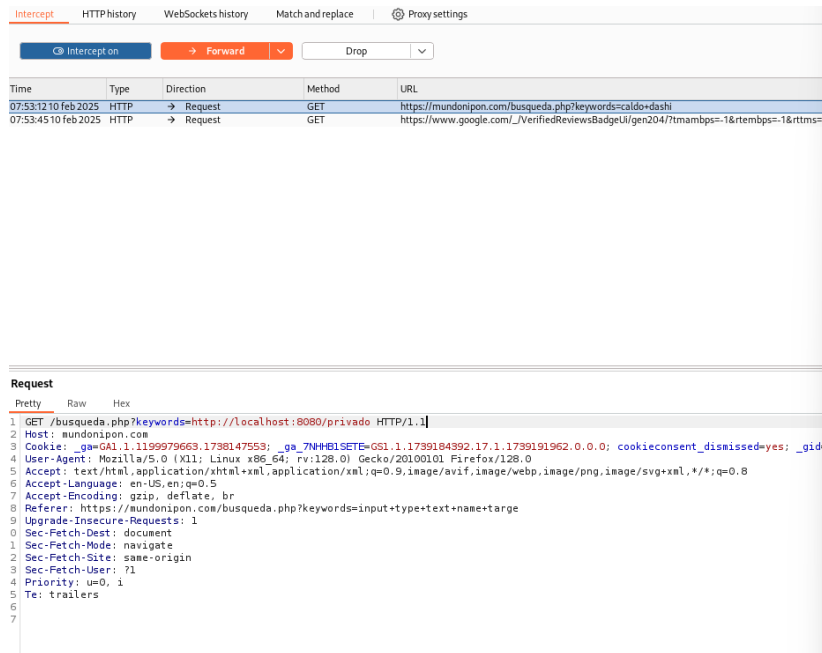


Imagen 18. Cambio de parámetro en campo de búsqueda.



Imagen 19. Respuesta del servidor a la solicitud enviada.

Por otro lado se ha probado la vulnerabilidad CSFR para ver si, a través de un enlace ya predefinido, se pueden cambiar datos como por ejemplo el password de un usuario.

Los datos viajan en método POST.

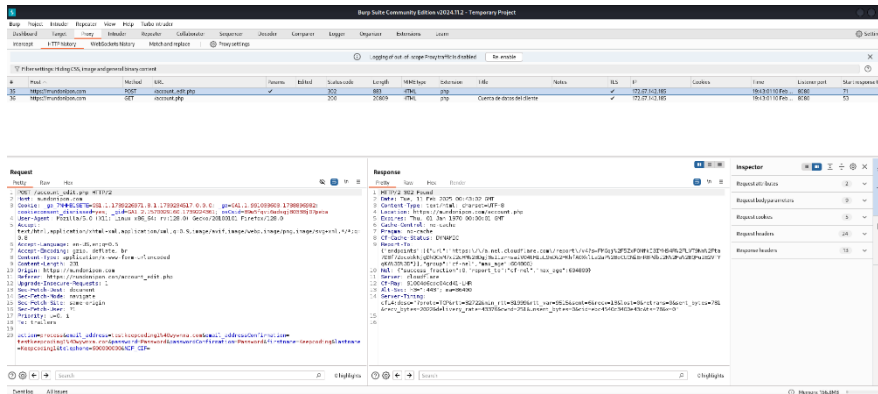


Imagen 20. Intento de cambio de password mediante CSFR.

Si cambiamos el método a GET y modificamos el password a Password2, vemos como la aplicación no valida los datos y sigue mostrando Password como contraseña.

