REPORT 1 (Group 30)

Vulnerability type:

Integrity Violation

Steps to reproduce

Enter amount 0 in Add amount to wallet.
Capture the packet in BurpSuite and modify 1000 to 15000
The change will be reflected in your profile on logging in again

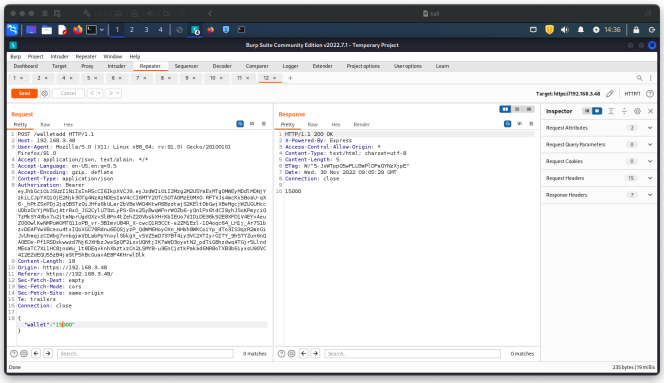
Proof of concept

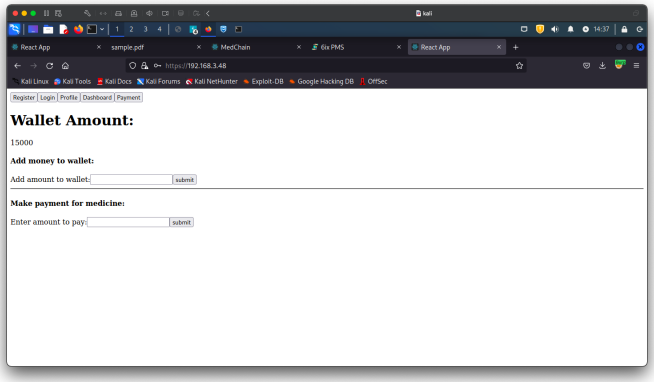
On modifying the packet in BurpSuite, my wallet balance increased.

Impact

Anyone can change his balance by intercepting the packets

Screenshots





REPORT 2 (Group 35)

Vulnerability type:

DoS

Steps to reproduce

I used the python library slowloris to send requests from multiple sockets of my kali machine. I saw using nmap that port 80 (for HTTP) and port 443 (for HTTPS) were open for requests. Hence, I used around 1000-2000 of my sockets to send requests using these commands: slowloris -s 2000 -p 80 192.168.3.104 slowloris -s 2000 -p 443 192.168.3.104

After this I tried to access the website but was unsuccessful

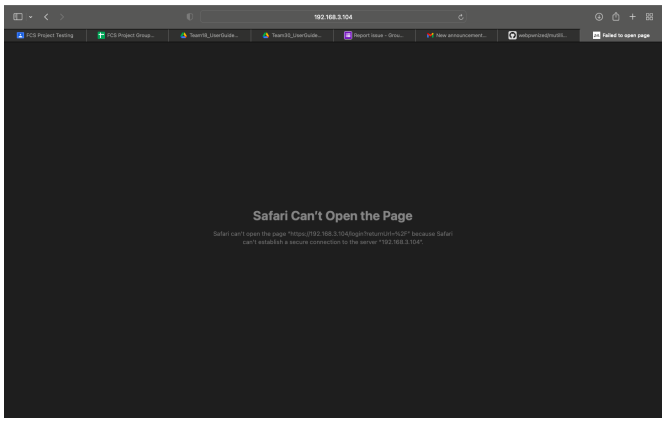
Proof of concept

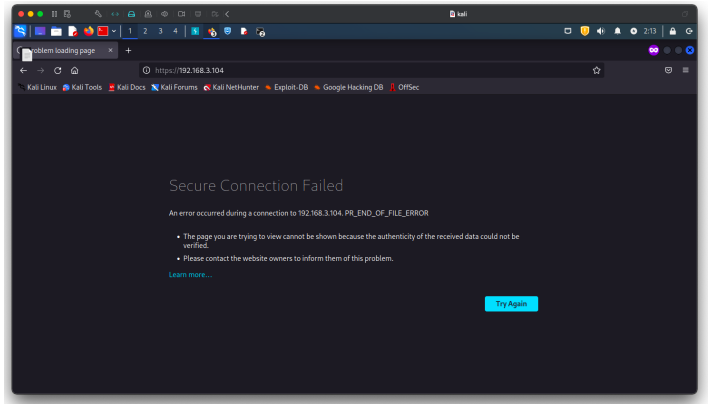
The system does not check for multiple requests from the same IP and gets flooded with requests. This makes the system unavailable for genuine requests

Impact

This vulnerability that the system is unavailable to be accessed by others for genuine requests. I have checked from my laptop's browser(safari) and from my VM's browser(Mozilla), the website is unavailable to furnish genuine requests.

Screenshots





REPORT 3 (Group 18)

Vulnerability type:

CSRF

Steps to reproduce

You can upload any html document. I exploited this by entering an HTML code to delete file

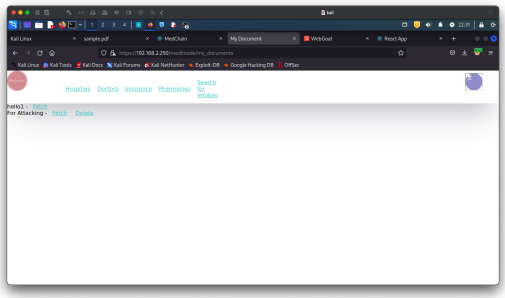
Proof of concept

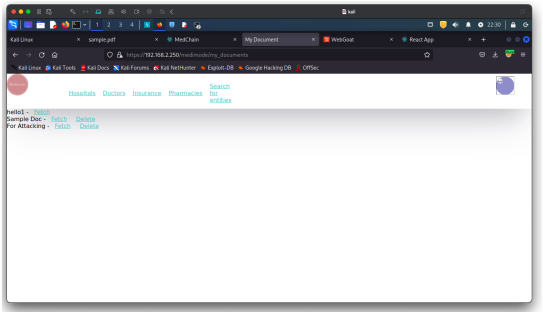
I first uploaded a file sample.pdf named Sample Doc (as in screenshots). Then uploaded an HTML file named 'For Attacking'. If I click the Fetch Button for that, the HTML file is executed and I put a copy of their own documents page but with many more junk documents. I even added an option 'Attacked' which when clicked would delete the 'Sample Doc' file

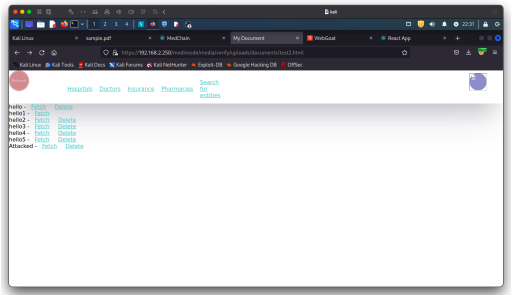
Impact

It is a very bad vunerability which can be exploited in a very bad sense as there is no check in the type of file that can be uploaded.

Screenshots







REPORT 4 (Group 45)

Vulnerability type:

Feature Bug

Steps to reproduce

Click on Services>Insurance --> No functionality; No functionality for hospitals. Uploading PDFs makes no sense as doctor cannot see it

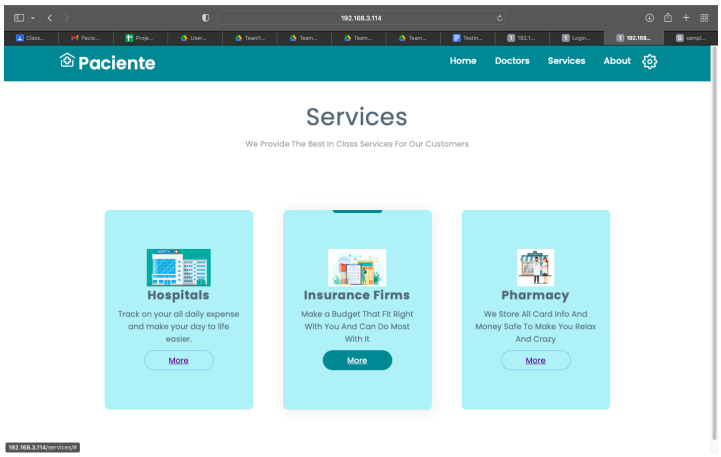
Proof of concept

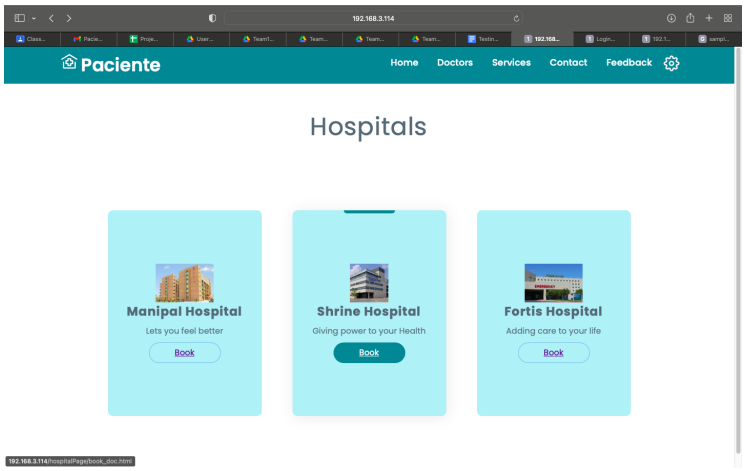
Clicking on insurance leads nowhere. No response on selecting the hospital. No point of uploading PDFs as the doctor cannot appointments allotted to him/her

Impact

Major things not implemented

Screenshots





REPORT 5 (Group 5)

Vulnerability type:

Feature Bug

Steps to reproduce

Login using given sample credentials, see no option to upload

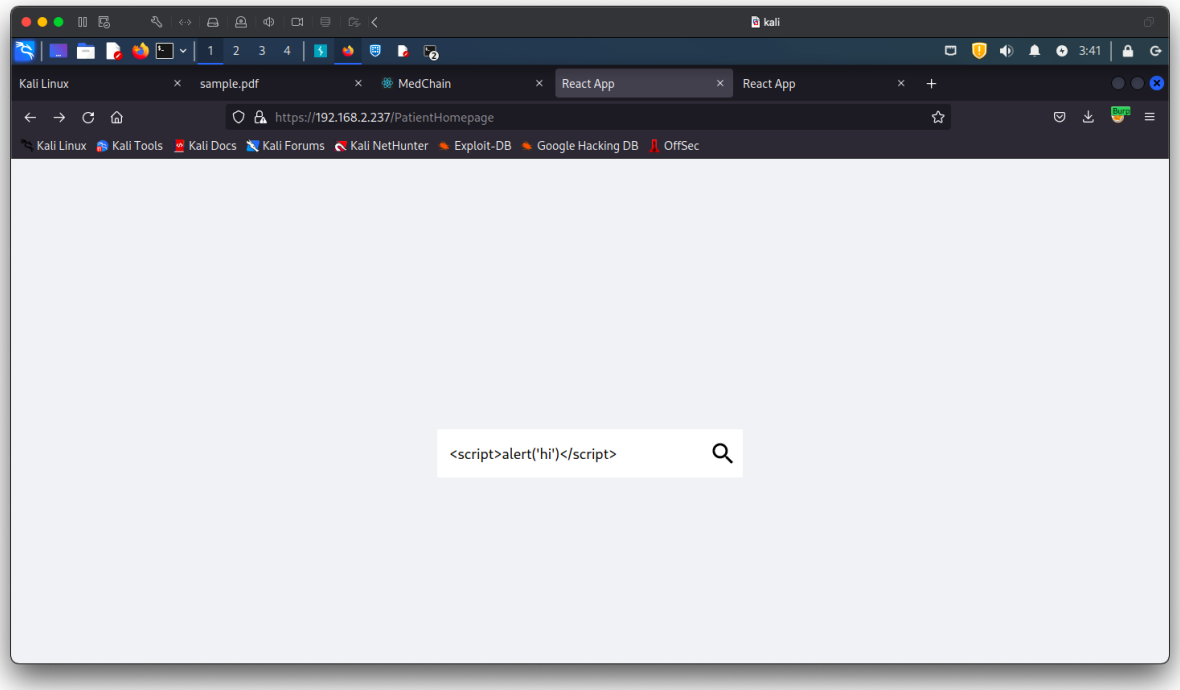
Proof of concept

No functionality to upload documents, payment system, sharing docs with organisations

Impact

Functionality Not implemented

Screenshots



REPORT 6 (Group 5)

Vulnerability type:

DoS

Steps to reproduce

Run the command: slowloris -s 6000 -p 443 192.168.2.237
Website is down on accessing it.

