MARMARA UNIVERSITY

FACULTY OF ENGINEERING

COMPUTER ENGINEERING DEPARTMENT

CSE 4057

INFORMATION SYSTEMS SECURITY

HOMEWORK-2 REPORT

Mikail Torun

150116021

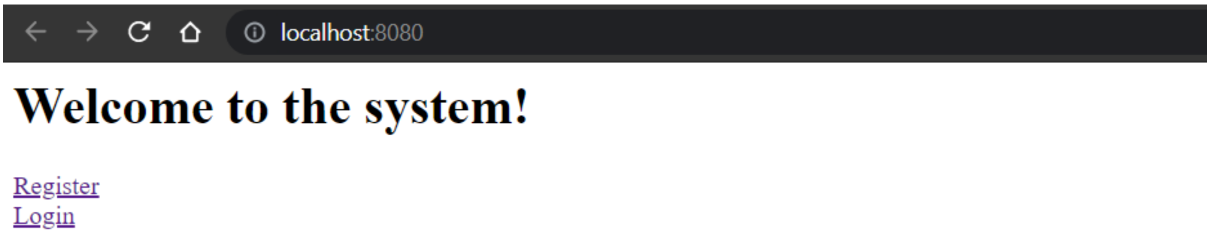
Enes Garip

150116034

Mert İsmail Eği

150115025

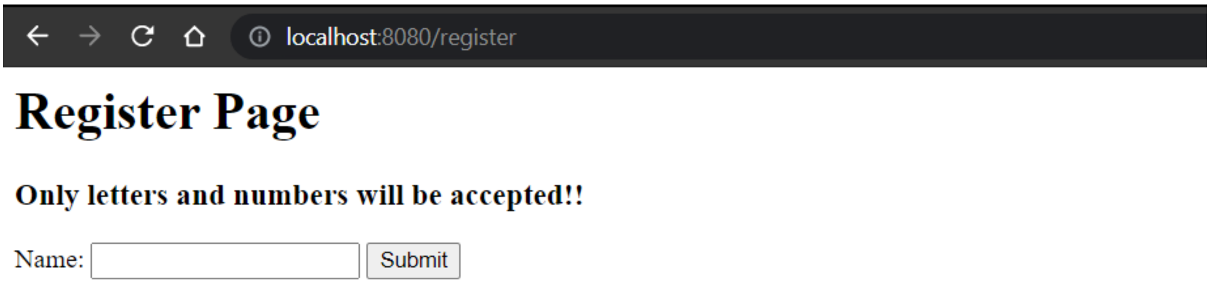
Homepage



Welcome to the system!

Homepage is where a user enters the system with a browser first time. There are two links to navigate another pages. One of them is register page and the other one is login page. Server public private key pair generated and saved to the txt file.

Register Page



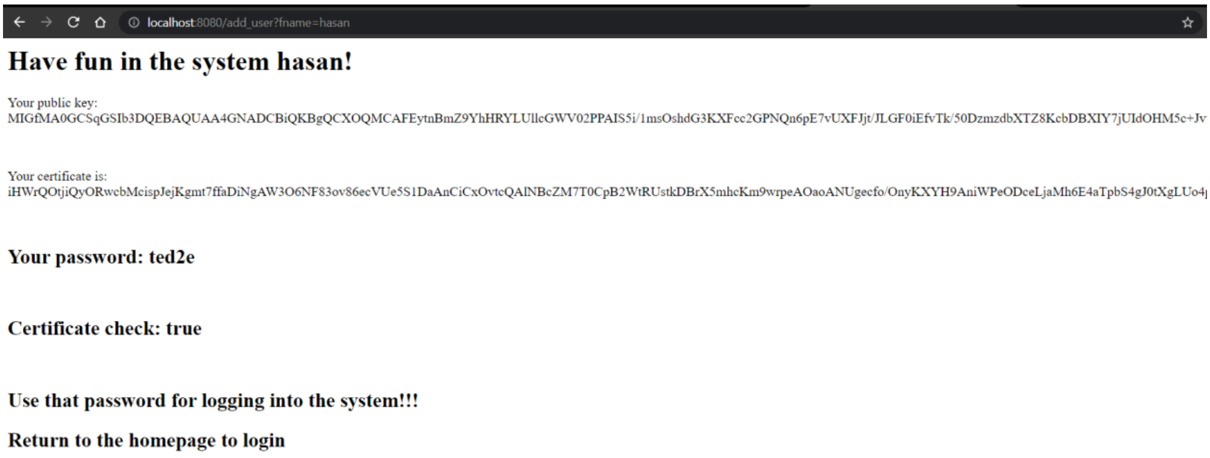
Register Page

Only letters and numbers will be accepted!!