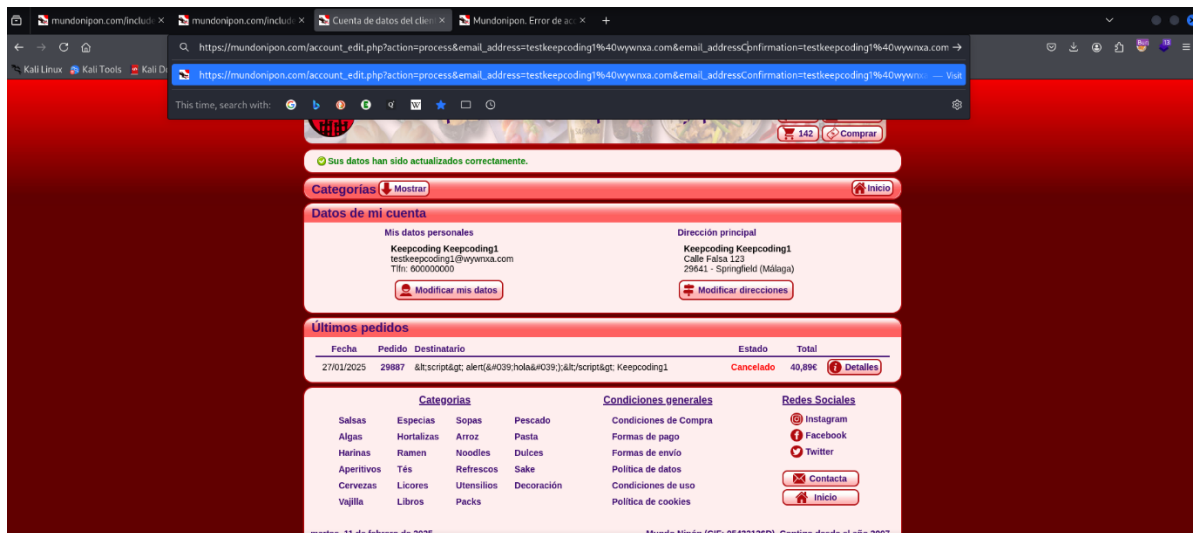


Imagen 21. Intento de modificación de password.

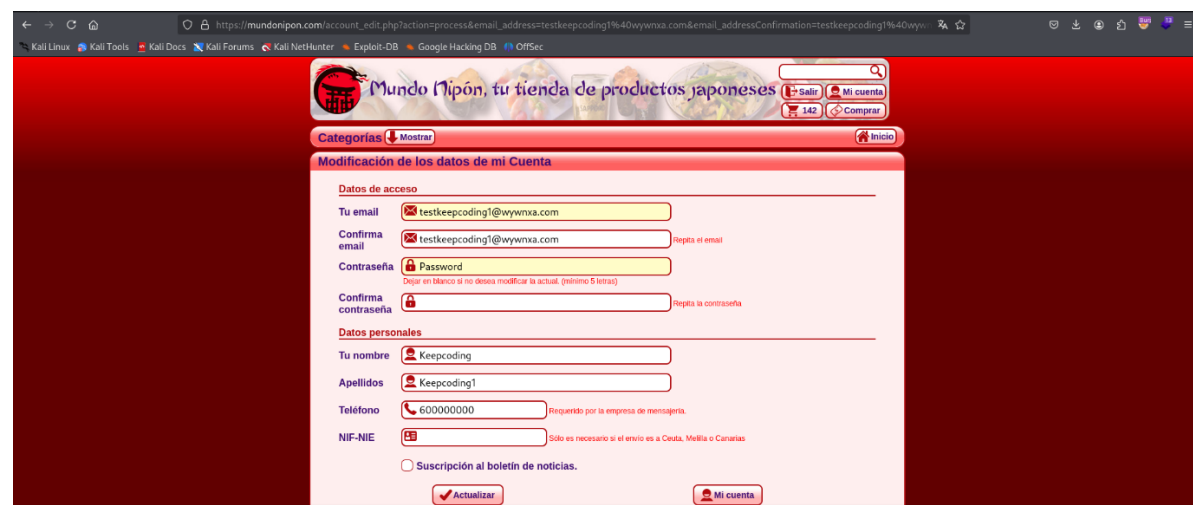


Imagen 22. Invalidación de cambio de contraseña.

Otras Vulnerabilidades

Full Path Disclosure:

Se han encontrado varias url que devuelven un error en el que se pueden ver directorios sensibles del servidor, que si bien por sí solo no ofrece gran repercusión, unido a otros ataques como LFI supone conocer de antemano la estructura de directorios del servidor.

https://mundonipon.com/includes/application_top.php

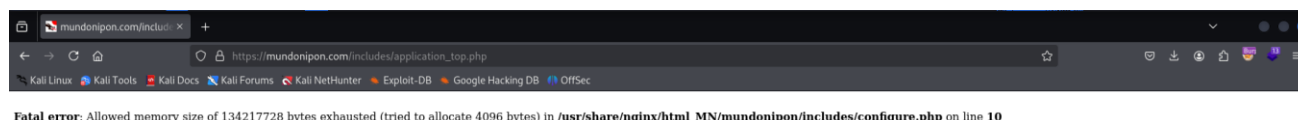


Imagen 23. Error devuelto por parte del servidor 1

<https://mundonipon.com/includes/configure.php>



Imagen 24. Error devuelto por parte del servidor 2

Finalmente se consigue enumerar el directorio /config/configure_web.php al cual la política de seguridad del servidor no nos da acceso.

