Martin
Dalla Pozza

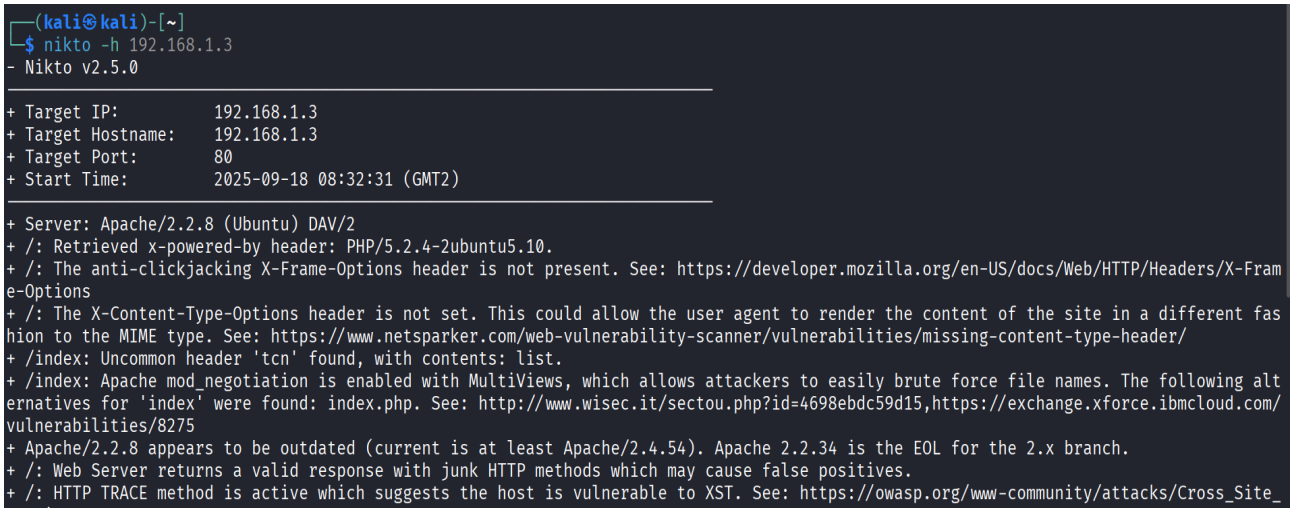
Trabajo Practico

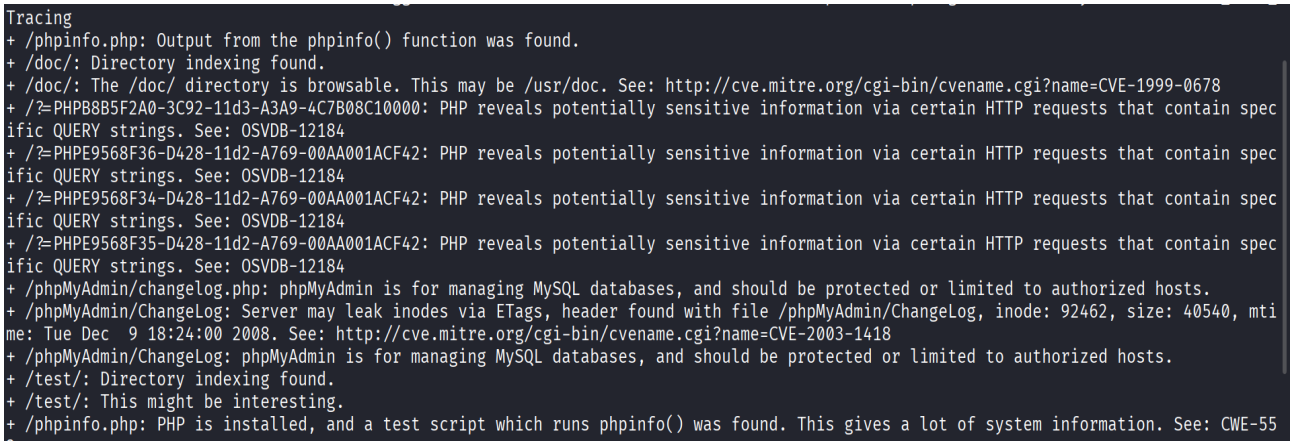
Analisis de vulnerabilidades

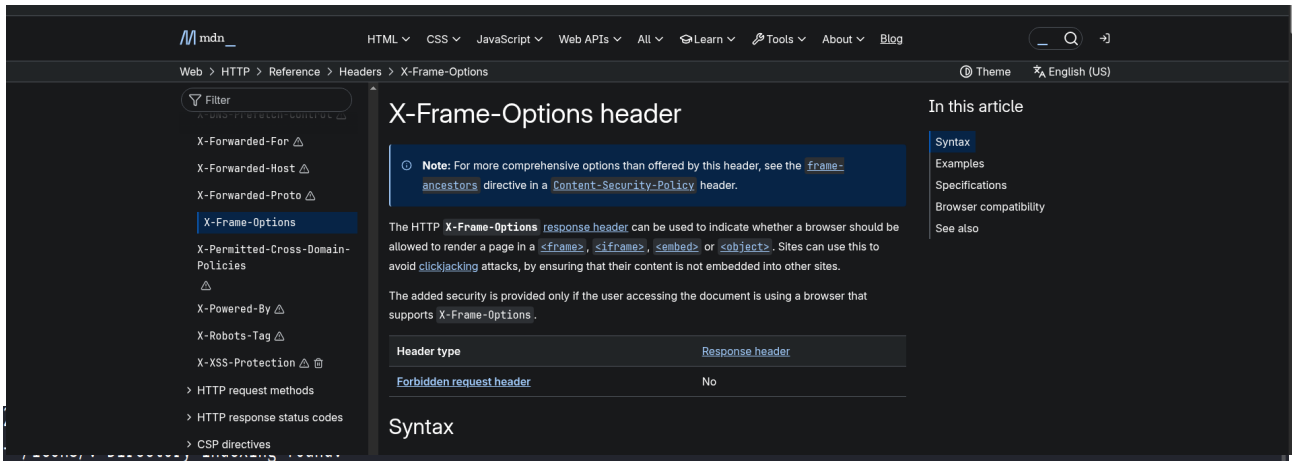
1…..Nikto
2…..OWASP ZAP

1…..Nikto

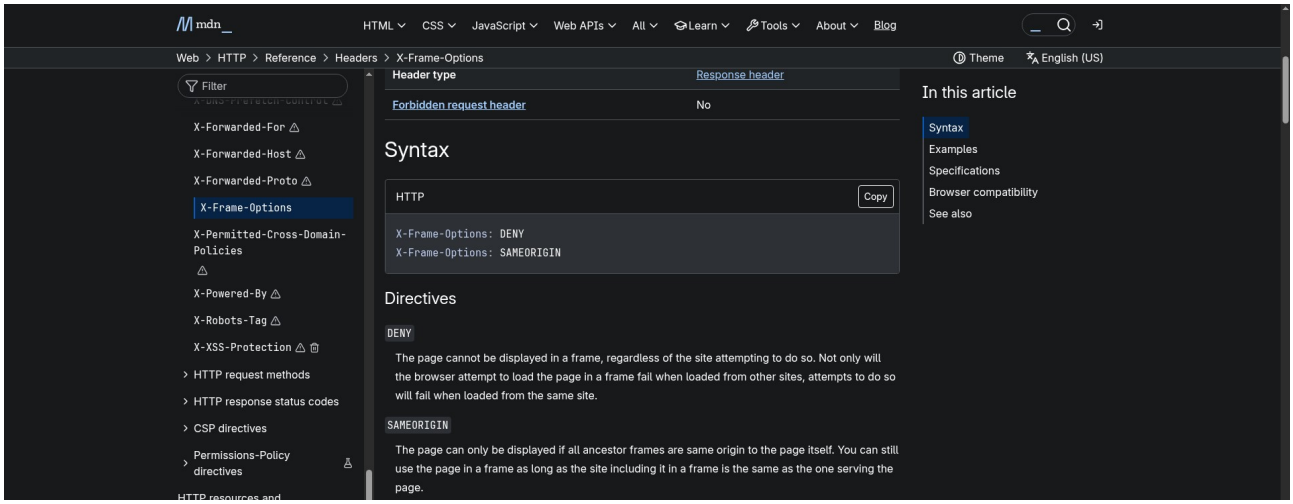
Abrimos la terminal de Kali y ponemos **nikto -h 192.168.1.3**
(es la IP de Metasploitable) y empieza el analisis donde cuando termine veremos los resultados y links para ver informes y descripcion de la vulnerabilidades.