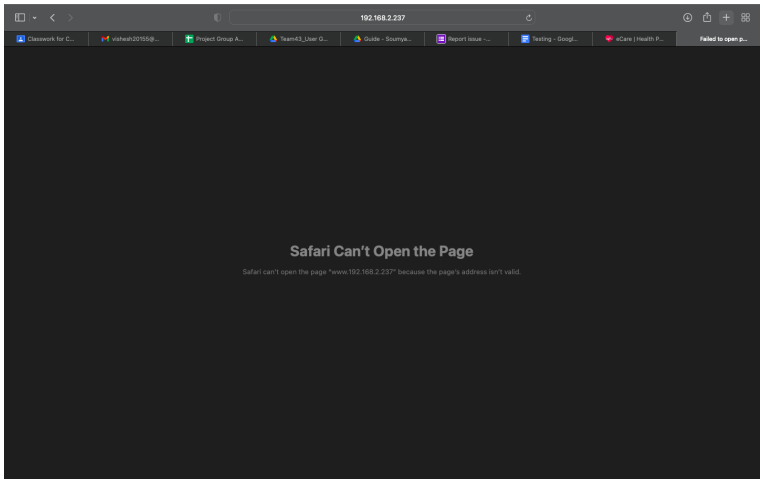
Proof of concept

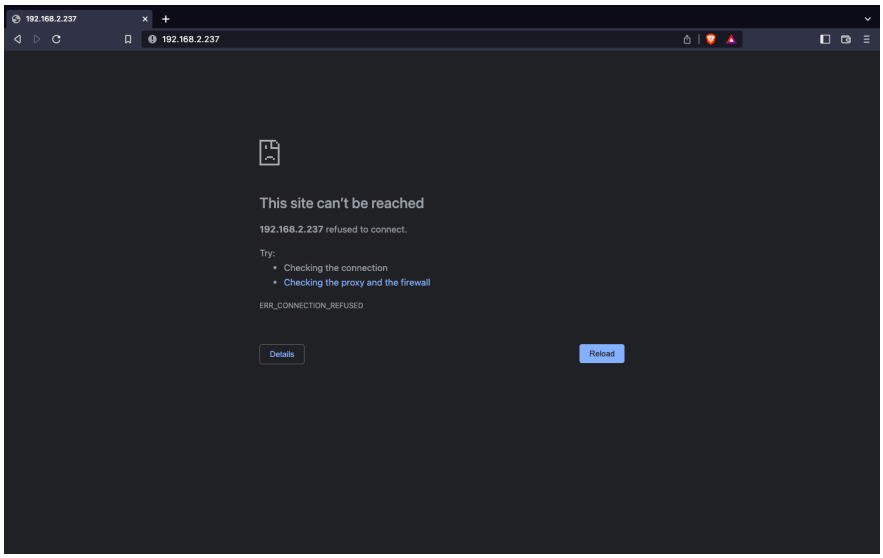
The website goes down for usage by others as many connections are attempted on the site.

Impact

Makes the website unavailable to others during the attack

Screenshots





REPORT 7 (Group 32)

Vulnerability type:

DoS

Steps to reproduce

I used python's slow loris tool to send make more than 10000 connections at regular interval using the command: slowloris -s 6000 -p 443 192.168.3.50. I attacked both port 80 and port 443.

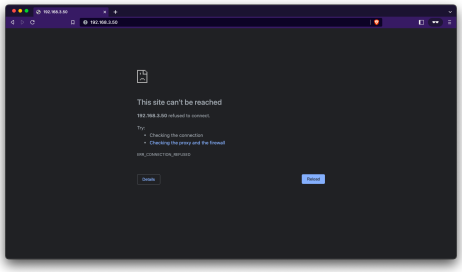
Proof of concept

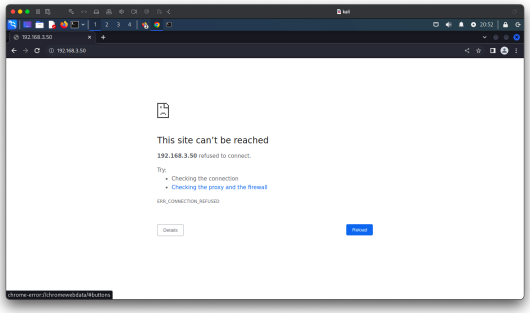
I tried to access the website from 2 websites, but it was not accessible. Attached are screenshots. This happens as the website does not block multiple request from the same IP and its overused.

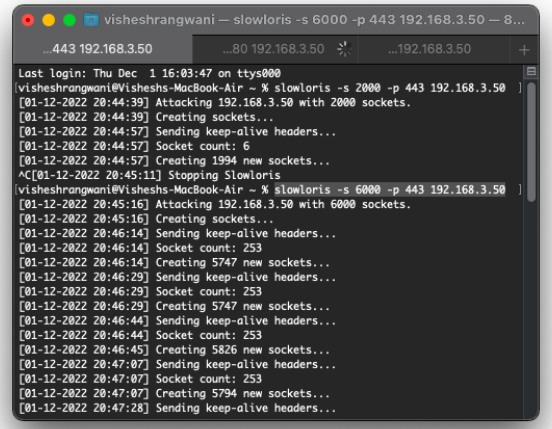
Impact

It can hamper the availability of the website for other legitimate users.

Screenshots







REPORT 8 (Group 29)

Vulnerability type:

Feature Bug

Steps to reproduce

One has to sign the document using own private given during login. Automatic verification does not take place. Also document signed by the user, not admin

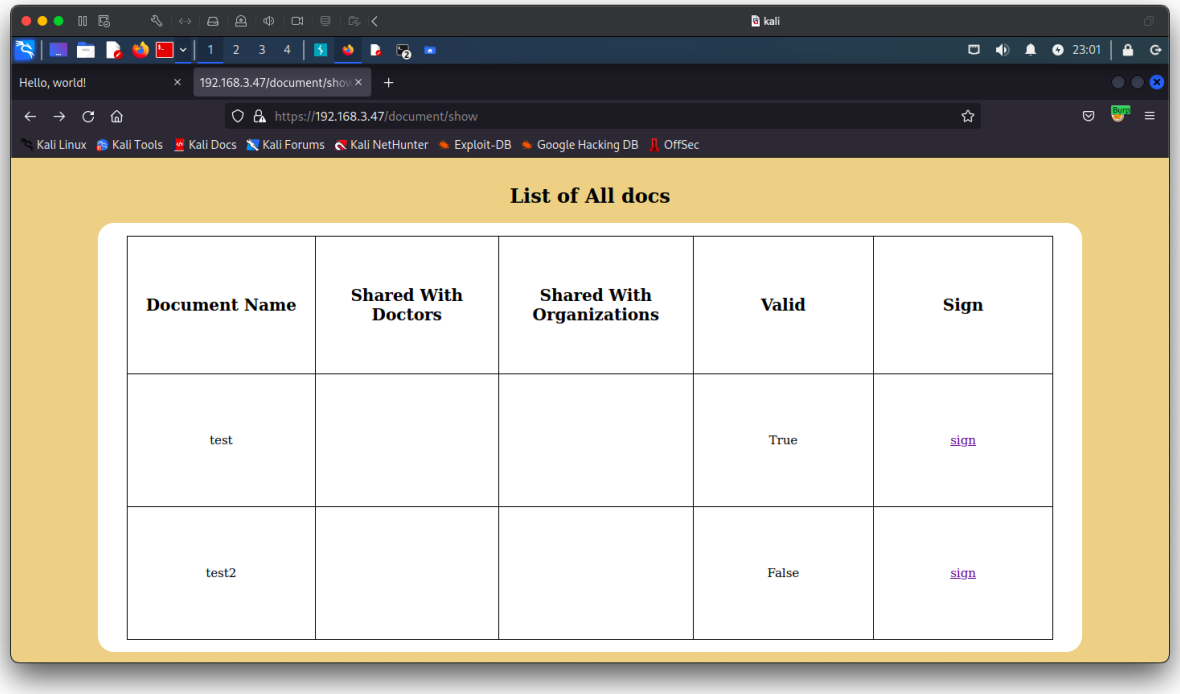
Proof of concept

Screenshot added regarding self signing.

Impact

A user can himself sign malicious document

Screenshots



REPORT 9 (Group 29)

Vulnerability type:

DoS

Steps to reproduce

Download the python's slowloris library and run this command on 2 terminals: slowloris -s 6000 -p 443 192.168.3.47

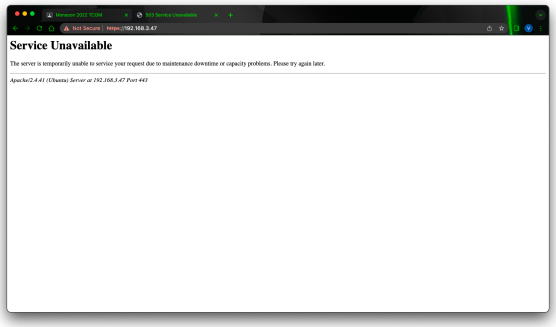
Proof of concept

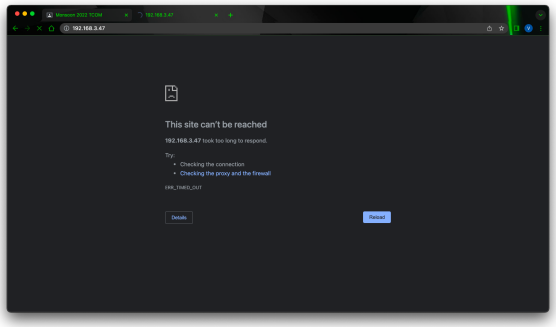
After running the command, the website is unreachable during the DoS attack. Screenshots from 2 different browsers attached.