Name:

In register page, a user provides a name to register to the system. There are some restrictions about username. It can only contain alphabetical characters and numbers.

Registering a User



Have fun in the system hasan!

Your public key:
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCXOQMCAFEytnBmZ9YhHRYLUllcGWV02PPAIS5i/1msOshdG3KXFcc2GPNQn6pE7vUXFJjt/JLGF0iEfvTk/50DzmzdbXTZ8KcbDBXIY7jUIdOHM5c+Jv

Your certificate is:
iHWrQOtjiQyORwcbMcispJejKgmt7ffaDiNgAW3O6NF83ov86ecVUe5S1DaAnCiCxOvtcQAlNBcZM7T0CpB2WtRUstkDBrX5mhcKm9wrpeAOaoANUgecfo/OnyKXYH9AniWPeODceLjaMh6E4aTpbS4gJ0tXgLUo4

Your password: ted2e

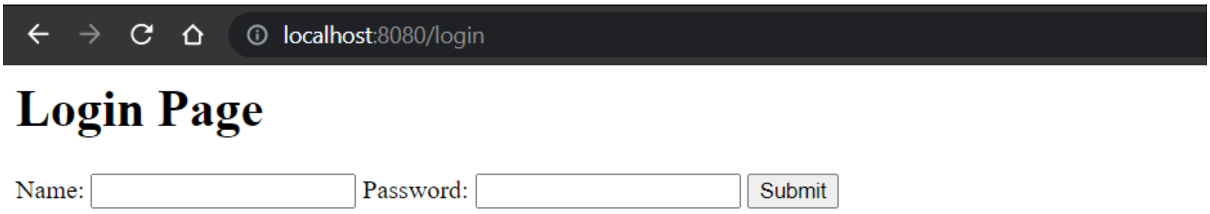
Certificate check: true

Use that password for logging into the system!!!

Return to the homepage to login

After a user provide a username, user public and private key pair generated. Also server signs the public key with username and check that the certificate is valid or not. In addition, there is a code that 5-character long generated for logging into the system. Also registered_users.txt file holds the information about registered users and certificates.txt file holds the certificates of the users.

Login Page

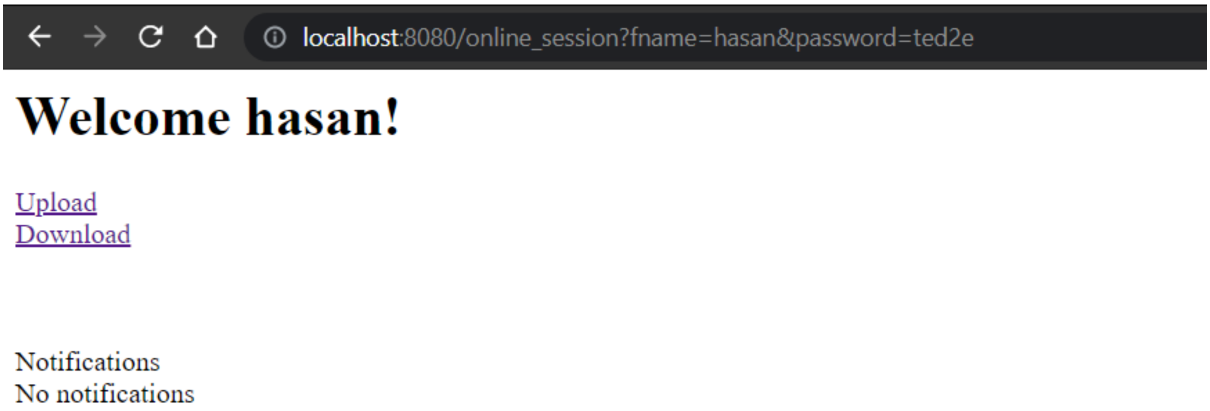


Login Page

Name: Password:

In login page, users can login into the system with their username and password.

