SECURITY ASSESSMENT

RANJITHA MANJUNATH

Submitted to: Development Team
Security Analyst: Security Analyst Team

Date of Testing: 03/18/2021
Date of Report Delivery: 03/19/2021

Table of Contents

Contents

Security Engagement Summary

Engagement Overview

The company Development team has requested the Vulnerability assessment from the security Analyst for better understanding of security risks in the web-application developed and also the understanding of risks which will be posing to the organization.

The main goal of this engagement by the development team is for the better understanding of security risks associated with the web-application and what security risk the web application is posing to the organization. Also, they wanted to understand what mitigations are possible to increase the security posture and reduce risk to the organization.

The engagement is completed by the Security analyst with proper information provided by the developmet team.

The assessment should be carried out once per quarter.

Scope

The systematic review of security weakness of the application developed is must necessary for the application to be secure.

The vulnerability report or assessment gives an idea on how secure system is and how we can make our application more stable. The application developed

The development team have developed an application before we market the software it is essential for the company to be aware of the security vulnerability.

Executive Risk Analysis

The risk of vulnerability listed in Executive Summary gives the overall risk. We can work on the highest priority first and consider the low-risk vulnerability later.

The risk levels were indicated to indicate if there are any immediate security risk so that we can work the solution as soon as possible to secure our data.

The executive summary form has been attached here for complete explanation:

Executive Recommendation

The Executive Summary form describes in brief the remediation effort. We have a medium risk which should be remediated first. The solution is described below.

Executive report:

Assessment Date:

03/18/2021

Report Date

03/18/2021

Prepared By:

Ranjitha Manjunath

Executive Board

Development Team

Notable Risk

Infomational,Medium,Low

PURPOSE/SCOPE

The development team have developed an application before we market the software it is essential for the company to be aware of the security vulnerability.

SYSTEM DESCRIPTION

The main goal of this engagement by the development team is for the better understanding of security risks associated with the web-application and what security risk the web application is posing to the organization. Also, they wanted to understand what mitigations are possible to increase the security posture and reduce risk to the organization.

PROBLEM/OPPORTUNITY

Vulnerability 1: Risk: Medium

Cross-Domain misconfiguration

Vulnerability 2: Risk: Low

Cross-Domain Javascript Source File Inclusion

Vulnerability 3: Risk: Informational

Information Disclosure – Suspicious Comments

Vulnerability 4: Risk: Informational

Time stamp Disclosure

SOLUTION/PRODUCT

Solution to Vulnerability 1:

Use Ip-whitelisting, making sure the data is unavailable in unauthenticated manner. The Access-Control-Allow-Origin HTTP header should be configured to restrictive set of domains.

Solution to Vulnerability 2:

Ensure JavaScript source files are loaded from only trusted sources. Also, make sure the sources can’t be controlled by end users of the application.

Solution to Vulnerability 3:

Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

Solution to Vulnerability 4:

Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

POTENTIAL IMPACTS

With the solutions provide we can have a secure application where there will be secure transmission of data and no unauthorized third-party interactions.

By not taking the preventive measure we could be exposed to Information like personal or unauthorized data exposure

EXECUTION PLAN

The recommended action would be to work according to the risk level and mitigate the issue as solution is provided above.