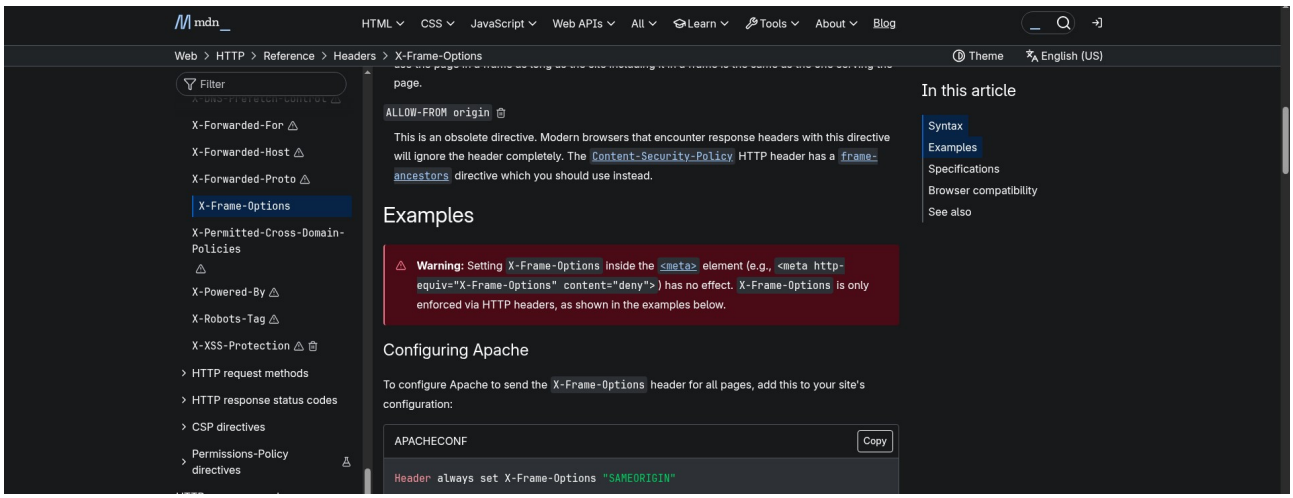


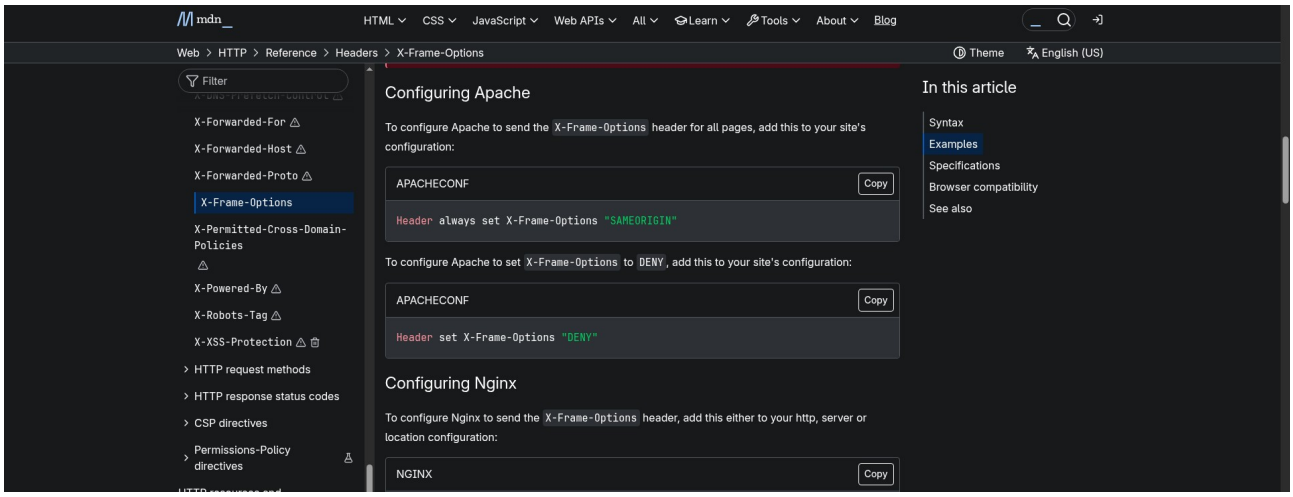


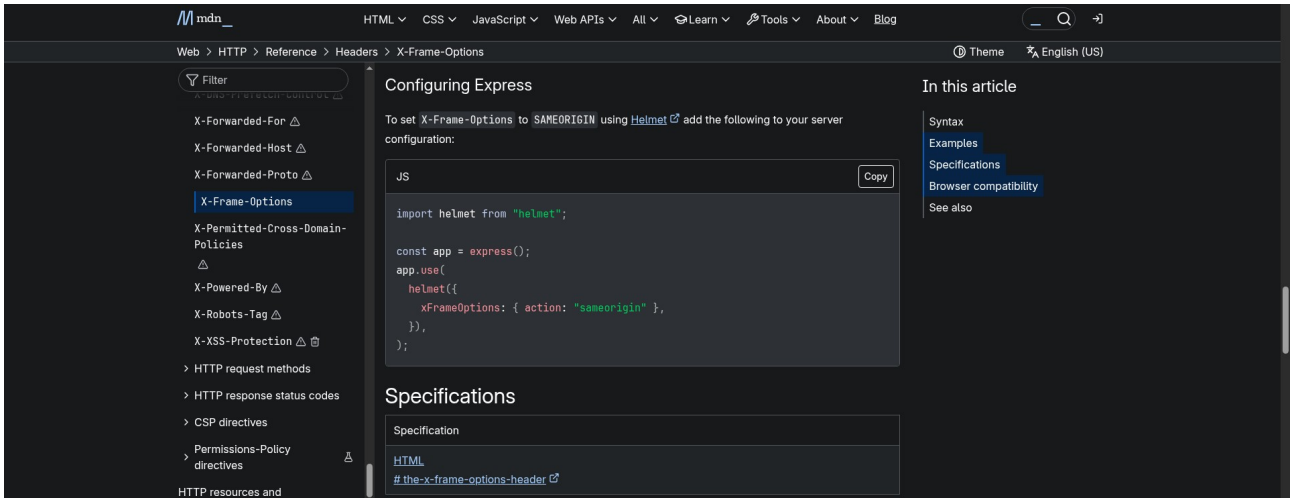


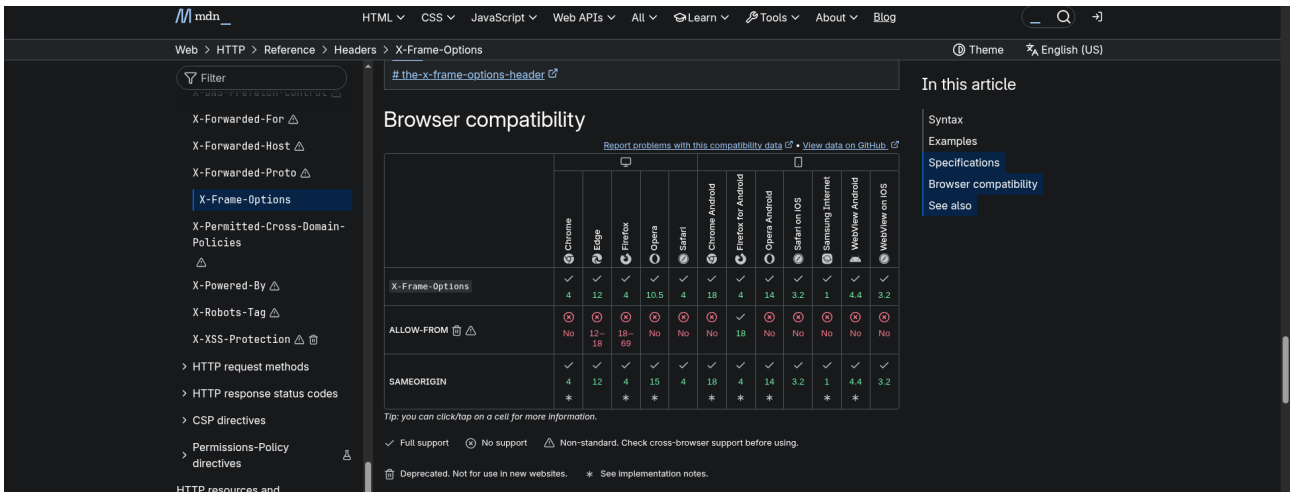

```
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2025-09-18 08:33:07 (GMT2) (36 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

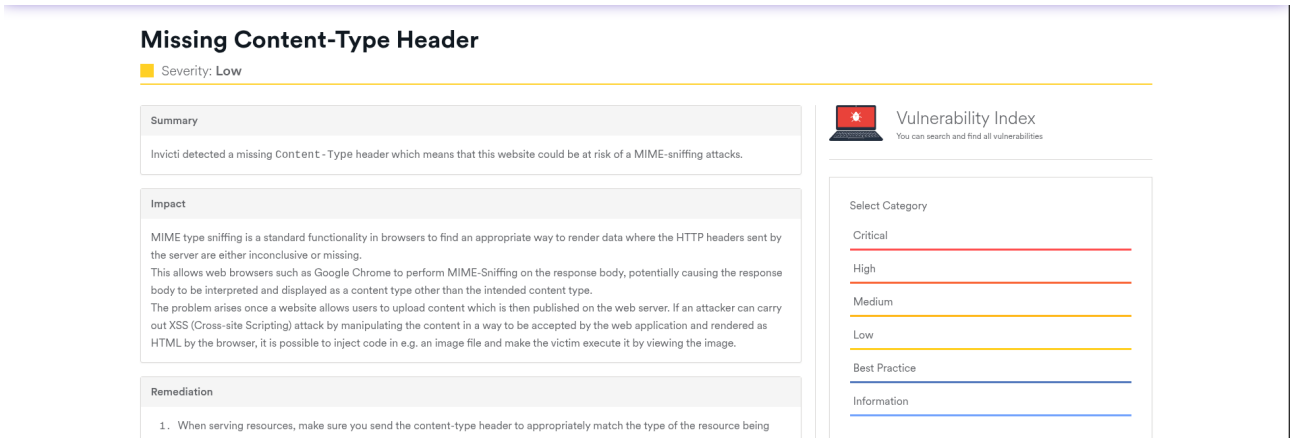


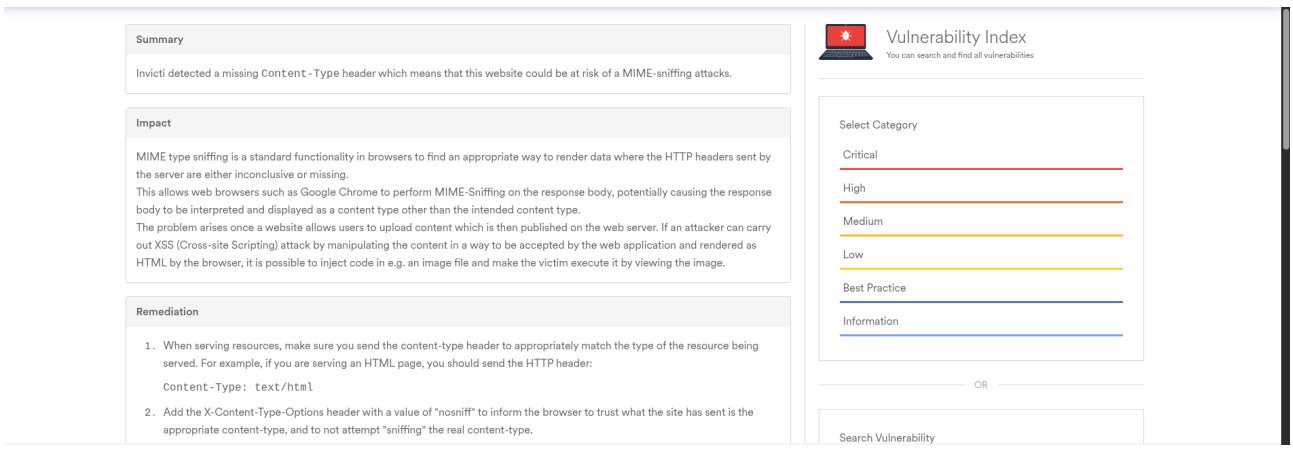

mdn_
HTML CSS JavaScript Web APIs All Learn Tools About Blog
Web > HTTP > Reference > Headers > X-Frame-Options
Theme English (US)
Filter
X-Forwarded-For
X-Forwarded-Host
X-Forwarded-Proto
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-Powered-By
X-Robots-Tag
X-XSS-Protection
HTTP request methods
HTTP response status codes
CSP directives
Permissions-Policy directives
page.