User page



localhost:8080/online_session?fname=hasan&password=ted2e

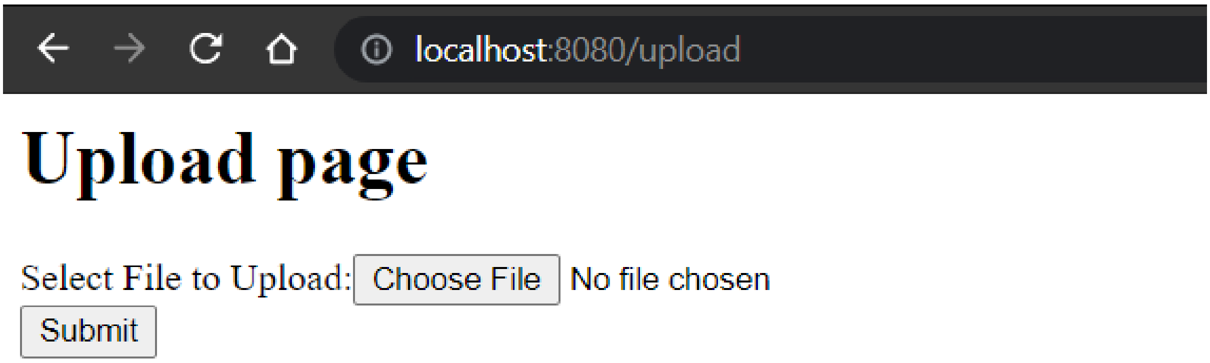
Welcome hasan!

Upload
Download

Notifications
No notifications

In user page, user creates an online session for doing some operation. There are upload and download page navigation for upload and download pages. Also when a user creates an online session, it becomes an online user and the user can get informative notification about upload operation.

