Martin Dalla Pozza

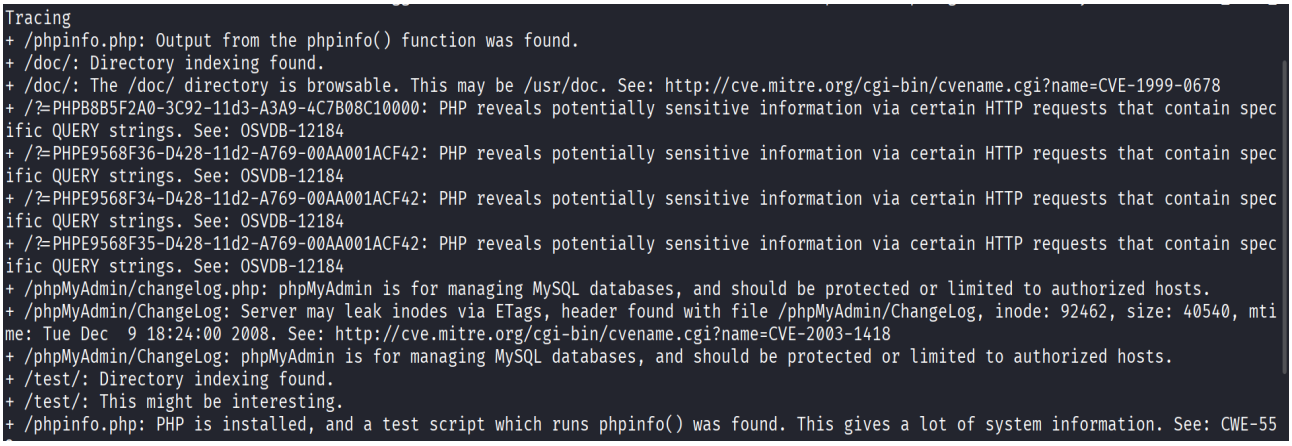
Trabajo Practico

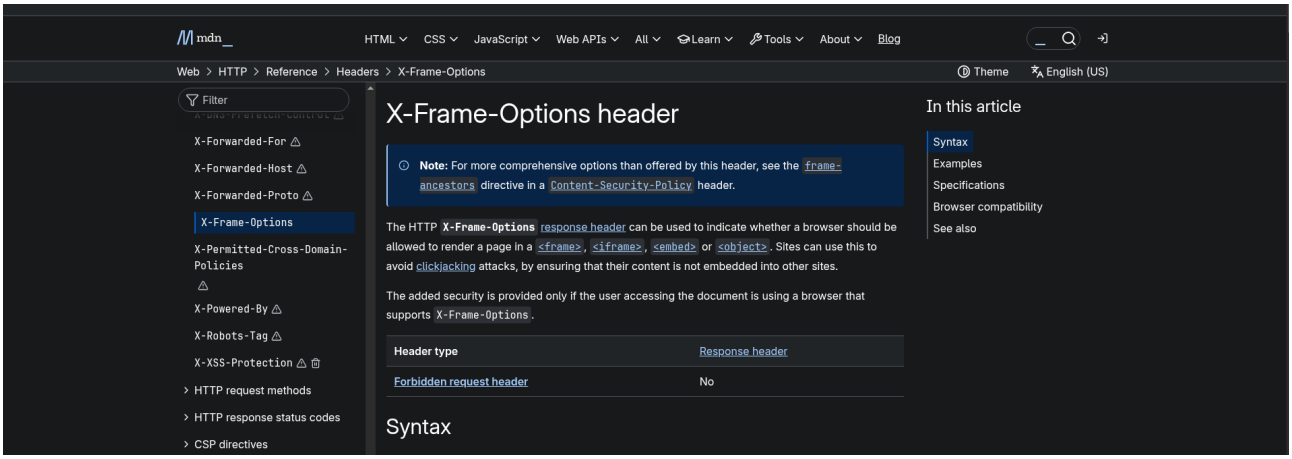
Analisis de vulnerabilidades

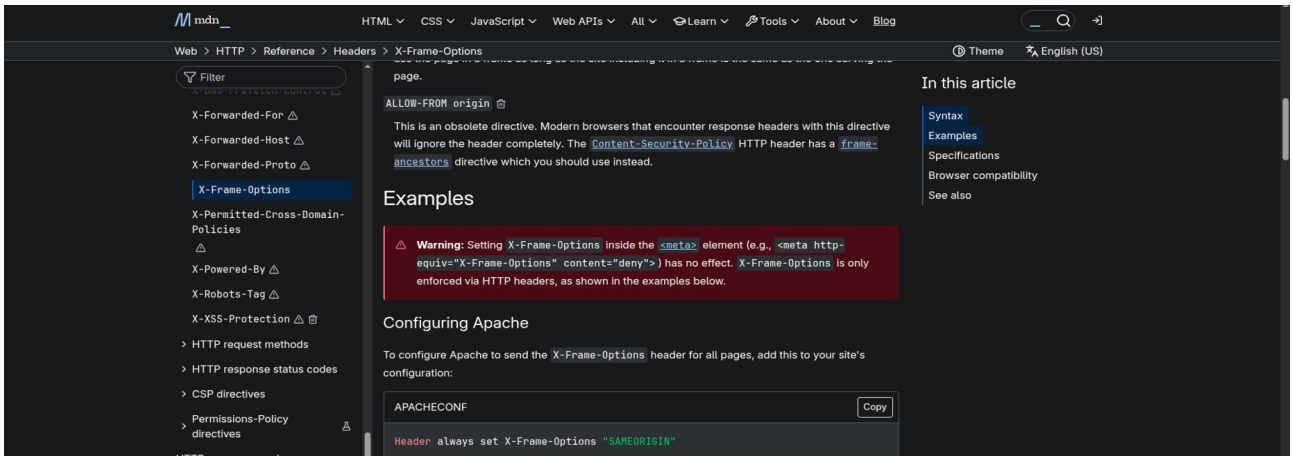
1…..Nikto
2…..OWASP ZAP

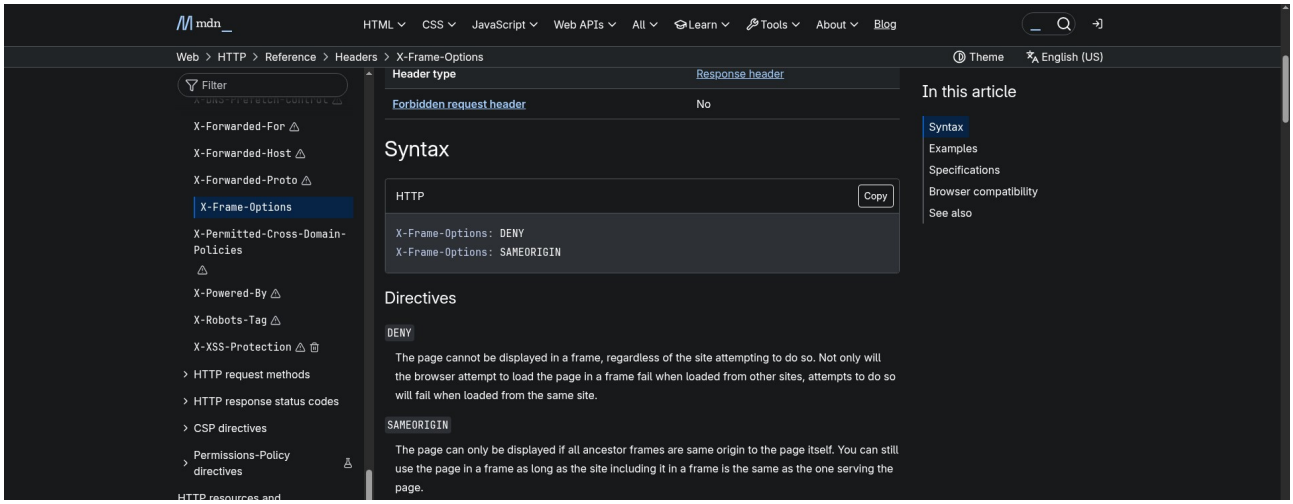
1…..Nikto

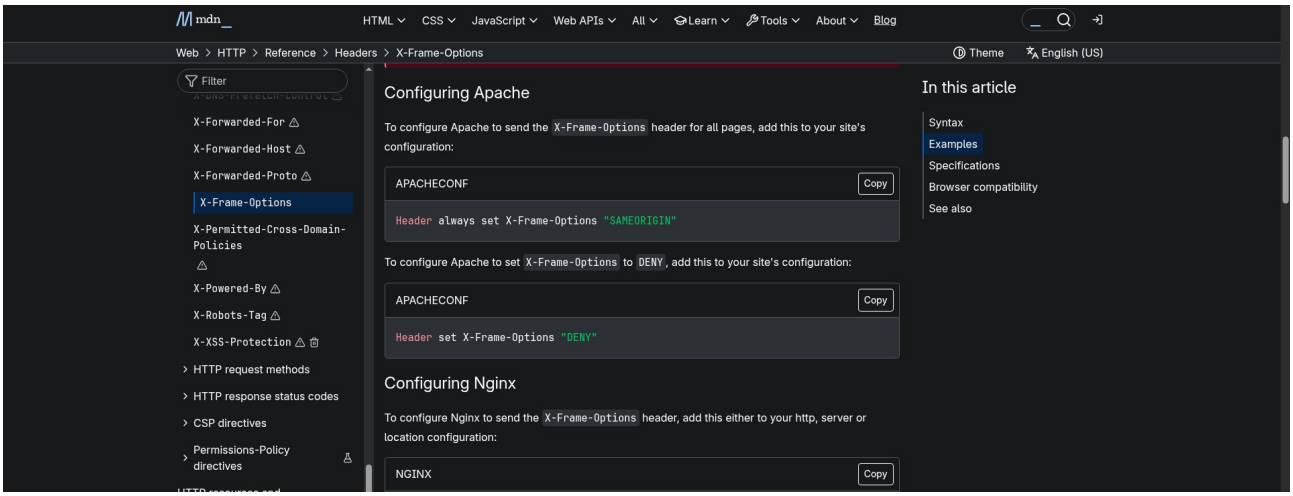
Abrimos la terminal de Kali y ponemos **nikto -h 192.168.1.3**
(es la IP de Metasploitable) y empieza el analisis donde cuando termine veremos los resultados y links para ver informes y descripcion de la vulnerabilidades.

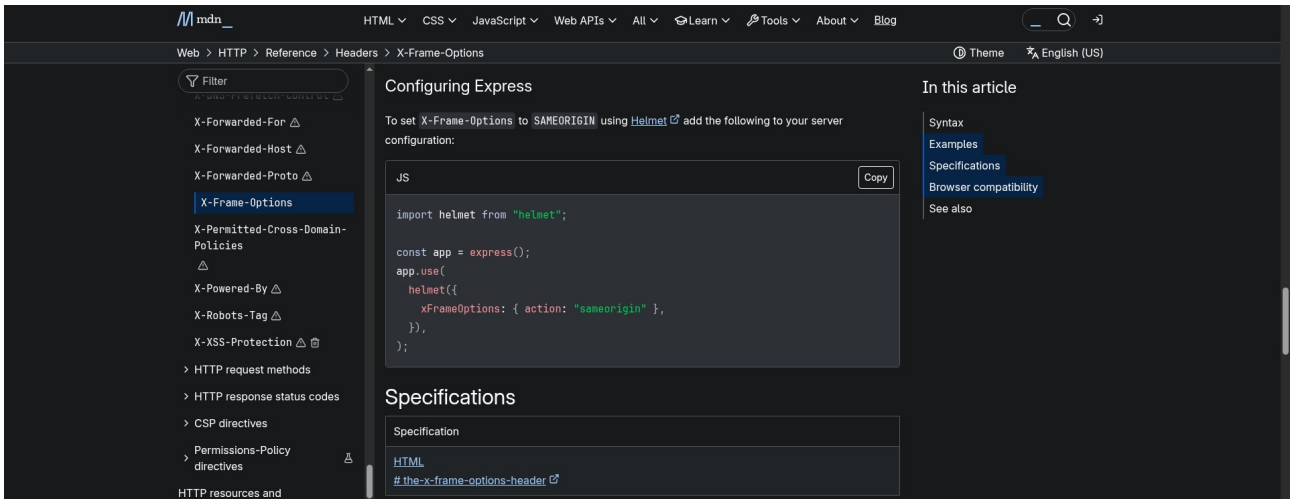


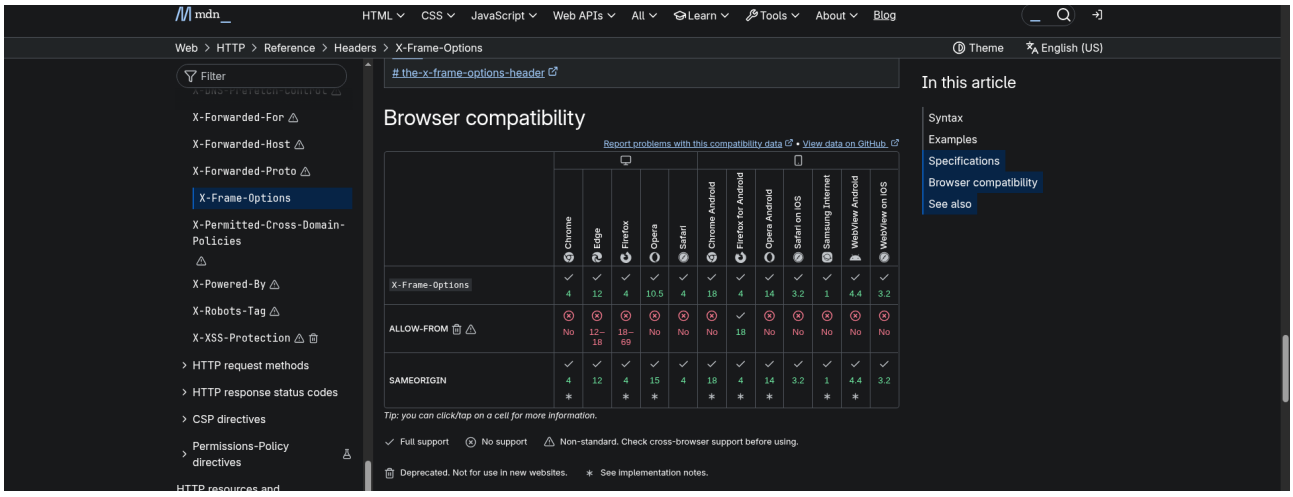

mdn
HTML CSS JavaScript Web APIs All Learn Tools About Blog
Web > HTTP > Reference > Headers > X-Frame-Options
Theme English (US)
Filter
X-Forwarded-For
X-Forwarded-Host
X-Forwarded-Proto
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-Powered-By
X-Robots-Tag
X-XSS-Protection
HTTP request methods
HTTP response status codes
CSP directives
X-Frame-Options header
