محمد عبدالهی 9530153

1-در این سوال سعی داشتیم تا یک فایل را برای کلاینت فرستاده و هش آن محاسبه شده و در صورت برابر بودن هش ارسالی با محاسبه شده برنامه سمت کلاینت اجرا شود. مرحله اول یک کلید عمومی برای کلاینت ایجاد کردیم سپس آن را برای سرور ارسال کردیم سپس سرور توسط کلید عمومی کلاینت فایل را رمز کرده و به همراه هش فایل برای خود کلاینت ارسال کردیم کلاینت هم فایل را دریافت و با هش ارسالی مقایسه کرد و چون یکی بودند برنامه را اجرا کرد.

```
(venv) mohammad@mohammad-X556UQ ~/Documents/amniat/az/hw3/q1 python server.py
Server Running
Allowing All Incoming Connections
PORT 5555
Waiting For Connection...
Connected by  ('127.0.0.1', 42246)
Press Enter To Send File For Client
done!!
(venv) mohammad@mohammad-X556UQ ~/Documents/amniat/az/hw3/q1
```

```
(venv) mohammad@mohammad-X556UQ ~/Documents/amniat/az/hw3/q1 python client.py
Client
Key generated
Press Enter To Send PublicKey For Server
e8d2aacd21ccaaca7d59ef70816e7d9d
excuting program
Hello World!!!
(venv) mohammad@mohammad-X556UQ ~/Documents/amniat/az/hw3/q1
```

2- در این تمرین از اسیب پذیری مربوط به md5 استفاده کرده و پیام ارسالی را با پیامی مخرب جایگزین میکنیم در حالیکه هش هر دو یکی است پس کلاینت توانایی تشخیص مخرب بودن برنامه ارسالی را ندارد.

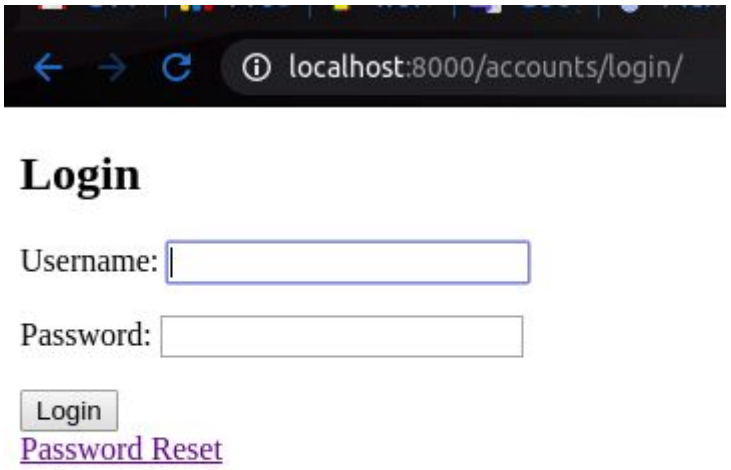
برای این نوشتن دو برنامه که هش یکسانی دارند با استفاده از لینک

https://www.mscs.dal.ca/~selinger/md5collision/

میتوان دو برنامه به زبان سی پیدا کرد که دارای هش یکسانی هستند پس این به جای برنامه امن برنامه مخرب را برای کلاینت ارسال کرده و کلاینت آنرا اجرا میکند. کلاینت چک میکند ایا هش فایل دریافتی با هش فایل اولیه برابر است و سپس انرا اجرا میکند.

3- از طریق جنگو میتوان لینک های بازیابی رمز را با استفاده از hmac پیاده سازی کرد.

برای انجام این پروژه ابتدا یک پروژه جنگو ایجاد کردیم سپس یک اپ به نام accounts ایجاد کردیم و در ادامه فرم لاگین را با پیاده سازی کردیم که اگر پروژه را اجرا کنید به فرم لاگین هدایت خواهید شد :



اگر بر روی لینک فراموشی پسورد کلیک کنید به فرم مربوط به آن منتقل میشویم که در انجا میتوان ایمیل خود را وارد کنید و لینک برای شما ارسال میشود. این پروژه را به گونه ای تنظیم کردم که ایمیل بازیابی پسورد در پوشه ی پروژه و در پوشه ی saved_emails ذخیره شود که برای این منظور در فایل confg/setting.py تنظیمات زیر را وارد کردیم:

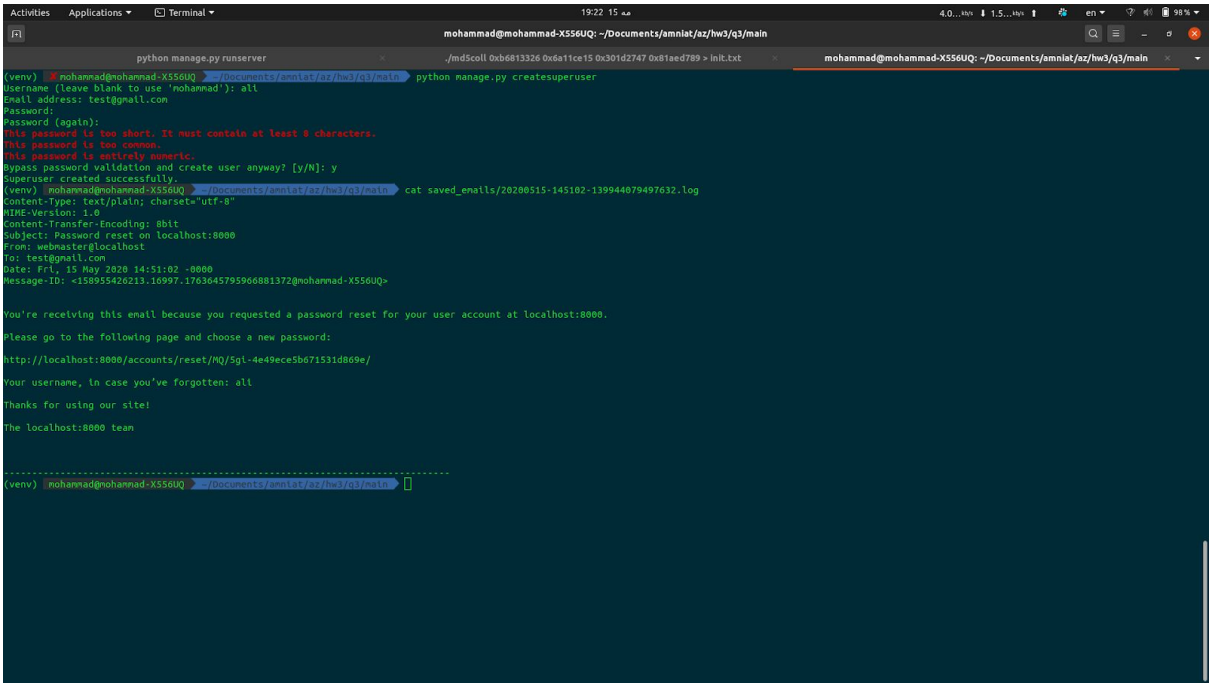
```
EMAIL_BACKEND = "django.core.mail.backends.filebased.EmailBackend"
EMAIL_FILE_PATH = os.path.join(BASE_DIR, "saved_emails")
```

و در انجا لینک ایجاد شده توسط hmac موجود است و این لینک یکبار مصرف بوده و فقط سه دقیقه اعتبار دارد که برای تنظیمات لازم برای تعیین مدت زمان اعتبار لینک خط زیر را در فایل config/setting.py اضافه کردیم.

PASSWORD_RESET_TIMEOUT_DAYS = (3/(60*24))

و روت های برنامه هم بعد از اجرا کاملا مشخص هستند.

به عنوان نمونه یک یوزر ایجاد کرده و درخواست رمز بازیابی دادیم و نتیجه و ایمیل ارسال شده را مشاهده میکنید:


Activities
Applications
Terminal
19:22 15 مه
mohammad@mohammad-X556UQ: ~/Documents/amnlat/az/hw3/q3/main
python manage.py runserver
./md5coll 0xb6813326 0x6a11ce15 0x301d2747 0x81aed789 > init.txt
mohammad@mohammad-X556UQ: ~/Documents/amnlat/az/hw3/q3/main
(venv) mohammad@mohammad-X556UQ ~/Documents/amnlat/az/hw3/q3/main python manage.py createsuperuser
Username (leave blank to use 'mohammad'): ali
Email address: test@gmail.com
Password:
Password (again):
This password is too short. It must contain at least 8 characters.
This password is too common.
This password is entirely numeric.
Bypass password validation and create user anyway? [y/N]: y
Superuser created successfully.
(venv) mohammad@mohammad-X556UQ ~/Documents/amnlat/az/hw3/q3/main cat saved_emails/20200515-145102-139944079497632.log
Content-Type: text/plain; charset="utf-8"
MIME-Version: 1.0
Content-Transfer-Encoding: 8bit
Subject: Password reset on localhost:8000
From: webmaster@localhost
To: test@gmail.com
Date: Fri, 15 May 2020 14:51:02 -0000
Message-ID: <158955426213.16997.17636457959668813728@mohammad-X556UQ>
You're receiving this email because you requested a password reset for your user account at localhost:8000.
Please go to the following page and choose a new password:
http://localhost:8000/accounts/reset/MQ/5gi-4e49ece5b671531d869e/
Your username, in case you've forgotten: ali
Thanks for using our site!
The localhost:8000 team
(venv) mohammad@mohammad-X556UQ ~/Documents/amnlat/az/hw3/q3/main