Upload Page

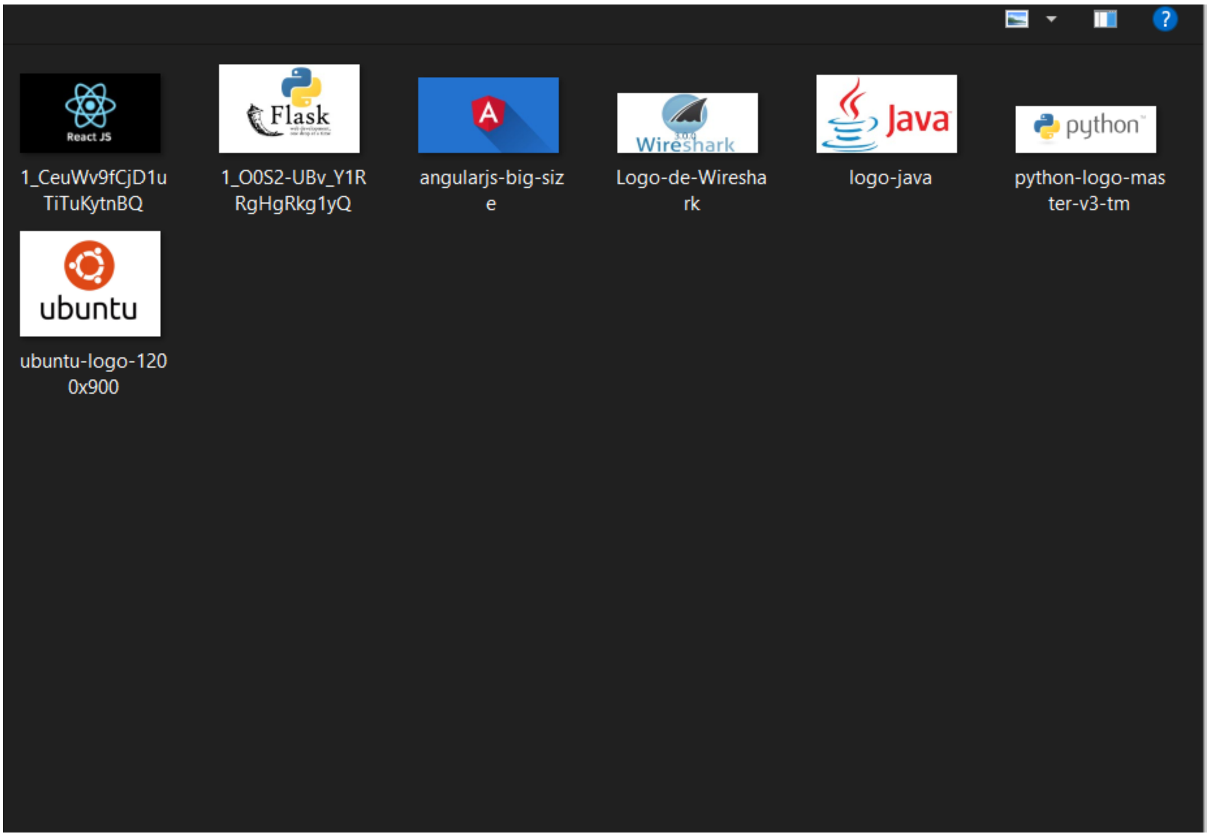


localhost:8080/upload

Upload page

Select File to Upload: No file chosen

In upload page, user selects an image in images folder and upload to the server.



Images folder that contains several images.

Upload an image

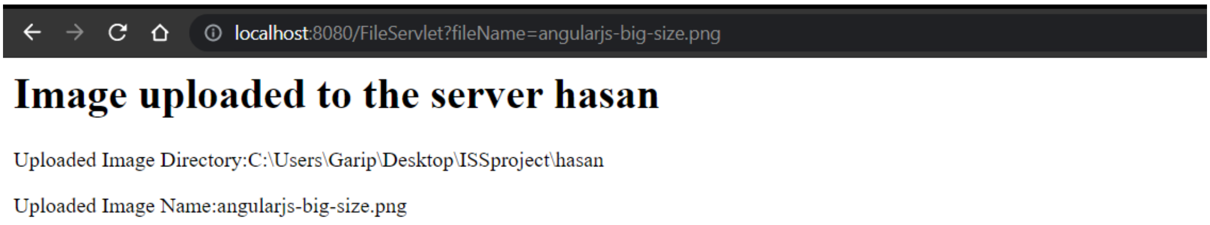
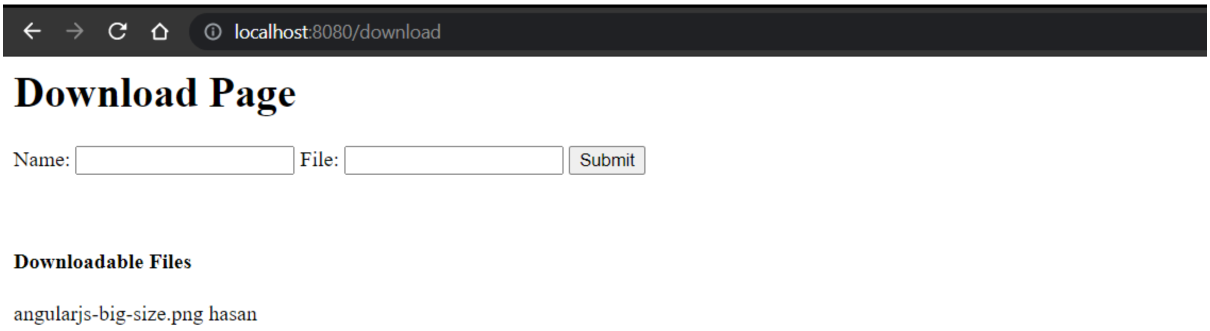


Image uploaded to the server hasan

Uploaded Image Directory:C:\Users\Garip\Desktop\ISSproject\hasan

Uploaded Image Name:angularjs-big-size.png

When user clicks the submit button, the image uploaded to the server. Server first creates a folder named with username. After that, it encrypts the image and uploaded that image to the user folder.