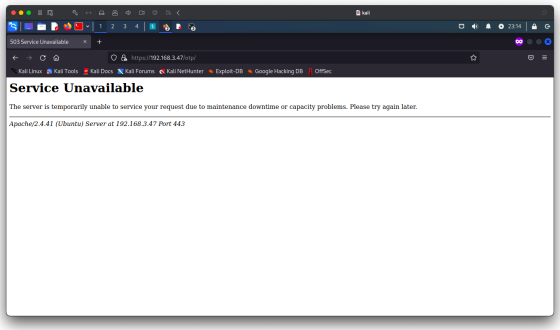
Impact

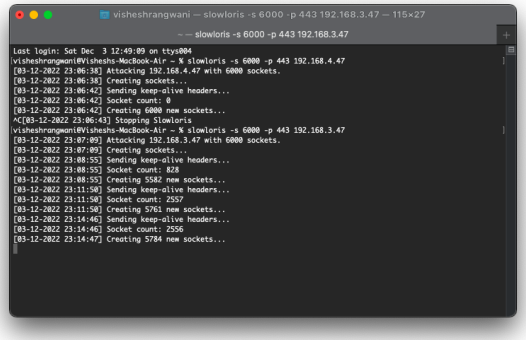
The website is unavailable for legitimate users and services are shut

Screenshots









REPORT 10 (Group 29)

Vulnerability type:

CSRF

Steps to reproduce

Upload an HTML file with the desired code. It will be uploaded. Since I was unable to view the DoC even after sharing with Hospital1, as that functionality isn't uploaded, otherwise the uploaded doc's script would have run on viewing the doc.

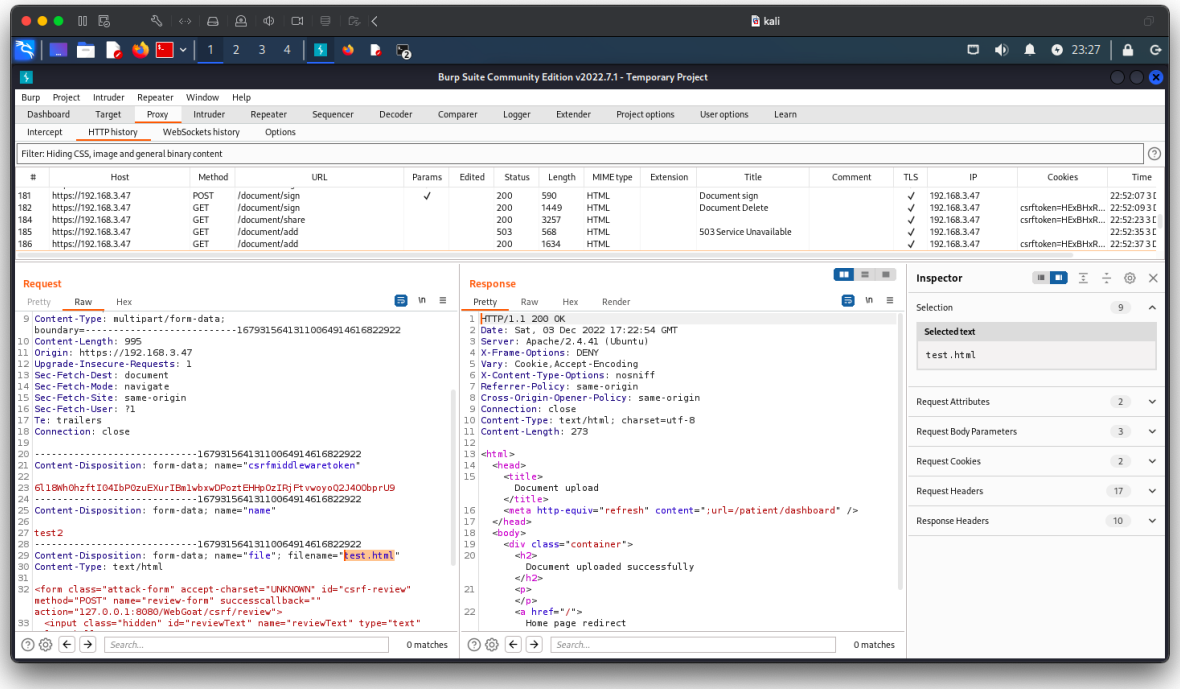
Proof of concept

As shown in BurpSuite screenshot attached, I was able to upload an html file, which would have run (tried on other systems with functionality implemented).

Impact

Uploading an HTML file means an attacker can execute any HTML code and even Javascript code under <script> tag and can get or manipulate a lot of data such as deleting certain files, changing adding links to redirect the users and a lot more.

Screenshots



REPORT 11 (Group 1)

Vulnerability type:

DoS

Steps to reproduce

DoS attack using SlowLoris module of python. Install SlowLoris module and run the command: slowloris -s 6000 -p 443 192.168.3.103 on multiple terminals. Also on port 80

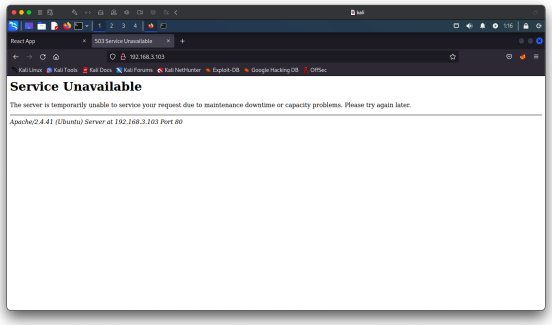
Proof of concept

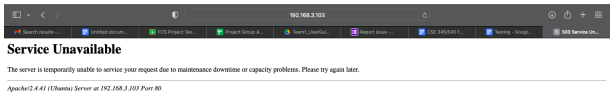
The site becomes unavailable during the attack. Attached screenshots of 2 browsers.

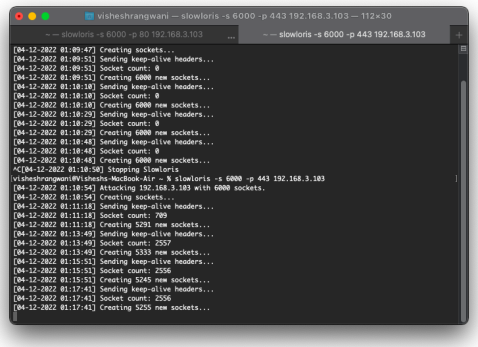
Impact

The site becomes unavailable for legitimate users, hence defeating the purpose of the site.

Screenshots







REPORT 12 (Group 2)

Vulnerability type:

DoS

Steps to reproduce

DoS attack using SlowLoris module of python. Install SlowLoris module and run the command: slowloris -s 6000 -p 443 192.168.2.234 on multiple terminals. Also on port 80

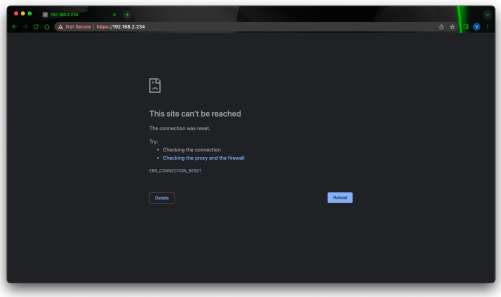
Proof of concept

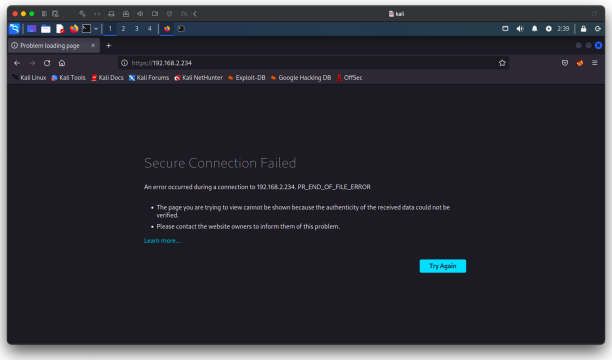
The site becomes unavailable during the attack. Attached screenshots of 2 browsers.

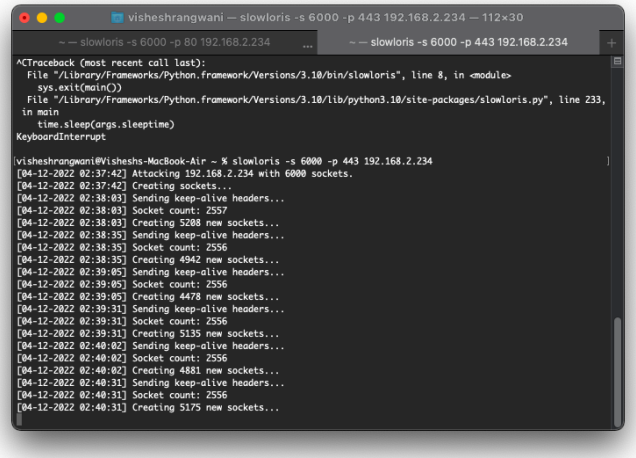
Impact

The site becomes unavailable for legitimate users, hence defeating the purpose of the site.

Screenshots







REPORT 13 (Group 3)

Vulnerability type:

DoS attack using SlowLoris module of python. Install SlowLoris module and run the command: slowloris -s 6000 -p 443 192.168.2.235 on multiple terminals. Also on port 80

Steps to reproduce

Enter amount 0 in Add amount to wallet.
Capture the packet in BurpSuite and modify 1000 to 15000
The change will be reflected in your profile on logging in again

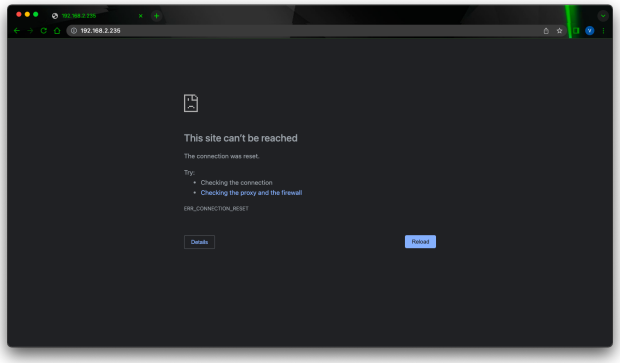
Proof of concept

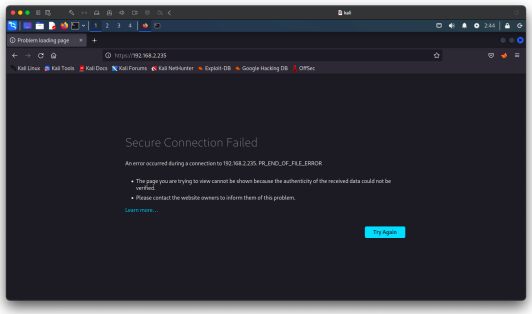
The site becomes unavailable during the attack. Attached screenshots of 2 browsers.

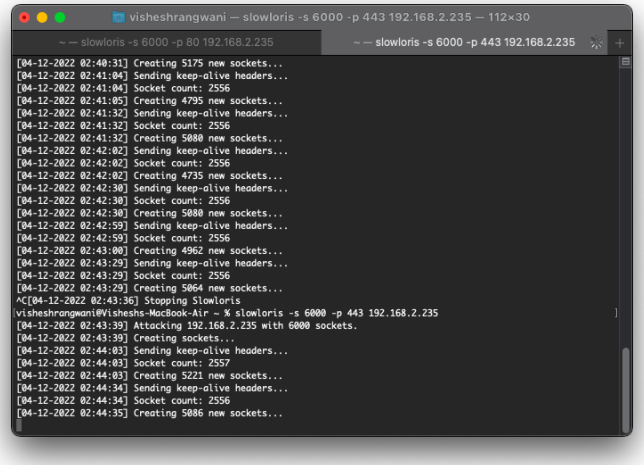
Impact

The site becomes unavailable for legitimate users, hence defeating the purpose of the site.

