

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.

```
(kali㉿kali)-[~]
$ nikto -h 192.168.1.3
- Nikto v2.5.0

+ Target IP:      192.168.1.3
+ Target Hostname: 192.168.1.3
+ Target Port:    80
+ Start Time:    2025-09-18 08:32:31 (GMT2)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Fram
e-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fas
hion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alt
ernatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/
vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_
```

```
Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain spec
ific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain spec
ific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain spec
ific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain spec
ific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mti
me: Tue Dec  9 18:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-55
```

The screenshot shows the MDN Web Docs page for the `X-Frame-Options` header. On the left, there's a sidebar with a tree view of HTTP headers. The `X-Frame-Options` node is selected. The main content area has a dark background with white text. It includes a note about the `Content-Security-Policy` header, a table comparing Header type and Response header, and a Syntax section. To the right, there's an "In this article" sidebar with links to Syntax, Examples, Specifications, and Browser compatibility. At the bottom, a dark panel displays a security audit log with various findings like Apache default files, MySQL databases, and wp-config.php.

```
+ /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
```

This screenshot shows the same MDN Web Docs page for the `X-Frame-Options` header. The sidebar and main content structure are identical to the first screenshot. The main content area now focuses on the "Syntax" section, which contains examples for both `HTTP` and `HTTP resources and frames`. The "Directives" section below it provides explanations for `DENY` and `SAMEORIGIN`.

```
HTTP
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN
```

The screenshot shows the MDN Web Docs interface. The top navigation bar includes links for HTML, CSS, JavaScript, Web APIs, All, Learn, Tools, About, and Blog. A search bar is on the right. The main content area has a breadcrumb trail: Web > HTTP > Reference > Headers > X-Frame-Options. On the left is a sidebar with a 'Filter' button and a tree view of other header types like X-Forwarded-For, X-Forwarded-Host, X-Forwarded-Proto, and X-Permitted-Cross-Domain-Policies. The 'X-Frame-Options' node is selected and highlighted in blue. The main content area starts with a heading 'page.' followed by the 'ALLOW-FROM origin' directive. It explains that this is an obsolete directive and recommends using the Content-Security-Policy header instead. Below this is a section titled 'Examples' containing a warning about setting it in a meta tag. The 'Configuring Apache' section follows, with configuration code shown in a code editor window.

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

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
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
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
header {
    set $xfo "SAMEORIGIN";
}
```

In this article

- Syntax
- Examples**
- Specifications
- Browser compatibility
- See also

The screenshot shows the MDN Web Docs interface for the 'X-Frame-Options' page. The left sidebar has a tree view of HTTP-related topics, with 'X-Frame-Options' selected. The main content area is titled 'Configuring Express' and contains code examples for setting up an Express server to use 'SAMEORIGIN' for X-Frame-Options. A 'Copy' button is available for the code. The right sidebar features a 'In this article' section with tabs for Syntax, Examples (which is selected), Specifications, and Browser compatibility. Below these are 'See also' links.

Configuring Express

To set `X-Frame-Options` to `SAMEORIGIN` using [Helmet](#) add the following to your server configuration:

```
JS
import helmet from "helmet";

const app = express();
app.use(
  helmet({
    xframeOptions: { action: "sameorigin" },
  }),
);
```

Specifications

Specification
HTML <code># the-x-frame-options-header</code>

Mdn_

HTML ▾ CSS ▾ JavaScript ▾ Web APIs ▾ All ▾ Learn ▾ Tools ▾ About ▾ Blog

Web > HTTP > Reference > Headers > X-Frame-Options

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 on 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 69	No 18 69	No No	No No	No No	No 18	No No	No No	No No	No 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

- 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
```

- 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

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

- 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
```

- 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

[News](#)
Flash Application Testing:
A New Vector for XSS and Cross Site Flashing.
IE and Firefox Digest Authentication Request System:
PHP import .req var
globals override Advisory:
Subverting Ajax - The Paper.
Adobe Plugin Multiple Vulnerabilities.
Wisec@23rd.CCC Congress in Berlin - 29th Dec. 2006 - Subverting Ajax.
SeeSearch, Search Engine for Security Community.
Mysql COM_TABLE_DUMP Flaws.
Mysql Anonymous login Flaw.
A new project to stop embeded records in PHP scripts - Passifier.
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 maintained by [Stefano Di Paola](#).

Wisec uses open standards, including XHTML, CSS2, and XML-RPC.



PROJECTS CHAPTERS EVENTS ABOUT

[Store](#)

[Donate](#)

[Join](#)

[Watch](#) 198 [Star](#) 1,264

Cross Site Tracing

Contributor(s): Koghost, 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.