localhost:8080/download

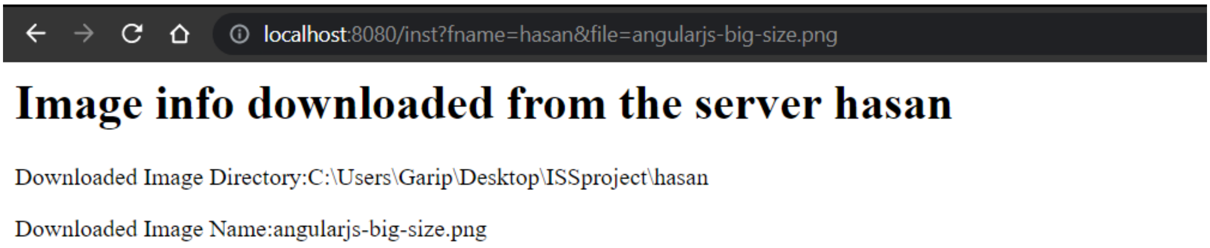
Download Page

Name: File:

Downloadable Files

angularjs-big-size.png hasan

In download page, user enters the name and username of an image listed in the downloadable files.



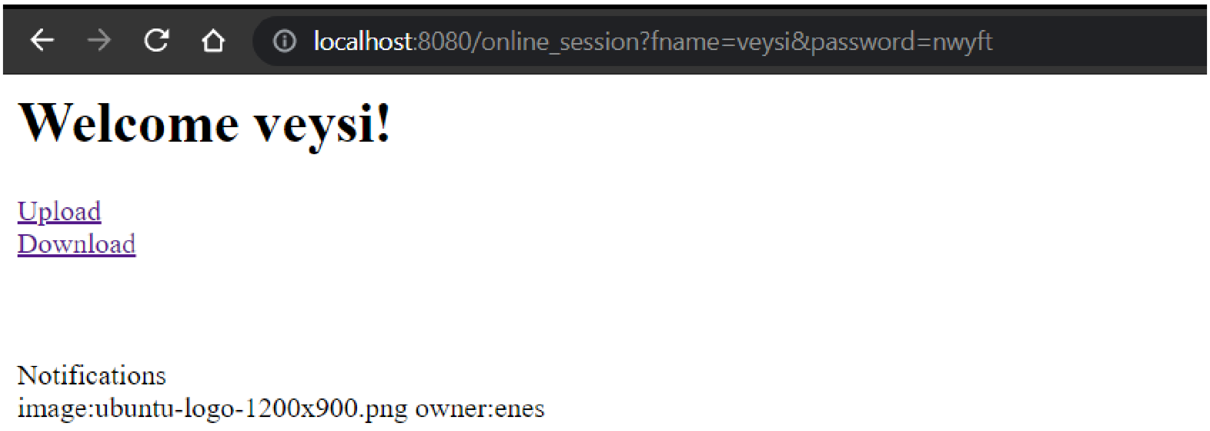
localhost:8080/inst?fname=hasan&file=angularjs-big-size.png

Image info downloaded from the server hasan

Downloaded Image Directory:C:\Users\Garip\Desktop\ISSproject\hasan

Downloaded Image Name:angularjs-big-size.png

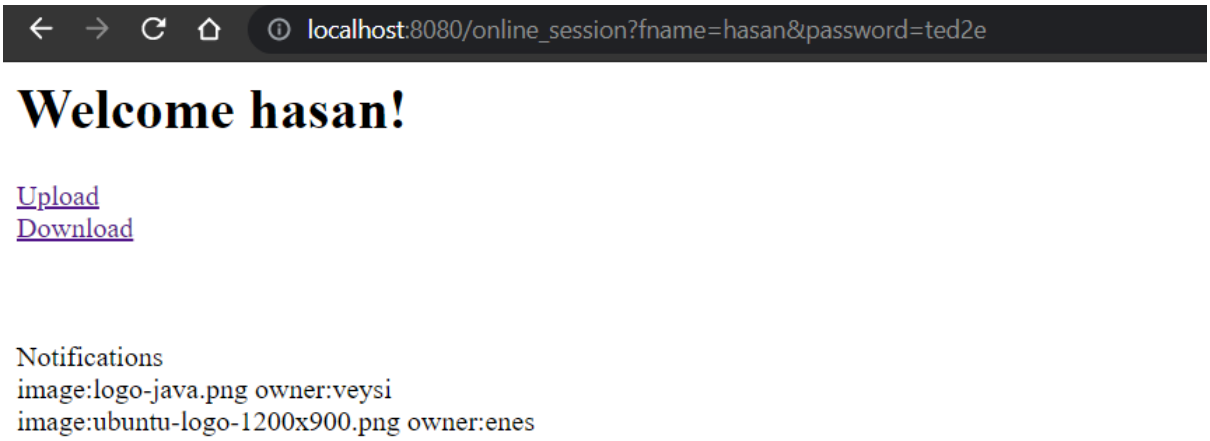
After clicking the submit button the image downloaded. (It won't work because decryption isn't work properly.)