ALLOW-FROM origin
This is an obsolete directive. Modern browsers that encounter response headers with this directive will ignore the header completely. The Content-Security-Policy HTTP header has a frame-ancestors directive which you should use instead.
Examples
Warning: Setting X-Frame-Options inside the <meta> element (e.g., <meta http-equiv="X-Frame-Options" content="deny">) has no effect. X-Frame-Options is only enforced via HTTP headers, as shown in the examples below.
Configuring Apache
To configure Apache to send the X-Frame-Options header for all pages, add this to your site's configuration:
APACHECONF
Copy
Header always set X-Frame-Options "SAMEORIGIN"
In this article
Syntax
Examples
Specifications
Browser compatibility
See also

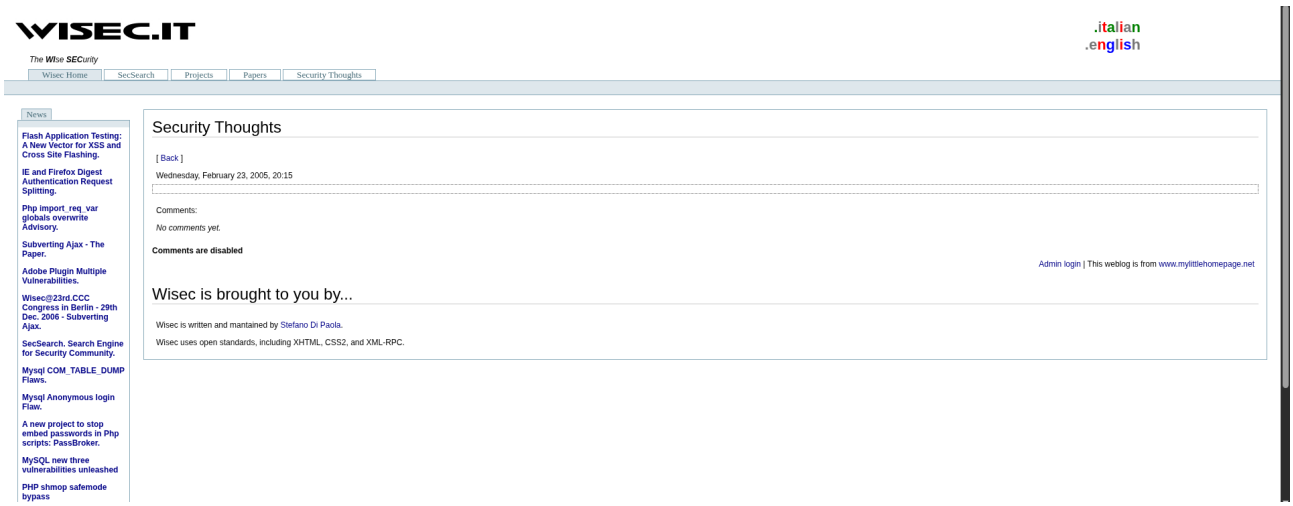

mdn_
HTML CSS JavaScript Web APIs All Learn Tools About Blog
Web > HTTP > Reference > Headers > X-Frame-Options
Theme English (US)
Filter
X-Forwarded-For
X-Forwarded-Host
X-Forwarded-Proto
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-Powered-By
X-Robots-Tag
X-XSS-Protection
HTTP request methods
HTTP response status codes
CSP directives
Permissions-Policy directives
Configuring Apache
To configure Apache to send the X-Frame-Options header for all pages, add this to your site's configuration:
APACHECONF
Copy
Header always set X-Frame-Options "SAMEORIGIN"
To configure Apache to set X-Frame-Options to DENY, add this to your site's configuration:
APACHECONF
Copy
Header set X-Frame-Options "DENY"
Configuring Nginx
To configure Nginx to send the X-Frame-Options header, add this either to your http, server or location configuration:
NGINX
Copy
In this article
Syntax
Examples
Specifications
Browser compatibility
See also

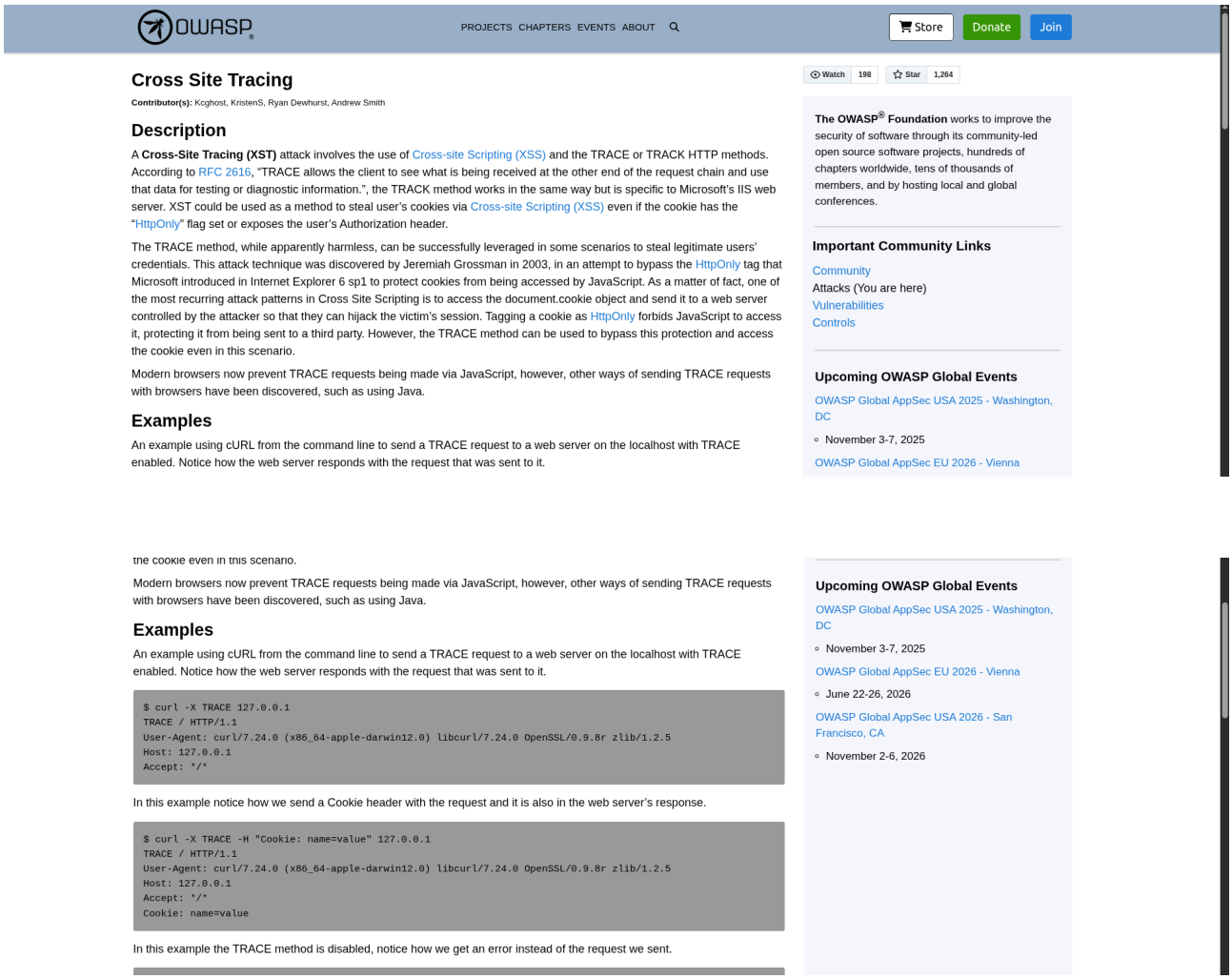

mdn_
HTML CSS JavaScript Web APIs All Learn Tools About Blog
Web > HTTP > Reference > Headers > X-Frame-Options
Theme English (US)
Filter
X-Forwarded-For
X-Forwarded-Host
X-Forwarded-Proto
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-Powered-By
X-Robots-Tag
X-XSS-Protection
HTTP request methods
HTTP response status codes
CSP directives
Permissions-Policy directives
HTTP resources and
Configuring Express
To set X-Frame-Options to SAMEORIGIN using Helmet add the following to your server configuration:
JS
Copy
import helmet from "helmet";
const app = express();
app.use(
helmet({
xFrameOptions: { action: "sameorigin" },
}),
);
Specifications
Specification
HTML
the-x-frame-options-header
In this article
Syntax
Examples
Specifications
Browser compatibility
See also


mdn
HTML
CSS
JavaScript
Web APIs
All
Learn
Tools
About
Blog
Web > HTTP > Reference > Headers > X-Frame-Options
Theme
English (US)
Filter
X-Forwarded-For
X-Forwarded-Host
X-Forwarded-Proto
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-Powered-By
X-Robots-Tag
X-XSS-Protection
HTTP request methods
HTTP response status codes
CSP directives
Permissions-Policy directives
the-x-frame-options-header
Browser compatibility
Report problems with this compatibility data • View data on GitHub
Chrome
Edge
Firefox
Opera
Safari
Chrome Android
Firefox for Android
Opera Android
Safari on iOS
Samsung Internet
WebView Android
WebView on iOS
X-Frame-Options
4 12 4 10.5 4 18 4 14 3.2 1 4.4 3.2
ALLOW-FROM
No 12–18 18–69 No No No 18 No No No No No
SAMEORIGIN
4 * 12 4 * 15 * 4 18 * 4 * 14 * 3.2 1 * 4.4 * 3.2
Tip: you can click/tap on a cell for more information.
Full support
No support
Non-standard. Check cross-browser support before using.
Deprecated. Not for use in new websites.
See implementation notes.
In this article
Syntax
Examples
Specifications
Browser compatibility
See also


Missing Content-Type Header
Severity: Low
Summary
Invicti detected a missing Content-Type header which means that this website could be at risk of a MIME-sniffing attacks.
Impact
MIME type sniffing is a standard functionality in browsers to find an appropriate way to render data where the HTTP headers sent by the server are either inconclusive or missing.
This allows web browsers such as Google Chrome to perform MIME-Sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the intended content type.
The problem arises once a website allows users to upload content which is then published on the web server. If an attacker can carry out XSS (Cross-site Scripting) attack by manipulating the content in a way to be accepted by the web application and rendered as HTML by the browser, it is possible to inject code in e.g. an image file and make the victim execute it by viewing the image.
Remediation
1. When serving resources, make sure you send the content-type header to appropriately match the type of the resource being
Vulnerability Index
You can search and find all vulnerabilities
Select Category
Critical
High
Medium
Low
Best Practice
Information


Summary
Invicti detected a missing Content-Type header which means that this website could be at risk of a MIME-sniffing attacks.
Impact
MIME type sniffing is a standard functionality in browsers to find an appropriate way to render data where the HTTP headers sent by the server are either inconclusive or missing.
This allows web browsers such as Google Chrome to perform MIME-Sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the intended content type.