Note: For more comprehensive options than offered by this header, see the frame-ancestors directive in a Content-Security-Policy header.
The HTTP X-Frame-Options response header can be used to indicate whether a browser should be allowed to render a page in a <frame>, <iframe>, <embed> or <object>. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.
The added security is provided only if the user accessing the document is using a browser that supports X-Frame-Options.
Header type
Response header
Forbidden request header
No
Syntax
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
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
Header type
Response header
Forbidden request header
No
Syntax
HTTP
Copy
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN
Directives
DENY
The page cannot be displayed in a frame, regardless of the site attempting to do so. Not only will the browser attempt to load the page in a frame fail when loaded from other sites, attempts to do so will fail when loaded from the same site.
SAMEORIGIN
The page can only be displayed if all ancestor frames are same origin to the page itself. You can still use the page in a frame as long as the site including it in a frame is the same as the one serving the page.
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
HTTP resources and
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

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.

```
  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

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.

References 1 Total

- securityfocus.com: 318 vdb-entry

CVE Program

Updated: 2024-08-01

This container includes required additional information provided by the CVE Program for this vulnerability.

References 1 Total

- securityfocus.com: 318 vdb-entry x_transferred

On This Page

Required CVE Record Information

CNA: MITRE Corporation

CVE Program

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

CVE Program

Updated: 2024-08-01

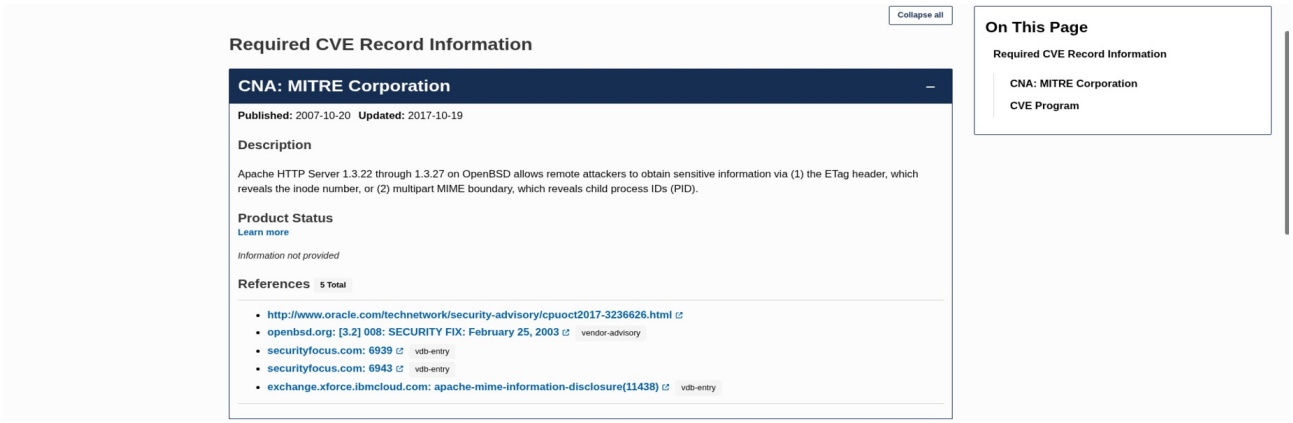
This container includes required additional information provided by the CVE Program for this vulnerability.