Significant Vulnerability Summary

High Risk Vulnerabilities

- NO VULNERABILITY

Medium Risk Vulnerabilities

- CROSS DOMAIN MISCONFIGURATION

Low Risk Vulnerabilities

- CROSS DOMAIN JAVASCRIPT SOURCE FILE INCLUSION

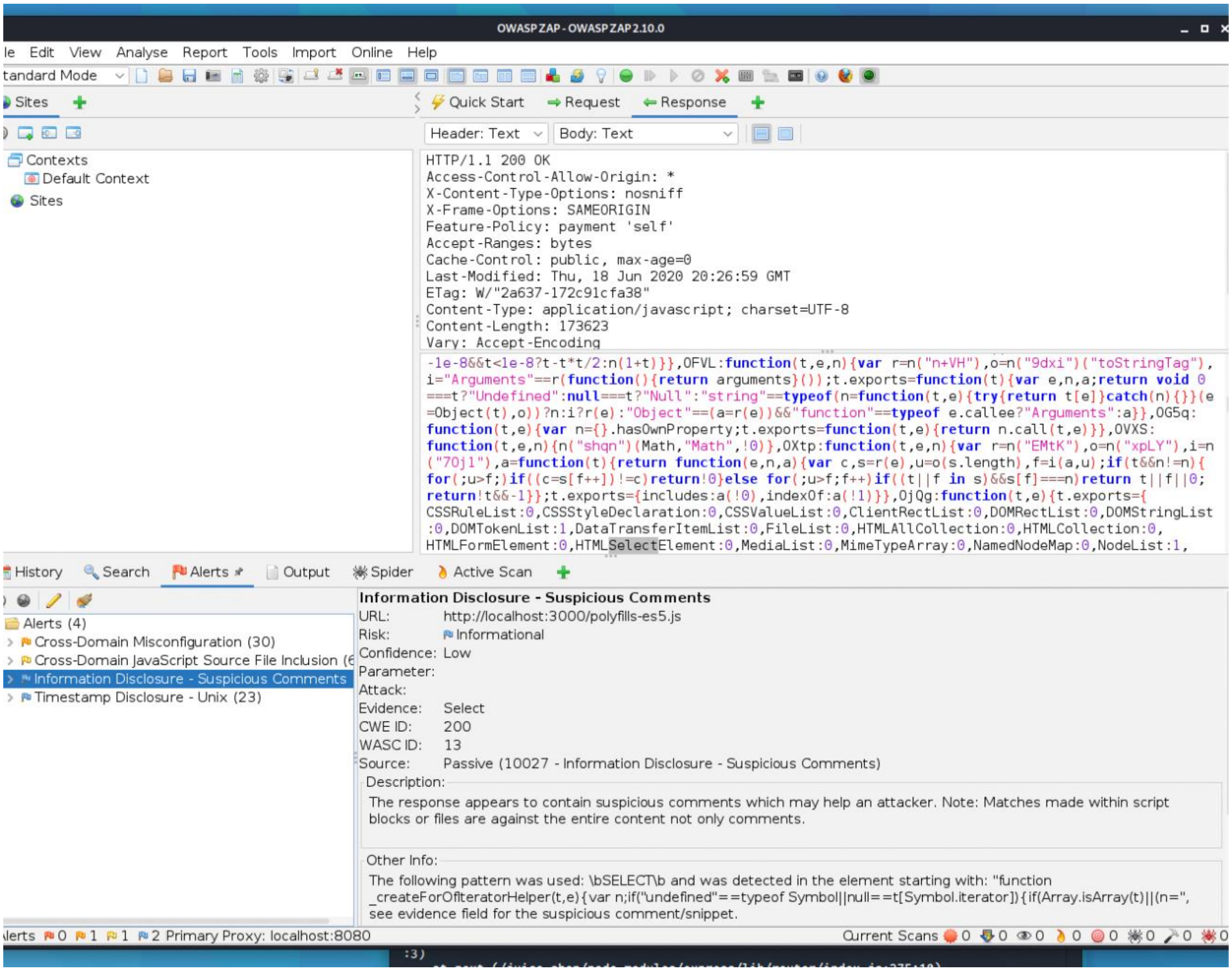
Significant Vulnerability Detail

Information Disclosure – Suspicious Comments

Informational Risk

Vulnerability detail

- The Vulnerability has Informational risk.
- The vulnerability was found following a pattern: **\bSELECT\b** and detected in the element starting with: **“function_createForOfIteratorHelper(t,e){var n;if(“undefined”==typeof Symbol|null==t[Symbol.Iterator]){id(Array.isArray(t)|(n=”**, see evidence field for the suspicious comment.
- The probability of exploit is not high as we can remove the comments which leads information for the attacker.
- This won’t affect anyone as this is just informational.
- Solution is to remove all comments that return information for the attacker and fix any underlying problems they refer to.


OWASP ZAP - OWASP ZAP 2.10.0
le Edit View Analyse Report Tools Import Online Help
tandard Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Text
Contexts
Default Context
Sites
History
Search
Alerts
Output
Spider
Active Scan
Alerts (4)
Cross-Domain Misconfiguration (30)
Cross-Domain JavaScript Source File Inclusion (6
Information Disclosure - Suspicious Comments
Timestamp Disclosure - Unix (23)
lerts 0 1 1 2 Primary Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Thu, 18 Jun 2020 20:26:59 GMT
ETag: W/"2a637-172c91cfa38"
Content-Type: application/javascript; charset=UTF-8
Content-Length: 173623
Vary: Accept-Encoding
```