Screenshots







REPORT 14(Group 4)

Vulnerability type:

DoS

Steps to reproduce

DoS attack using SlowLoris module of python. Install SlowLoris module and run the command: slowloris -s 6000 -p 443 192.168.2.236 on multiple terminals. Also on port 80

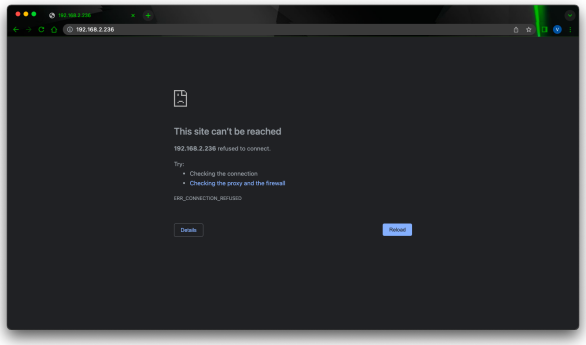
Proof of concept

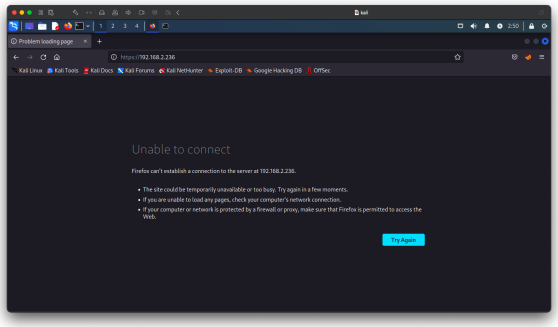
The site becomes unavailable during the attack. Attached screenshots of 2 browsers.

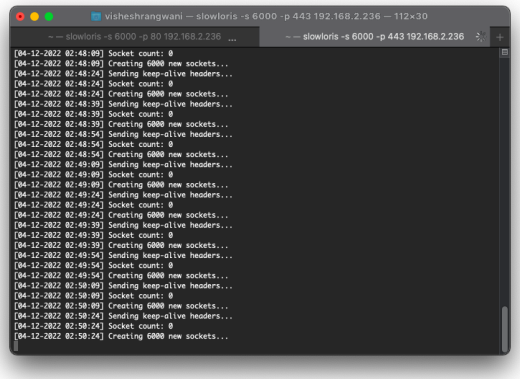
Impact

The site becomes unavailable for legitimate users, hence defeating the purpose of the site.

Screenshots







REPORT 15 (Group 7)

Vulnerability type:

DoS

Steps to reproduce

DoS attack using SlowLoris module of python. Install SlowLoris module and run the command: slowloris -s 6000 -p 443 192.168.2.239 on multiple terminals. Also on port 80

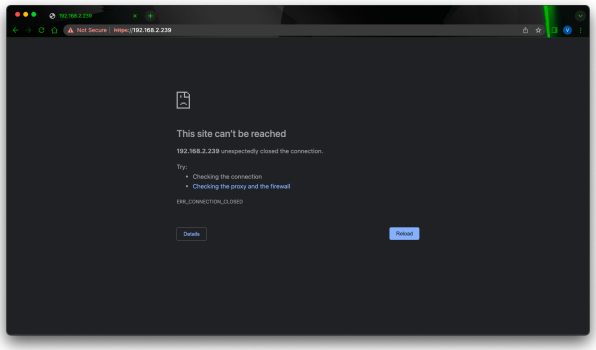
Proof of concept

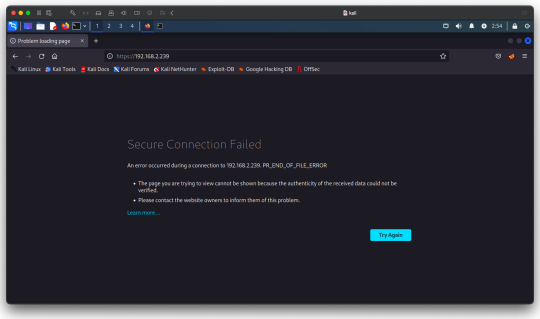
The site becomes unavailable during the attack. Attached screenshots of 2 browsers.

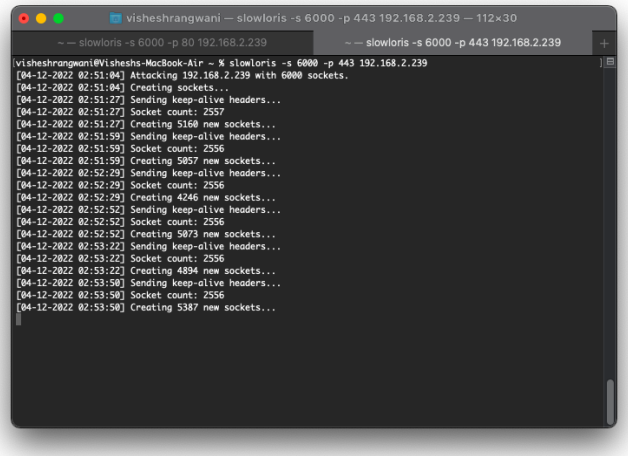
Impact

The site becomes unavailable for legitimate users, hence defeating the purpose of the site.

Screenshots







REPORT 16 (Group 8)

Vulnerability type:

DoS

Steps to reproduce

DoS attack using SlowLoris module of python. Install SlowLoris module and run the command: slowloris -s 6000 -p 443 192.168.2.240 on multiple terminals. Also on port 80

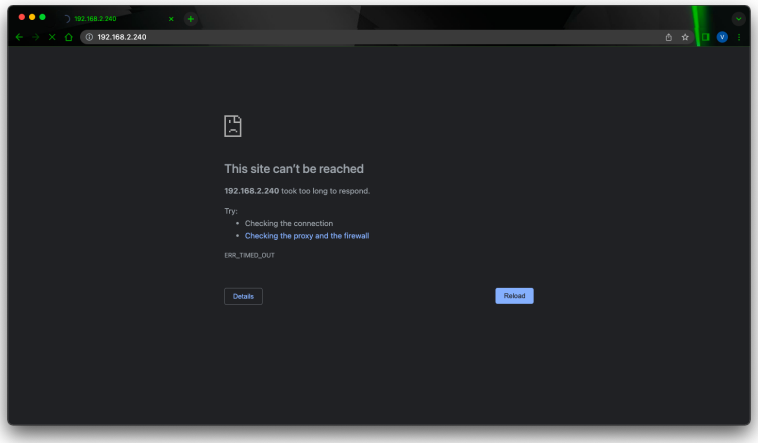
Proof of concept

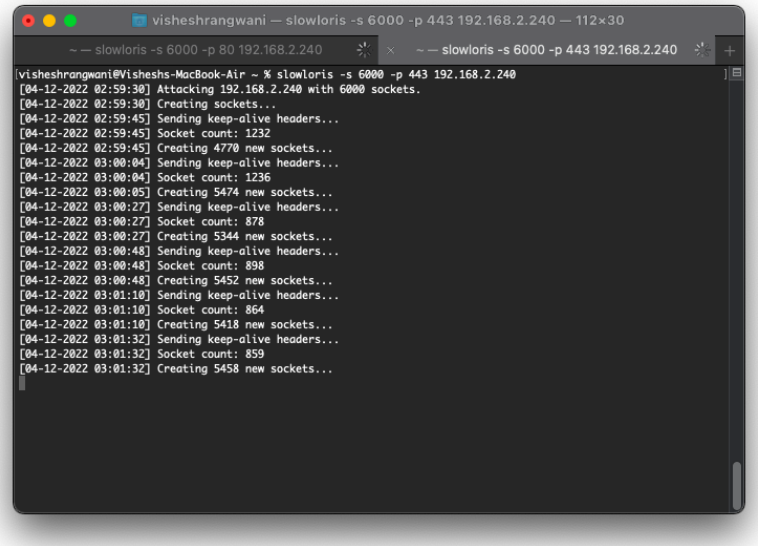
The site becomes unavailable during the attack. Attached screenshots of 2 browsers.

Impact

The site becomes unavailable for legitimate users, hence defeating the purpose of the site.

Screenshots





REPORT 17 (Group 9)

Vulnerability type:

DoS

Steps to reproduce

DoS attack using SlowLoris module of python. Install SlowLoris module and run the command: slowloris -s 6000 -p 443 192.168.2.241 on multiple terminals. Also on port 80

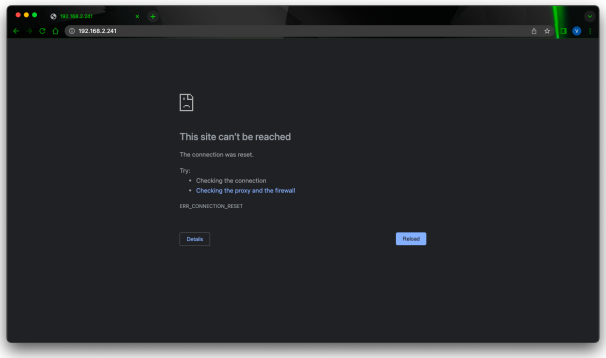
Proof of concept

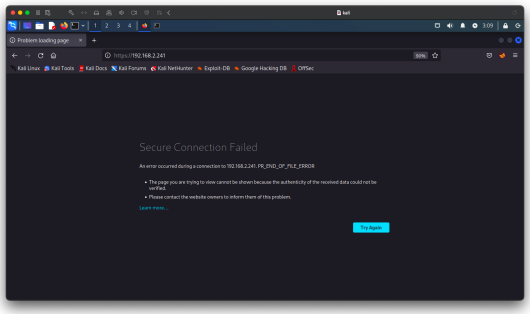
The site becomes unavailable during the attack. Attached screenshots of 2 browsers.

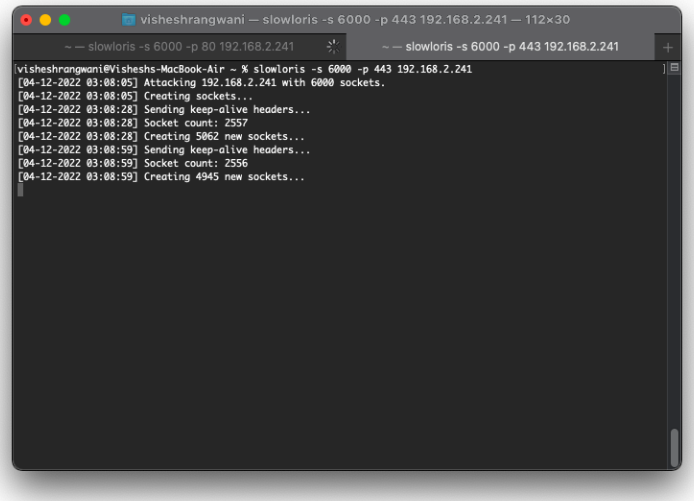
Impact

The site becomes unavailable for legitimate users, hence defeating the purpose of the site.

Screenshots







REPORT 18 (Group 10)

Vulnerability type:

DoS

Steps to reproduce

DoS attack using SlowLoris module of python. Install SlowLoris module and run the command: slowloris -s 6000 -p 80 192.168.2.242 on multiple terminals

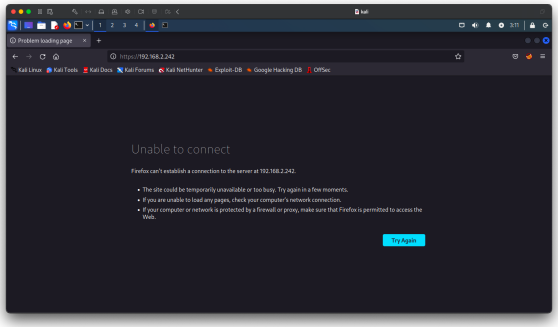
Proof of concept

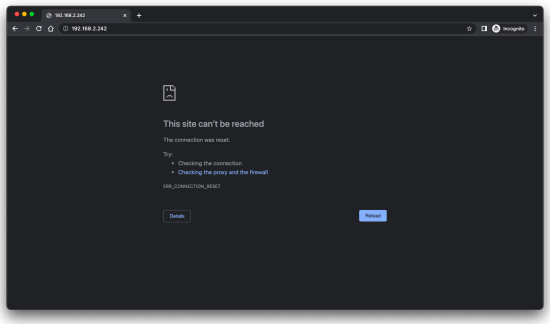
The site becomes unavailable during the attack. Attached screenshots of 2 browsers.