localhost:8080/online_session?fname=veysi&password=nwyft

Welcome veysi!

Notifications
image:ubuntu-logo-1200x900.png owner:enes



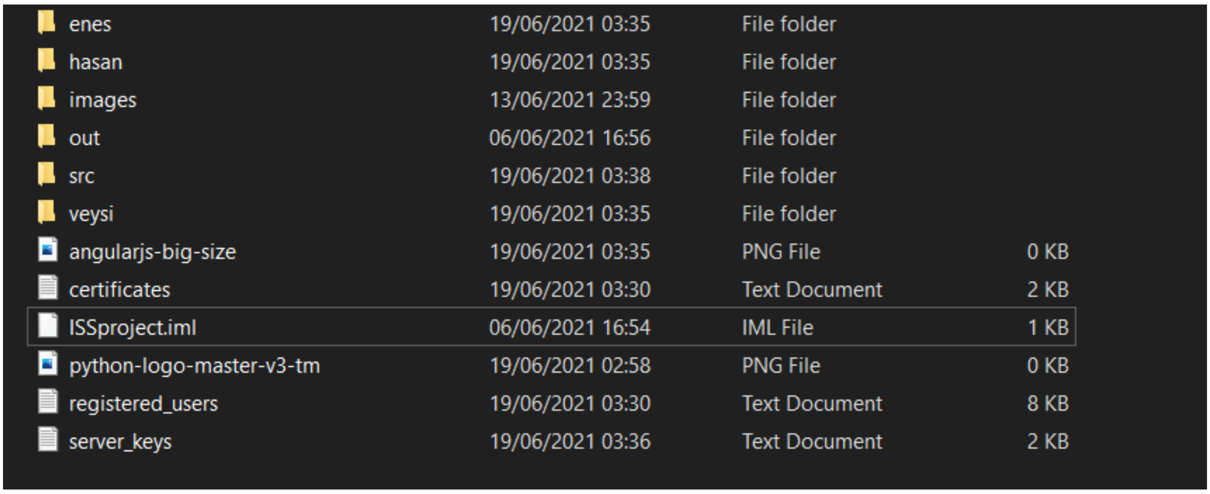
localhost:8080/online_session?fname=hasan&password=ted2e

Welcome hasan!

Upload
Download

Notifications
image:logo-java.png owner:veysi
image:ubuntu-logo-1200x900.png owner:enes