The problem arises once a website allows users to upload content which is then published on the web server. If an attacker can carry out XSS (Cross-site Scripting) attack by manipulating the content in a way to be accepted by the web application and rendered as HTML by the browser, it is possible to inject code in e.g. an image file and make the victim execute it by viewing the image.
Remediation
1. When serving resources, make sure you send the content-type header to appropriately match the type of the resource being served. For example, if you are serving an HTML page, you should send the HTTP header:
Content-Type: text/html
2. Add the X-Content-Type-Options header with a value of "nosniff" to inform the browser to trust what the site has sent is the appropriate content-type, and to not attempt "sniffing" the real content-type.
Vulnerability Index
You can search and find all vulnerabilities
Select Category
Critical
High
Medium
Low
Best Practice
Information
OR
Search Vulnerability


WISEC.IT
The Wise SECurity
.italian
.english
Wisec Home
SecSearch
Projects
Papers
Security Thoughts
News
Flash Application Testing: A New Vector for XSS and Cross Site Flashing.
IE and Firefox Digest Authentication Request Splitting.
Php import_req_var globals overwrite Advisory.
Subverting Ajax - The Paper.
Adobe Plugin Multiple Vulnerabilities.
Wisec@23rd.CCC Congress in Berlin - 29th Dec. 2006 - Subverting Ajax.
SecSearch, Search Engine for Security Community.
Mysql COM_TABLE_DUMP Flaws.
Mysql Anonymous login Flaw.
A new project to stop embed passwords in Php scripts: PassBroker.
MySQL new three vulnerabilities unleashed
PHP shmop safemode bypass
Security Thoughts
[Back]
Wednesday, February 23, 2005, 20:15
Comments:
No comments yet.
Comments are disabled
Admin login | This weblog is from www.mylittlehomepage.net
Wisec is brought to you by...
Wisec is written and mantained by Stefano Di Paola.
Wisec uses open standards, including XHTML, CSS2, and XML-RPC.


OWASP
PROJECTS CHAPTERS EVENTS ABOUT
Store
Donate
Join
Cross Site Tracing
Contributor(s): Kcghost, KristenS, Ryan Dewhurst, Andrew Smith
Description
A Cross-Site Tracing (XST) attack involves the use of Cross-site Scripting (XSS) and the TRACE or TRACK HTTP methods. According to RFC 2616, "TRACE allows the client to see what is being received at the other end of the request chain and use that data for testing or diagnostic information.", the TRACK method works in the same way but is specific to Microsoft's IIS web server. XST could be used as a method to steal user's cookies via Cross-site Scripting (XSS) even if the cookie has the "HttpOnly" flag set or exposes the user's Authorization header.
The TRACE method, while apparently harmless, can be successfully leveraged in some scenarios to steal legitimate users' credentials. This attack technique was discovered by Jeremiah Grossman in 2003, in an attempt to bypass the HttpOnly tag that Microsoft introduced in Internet Explorer 6 sp1 to protect cookies from being accessed by JavaScript. As a matter of fact, one of the most recurring attack patterns in Cross Site Scripting is to access the document.cookie object and send it to a web server controlled by the attacker so that they can hijack the victim's session. Tagging a cookie as HttpOnly forbids JavaScript to access it, protecting it from being sent to a third party. However, the TRACE method can be used to bypass this protection and access the cookie even in this scenario.
Modern browsers now prevent TRACE requests being made via JavaScript, however, other ways of sending TRACE requests with browsers have been discovered, such as using Java.
Examples
An example using cURL from the command line to send a TRACE request to a web server on the localhost with TRACE enabled. Notice how the web server responds with the request that was sent to it.
Watch 198
Star 1,264
The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.
Important Community Links
Community
Attacks (You are here)
Vulnerabilities
Controls
Upcoming OWASP Global Events
OWASP Global AppSec USA 2025 - Washington, DC
November 3-7, 2025
OWASP Global AppSec EU 2026 - Vienna

the cookie even in this scenario.
Modern browsers now prevent TRACE requests being made via JavaScript, however, other ways of sending TRACE requests with browsers have been discovered, such as using Java.
Examples
An example using cURL from the command line to send a TRACE request to a web server on the localhost with TRACE enabled. Notice how the web server responds with the request that was sent to it.
$ curl -X TRACE 127.0.0.1
TRACE / HTTP/1.1
User-Agent: curl/7.24.0 (x86_64-apple-darwin12.0) libcurl/7.24.0 OpenSSL/0.9.8r zlib/1.2.5
Host: 127.0.0.1
Accept: */*
In this example notice how we send a Cookie header with the request and it is also in the web server's response.
$ curl -X TRACE -H "Cookie: name=value" 127.0.0.1
TRACE / HTTP/1.1
User-Agent: curl/7.24.0 (x86_64-apple-darwin12.0) libcurl/7.24.0 OpenSSL/0.9.8r zlib/1.2.5
Host: 127.0.0.1
Accept: */*
Cookie: name=value
In this example the TRACE method is disabled, notice how we get an error instead of the request we sent.