```
-1e-8&&t<1e-8?t-t*t/2:n(1+t)}},OFVL:function(t,e,n){var r=n("n+VH"),o=n("9dxi")("toStringTag"),
i="Arguments"==r(function(){return arguments}());t.exports=function(t){var e,n,a;return void 0
===t?"Undefined":null===t?"Null":"string"==typeof(n=function(t,e){try{return t[e]}catch(n){}}(e
=Object(t),o))?n:i?r(e):"Object"==(a=r(e))&&"function"==typeof e.callee?"Arguments":a}},OG5q:
function(t,e){var n={}.hasOwnProperty;t.exports=function(t,e){return n.call(t,e)}},OVXS:
function(t,e,n){n("shqn")(Math,"Math",!0)},OXtp:function(t,e,n){var r=n("EMtK"),o=n("xpLY"),i=n
("70j1"),a=function(t){return function(e,n,a){var c,s=r(e),u=o(s.length),f=i(a,u);if(t&&n!=n){
for(;u>f;)if((c=s[f++])!=c)return!0}else for(;u>f;f++)if((t||f in s)&&s[f]===n)return t||f||0;
return!t&&-1}};t.exports={includes:a(!0),indexOf:a(!1)}},OjQg:function(t,e){t.exports={
CSSRuleList:0,CSSStyleDeclaration:0,CSSValueList:0,ClientRectList:0,DOMRectList:0,DOMStringList
:0,DOMTokenList:1,DataTransferItemList:0,FileList:0,HTMLAllCollection:0,HTMLCollection:0,
HTMLFormElement:0,HTMLSelectElement:0,MediaList:0,MimeTypeArray:0,NamedNodeMap:0,NodeList:1,
```

Information Disclosure - Suspicious Comments

URL: http://localhost:3000/polyfills-es5.js
Risk: Informational
Confidence: Low
Parameter:
Attack:
Evidence: Select
CWE ID: 200
WASC ID: 13
Source: Passive (10027 - Information Disclosure - Suspicious Comments)

Description:

The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Other Info:

The following pattern was used: \bSELECT\b and was detected in the element starting with: "function _createForOfIteratorHelper(t,e){var n;if("undefined"==typeof Symbol||null==t[Symbol.iterator]){if(Array.isArray(t)||(n=", see evidence field for the suspicious comment/snippet.

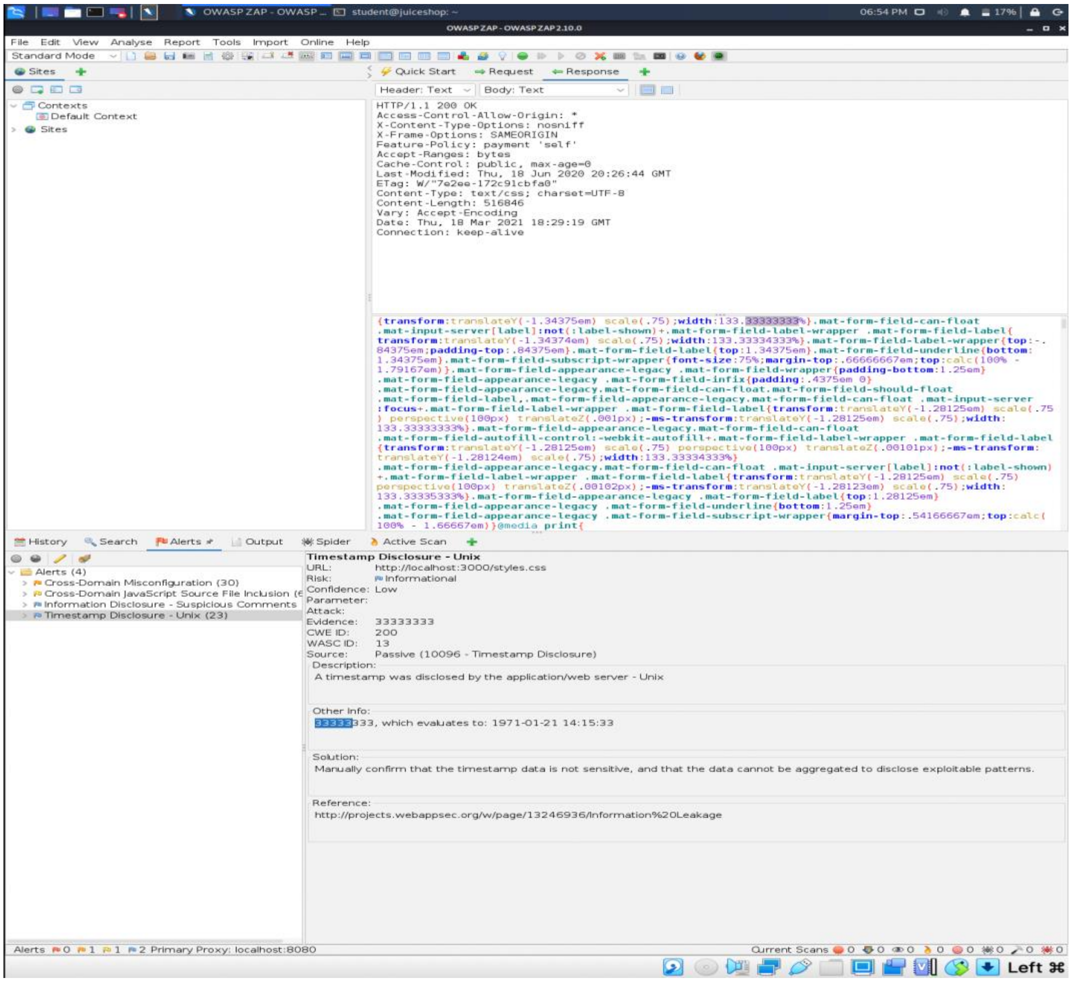
Timestamp Disclosure - Unix(23)

Informational Risk

<<

Vulnerability detail

- The Vulnerability has Informational risk.
- The timestamp was disclosed by application/web server – Unix. The Evidence was identified when 33333333, which evaluates to: 1971-01-21 14:15:33
- Discuss the probability of exploit/attack.
- The probability of this risk is not high.
- This won’t affect anyone as this is just informational.
- Remediation is to manually confirm that the timestamp data is not sensitive,and that the data cannot be aggregated to disclose exploitable patterns.



```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Thu, 18 Jun 2020 20:26:44 GMT
ETag: W/"7e2ee-172c91cbfa0"
Content-Type: text/css; charset=UTF-8
Content-Length: 516846
Vary: Accept-Encoding
Date: Thu, 18 Mar 2021 18:29:19 GMT
Connection: keep-alive
```