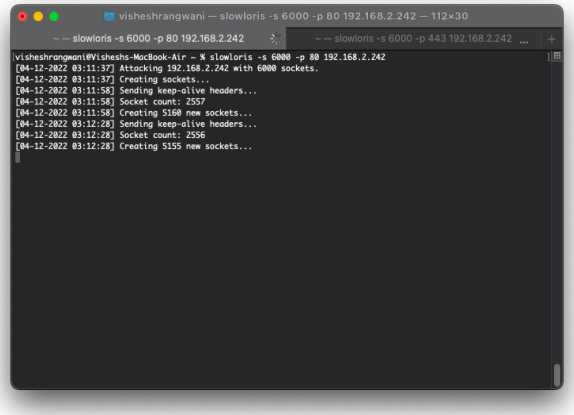
Impact

The site becomes unavailable for legitimate users, hence defeating the purpose of the site.

Screenshots







REPORT 19 (Group 11)

Vulnerability type:

DoS

Steps to reproduce

DoS attack using SlowLoris module of python. Install SlowLoris module and run the command: slowloris -s 6000 -p 443 192.168.2.243 on multiple terminals. Also on port 80

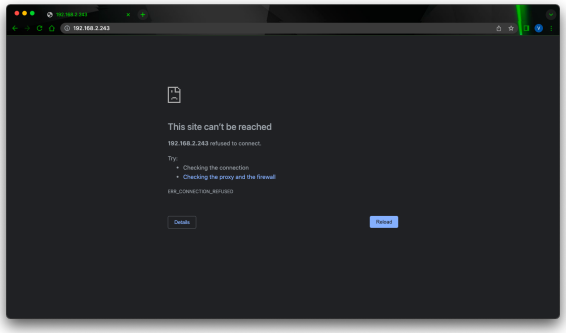
Proof of concept

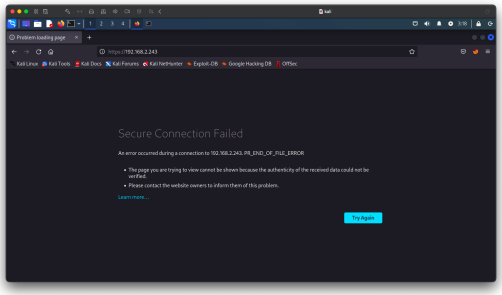
The site becomes unavailable during the attack. Attached screenshots of 2 browsers.

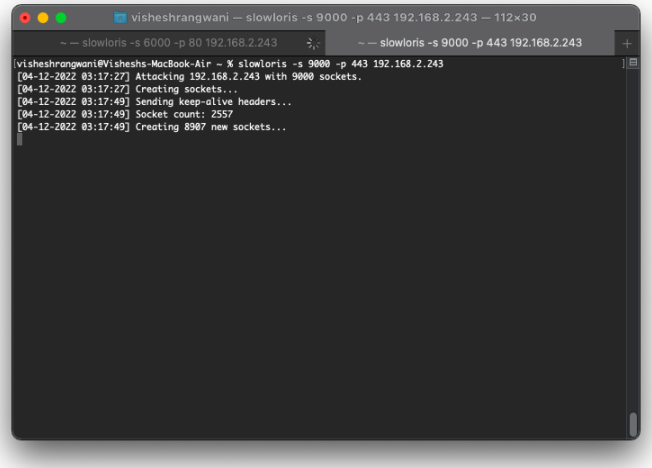
Impact

The site becomes unavailable for legitimate users, hence defeating the purpose of the site.

Screenshots







REPORT 20 (Group 12)

Vulnerability type:

DoS

Steps to reproduce

DoS attack using SlowLoris module of python. Install SlowLoris module and run the command: slowloris -s 9000 -p 443 192.168.2.244 on multiple terminals. Also on port 80

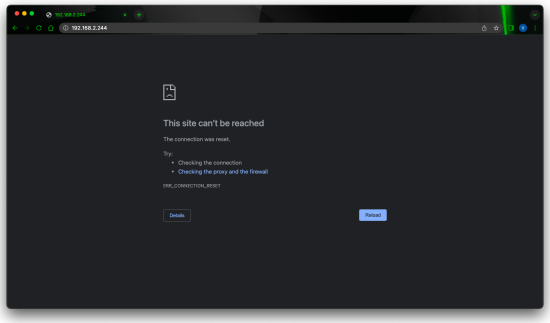
Proof of concept

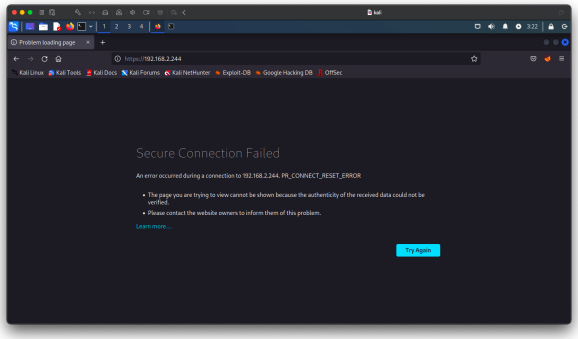
The site becomes unavailable during the attack. Attached screenshots of 2 browsers.

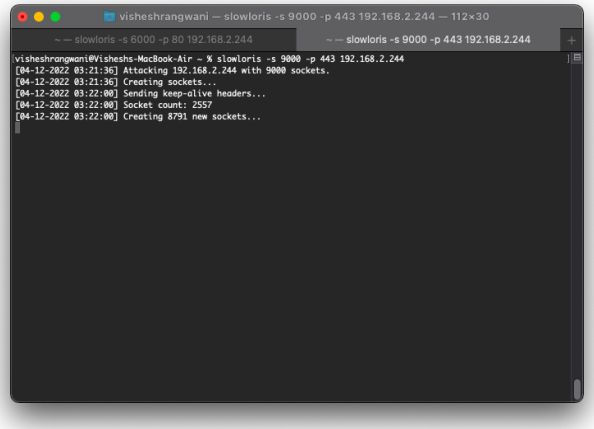
Impact

The site becomes unavailable for legitimate users, hence defeating the purpose of the site.

Screenshots







REPORT 21 (Group 13)

Vulnerability type:

DoS

Steps to reproduce

DoS attack using SlowLoris module of python. Install SlowLoris module and run the command: slowloris -s 9000 -p 443 192.168.2.245 on multiple terminals. Also on port 80

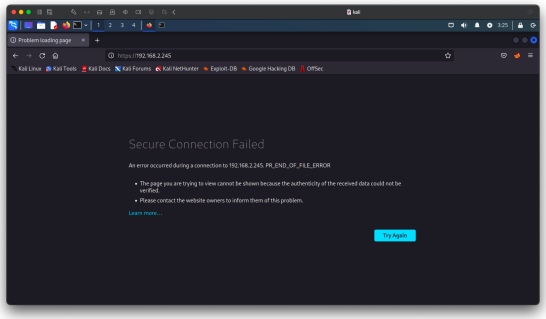
Proof of concept

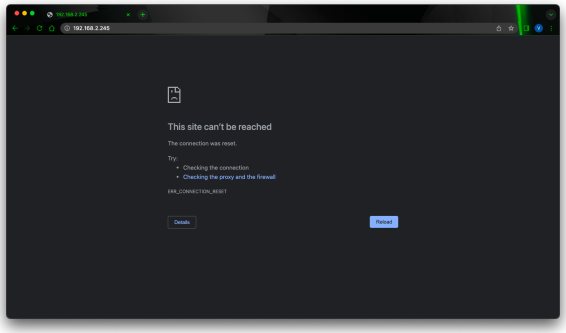
The site becomes unavailable during the attack. Attached screenshots of 2 browsers.

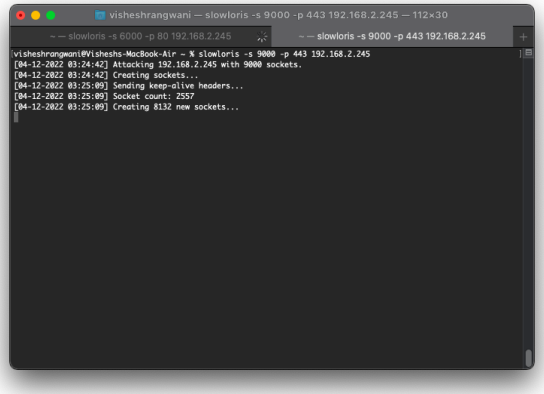
Impact

The site becomes unavailable for legitimate users, hence defeating the purpose of the site.

Screenshots







REPORT 22 (Group 14)

Vulnerability type:

DoS

DoS attack using SlowLoris module of python. Install SlowLoris module and run the command: slowloris -s 9000 -p 443 192.168.2.246 on multiple terminals. Also on port 80

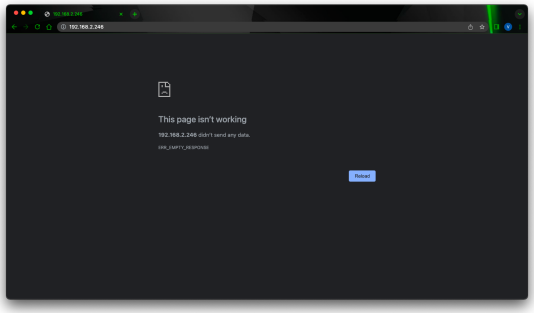
Proof of concept

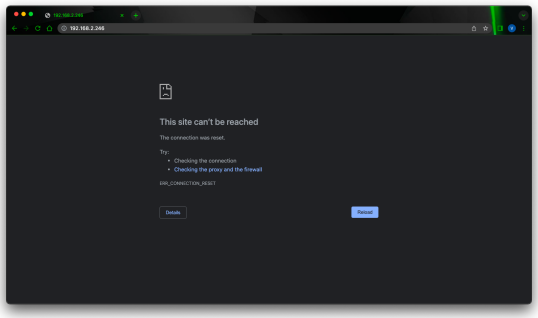
The site becomes unavailable during the attack. Attached screenshots of 2 browsers.

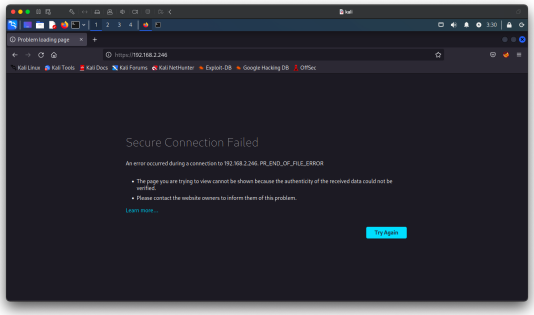
Impact

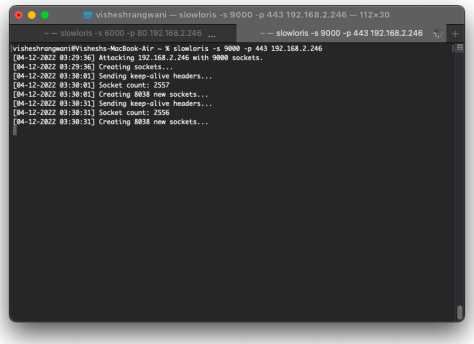
The site becomes unavailable for legitimate users, hence defeating the purpose of the site.