Upcoming OWASP Global Events
OWASP Global AppSec USA 2025 - Washington, DC
November 3-7, 2025
OWASP Global AppSec EU 2026 - Vienna
June 22-26, 2026
OWASP Global AppSec USA 2026 - San Francisco, CA
November 2-6, 2026

```
  var url = 'http://127.0.0.1/';

  xmlhttp.withCredentials = true; // send cookie header
  xmlhttp.open('TRACE', url, false);
  xmlhttp.send();
</script>
```

Remediation

Apache

In Apache versions 1.3.34, 2.0.55 and later, set the TraceEnable directive to "off" in the main configuration file and then restart Apache. See TraceEnable for further information.

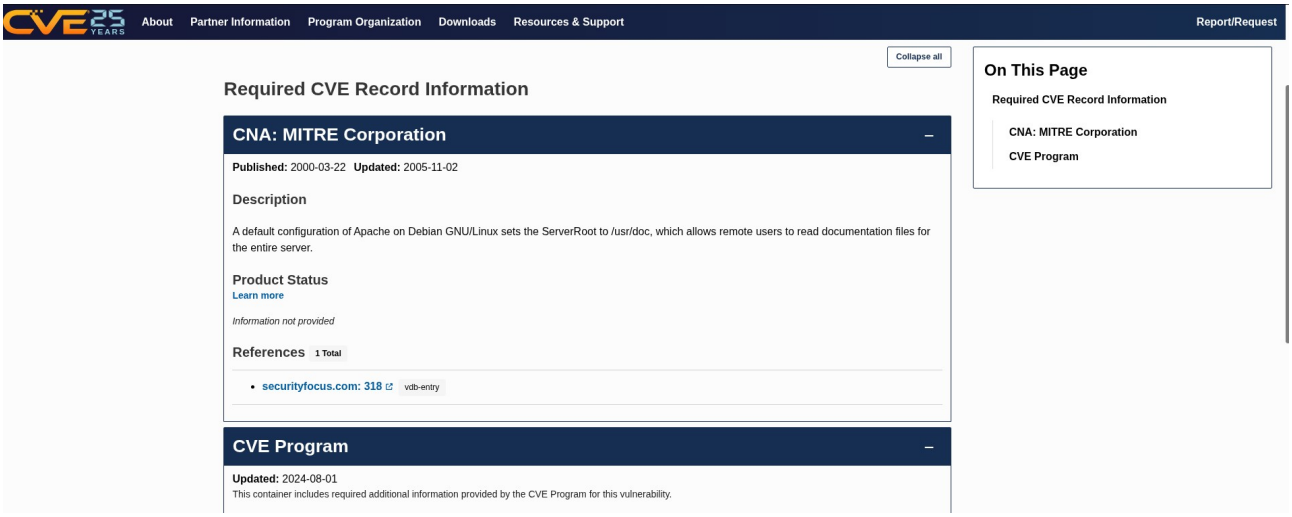
```
TraceEnable off
```

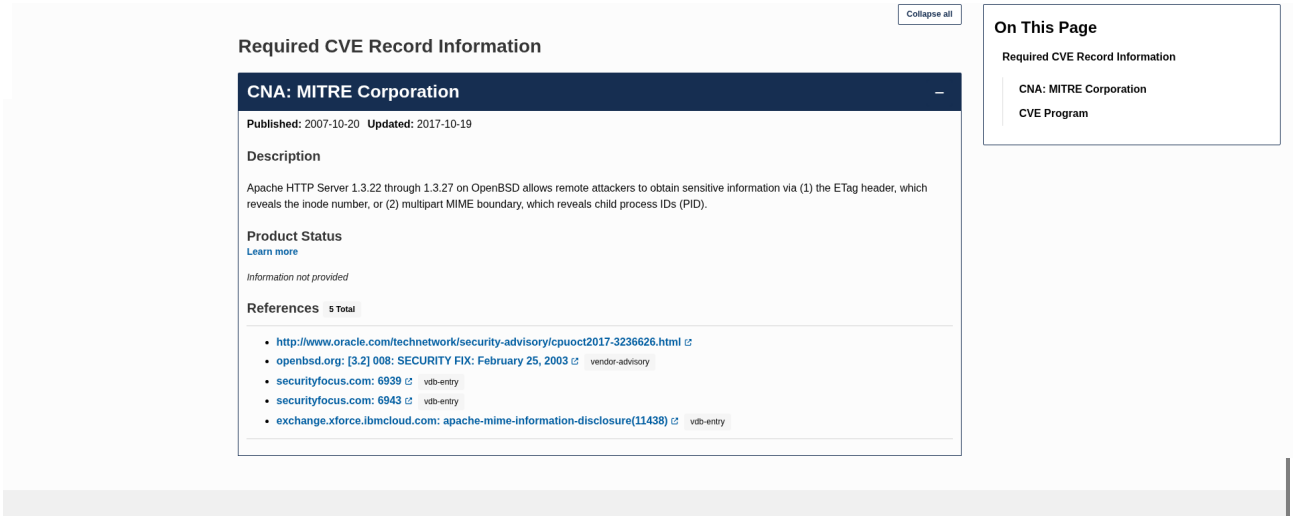
Related Attacks

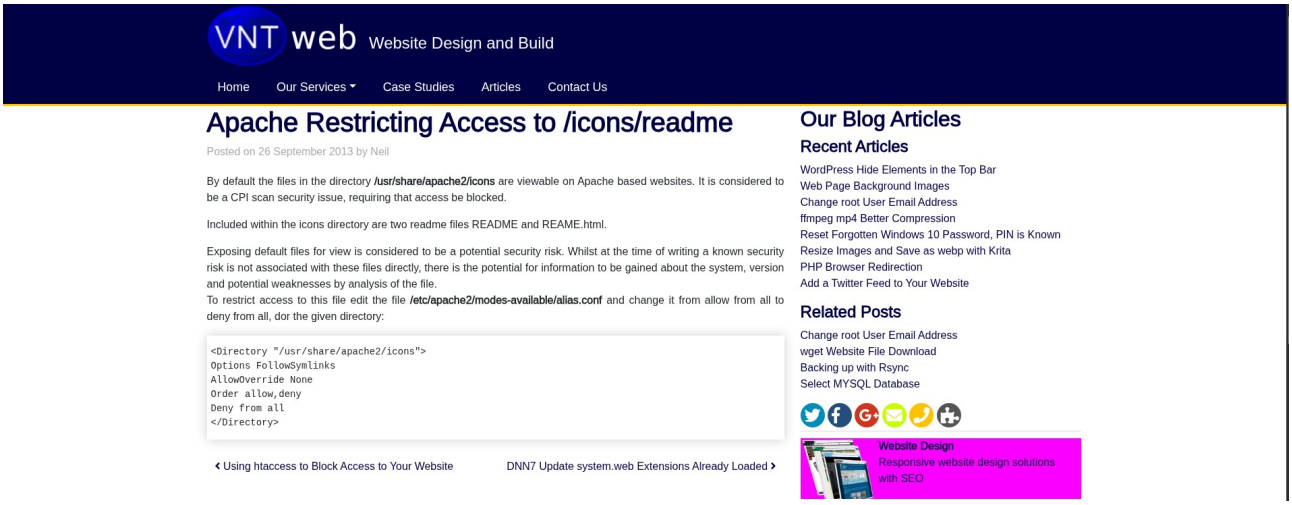
- Cross-site Scripting(XSS)

References

- Cross-Site Tracing (XST): http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
- Testing for HTTP Methods and XST (OWASP-CM-008)
- OSVDB 877
- CVE-2005-3398
- XSS: Gaining access to HttpOnly Cookie in 2012
- Mozilla Bug 302489
- Mozilla Bug 381264







2…..OWASP ZAP

Abrimos la terminal de Kali y ponemos **zaproxy**, para abrir la herramienta y nos da la opcion de guardar la sesion. En este caso, ponemos que no. Donde dice URL a atacar ponemos la direccion. (en este caso la IP de Metasploitable2) y presionamos atacar.

Vamos a explicar algunas cosas despues de un analisis. En el dashboard vamos a ver…….

Hay dos tipos principales de 'arañas' en ZAP:

Spider (Tradicional):

Esta es la araña original de ZAP. Funciona de manera similar a un rastreador de motores de búsqueda. Analiza el código HTML de las páginas web en busca de enlaces (`<a>` tags), formularios, y otros elementos para seguirlos. Es muy eficaz para sitios web tradicionales que dependen de la navegación basada en enlaces HTML estáticos.

Ajax Spider:

Este tipo de araña está diseñado específicamente para aplicaciones web modernas que utilizan mucho **JavaScript** y tecnologías como **AJAX** (Asynchronous JavaScript and XML). Las aplicaciones AJAX cargan contenido dinámicamente sin necesidad de recargar toda la página. La araña tradicional no puede "ver" este contenido. El Ajax Spider funciona de manera diferente: utiliza un navegador web real (como un navegador sin interfaz gráfica) para renderizar y ejecutar el JavaScript de la página. Al hacerlo, puede descubrir URLs y funcionalidades que solo se revelan después de que el código JavaScript se ha ejecutado, lo que lo hace indispensable para probar aplicaciones web modernas.

En la parte de **“Contextos” (Contexts)** es súper importante porque sirve para definir el alcance y las reglas de un análisis.