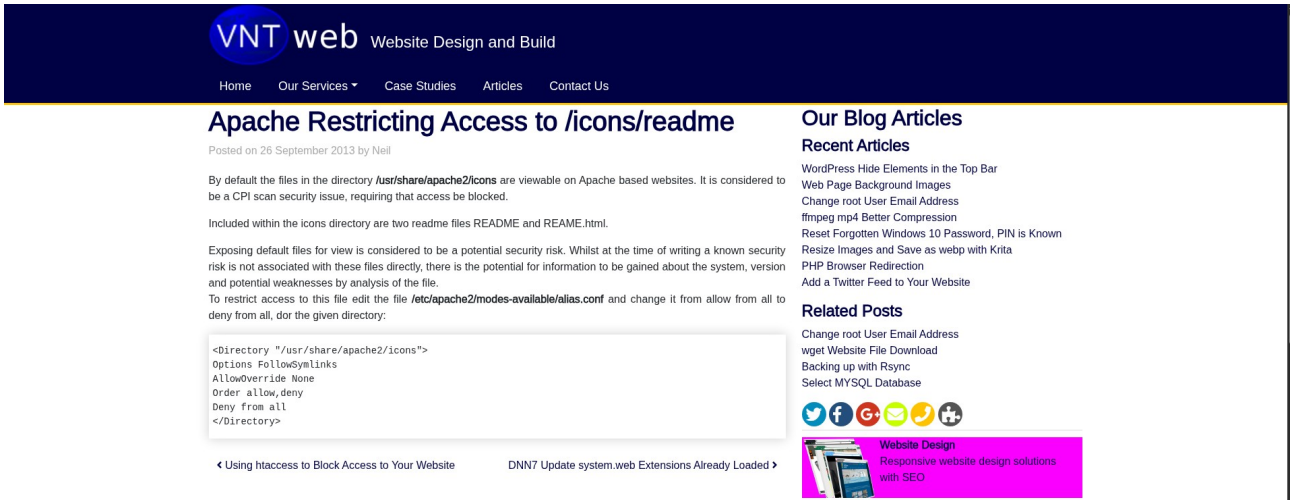
On This Page

Required CVE Record Information

CNA: MITRE Corporation

CVE Program





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.

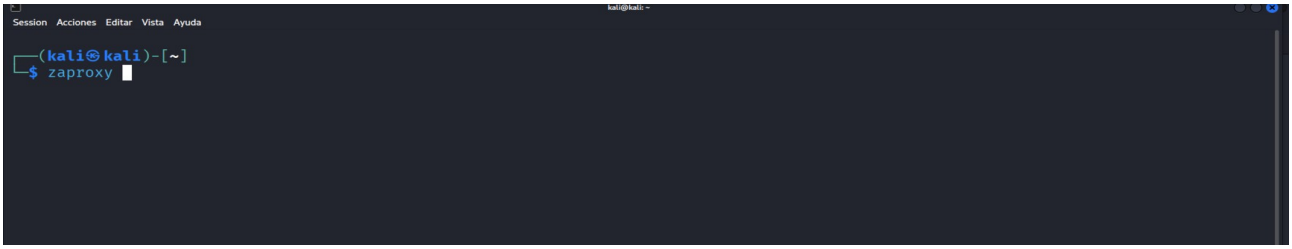
Cuando corres un escaneo (activo o pasivo), ZAP va generando alertas y ahí es donde puedes revisarlas.

Cada alerta tiene varios campos de información:

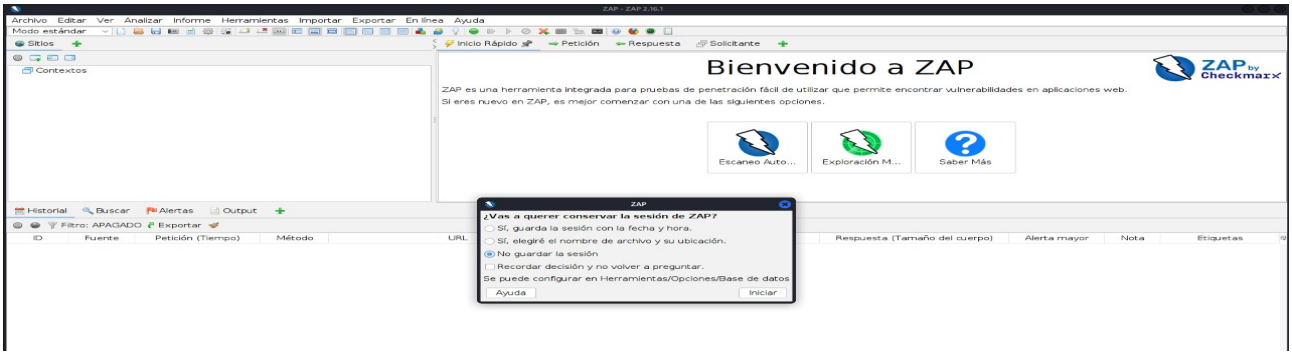
1. **Nivel de riesgo**
2. **High (Alto)** → Vulnerabilidad crítica (ej. SQL Injection).
3. **Medium (Medio)** → Riesgo importante (ej. XSS reflejado).
4. **Low (Bajo)** → Riesgo menor (ej. información sensible expuesta en headers).
5. **Informational (Info)** → No es un fallo, pero puede ser útil (ej. 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.

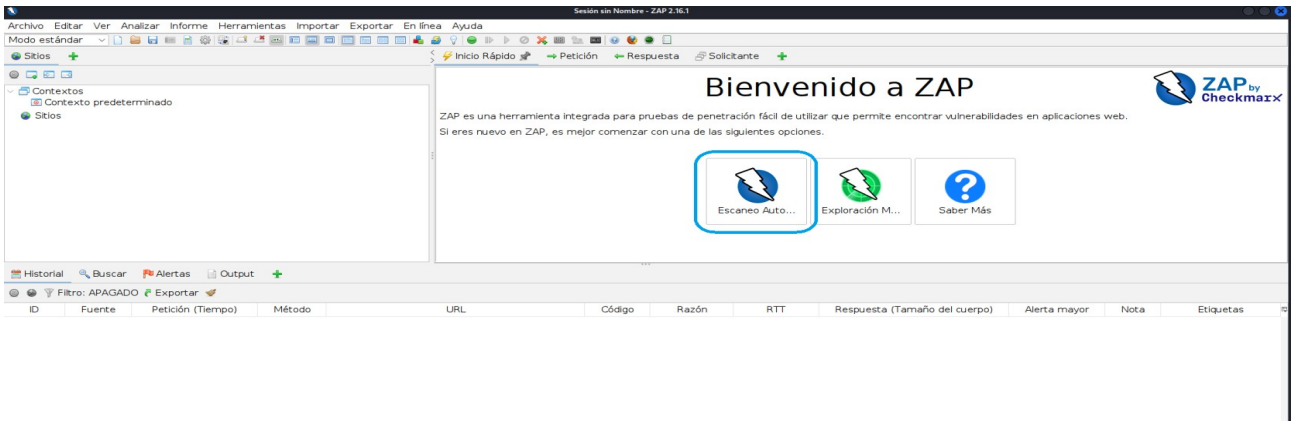
En resumen:
La pestaña de **Alertas en ZAP** es el “informe en vivo” de todas las vulnerabilidades que ZAP detecta, con riesgo, ubicación, explicación y cómo arreglarlo.