Screenshots









REPORT 23 (Group 15)

Vulnerability type:

DoS

Steps to reproduce

DoS attack using SlowLoris module of python. Install SlowLoris module and run the command: slowloris -s 9000 -p 443 192.168.2.247 on multiple terminals. Also on port 80

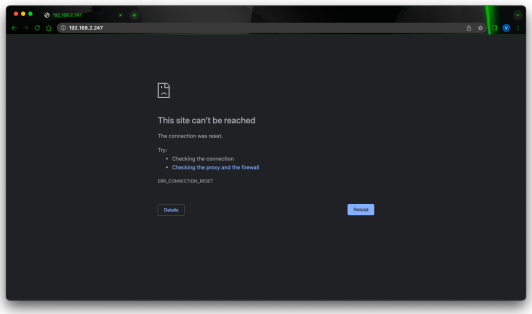
Proof of concept

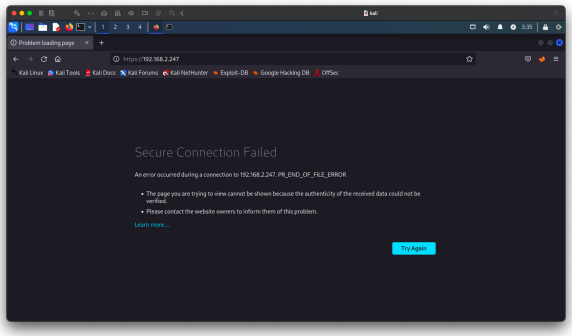
The site becomes unavailable during the attack. Attached screenshots of 2 browsers.

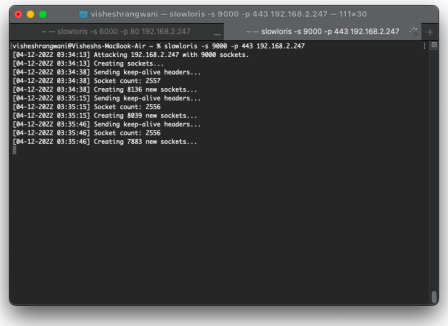
Impact

The site becomes unavailable for legitimate users, hence defeating the purpose of the site.

Screenshots







REPORT 24 (Group 16)

Vulnerability type:

DoS

Steps to reproduce

DoS attack using SlowLoris module of python. Install SlowLoris module and run the command: slowloris -s 9000 -p 443 192.168.2.248 on multiple terminals. Also on port 80

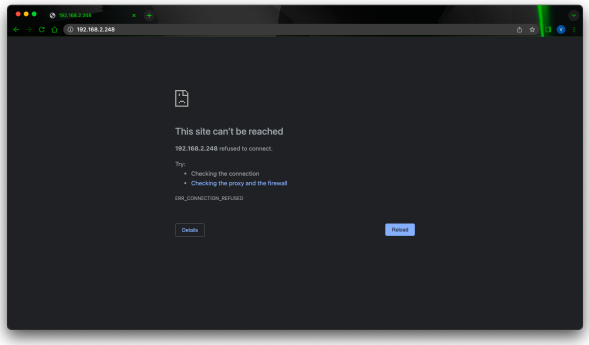
Proof of concept

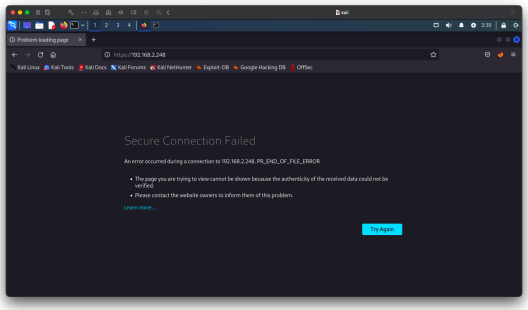
The site becomes unavailable during the attack. Attached screenshots of 2 browsers.

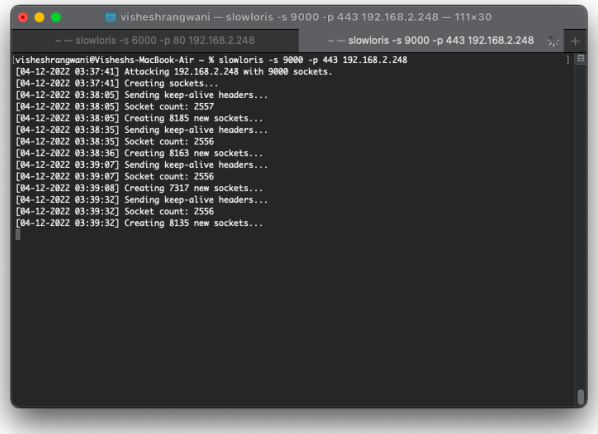
Impact

The site becomes unavailable for legitimate users, hence defeating the purpose of the site.

Screenshots







REPORT 25 (Group 44)

Vulnerability type:

DoS

Steps to reproduce

DoS attack using SlowLoris module of python. Install SlowLoris module and run the command: slowloris -s 6000 -p 80 192.168.3.113 on multiple terminals.

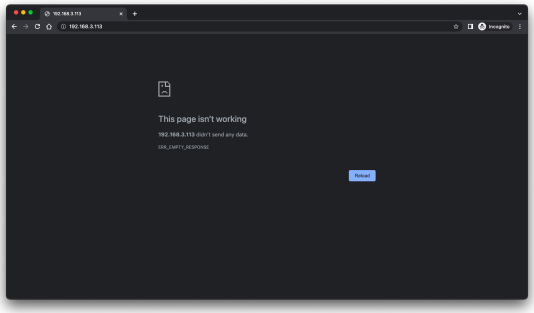
Proof of concept

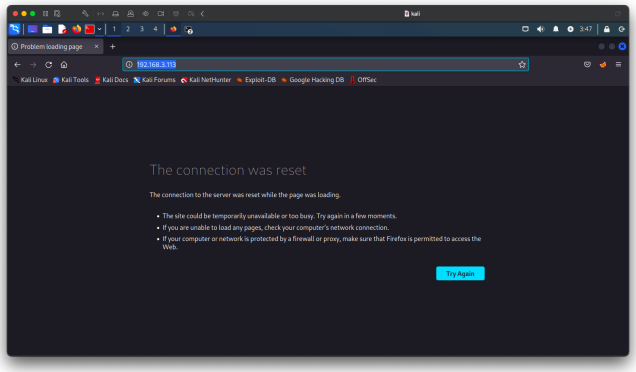
The site becomes unavailable during the attack. Attached screenshots of 2 browsers.

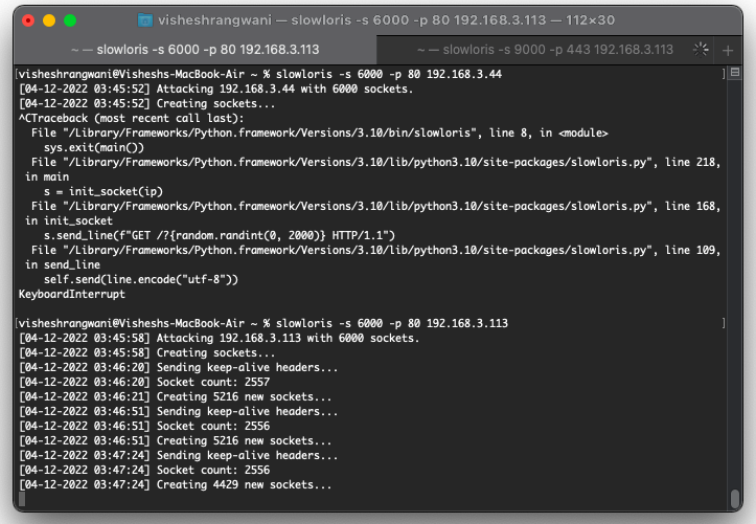
Impact

The site becomes unavailable for legitimate users, hence defeating the purpose of the site. Although site isn't even made, just Nginx home page is there

Screenshots







REPORT 26 (Group 20)

Vulnerability type:

DoS

Steps to reproduce

DoS attack using SlowLoris module of python. Install SlowLoris module and run the command: slowloris -s 9000 -p 443 192.168.3.38 on multiple terminals. Also on port 80

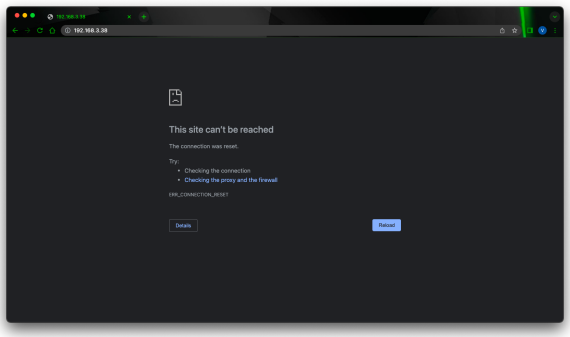
Proof of concept

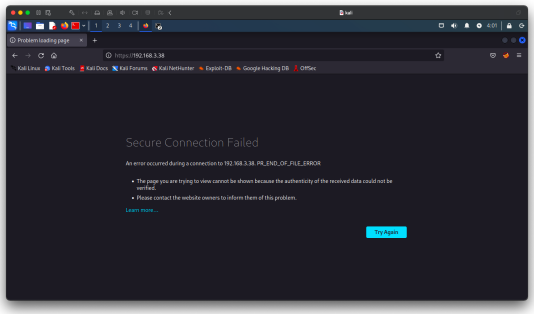
The site becomes unavailable during the attack. Attached screenshots of 2 browsers.

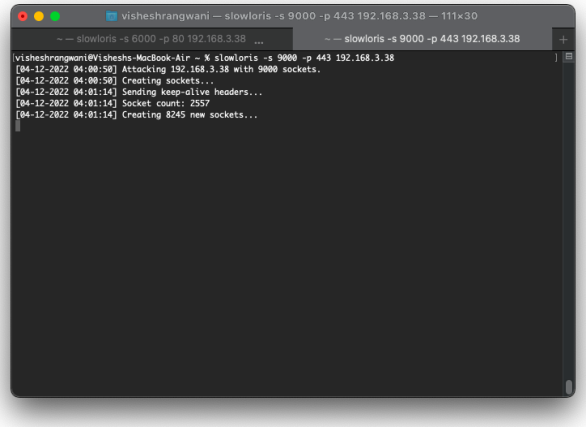
Impact

The site becomes unavailable for legitimate users, hence defeating the purpose of the site.