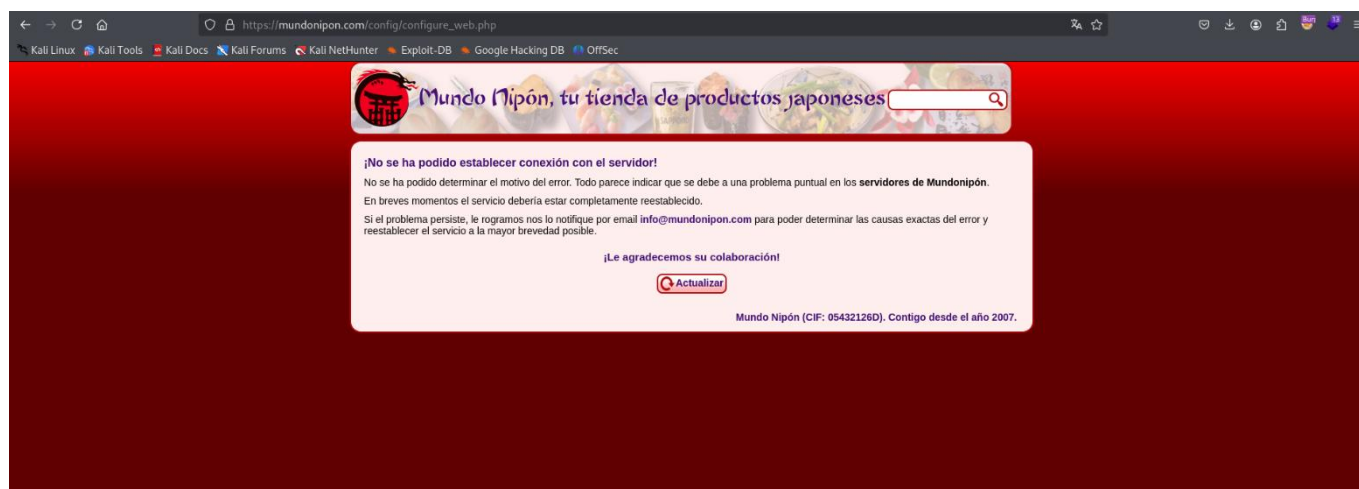


Imagen 25. Error devuelto por parte del servidor 3

Conclusión

Durante la auditoría de seguridad realizada en el sitio web **mundonipon.com**, se llevaron a cabo diferentes pruebas para identificar posibles vulnerabilidades según el método OWASP. Sin embargo, debido a la implementación de Cloudflare como proveedor de protección y distribución de contenido, sanitización de entradas e implementaciones de seguridad, no se lograron obtener resultados significativos en la mayoría de las pruebas de vulnerabilidad.

Resumen de Resultados

- **Protección Efectiva por Cloudflare:** Las medidas de seguridad implementadas por Cloudflare, incluyendo su Firewall de Aplicaciones Web (WAF) y protección contra ataques DDoS, demostraron ser efectivas para mitigar los intentos de explotación de vulnerabilidades.
- **Intentos de Fuerza Bruta:** Todos los intentos de fuerza bruta fueron bloqueados por las medidas de seguridad de Cloudflare.
- **Inyección SQL:** Las pruebas de inyección SQL resultaron en mensajes de error genéricos, lo que sugiere una protección adecuada contra estos ataques.
- **Control de Acceso:** Los intentos de acceder a áreas restringidas utilizando manipulación de parámetros en la URL resultaron en errores de acceso (HTTP 401 y 404), indicando un control de acceso robusto.
- **Manejo de Errores en la web:** La aplicación devolvió mensajes de error genéricos en varios intentos de explotación, lo que podría indicar una falta de manejo adecuado de excepciones.
- **Manejo de Errores en el servidor:** El servidor devolvió rutas sensibles que deberían no ser accesibles.

Recomendaciones

1. **Mejorar el Manejo de Errores:**
 - Asegurarse de que la aplicación maneje adecuadamente las excepciones y errores para evitar que se devuelvan mensajes de error genéricos a los usuarios.
 - Implementar una gestión de errores robusta y asegurarse de que los logs de errores sean revisados periódicamente.
2. **Revisión Regular de Seguridad:**
 - Rauditorías de seguridad periódicas para asegurarse de que las medidas de seguridad de Cloudflare y de la aplicación se mantengan actualizadas y efectivas.
 - Utilizar herramientas de escaneo automatizadas para detectar configuraciones de seguridad incorrectas y vulnerabilidades conocidas.
3. **Capacitación y Concienciación:**
 - Proporcionar capacitación continua al equipo técnico sobre las mejores prácticas de seguridad y la importancia de mantener una postura proactiva en la seguridad.
 - Fomentar una cultura de seguridad en la organización para que todos comprendan la importancia de proteger los datos y la infraestructura.
4. **Protección de Información Confidencial:**
 - Asegurarse de que ninguna información confidencial, como URLs del panel de control con IDs, sea visible o enviada a los clientes.
 - Revisar y eliminar comentarios en el código que puedan revelar información sensible o prácticas inseguras.

Aunque la protección proporcionada por Cloudflare ha demostrado ser efectiva para bloquear intentos de explotación directa, es crucial seguir implementando y manteniendo prácticas de seguridad robustas. Se recomienda seguir las mejores prácticas de seguridad, realizar auditorías regulares y mejorar el manejo de errores en la aplicación para asegurar la protección continua del sitio web. Además, es esencial revisar y proteger la información confidencial para evitar posibles filtraciones de datos y garantizar la seguridad integral de la aplicación.