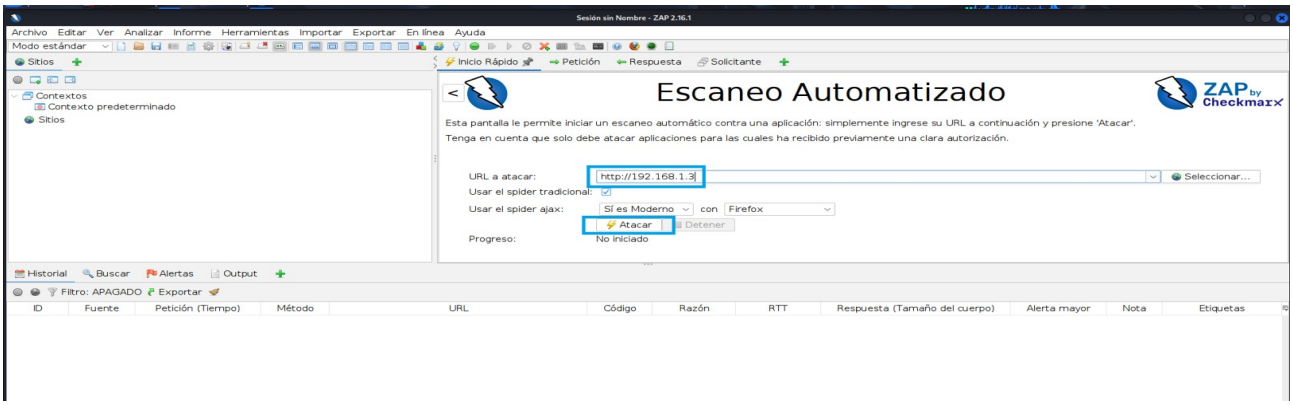
Vamos a verlo de forma grafica

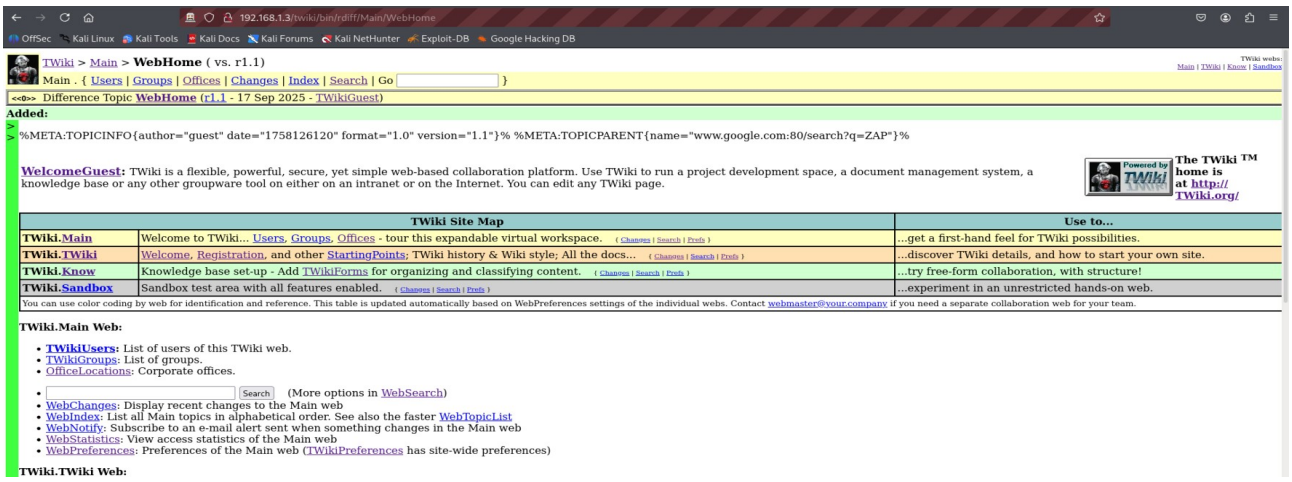


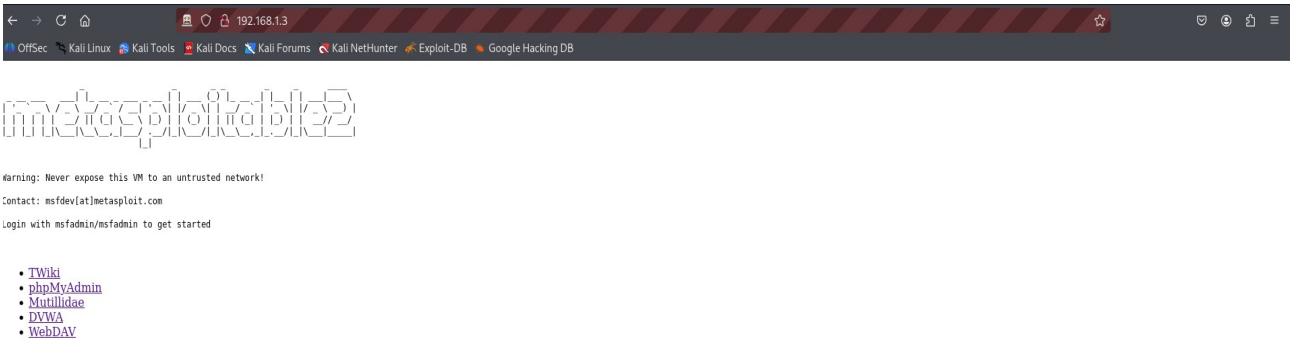
```
4375 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.control.ExtensionFactory - Loading extensions
5381 [ZAP-BootstrapGUI] INFO  org.zaproxy.addon.network.internal.TlsUtils - Using supported SSL/TLS protocols: [TLSv1.2, TLSv1.3]
5804 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.control.ExtensionFactory - Extensions 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.Flywa                              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
```

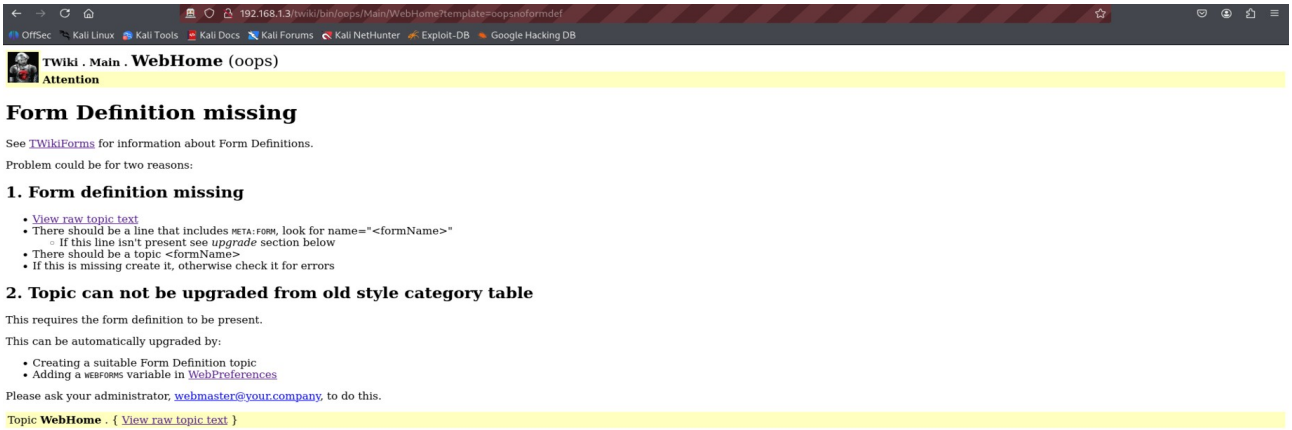


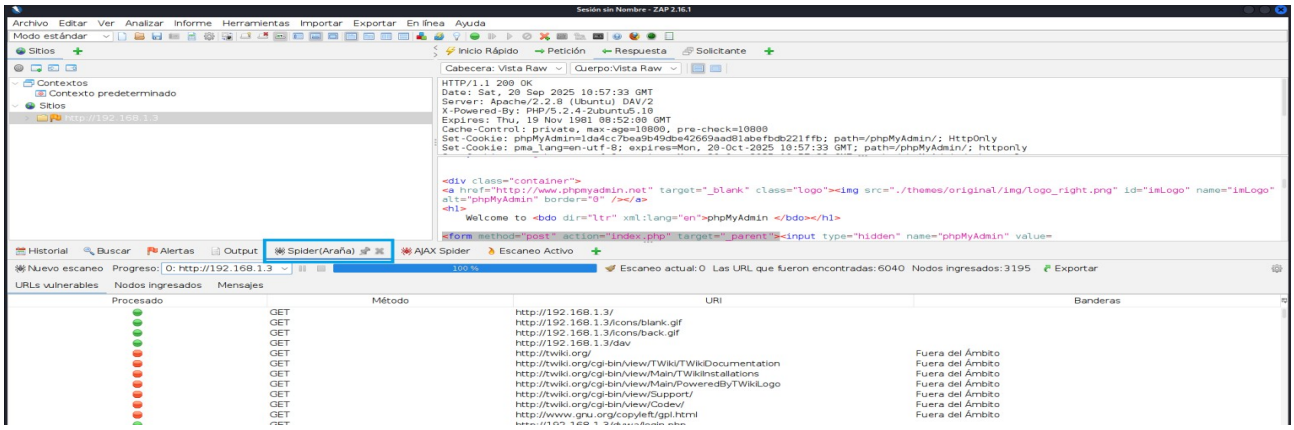



Sesión sin Nombre - ZAP 2.16.1
Archivo Editar Ver Analizar Informe Herramientas Importar Exportar En línea Ayuda
Modo estándar
Sitios
Contextos
Contexto predeterminado
Sitios
Inicio Rápido
Petición
Respuesta
Solicitante
Escaneo Automatizado
ZAP by Checkmarx
Esta pantalla le permite iniciar un escaneo automático contra una aplicación: simplemente ingrese su URL a continuación y presione 'Atacar'.
Tenga en cuenta que solo debe atacar aplicaciones para las cuales ha recibido previamente una clara autorización.