```
$ 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: */*
Cookie: name=value
```

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.

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](#)

- June 22-26, 2026

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

```

<script>
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



About

Partner Information

Program Organization

Downloads

Resources & Support

Report/Request

[Collapse all](#)

Required CVE Record Information

CNA: MITRE Corporation

Published: 2000-03-22 Updated: 2005-11-02

Description

A default configuration of Apache on Debian GNU/Linux sets the ServerRoot to /usr/doc, which allows remote users to read documentation files for the entire server.

Product Status

[Learn more](#)

Information not provided

References 1 Total

- [securityfocus.com: 318](#) vdb-entry

On This Page

Required CVE Record Information

CNA: MITRE Corporation

CVE Program

[Collapse all](#)

Required CVE Record Information

CNA: MITRE Corporation

Published: 2007-10-20 Updated: 2017-10-19

Description

Apache HTTP Server 1.3.22 through 1.3.27 on OpenBSD allows remote attackers to obtain sensitive information via (1) the ETag header, which reveals the inode number, or (2) multipart MIME boundary, which reveals child process IDs (PID).

Product Status

[Learn more](#)

Information not provided

References 5 Total

- <http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html> vdb-entry
- [openbsd.org: \[3.2\] 008: SECURITY FIX: February 25, 2003](https://openbsd.org/3.2/008) vendor-advisory
- [securityfocus.com: 6939](#) vdb-entry
- [securityfocus.com: 6943](#) vdb-entry
- [exchange.xforce.ibmcloud.com: apache-mime-information-disclosure\(11438\)](#) vdb-entry

On This Page

Required CVE Record Information

CNA: MITRE Corporation

CVE Program

VNT web Website Design and Build

Home Our Services Case Studies Articles Contact Us

Apache Restricting Access to /icons/readme

Posted on 26 September 2013 by Neil

By default the files in the directory `/usr/share/apache2/icons` are viewable on Apache based websites. It is considered to be a CPI scan security issue, requiring that access be blocked.

Included within the icons directory are two readme files README and README.html.

Exposing default files for view is considered to be a potential security risk. Whilst at the time of writing a known security risk is not associated with these files directly, there is the potential for information to be gained about the system, version and potential weaknesses by analysis of the file.

To restrict access to this file edit the file `/etc/apache2/modes-available/alias.conf` and change it from allow from all to deny from all, for the given directory:

```
<Directory "/usr/share/apache2/icons">
Options FollowSymlinks
AllowOverride None
Order allow,deny
Deny from all
</Directory>
```

[◀ Using htaccess to Block Access to Your Website](#) [DNN7 Update system.web Extensions Already Loaded ▶](#)

Our Blog Articles

Recent Articles

- [WordPress Hide Elements in the Top Bar](#)
- [Web Page Background Images](#)
- [Change root User Email Address](#)
- [ffmpeg mp4 Better Compression](#)
- [Reset Forgotten Windows 10 Password, PIN is Known](#)
- [Resize Images and Save as webp with Krta](#)
- [PHP Browser Redirection](#)
- [Add a Twitter Feed to Your Website](#)

Related Posts

- [Change root User Email Address](#)
- [wget Website File Download](#)
- [Backing up with Rsync](#)
- [Select MySQL Database](#)

Website Design
Responsive website design solutions with SEO

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.

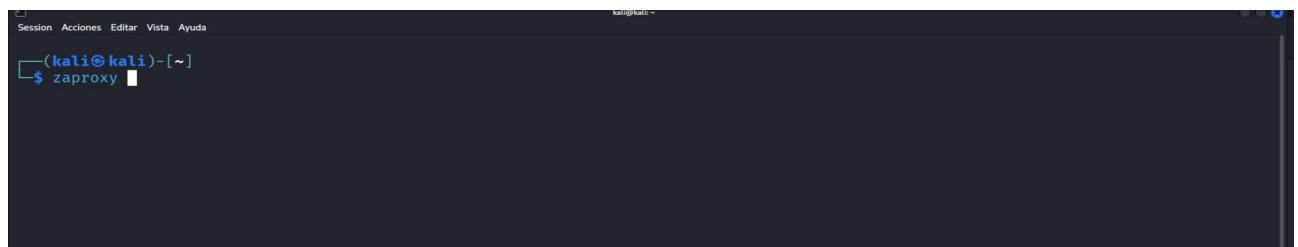
Cada alerta tiene varios campos de información:

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

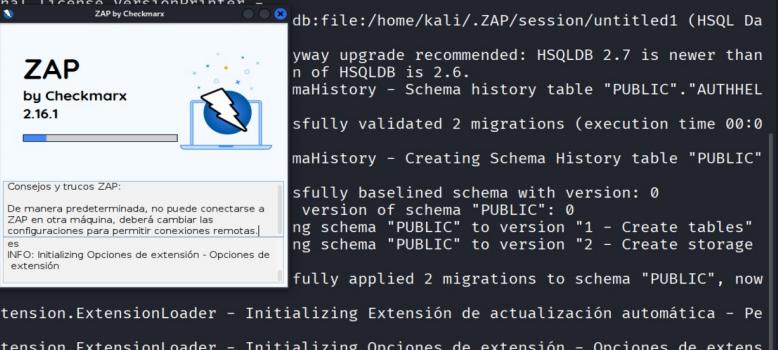


The screenshot shows a terminal window within the ZAP application. The window title is '(kali㉿kali)-[~]'. The command '\$ zaproxy' has been entered and is visible at the bottom of the terminal. The rest of the screen is mostly blank, indicating that no alerts have been generated yet.

```

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/4160bMi
6794 [ZAP-BootstrapGUI] INFO org.flywaydb.core.internal.license.VersionPrinter -
6833 [ZAP-BootstrapGUI] INFO org.flywaydb.core.Flywa db:file:/home/kali/.ZAP/session/untitled1 (HSQL Database Engine 2.7)
6852 [ZAP-BootstrapGUI] WARN org.flywaydb.core.inte this version of Flyway and support has not been test
6946 [ZAP-BootstrapGUI] INFO org.flywaydb.core.inte PER_FLYWAY_SCHEMA_HISTORY" does not exist yet
6953 [ZAP-BootstrapGUI] INFO org.flywaydb.core.inte 0.073s)
6979 [ZAP-BootstrapGUI] INFO org.flywaydb.core.inte .AUTHHELPER_FLYWAY_SCHEMA_HISTORY" with baseline ...
7086 [ZAP-BootstrapGUI] INFO org.flywaydb.core.inte
7114 [ZAP-BootstrapGUI] INFO org.flywaydb.core.inte
7145 [ZAP-BootstrapGUI] INFO org.flywaydb.core.inte
7187 [ZAP-BootstrapGUI] INFO org.flywaydb.core.inte
7203 [ZAP-BootstrapGUI] INFO org.flywaydb.core.inte 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 extensión

```



1

Warning: Never expose this VM to an untrusted network!
Contact: msfdev@metasploit.com
Login with msfadmin/msfadmin to get started



Warning: Never expose this VM to an untrusted network!

Contact: msfdev@metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutilidae](#)
- [DVWA](#)
- [WebDAV](#)

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 `WEBSITES` variable in [WebPreferences](#)

Please ask your administrator, webmaster@your.company, to do this.

Topic [WebHome](#) . { [View raw topic text](#) }

Sesión sin Nombre - ZAP 2.16.0

Archivo Editar Ver Analizar Informe Herramientas Importar En línea Ayuda

Modo estándar ▾

Sitios +

Contextos

Contexto predeterminado

Sitios

http://192.168.1.3

Cabecera: Vista Raw | Cuerpo: Vista Raw |

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/8.1.12

Content-Type: text/html; charset=UTF-8

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: private

Age: 10800

Set-Cookie: pma_lang=en-utf-8; expires=Mon, 29-Oct-2925 10:57:33 GMT; path=/phpMyAdmin/; HttpOnly

Set-Cookie: pma_lang=en-utf-8; expires=Mon, 29-Oct-2925 10:57:33 GMT; path=/phpMyAdmin/; httponly

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) 36 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/	Fuera del Ámbito
●	GET	http://192.168.1.3/icons/blank.gif	Fuera del Ámbito
●	GET	http://192.168.1.3/icons/back.gif	Fuera del Ámbito
●	GET	http://192.168.1.3/dav	Fuera del Ámbito
●	GET	http://192.168.1.3/favicon.ico	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/Main/Support	Fuera del Ámbito
●	GET	http://twiki.org/cgi-bin/view/CodeView	Fuera del Ámbito
●	GET	http://www.gnu.org/copyleft/gpl.html	Fuera del Ámbito
●	GET	http://192.168.1.3/index.php	Fuera del Ámbito

The screenshot shows the ZAP interface with the following details:

- Sessions:** Shows Contextos (Contexts) and Sitios (Sites). A context named "http://192.168.1.3" is selected.
- Alerts (21):** A single alert is listed: "Ausencia de Tokens Anti-CSRF (1140)".
- Spider (Araña):** Shows the URL <http://192.168.1.3/phpMyAdmin/>.
- Ajax Spider:**
- Escaneo Activo (Active Scan):** Shows the following exploit code injected into the page source:

```
<div class="container">
<a href="http://www.phpmyadmin.net" target="_blank" class="logo"></a>
<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="
```
- HTTP Response Headers:**

```
HTTP/1.1 200 OK
Date: Sat, 28 Sep 2015 10:57:33 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1991 08:52:00 GMT
Cache-Control: private, max-age=10800
Set-Cookie: phpmayadmin=id4cc5beab9d5de4269aa981abe8db221ff9; path=/phpMyAdmin/; HttpOnly
Set-Cookie: pma_lang=en; expires=Mon, 28-Oct-2025 10:57:33 GMT; path=/phpMyAdmin/; httpOnly
```