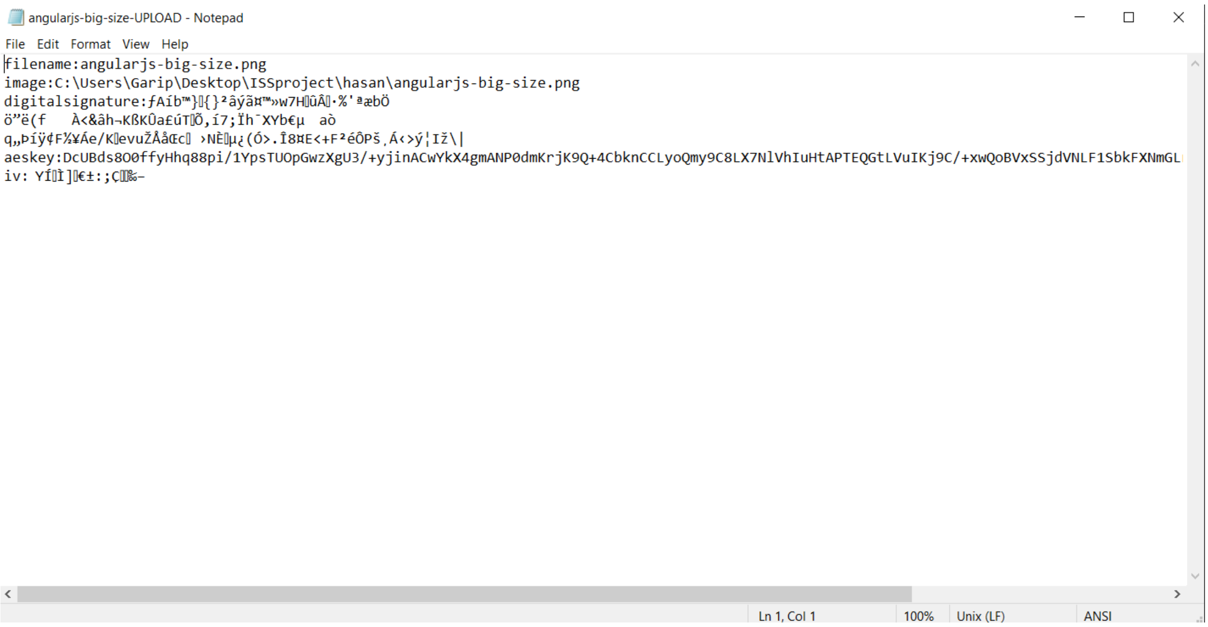
After some upload operations with different users, there is a notification about who uploaded the image and uploaded image name appears in the user's window.



enes	19/06/2021 03:35	File folder	
hasan	19/06/2021 03:35	File folder	
images	13/06/2021 23:59	File folder	
out	06/06/2021 16:56	File folder	
src	19/06/2021 03:38	File folder	
veysi	19/06/2021 03:35	File folder	
angularjs-big-size	19/06/2021 03:35	PNG File	0 KB
certificates	19/06/2021 03:30	Text Document	2 KB
ISSproject.iml	06/06/2021 16:54	IML File	1 KB
python-logo-master-v3-tm	19/06/2021 02:58	PNG File	0 KB
registered_users	19/06/2021 03:30	Text Document	8 KB
server_keys	19/06/2021 03:36	Text Document	2 KB

The folder structure of the project.

- Named folders holds the uploaded images and a txt file about the file.
- Images folder holds the images that can be uploaded to the server.
- Certificates.txt holds the certificates of the users.
- registered_users.txt file holds the information about registered users.
- server_keys holds the key pair of the server.


angularjs-big-size-UPLOAD - Notepad
File Edit Format View Help
Ln 1, Col 1
100%
Unix (LF)
ANSI

```
filename:angularjs-big-size.png
image:C:\Users\Garip\Desktop\ISSproject\hasan\angularjs-big-size.png
digitalsignature:ƒAíb™}□{}²âýã¤™»w7H□ûÂ□·%'ªæbÖ
ö”ë(f   À<&âh¬KßKÛa£úT□Õ,í7;Ïh¯XYb€µ  aò
q„þíÿ¢F½¥Áe/K□evuŽÅåŒc□ ›NÈ□µ¿(Ó>.Î8¤E<+F²éÔPš¸Á‹>ý¦Iž\|
aeskey:DcUBds8O0ffyHhq88pi/1YpsTUOpGwzXgU3/+yjinACwYkX4gmANP0dmKrjK9Q+4CbknCCLyoQmy9C8LX7NlVhIuHtAPTEQGtLVuIKj9C/+xwQoBVxSSjdVNLF1SbkFXNmGL
iv: YÍ□Ì]□€±:;Ç□□‰–
```

When an image uploaded to the server, a txt file created and it contains file name, image path, digital signature, AES key and iv parameter.

Design Choices and Comments

We firstly design the server and how to handle requests. Because of user operations are made in html template, the user and server files are together and it may be confusing. But the registering part, encryption part, key generation and notification part are working well. On the other hand, there are bugs in download and verification part.

We think one of the most important security hole is that when if Trudy can reach the system, she can get information about other user's keys and certificates. This is a major security hole for the system. Also, when a user knows other user's name and password, he/she can get into the system without warning. Because of that, users shouldn't share anything about the generated password.

(Downloading and verification part won't work properly.)