URL a atacar:
http://192.168.1.3
Seleccionar...
Usar el spider tradicional:
Usar el spider ajax:
Sí es Moderno
con
Firefox
Atacar
Detener
Progreso:
No iniciado
Historial
Buscar
Alertas
Output
Filtro: APAGADO
Exportar
ID
Fuente
Petición (Tiempo)
Método
URL
Código
Razón
RTT
Respuesta (Tamaño del cuerpo)
Alerta mayor
Nota
Etiquetas


192.168.1.3/twiki/bin/rdiff/Main/WebHome
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
TWiki > Main > WebHome (vs. r1.1)
Main . { Users | Groups | Offices | Changes | Index | Search | Go }
<<0>> Difference Topic WebHome (r1.1 - 17 Sep 2025 - TWikiGuest)
Added:
%META:TOPICINFO{author="guest" date="1758126120" format="1.0" version="1.1"}% %META:TOPICPARENT{name="www.google.com:80/search?q=ZAP"}%
WelcomeGuest: TWiki is a flexible, powerful, secure, yet simple web-based collaboration platform. Use TWiki to run a project development space, a document management system, a knowledge base or any other groupware tool on either on an intranet or on the Internet. You can edit any TWiki page.
The TWiki ™ home is at http://TWiki.org/
TWiki Site Map
Use to...
TWiki.Main
Welcome to TWiki... Users, Groups, Offices - tour this expandable virtual workspace.