```
{transform:translateY(-1.34375em) scale(.75);width:133.33333333%}.mat-form-field-can-float
.mat-input-server[label]:not(:label-shown)+.mat-form-field-label-wrapper .mat-form-field-label{
transform:translateY(-1.34374em) scale(.75);width:133.33334333%}.mat-form-field-label-wrapper{top:-.
84375em;padding-top:.84375em}.mat-form-field-label{top:1.34375em}.mat-form-field-underline{bottom:
1.34375em}.mat-form-field-subscript-wrapper{font-size:75%;margin-top:.66666667em;top:calc(100% -
1.79167em)}.mat-form-field-appearance-legacy .mat-form-field-wrapper{padding-bottom:1.25em}
.mat-form-field-appearance-legacy .mat-form-field-infix{padding:.4375em 0}
.mat-form-field-appearance-legacy.mat-form-field-can-float.mat-form-field-should-float
.mat-form-field-label,.mat-form-field-appearance-legacy.mat-form-field-can-float .mat-input-server
:focus+.mat-form-field-label-wrapper .mat-form-field-label{transform:translateY(-1.28125em) scale(.75
) perspective(100px) translateZ(.001px);-ms-transform:translateY(-1.28125em) scale(.75);width:
133.33333333%}.mat-form-field-appearance-legacy.mat-form-field-can-float
.mat-form-field-autofill-control:-webkit-autofill+.mat-form-field-label-wrapper .mat-form-field-label
{transform:translateY(-1.28125em) scale(.75) perspective(100px) translateZ(.00101px);-ms-transform:
translateY(-1.28124em) scale(.75);width:133.33334333%}
.mat-form-field-appearance-legacy.mat-form-field-can-float .mat-input-server[label]:not(:label-shown)
+.mat-form-field-label-wrapper .mat-form-field-label{transform:translateY(-1.28125em) scale(.75)
perspective(100px) translateZ(.00102px);-ms-transform:translateY(-1.28123em) scale(.75);width:
133.33335333%}.mat-form-field-appearance-legacy .mat-form-field-label{top:1.28125em}
.mat-form-field-appearance-legacy .mat-form-field-underline{bottom:1.25em}
.mat-form-field-appearance-legacy .mat-form-field-subscript-wrapper{margin-top:.54166667em;top:calc(
100% - 1.66667em)}@media print{
```

- Alerts (4)
  - Cross-Domain Misconfiguration (30)
  - Cross-Domain JavaScript Source File Inclusion (6
  - Information Disclosure - Suspicious Comments
  - Timestamp Disclosure - Unix (23)

Timestamp Disclosure - Unix

URL: http://localhost:3000/styles.css
Risk: Informational
Confidence: Low
Parameter:
Attack:
Evidence: 33333333
CWE ID: 200
WASC ID: 13
Source: Passive (10096 - Timestamp Disclosure)

Description:
A timestamp was disclosed by the application/web server - Unix

Other Info:
33333333, which evaluates to: 1971-01-21 14:15:33

Solution:
Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

Reference:
http://projects.webappsec.org/w/page/13246936/Information%20Leakage

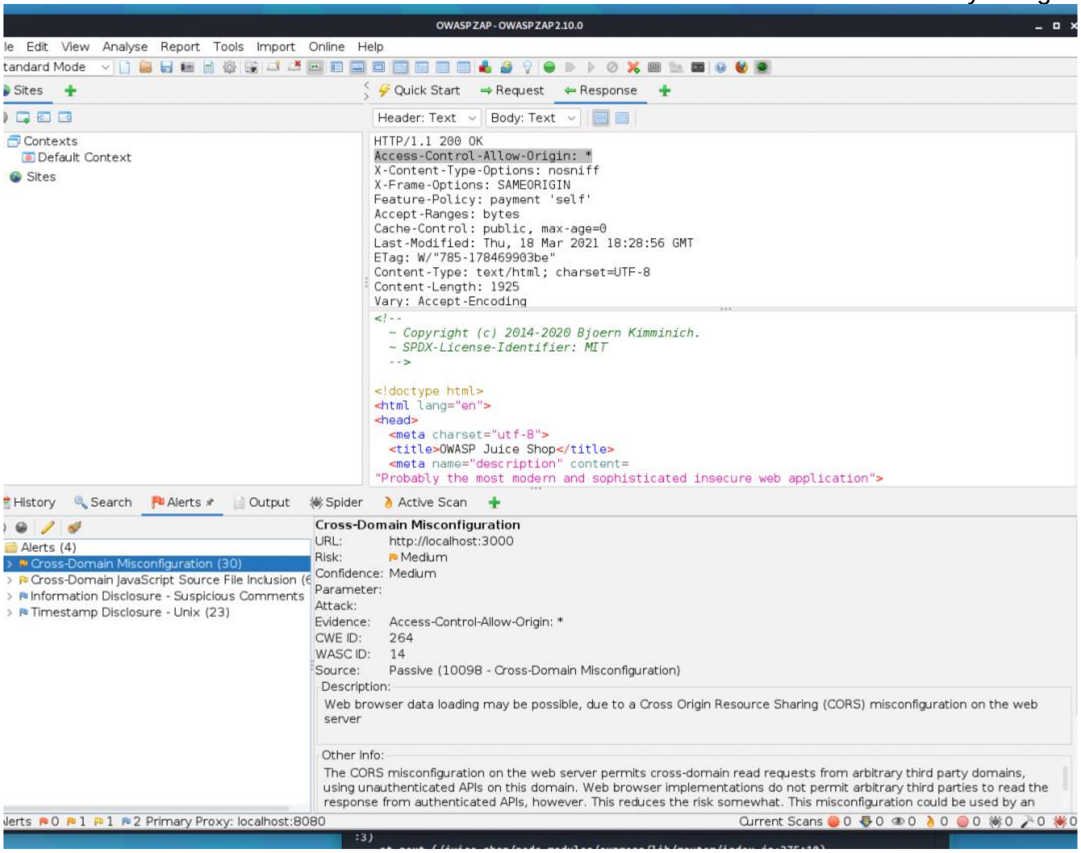
Alerts 0 1 1 2 Primary Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0

Cross Domain Misconfiguration(30)

Medium

Vulnerability detail

- The Vulnerability has Medium risk.
- The CORS misconfiguration on the webserver permits cross domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web server implementations don’t permit arbitrary third parties to read the response from authenticated APIs.
- The probability of exploit is medium. The vulnerability should be taken care as soon as possible.
- The departments and Company will be affected much from this as the domain will be cross configured.
- Solution is to ensure sensitive data is unavailable in an unauthenticated manner by using IP address white listing



```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Thu, 18 Mar 2021 18:28:56 GMT
ETag: W/"785-178469903be"
Content-Type: text/html; charset=UTF-8
Content-Length: 1925
Vary: Accept-Encoding
```

```
<!--
  ~ Copyright (c) 2014-2020 Bjoern Kimminich.
  ~ SPDX-License-Identifier: MIT
  -->