Un Contexto es como una carpeta de configuración donde agrupas un conjunto de URLs y parámetros de un sitio con ciertas políticas.

Cuando abres o configuras un contexto, puedes ver y ajustar:

URLs incluidas y excluidas

Definir qué parte del sitio pertenece al contexto (ejemplo: solo `http://testsite.com/app/` y no todo el dominio).

Usas expresiones regulares para incluir/excluir rutas.

Usuarios y Autenticación

Configurar credenciales, formularios de login, tokens de sesión, etc.

Te permite hacer pruebas como un usuario autenticado.

Roles o perfiles

Puedes guardar varios usuarios (por ejemplo, “admin” y “user normal”) para simular diferentes niveles de acceso.

Políticas de escaneo

Qué reglas aplicar (por ejemplo, inyecciones SQL, XSS, fuerza bruta, etc.).

Sesiones

Define cómo ZAP reconoce si la sesión sigue activa (cookies, cabeceras, tokens).

Opciones de protección

Límites de profundidad, tiempos, configuración de ataques, etc.

En pocas palabras:
El **Spider** te descubre nodos y URLs, pero el **Contexto** te deja decidir qué parte del sitio es relevante y cómo interactuar con él (usuarios, sesiones, políticas).

En la sección de **Alertas (Alerts)** es donde se muestran los resultados del análisis de seguridad que ha detectado la herramienta.

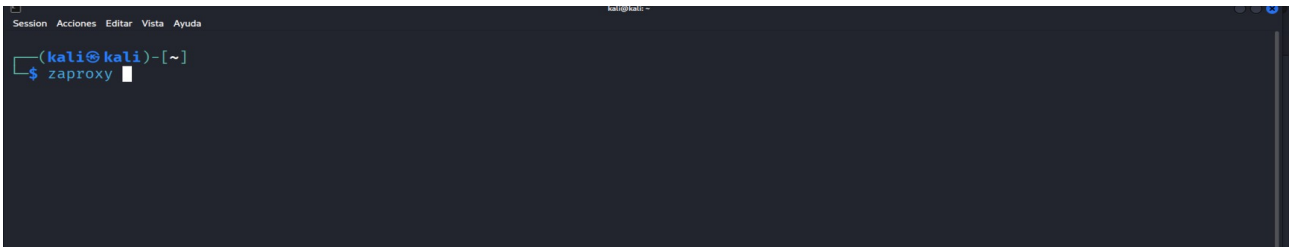
Cuando corres un escaneo (activo o pasivo), ZAP va generando alertas y ahí es donde puedes revisarlas.

Cada alerta tiene varios campos de información:

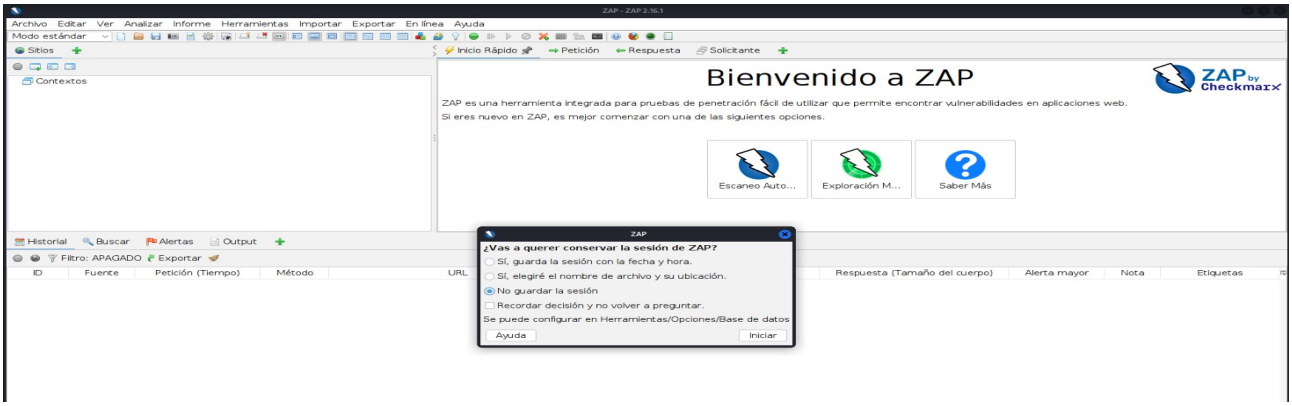
1. **Nivel de riesgo**
2. **High (Alto)** → Vulnerabilidad crítica (ej. SQL Injection).
3. **Medium (Medio)** → Riesgo importante (ej. XSS reflejado).
4. **Low (Bajo)** → Riesgo menor (ej. información sensible expuesta en headers).
5. **Informational (Info)** → No es un fallo, pero puede ser útil (ej. tecnologías detectadas).
6. **Nombre de la vulnerabilidad** Ejemplo: “Cross Site Scripting (Reflected)”.
7. **Descripción** Explica qué significa la vulnerabilidad.
8. **URL afectada** La dirección exacta donde se encontró el problema.
9. **Evidencia** Qué respuesta o comportamiento del servidor confirma la vulnerabilidad.
10. **Solución o recomendación** Consejos para mitigar o corregir el fallo.
11. **Referencia** Links a OWASP, CWE, CVE u otra documentación relevante.

En resumen:
La pestaña de **Alertas en ZAP** es el “informe en vivo” de todas las vulnerabilidades que ZAP detecta, con riesgo, ubicación, explicación y cómo arreglarlo.

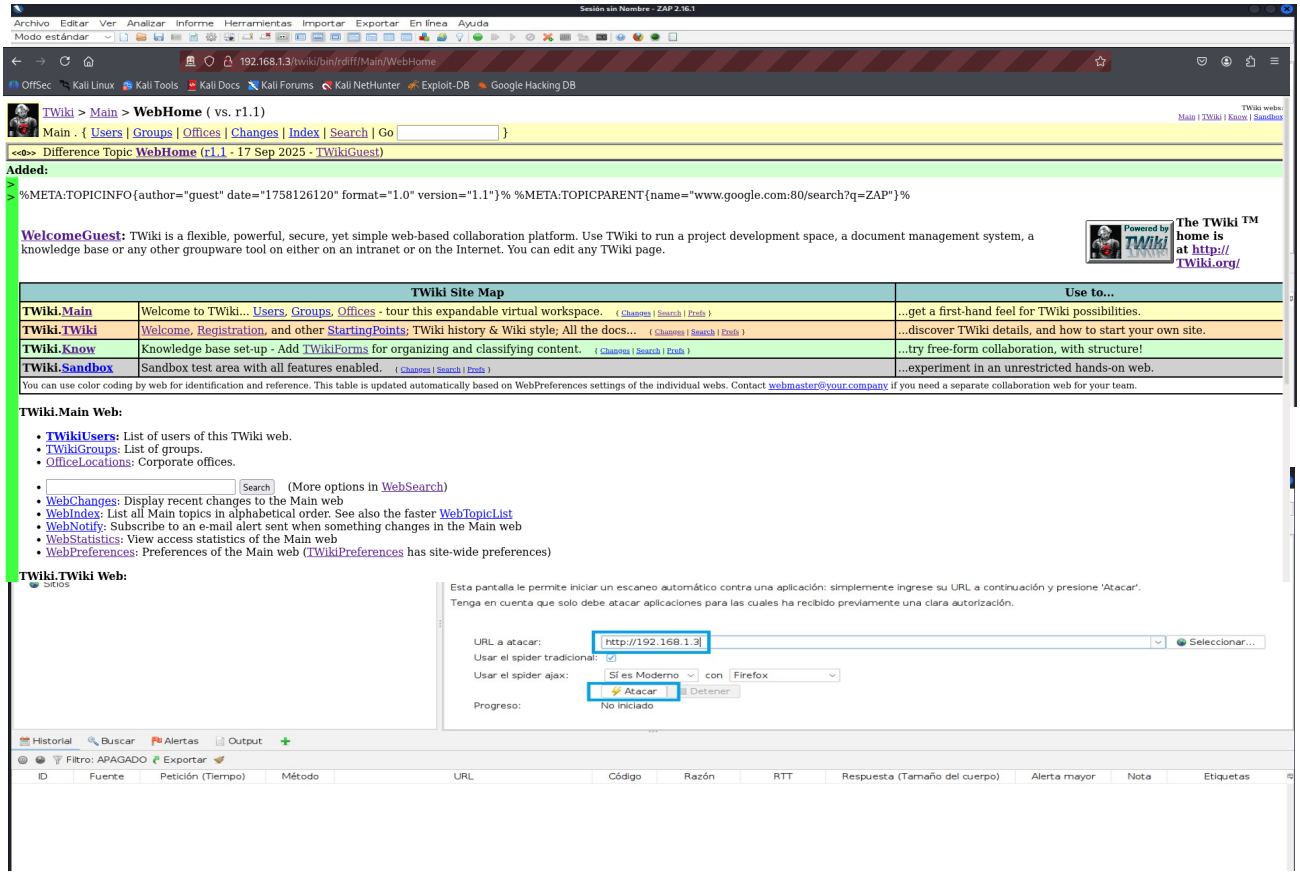
Vamos a verlo de forma grafica

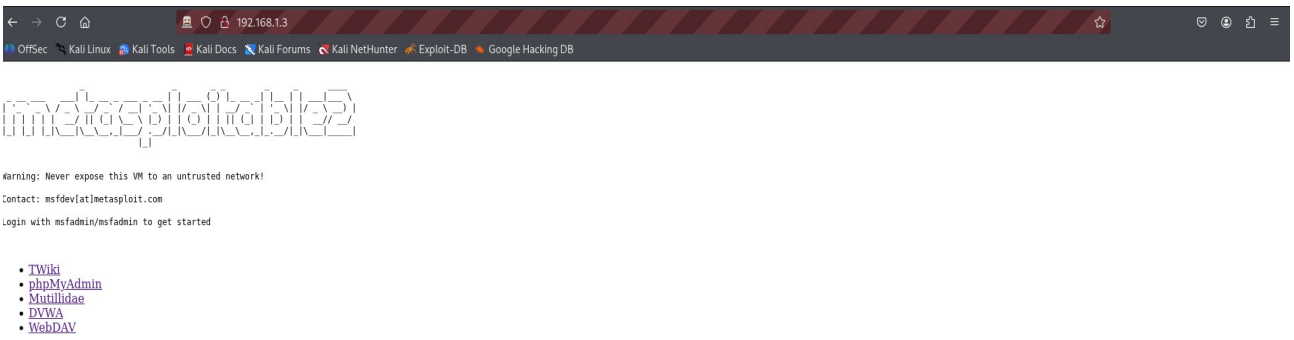


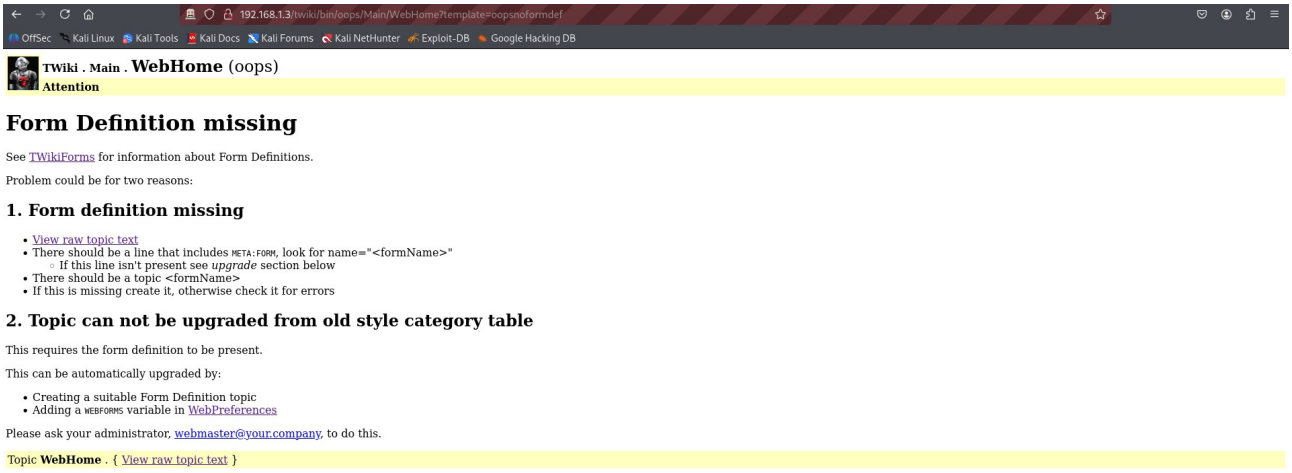
```
4375 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.control.ExtensionFactory - Loading extensions
5381 [ZAP-BootstrapGUI] INFO  org.zaproxy.addon.network.internal.TlsUtils - Using supported SSL/TLS protocols: [TLSv1.2, TLSv1.3]