Screenshots







REPORT 27 (Group 42)

Vulnerability type:

Feature Bug

Steps to reproduce

Sign up as a new patient, approve using given admin credentials and then try to login with that. Even try to login with given credentials of patient. See from admin page, no OTP functionality

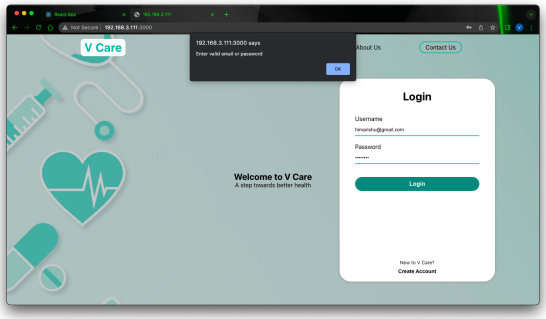
Proof of concept

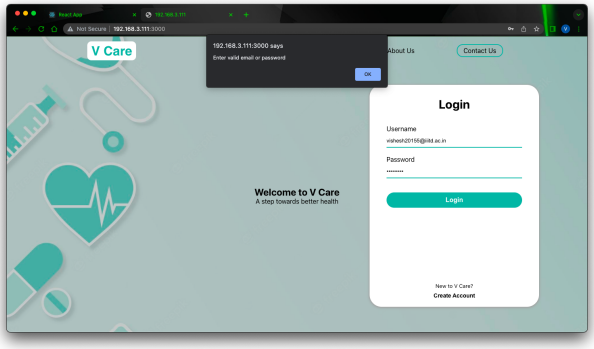
I tried to create a new user, and approve it using the given admin credentials and then login using that, I was unable to login and it said invalid user or password. Even the given user guide's patient was unable to login. Moreover, from admin and hospital page, I could not see an OTP functionality. I think the approve button doesn't work

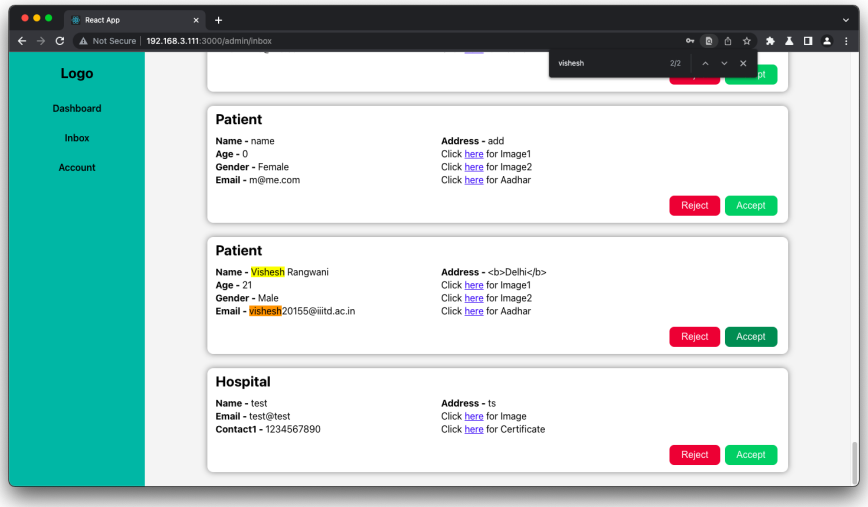
Impact

Unable to login as patient means, patient functionality of the website isn't supported. No OTP means no 2 layer of security and higher risk.

Screenshots







REPORT 28 (Group 20)

Vulnerability type:

CSRF

Steps to reproduce

Try to change the name or any other parameter from edit profile option. When it changes successfully, capture its packet in BurpSuite. Then in the payload of POST request, change the parameters by adding html code.

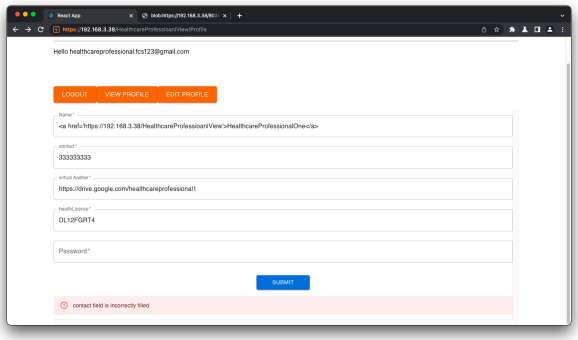
Proof of concept

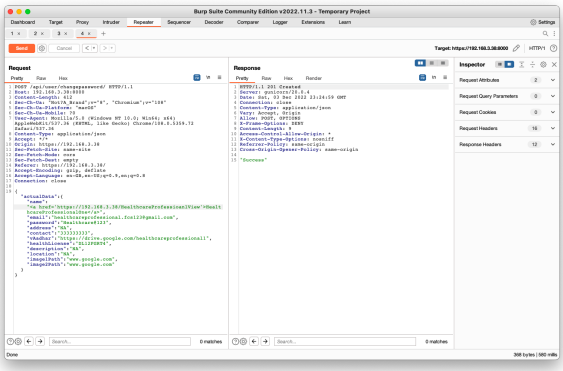
On the given 1st healthcare professional, I have added a redirection to the Hospital's login page using anchor <a> tag. in BurpSuite.

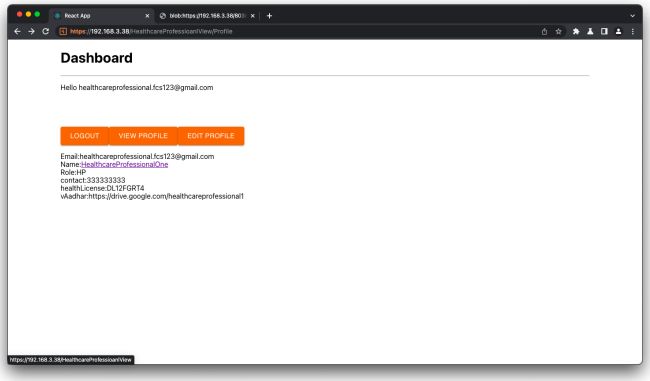
Impact

One can add redirection to any malicious page as well which can be very harmful.

Screenshots







REPORT 29 (Group 40)

Vulnerability type:

CSRF

Steps to reproduce

Sign in with username: Doctor1 passed: Vishesh@1
Try upload a prescription as an HTML document. You will be upload it.

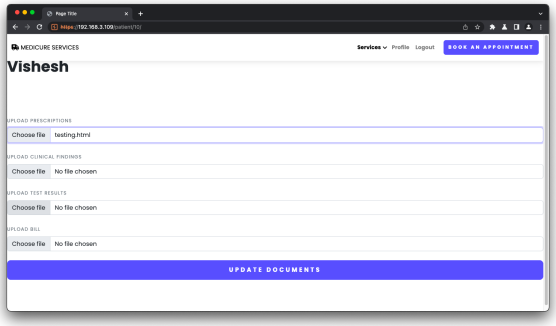
Proof of concept

I uploaded it with a simple HTML file attached here. Although HTML script couldn't be open as it's a feature bug as well. However, if it would run, I would have run HTML code. In the Screenshot, we can also see that the doc can be seen by the patient. Since no docs are uploaded on Database, I can't see that but if it functionality were implemented, it would have been bad.

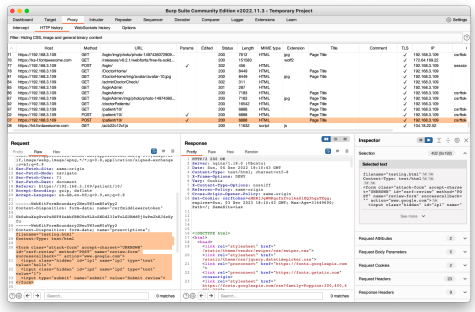
Impact

An HTML code creatively made can maybe redirect the legitimate user or even cause other malicious action such as deleting files, etc.

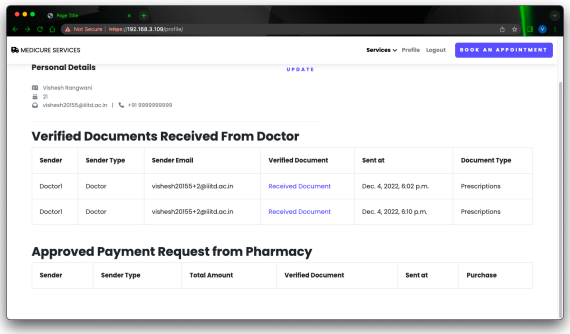
Screenshots



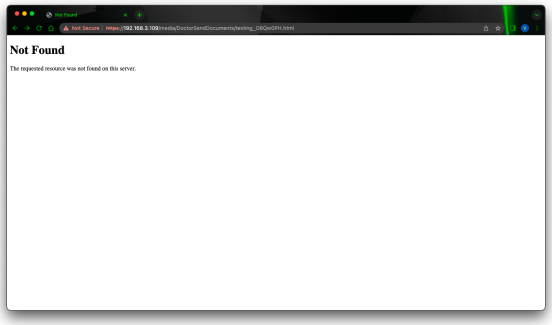
Doc uploading html file



Successfully Uploaded



File visible to patient



Patient can even open it

REPORT 30 (Group 40)

Vulnerability type:

Feature Bug

Steps to reproduce

Upload doc(pdf) by sharing with Vishesh patient. Uploaded by doctor.
username: Doctor1 passwd: Vishesh@1
It will show in Vishesh's profile
username: vishesh passwd: Vishesh@1
You'll see the doc, but won't be able to see it.

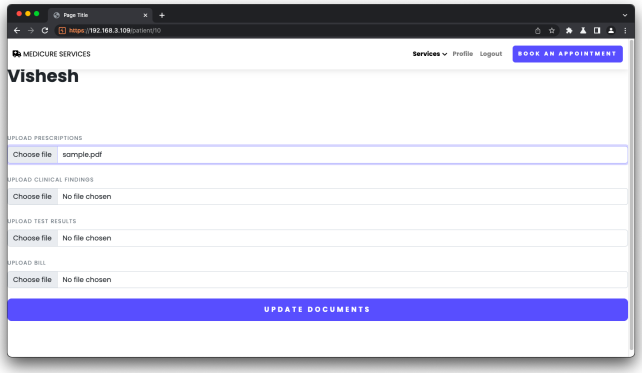
Proof of concept

Added screenshot that doc is shared by doctor to patient but is not stored in database. Hence patient can't view it.

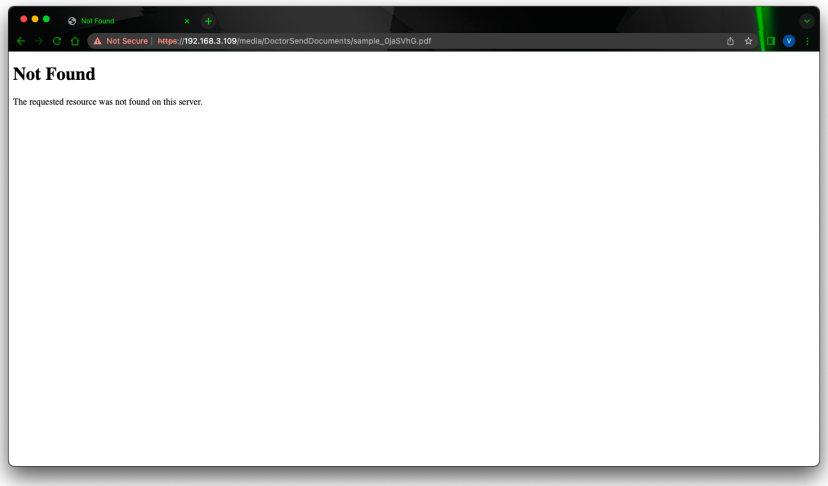
Impact

Sharing of document functionality not working from doctor to patient

Screenshots



Doc uploaded



Patient can’t see document

REPORT 31 (Group 44)

Vulnerability type:

Feature Bug

Steps to reproduce

Try to open website

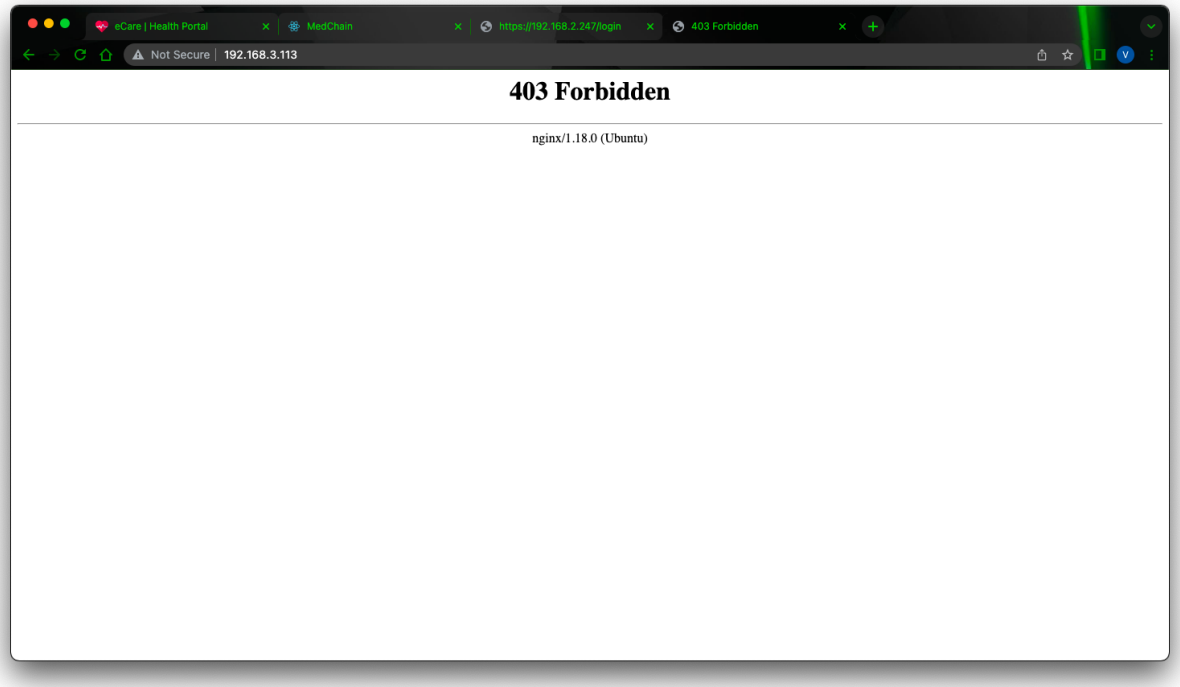
Proof of concept

The website was unavailable in the entire testing period.

Impact

Unavailable website for all users.

Screenshots



REPORT 32 (Group 9)

Vulnerability type:

Feature Bug

Steps to reproduce

Login.
Sample email id for patient: vishesh20155+5@iiitd.ac.in
password: Vishesh@1

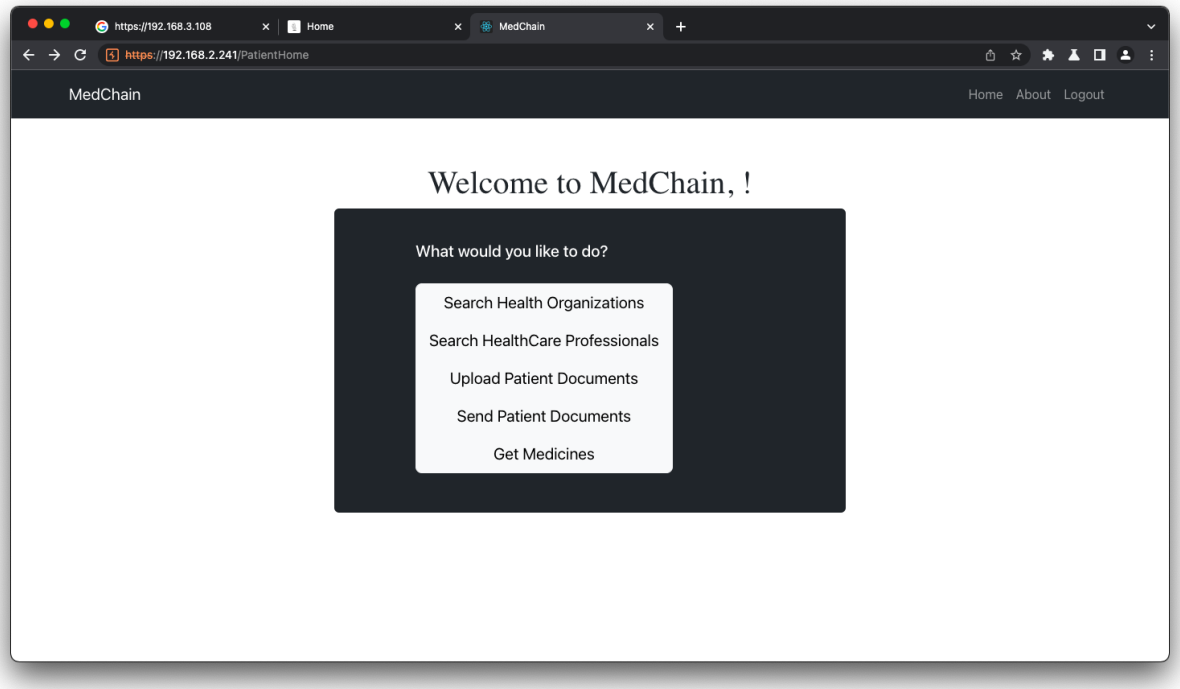
Proof of concept

No payment portal

Impact

Payments not implemented

Screenshots



REPORT 33 (Group 9)

Vulnerability type:

Feature Bug

Steps to reproduce

After logging in try to submit documents. No option to upload.

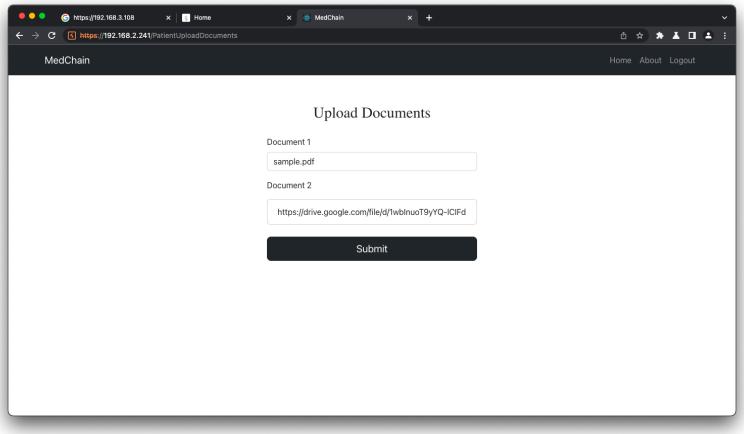
Proof of concept

I tried to add drive link as well as some name, 'sample.pdf', but showed error (404) in BurpSuite

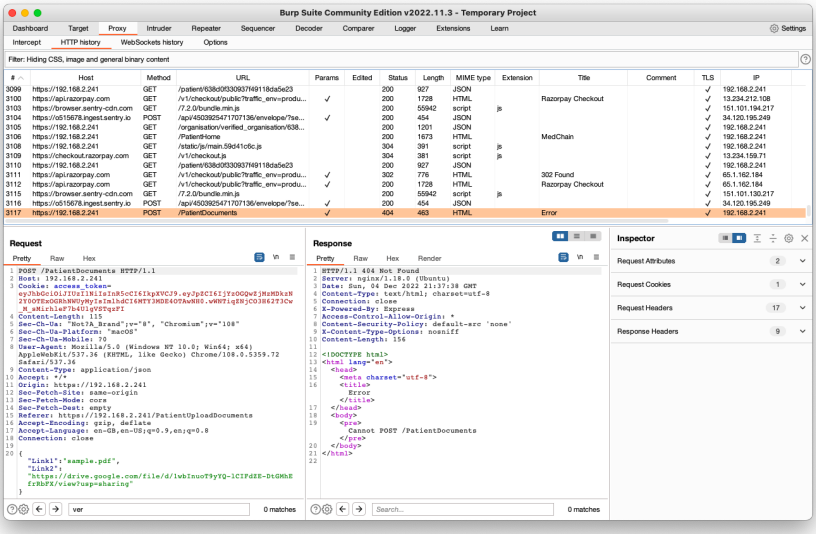
Impact

No functionality of uploading and sharing documents

Screenshots



Trying to upload



Cannot upload. Error 404

REPORT 34 (Group 31)

Vulnerability type:

Feature Bug

Steps to reproduce

Just visit the website

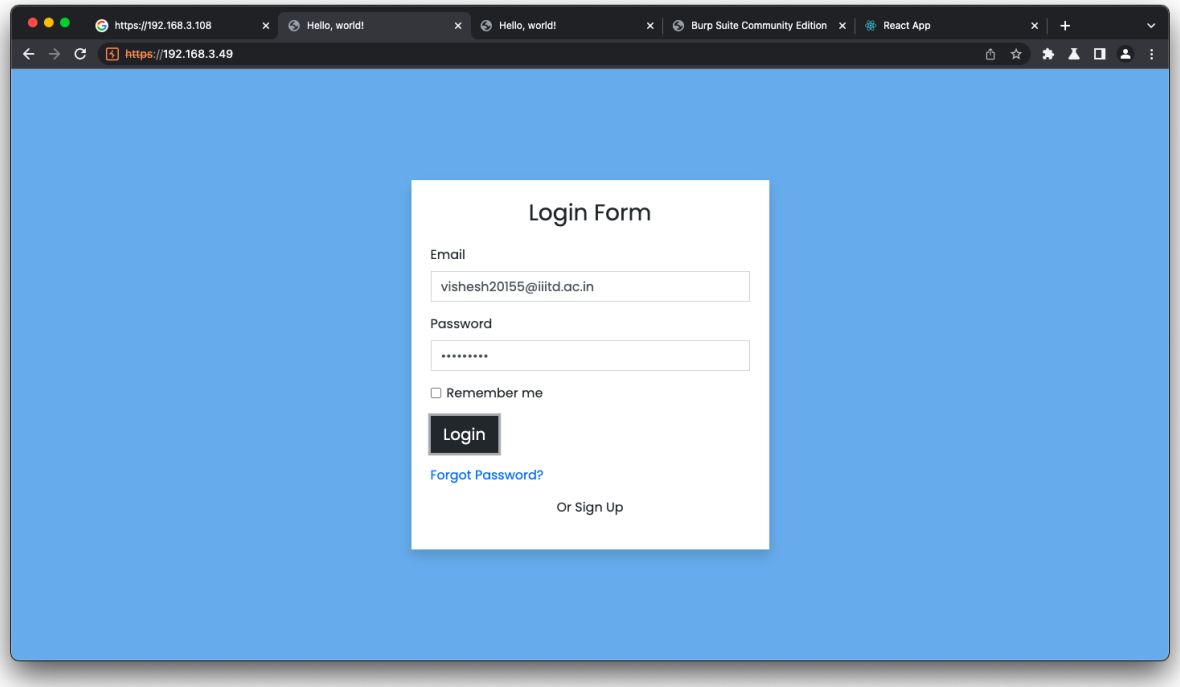
Proof of concept

No functionality working, not even Login is working

Impact

Nothing implemented

Screenshots



REPORT 35 (Group 37)

Vulnerability type:

Feature Bug

Steps to reproduce

Try to login with given admin credentials to approve the user. Also on logging in with any newly rergistered account, no functionality of OTP

Proof of concept

Unable to login with admin credentials, hence no feature can be used. Admin not created.
OTP is also nowhere implemented in registering and logging in with user.

Impact

Admin not implemented hence no user and document verification. No functionality can be used of the system with newly created users.
No OTP means unsecure system and no 2 factor authentication.

Screenshots