<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>OWASP Juice Shop</title>
  <meta name="description" content=
"Probably the most modern and sophisticated insecure web application">
```

Alerts (4)
- Cross-Domain Misconfiguration (30)
- Cross-Domain JavaScript Source File Inclusion (6
- Information Disclosure - Suspicious Comments
- Timestamp Disclosure - Unix (23)

Cross-Domain Misconfiguration

URL: http://localhost:3000
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
WASC ID: 14
Source: Passive (10098 - Cross-Domain Misconfiguration)

Description:

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server

Other Info:

The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an

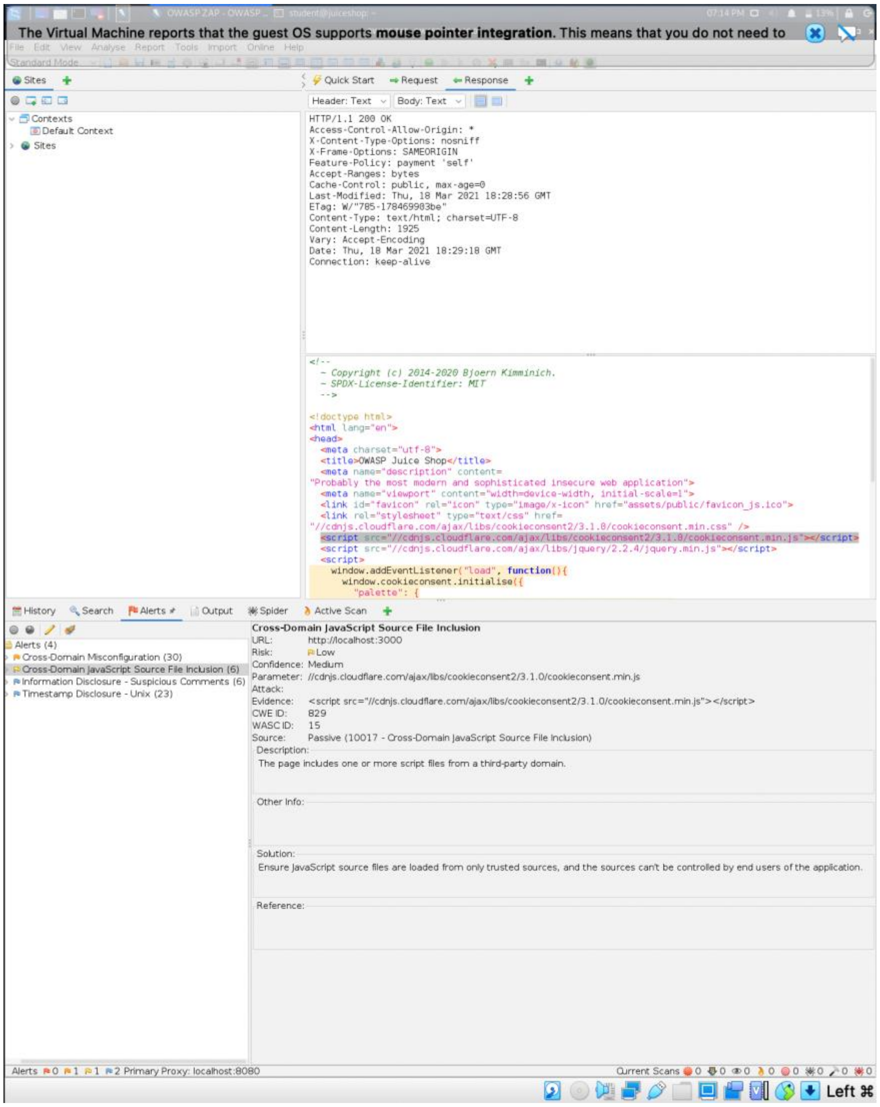
lerts 0 1 1 2 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

Cross Domain JavaScript Source File Inclusion

Low

Vulnerability detail

- The Vulnerability has Low risk.
- The page had one or more script files from a third-party domain.
- The probability of exploit is Low as the exploit might not give important information to the user.
- The department will be affected as they have to reconfigure few scripts.
- Solution is to ensure JavaScript files are loaded from only trusted sources and the sources can’t be controlled by end users of the application.



The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Thu, 18 Mar 2021 18:28:56 GMT
ETag: W/"785-178469903be"
Content-Type: text/html; charset=UTF-8
Content-Length: 1925
Vary: Accept-Encoding
Date: Thu, 18 Mar 2021 18:29:18 GMT
Connection: keep-alive
```

```
<!--
  - Copyright (c) 2014-2020 Bjoern Kimminich.
  - SPDX-License-Identifier: MIT
  -->

<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>OWASP Juice Shop</title>
  <meta name="description" content=
"Probably the most modern and sophisticated insecure web application">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link id="favicon" rel="icon" type="image/x-icon" href="assets/public/favicon_js.ico">
  <link rel="stylesheet" type="text/css" href=
"//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css" />
  <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
  <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
  <script>
   window.addEventListener("load", function(){
     window.cookieconsent.initialise({
       "palette": {
```

Alerts (4)
- Cross-Domain Misconfiguration (30)
- Cross-Domain JavaScript Source File Inclusion (6)
- Information Disclosure - Suspicious Comments (6)
- Timestamp Disclosure - Unix (23)

Cross-Domain JavaScript Source File Inclusion

URL: http://localhost:3000
Risk: Low
Confidence: Medium
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Attack:
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829
WASC ID: 15
Source: Passive (10017 - Cross-Domain JavaScript Source File Inclusion)

Description:
The page includes one or more script files from a third-party domain.

Other Info:

Solution:
Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

Reference:

Alerts 0 1 1 2 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

Methodology

The methodology for the assessment is followed by the steps described below:

Initial Planning: The Planning was done by development team for the assessment.