5804 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.control.ExtensionFactory - Extensions loaded
6759 [ZAP-BootstrapGUI] INFO  org.flywaydb.core.internal.license.VersionPrinter - Flyway Community Edition 9.22.3 by Redgate
6769 [ZAP-BootstrapGUI] INFO  org.flywaydb.core.internal.license.VersionPrinter - See release notes here: https://rd.gt/416ObMi
6794 [ZAP-BootstrapGUI] INFO  org.flywaydb.core.internal.license.VersionPrinter -
6833 [ZAP-BootstrapGUI] INFO  org.flywaydb.core.Flyw                                  db:file:/home/kali/.ZAP/session/untitled1 (HSQL Da
tabase Engine 2.7)
6852 [ZAP-BootstrapGUI] WARN  org.flywaydb.core.inte                                  yway upgrade recommended: HSQLDB 2.7 is newer than
 this version of Flyway and support has not been tes                                 n of HSQLDB is 2.6.
6946 [ZAP-BootstrapGUI] INFO  org.flywaydb.core.inte                                  maHistory - Schema history table "PUBLIC"."AUTHHEL
PER_FLYWAY_SCHEMA_HISTORY" does not exist yet
6953 [ZAP-BootstrapGUI] INFO  org.flywaydb.core.inte                                  sfully validated 2 migrations (execution time 00:0
0.073s)
6979 [ZAP-BootstrapGUI] INFO  org.flywaydb.core.inte                                  maHistory - Creating Schema History table "PUBLIC"
."AUTHHELPER_FLYWAY_SCHEMA_HISTORY" with baseline ...
7086 [ZAP-BootstrapGUI] INFO  org.flywaydb.core.inte                                  sfully baselined schema with version: 0
7114 [ZAP-BootstrapGUI] INFO  org.flywaydb.core.inte                                   version of schema "PUBLIC": 0
7145 [ZAP-BootstrapGUI] INFO  org.flywaydb.core.inte                                  ng schema "PUBLIC" to version "1 - Create tables"
7187 [ZAP-BootstrapGUI] INFO  org.flywaydb.core.inte                                  ng schema "PUBLIC" to version "2 - Create storage
tables"
7203 [ZAP-BootstrapGUI] INFO  org.flywaydb.core.inte                                  fully applied 2 migrations to schema "PUBLIC", now
 at version v2 (execution time 00:00.025s)
9208 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Extensión de actualización automática - Pe
rmitir a ZAP comprobar si existen actualizaciones
9313 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Opciones de extensión - Opciones de extens
ión
```

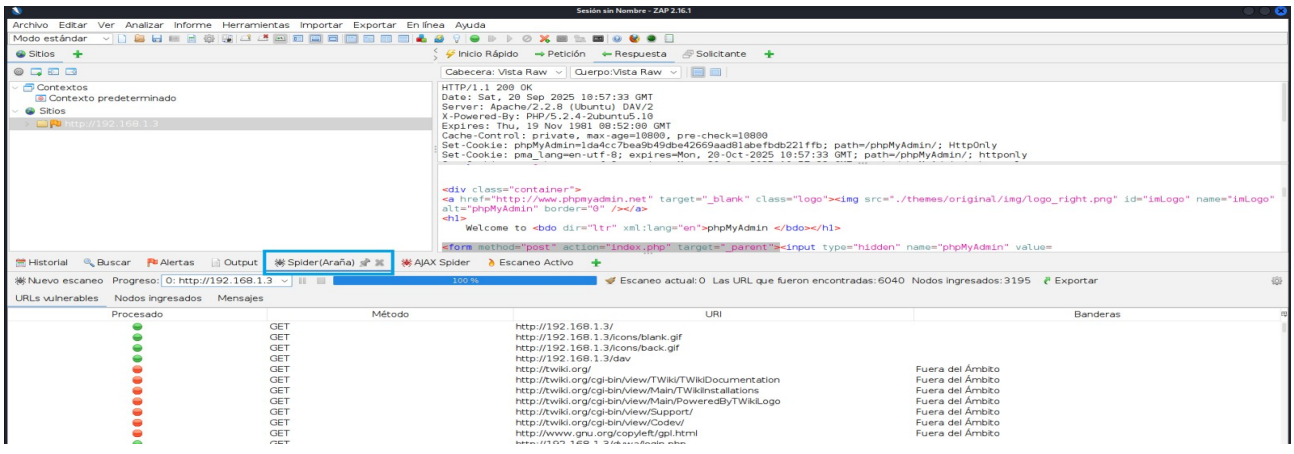


l



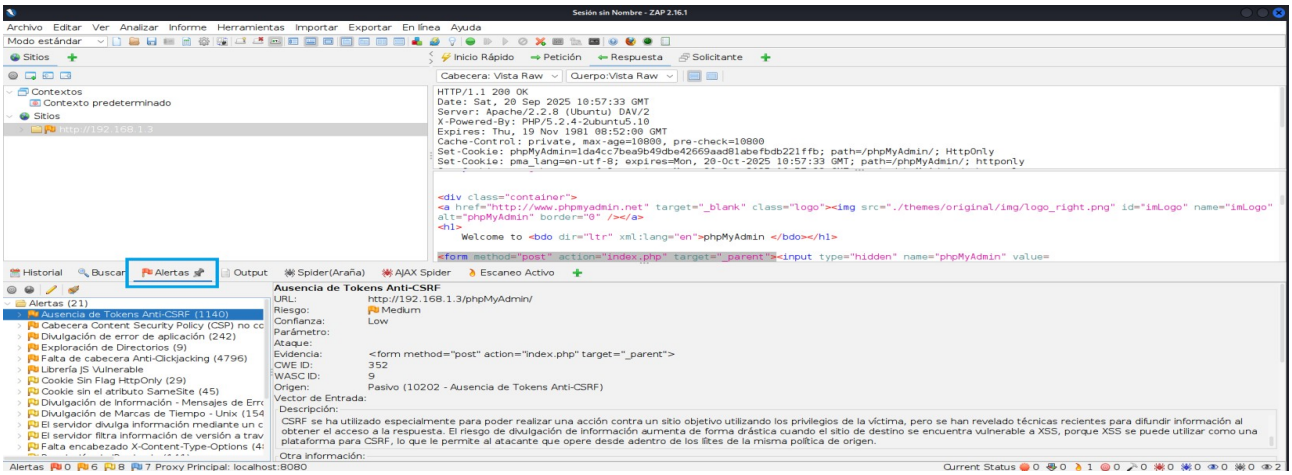

192.168.1.3
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
TWiki
phpMyAdmin
Mutillidae
DVWA
WebDAV

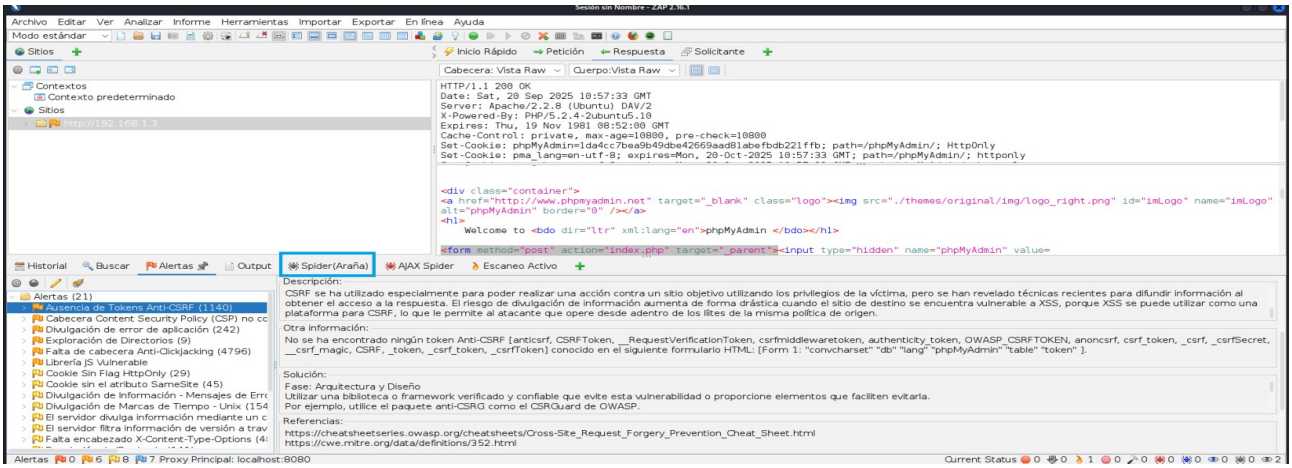

192.168.1.3/twiki/bin/oops/Main/WebHome?template=oopsnoformdef
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
TWiki . Main . WebHome (oops)
Attention
Form Definition missing
See TWikiForms for information about Form Definitions.
Problem could be for two reasons:
1. Form definition missing