...get a first-hand feel for TWiki possibilities.
TWiki.TWiki
Welcome, Registration, and other StartingPoints; TWiki history & Wiki style; All the docs...
...discover TWiki details, and how to start your own site.
TWiki.Know
Knowledge base set-up - Add TWikiForms for organizing and classifying content.
...try free-form collaboration, with structure!
TWiki.Sandbox
Sandbox test area with all features enabled.
...experiment in an unrestricted hands-on web.
You can use color coding by web for identification and reference. This table is updated automatically based on WebPreferences settings of the individual webs. Contact webmaster@your.company if you need a separate collaboration web for your team.
TWiki.Main Web:
TWikiUsers: List of users of this TWiki web.
TWikiGroups: List of groups.
OfficeLocations: Corporate offices.
Search (More options in WebSearch)
WebChanges: Display recent changes to the Main web
WebIndex: List all Main topics in alphabetical order. See also the faster WebTopicList
WebNotify: Subscribe to an e-mail alert sent when something changes in the Main web
WebStatistics: View access statistics of the Main web
WebPreferences: Preferences of the Main web (TWikiPreferences has site-wide preferences)
TWiki.TWiki Web:

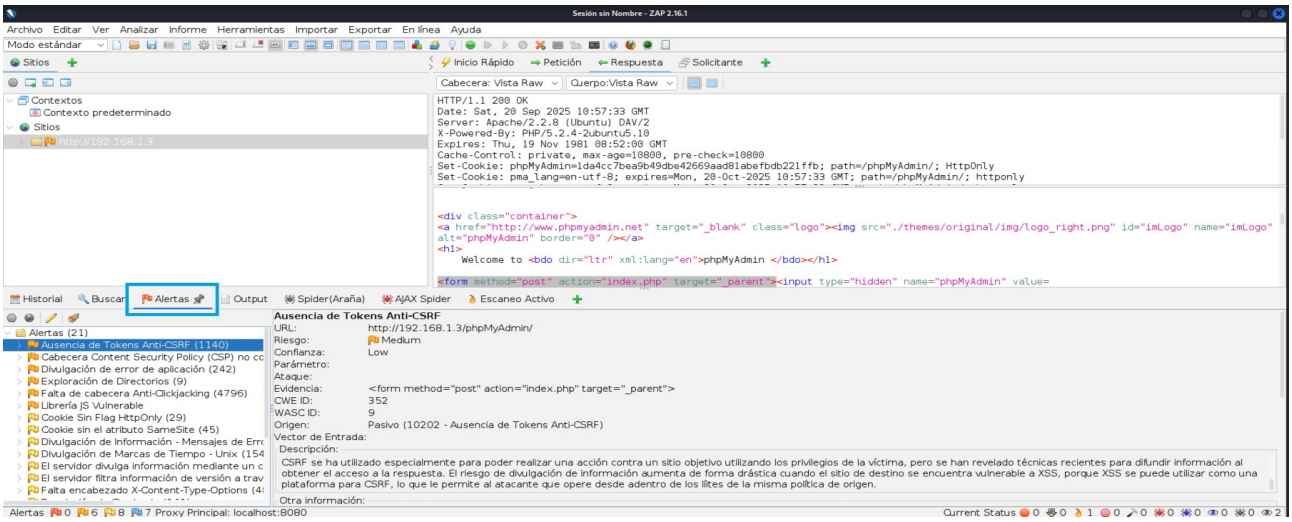

192.168.1.3
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
TWiki
phpMyAdmin
Mutillidae
DVWA
WebDAV


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 }

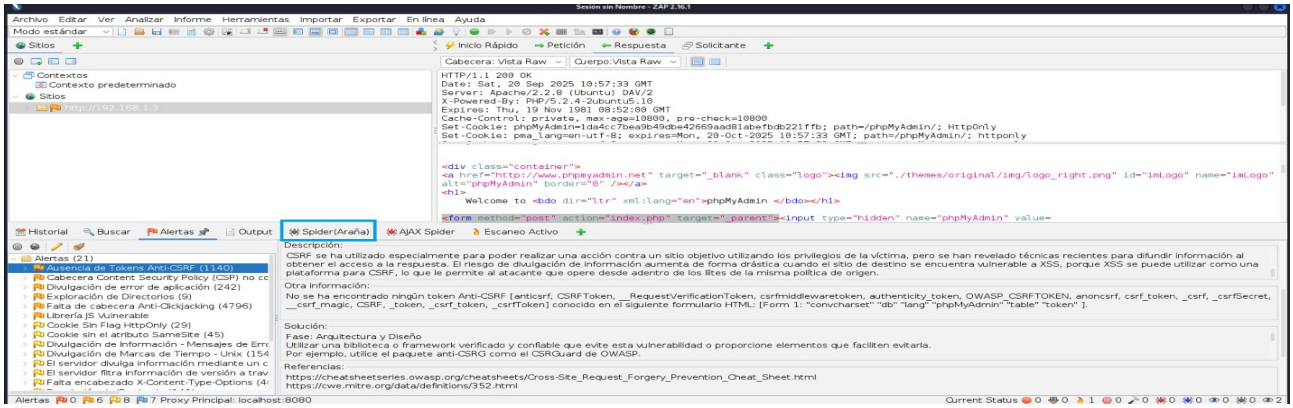

Sesión sin Nombre - ZAP 2.16.1
Archivo Editar Ver Analizar Informe Herramientas Importar Exportar En línea Ayuda
Modo estándar
Sitios
Inicio Rápido Petición Respuesta Solicitante
Cabecera: Vista Raw Cuerpo:Vista Raw
HTTP/1.1 200 OK
Date: Sat, 20 Sep 2025 10:57:33 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
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

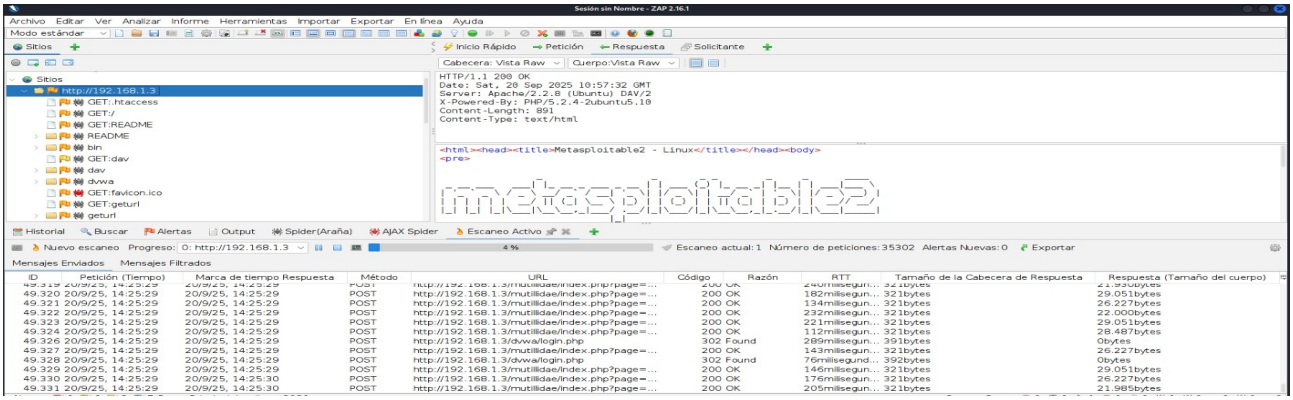
+


Sesión sin Nombre - ZAP 2.16.1
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
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
Alertas (21)
Ausencia de Tokens Anti-CSRF (1140)
Cabecera Content Security Policy (CSP) no co
Divulgación de error de aplicación (242)
Exploración de Directorios (9)
Falta de cabecera Anti-Clickjacking (4796)
Librería JS Vulnerable
Cookie Sin Flag HttpOnly (29)
Cookie sin el atributo SameSite (45)
Divulgación de Información - Mensajes de Err
Divulgación de Marcas de Tiempo - Unix (154
El servidor divulga información mediante un c
El servidor filtra información de versión a trav
Falta encabezado X-Content-Type-Options (4
Ausencia de Tokens Anti-CSRF
URL: http://192.168.1.3/phpMyAdmin/
Riesgo: Medium
Confianza: Low
Parámetro:
Ataque:
Evidencia: <form method="post" action="index.php" target="_parent">
CWE ID: 352
WASC ID: 9
Origen: Pasivo (10202 - Ausencia de Tokens Anti-CSRF)
Vector de Entrada:
Descripción:
CSRF se ha utilizado especialmente para poder realizar una acción contra un sitio objetivo utilizando los privilegios de la víctima, pero se han revelado técnicas recientes para difundir información al obtener el acceso a la respuesta. El riesgo de divulgación de información aumenta de forma drástica cuando el sitio de destino se encuentra vulnerable a XSS, porque XSS se puede utilizar como una plataforma para CSRF, lo que le permite al atacante que opere desde adentro de los límites de la misma política de origen.
Otra información:
Alertas 0 6 8 7 Proxy Principal: localhost:8080
Current Status 0 0 1 0 0 0 0 0 0 0 2


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