Scanning: OWASP ZAP tool was used to scan the port localhost:3000. We found one medium risk vulnerability which should be taken care. And a low risk which is not so important. There are two informational risks.

The exploitable risk is the Cross Domain misconfiguration which will lead to requests and unauthorized requests from third party access.

Analysis: According to the Vulnerability report, we have one vulnerability at medium risk which should be taken care of, if not it might cause minor injury to the company. The remediation is explained above.

Remediation: The remediation of medium risk is explained. Overall as we have one medium risk the application is not much vulnerable but if we see overall, we have to take care of making system secure by considering the informational and low risks.

OWASP ZAP gave complete report of all three vulnerabilities and Kali Linux was the platform used.

Assessment Toolset Selection

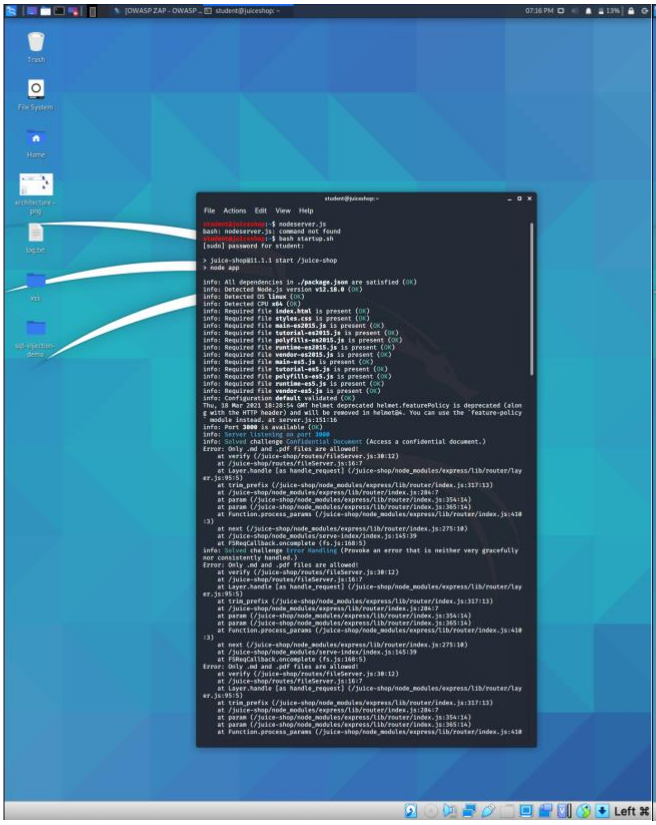
Kali Linux - Platform

Virtual box – Environment setup

OWASP ZAP – Scanning tool

Assessment Methodology Detail

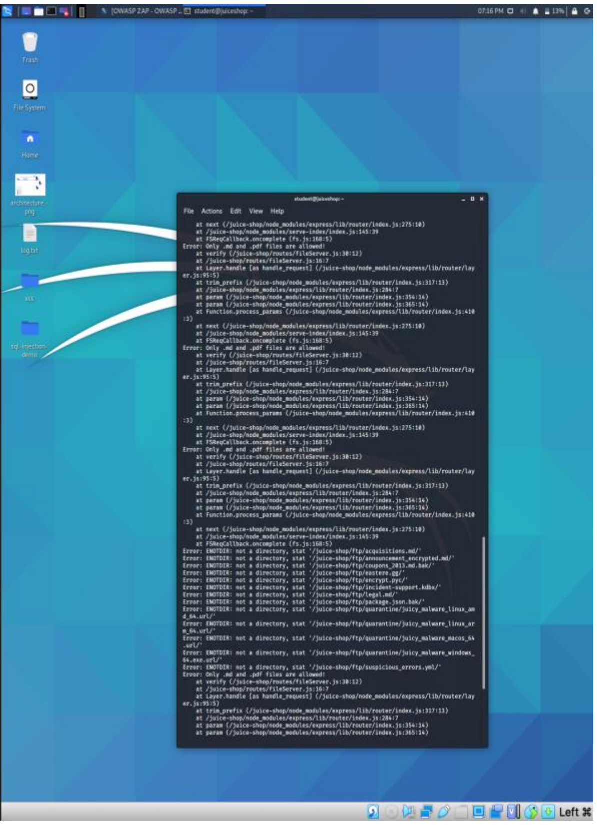
Below are the screenshots of all the commands and reports:



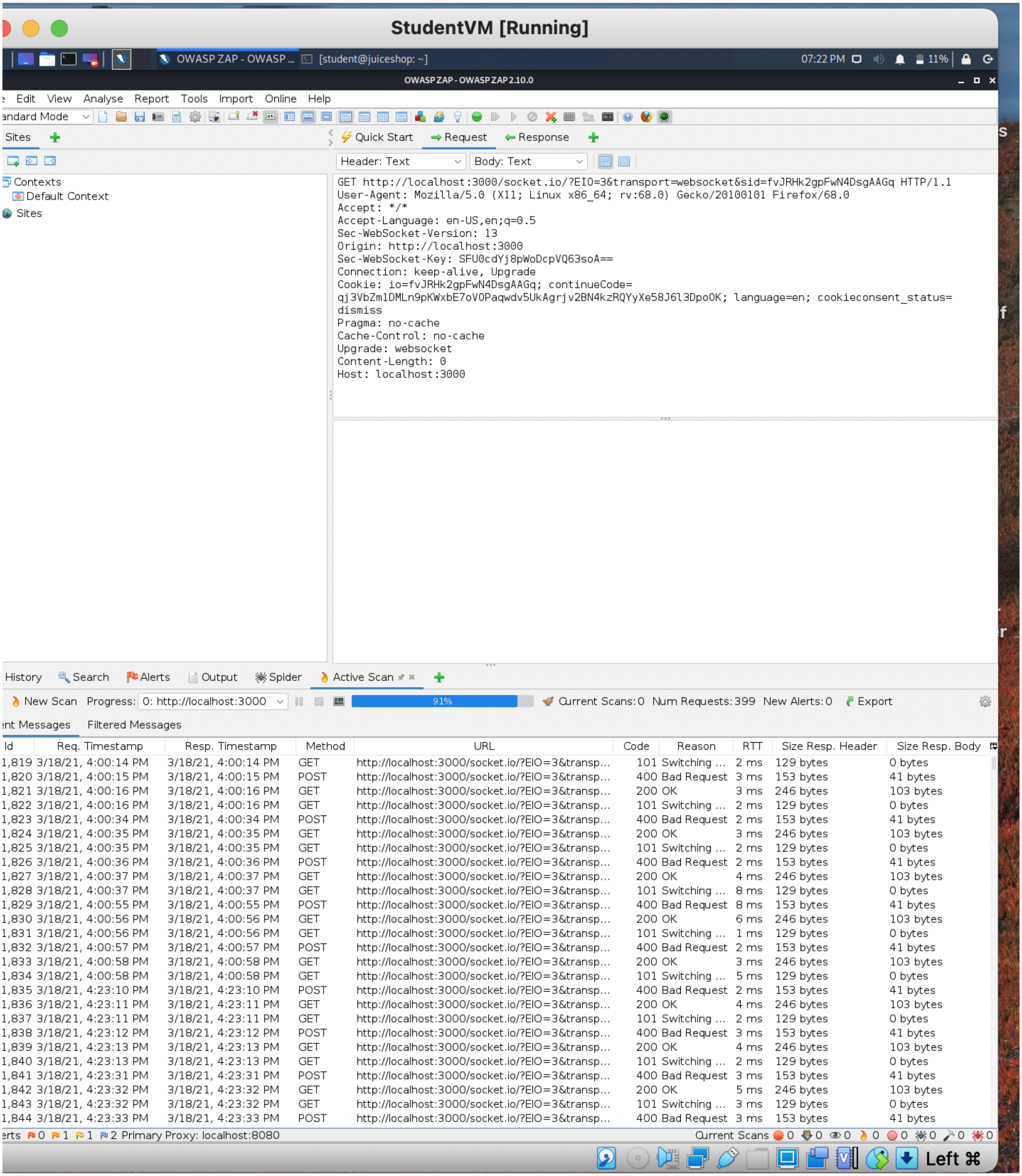
```
student@juiceshop:~$ nodeserver.js
bash: nodeserver.js: command not found
student@juiceshop:~$ bash startup.sh
[sudo] password for student:

> juice-shop@11.1.1 start /juice-shop
> node app

info: All dependencies in ./package.json are satisfied (OK)
info: Detected Node.js version v12.18.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Required file index.html is present (OK)
info: Required file styles.css is present (OK)
info: Required file main-es2015.js is present (OK)
info: Required file tutorial-es2015.js is present (OK)
info: Required file polyfills-es2015.js is present (OK)
info: Required file runtime-es2015.js is present (OK)
info: Required file vendor-es2015.js is present (OK)
info: Required file main-es5.js is present (OK)
info: Required file tutorial-es5.js is present (OK)
info: Required file polyfills-es5.js is present (OK)
info: Required file runtime-es5.js is present (OK)
info: Required file vendor-es5.js is present (OK)
info: Configuration default validated (OK)
Thu, 18 Mar 2021 18:28:54 GMT helmet deprecated helmet.featurePolicy is deprecated (alon
g with the HTTP header) and will be removed in helmet@4. You can use the `feature-policy
` module instead. at server.js:151:16
info: Port 3000 is available (OK)
info: Server listening on port 3000
info: Solved challenge Confidential Document (Access a confidential document.)
Error: Only .md and .pdf files are allowed!
    at verify (/juice-shop/routes/fileServer.js:30:12)
    at /juice-shop/routes/fileServer.js:16:7
    at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/lay
er.js:95:5)
    at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:317:13)
    at /juice-shop/node_modules/express/lib/router/index.js:284:7
    at param (/juice-shop/node_modules/express/lib/router/index.js:354:14)
    at param (/juice-shop/node_modules/express/lib/router/index.js:365:14)
    at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:410
:3)
    at next (/juice-shop/node_modules/express/lib/router/index.js:275:10)
    at /juice-shop/node_modules/serve-index/index.js:145:39
    at FSReqCallback.oncomplete (fs.js:168:5)
info: Solved challenge Error Handling (Provoke an error that is neither very gracefully
nor consistently handled.)
Error: Only .md and .pdf files are allowed!
    at verify (/juice-shop/routes/fileServer.js:30:12)
    at /juice-shop/routes/fileServer.js:16:7
    at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/lay
er.js:95:5)
    at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:317:13)
    at /juice-shop/node_modules/express/lib/router/index.js:284:7
    at param (/juice-shop/node_modules/express/lib/router/index.js:354:14)
    at param (/juice-shop/node_modules/express/lib/router/index.js:365:14)
    at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:410
:3)
    at next (/juice-shop/node_modules/express/lib/router/index.js:275:10)
    at /juice-shop/node_modules/serve-index/index.js:145:39
    at FSReqCallback.oncomplete (fs.js:168:5)
Error: Only .md and .pdf files are allowed!
    at verify (/juice-shop/routes/fileServer.js:30:12)
    at /juice-shop/routes/fileServer.js:16:7
    at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/lay
er.js:95:5)
    at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:317:13)
    at /juice-shop/node_modules/express/lib/router/index.js:284:7
    at param (/juice-shop/node_modules/express/lib/router/index.js:354:14)
    at param (/juice-shop/node_modules/express/lib/router/index.js:365:14)
    at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:410
```



```
    at next (/juice-shop/node_modules/express/lib/router/index.js:275:10)
    at /juice-shop/node_modules/serve-index/index.js:145:39
    at FSReqCallback.oncomplete (fs.js:168:5)
Error: Only .md and .pdf files are allowed!
    at verify (/juice-shop/routes/fileServer.js:30:12)
    at /juice-shop/routes/fileServer.js:16:7
    at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/lay
er.js:95:5)
    at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:317:13)
    at /juice-shop/node_modules/express/lib/router/index.js:284:7
    at param (/juice-shop/node_modules/express/lib/router/index.js:354:14)
    at param (/juice-shop/node_modules/express/lib/router/index.js:365:14)