View raw topic text
There should be a line that includes META:FORM, look for name="<formName>"
If this line isn't present see upgrade section below
There should be a topic <formName>
If this is missing create it, otherwise check it for errors
2. Topic can not be upgraded from old style category table
This requires the form definition to be present.
This can be automatically upgraded by:
Creating a suitable Form Definition topic
Adding a WEBFORMS variable in WebPreferences
Please ask your administrator, webmaster@your.company, to do this.
Topic WebHome . { View raw topic text }

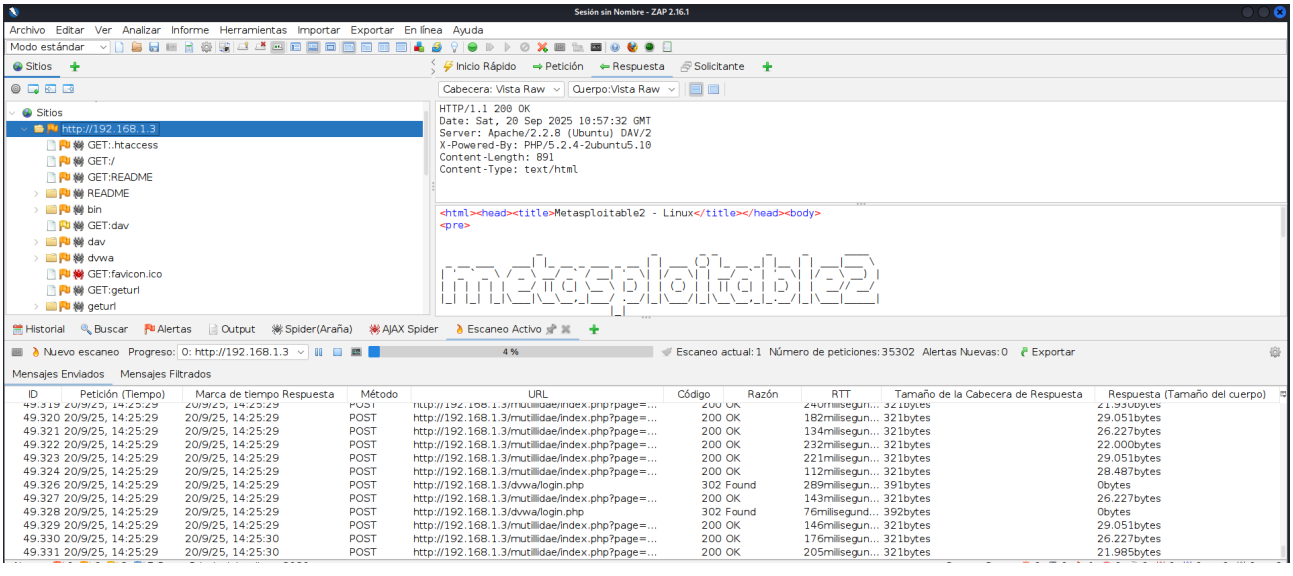

Sesión sin Nombre - ZAP 2.16.1
Archivo Editar Ver Analizar Informe Herramientas Importar Exportar En línea Ayuda
Modo estándar
Sitios
Inicio Rápido Petición Respuesta Solicitante
Cabecera: Vista Raw Cuerpo:Vista Raw
Contextos
Contexto predeterminado
Sitios
http://192.168.1.3
HTTP/1.1 200 OK
Date: Sat, 20 Sep 2025 10:57:33 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private, max-age=10800, pre-check=10800
Set-Cookie: phpMyAdmin=1da4cc7bea9b49dbe42669aad81abefbdb221ffb; path=/phpMyAdmin/; HttpOnly
Set-Cookie: pma_lang=en-utf-8; expires=Mon, 20-Oct-2025 10:57:33 GMT; path=/phpMyAdmin/; httponly

<h1>
Welcome to <bdo dir="ltr" xml:lang="en">phpMyAdmin </bdo></h1>
<form method="post" action="index.php" target="_parent"><input type="hidden" name="phpMyAdmin" value=
Historial Buscar Alertas Output Spider(Araña) AJAX Spider Escaneo Activo
Nuevo escaneo Progreso: 0: http://192.168.1.3 100 % Escaneo actual: 0 Las URL que fueron encontradas: 6040 Nodos ingresados: 3195 Exportar
URLs vulnerables Nodos ingresados Mensajes
Procesado Método URI Banderas
GET http://192.168.1.3/
GET http://192.168.1.3/icons/blank.gif
GET http://192.168.1.3/icons/back.gif
GET http://192.168.1.3/dav
GET http://twiki.org/ Fuera del Ámbito
GET http://twiki.org/cgi-bin/view/TWiki/TWikiDocumentation Fuera del Ámbito
GET http://twiki.org/cgi-bin/view/Main/TWikiInstallations Fuera del Ámbito
GET http://twiki.org/cgi-bin/view/Main/PoweredByTWikiLogo Fuera del Ámbito
GET http://twiki.org/cgi-bin/view/Support/ Fuera del Ámbito
GET http://twiki.org/cgi-bin/view/Codev/ Fuera del Ámbito
GET http://www.gnu.org/copyleft/gpl.html Fuera del Ámbito

+


Sesión sin Nombre - ZAP 2.16.1
Ausencia de Tokens Anti-CSRF
URL: http://192.168.1.3/phpMyAdmin/
Riesgo: Medium
Confianza: Low
CWE ID: 352
WASC ID: 9
Origen: Pasivo (10202 - Ausencia de Tokens Anti-CSRF)


Sesión sin Nombre - ZAP 2.16.1
Spider(Araña)
Ausencia de Tokens Anti-CSRF
URL: http://192.168.1.3/phpMyAdmin/
Riesgo: Medium
Confianza: Low
CWE ID: 352
WASC ID: 9
Origen: Pasivo (10202 - Ausencia de Tokens Anti-CSRF)


Sesión sin Nombre - ZAP 2.16.1
http://192.168.1.3
GET:.htaccess
GET:/
GET:README
dvwa
GET:favicon.ico
GET:geturl
Escaneo Activo
Mensajes Enviados
Mensajes Filtrados