The screenshot shows the ZAP interface with the following details:

- Header:** Cabecera: Vista Raw
- Body:** HTTP/1.1 200 OK Date: Sat, 29 Sep 2025 10:57:33 GMT Server: Apache/2.4.41 (Ubuntu) DAV/2 X-Powered-By: PHP/8.2.4-ubuntu0.24.0 Expires: Thu, 19 Nov 1991 08:52:00 GMT Cache-Control: private, max-age=10800, pre-check=10800 Set-Cookie: phpMyAdmin=id4cc7bea9b49cbe42659a8d9fbdb21ff: path=/phpMyAdmin/: HttpOnly Set-Cookie: pma_lang=en-utf-8; expires=Mon, 29-Oct-2025 10:57:33 GMT; path=/phpMyAdmin/; httpOnly
- Content:** Welcome to <bdo dir="ltr" xml:lang="en">phpMyAdmin </bdo>
- Form:** <form method="post" action="index.php" target="parent"><input type="hidden" name="phpMyAdmin" value="imLogo" />
- Tool Buttons:** Spider(Araña), AJAX Spider, Escaneo Activo

Sesión sin Nombre - ZAP 2.16.1

Archivo Editar Ver Analizar Informe Herramientas Importar Exportar En línea Ayuda

Sitios + Inicio Rápido Petición Respuesta Solicitante

Cabecera: Vista Raw | Cuerpo: Vista Raw

HTTP/1.1 200 OK
Date: Sat, 20 Sep 2025 10:57:32 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>

Historial Buscar Alertas Output Spider(Araña) AJAX Spider Escaneo Activo Exportar

Nuevo escaneo Progreso: 0: http://192.168.1.3 4 % Escaneo actual: 1 Número de peticiones: 35302 Alertas Nuevas: 0 Exportar

ID	Petición (Tiempo)	Marca de tiempo	Respuesta	Método	URL	Código	Razón	RTT	Tamaño de la Cabecera de Respuesta	Respuesta (Tamaño del cuerpo)
49.319	20/9/25, 14:25:29	20/9/25, 14:25:29		PUT	http://192.168.1.3/mutillidae/index.php?page=...	200	OK	4ms	31 bytes	21.05bytes
49.320	20/9/25, 14:25:29	20/9/25, 14:25:29		POST	http://192.168.1.3/mutillidae/index.php?page=...	200	OK	182ms	321bytes	29.05bytes
49.321	20/9/25, 14:25:29	20/9/25, 14:25:29		POST	http://192.168.1.3/mutillidae/index.php?page=...	200	OK	134ms	321bytes	26.227bytes
49.322	20/9/25, 14:25:29	20/9/25, 14:25:29		POST	http://192.168.1.3/mutillidae/index.php?page=...	200	OK	232ms	321bytes	22.00bytes
49.323	20/9/25, 14:25:29	20/9/25, 14:25:29		POST	http://192.168.1.3/mutillidae/index.php?page=...	200	OK	221ms	321bytes	29.05bytes
49.324	20/9/25, 14:25:29	20/9/25, 14:25:29		POST	http://192.168.1.3/mutillidae/index.php?page=...	200	OK	112ms	321bytes	28.487bytes
49.326	20/9/25, 14:25:29	20/9/25, 14:25:29		POST	http://192.168.1.3/dvwa/login.php	302	Found	289ms	391bytes	0bytes
49.327	20/9/25, 14:25:29	20/9/25, 14:25:29		POST	http://192.168.1.3/mutillidae/index.php?page=...	200	OK	143ms	321bytes	26.227bytes
49.328	20/9/25, 14:25:29	20/9/25, 14:25:29		POST	http://192.168.1.3/dvwa/login.php	302	Found	76ms	392bytes	0bytes
49.329	20/9/25, 14:25:29	20/9/25, 14:25:29		POST	http://192.168.1.3/mutillidae/index.php?page=...	200	OK	146ms	321bytes	29.05bytes
49.330	20/9/25, 14:25:29	20/9/25, 14:25:30		POST	http://192.168.1.3/mutillidae/index.php?page=...	200	OK	176ms	321bytes	26.227bytes
49.331	20/9/25, 14:25:29	20/9/25, 14:25:30		POST	http://192.168.1.3/mutillidae/index.php?page=...	200	OK	205ms	321bytes	21.98bytes