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/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=1da4c7bea9b49dbe42669aad81abefbdb221ffb; path=/phpMyAdmin/; HttpOnly
Set-Cookie: pma_lang=en-utf-8; expires=Mon, 20-Oct-2025 10:57:33 GMT; path=/phpMyAdmin/; httponly

<img src="./themes/original/img/logo_right.png" id="imLogo" name="imLogo"
alt="phpMyAdmin" border="0" />
<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
Alertas (21)
Ausencia de Tokens Anti-CSRF (1140)
Cabecera Content Security Policy (CSP) no co
División de error de aplicación (242)
Exploración de Directorios (9)
Falta de cabecera Anti-Clickjacking (4796)
Librería JS Vulnerable
Cookie Sin Flag HttpOnly (29)
Cookie sin el atributo SameSite (45)
Divulgación de Información - Mensajes de Err
División de Marcas de Tiempo - Unix (154
El servidor divulga información mediante un c
El servidor filtra información de versión a trav
Falta encabezado X-Content-Type-Options (4
Descripción:
CSRF se ha utilizado especialmente para poder realizar una acción contra un sitio objetivo utilizando los privilegios de la víctima, pero se han revelado técnicas recientes para difundir información al obtener el acceso a la respuesta. El riesgo de divulgación de información aumenta de forma drástica cuando el sitio de destino se encuentra vulnerable a XSS, porque XSS se puede utilizar como una plataforma para CSRF, lo que le permite al atacante que opere desde adentro de los límites de la misma política de origen.
Otra Información:
No se ha encontrado ningún token Anti-CSRF [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] conocido en el siguiente formulario HTML: [Form 1: "convcharset" "db" "lang" "phpMyAdmin" "table" "token"].
Solución:
Fase: Arquitectura y Diseño
Utilizar una biblioteca o framework verificado y confiable que evite esta vulnerabilidad o proporcione elementos que faciliten evitarla.
Por ejemplo, utilice el paquete anti-CSRG como el CSRGuard de OWASP.
Referencias:
https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html
https://cwe.mitre.org/data/definitions/352.html
Alertas 0 6 8 7 Proxy Principal: localhost:8080
Current Status 0 0 1 0 0 0 0 0 0 0 2


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
Sitios
http://192.168.1.3
GET:.htaccess
GET:/
GET:README
README
bin
GET:dav
dav
dvwa
GET:favicon.ico
GET:geturl
geturl
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>
<pre>
Historial
Buscar
Alertas
Output
Spider(Araña)
AJAX Spider
Escaneo Activo
Nuevo escaneo
Progreso: 0: http://192.168.1.3
4 %
Escaneo actual: 1
Número de peticiones: 35302
Alertas Nuevas: 0
Exportar
Mensajes Enviados
Mensajes Filtrados
ID Petición (Tiempo) Marca de tiempo Respuesta Método URL Código Razón RTT Tamaño de la Cabecera de Respuesta Respuesta (Tamaño del cuerpo)
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 182milisegun... 321bytes 29.051bytes
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 134milisegun... 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 232milisegun... 321bytes 22.000bytes
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 221milisegun... 321bytes 29.051bytes
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 112milisegun... 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 289milisegun... 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 143milisegun... 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 76milisegund... 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 146milisegun... 321bytes 29.051bytes
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 176milisegun... 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 205milisegun... 321bytes 21.985bytes