    at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:410
:3)
    at next (/juice-shop/node_modules/express/lib/router/index.js:275:10)
    at /juice-shop/node_modules/serve-index/index.js:145:39
    at FSReqCallback.oncomplete (fs.js:168:5)
Error: Only .md and .pdf files are allowed!
    at verify (/juice-shop/routes/fileServer.js:30:12)
    at /juice-shop/routes/fileServer.js:16:7
    at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/lay
er.js:95:5)
    at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:317:13)
    at /juice-shop/node_modules/express/lib/router/index.js:284:7
    at param (/juice-shop/node_modules/express/lib/router/index.js:354:14)
    at param (/juice-shop/node_modules/express/lib/router/index.js:365:14)
    at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:410
:3)
    at next (/juice-shop/node_modules/express/lib/router/index.js:275:10)
    at /juice-shop/node_modules/serve-index/index.js:145:39
    at FSReqCallback.oncomplete (fs.js:168:5)
Error: Only .md and .pdf files are allowed!
    at verify (/juice-shop/routes/fileServer.js:30:12)
    at /juice-shop/routes/fileServer.js:16:7
    at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/lay
er.js:95:5)
    at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:317:13)
    at /juice-shop/node_modules/express/lib/router/index.js:284:7
    at param (/juice-shop/node_modules/express/lib/router/index.js:354:14)
    at param (/juice-shop/node_modules/express/lib/router/index.js:365:14)
    at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:410
:3)
    at next (/juice-shop/node_modules/express/lib/router/index.js:275:10)
    at /juice-shop/node_modules/serve-index/index.js:145:39
    at FSReqCallback.oncomplete (fs.js:168:5)
Error: ENOTDIR: not a directory, stat '/juice-shop/ftp/acquisitions.md/'
Error: ENOTDIR: not a directory, stat '/juice-shop/ftp/announcement_encrypted.md/'
Error: ENOTDIR: not a directory, stat '/juice-shop/ftp/coupons_2013.md.bak/'
Error: ENOTDIR: not a directory, stat '/juice-shop/ftp/eastere.gg/'
Error: ENOTDIR: not a directory, stat '/juice-shop/ftp/encrypt.pyc/'
Error: ENOTDIR: not a directory, stat '/juice-shop/ftp/incident-support.kdbx/'
Error: ENOTDIR: not a directory, stat '/juice-shop/ftp/legal.md/'
Error: ENOTDIR: not a directory, stat '/juice-shop/ftp/package.json.bak/'
Error: ENOTDIR: not a directory, stat '/juice-shop/ftp/quarantine/juicy_malware_linux_am
d_64.url/'
Error: ENOTDIR: not a directory, stat '/juice-shop/ftp/quarantine/juicy_malware_linux_ar
m_64.url/'
Error: ENOTDIR: not a directory, stat '/juice-shop/ftp/quarantine/juicy_malware_macos_64
.url/'
Error: ENOTDIR: not a directory, stat '/juice-shop/ftp/quarantine/juicy_malware_windows_
64.exe.url/'
Error: ENOTDIR: not a directory, stat '/juice-shop/ftp/suspicious_errors.yml/'
Error: Only .md and .pdf files are allowed!
    at verify (/juice-shop/routes/fileServer.js:30:12)
    at /juice-shop/routes/fileServer.js:16:7
    at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/lay
er.js:95:5)
    at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:317:13)
    at /juice-shop/node_modules/express/lib/router/index.js:284:7
    at param (/juice-shop/node_modules/express/lib/router/index.js:354:14)
    at param (/juice-shop/node_modules/express/lib/router/index.js:365:14)
```



```
GET http://localhost:3000/socket.io/?EIO=3&transport=websocket&sid=fvJRHk2gpFwN4DsgAAGq HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Sec-WebSocket-Version: 13
Origin: http://localhost:3000
Sec-WebSocket-Key: SFU0cdYj8pWoDcpVQ63soA==
Connection: keep-alive, Upgrade
Cookie: io=fvJRHk2gpFwN4DsgAAGq; continueCode=
qj3VbZm1DMLn9pKWxbE7oVOPaqwdv5UkAgrjv2BN4kzRQYyXe58J6l3DpoOK; language=en; cookieconsent_status=
dismiss
Pragma: no-cache
Cache-Control: no-cache
Upgrade: websocket
Content-Length: 0
Host: localhost:3000
```

New Scan Progress: 0: http://localhost:3000 91% Current Scans: 0 Num Requests: 399 New Alerts: 0 Export

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
1,819	3/18/21, 4:00:14 PM	3/18/21, 4:00:14 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	101	Switching ...	2 ms	129 bytes	0 bytes
1,820	3/18/21, 4:00:15 PM	3/18/21, 4:00:15 PM	POST	http://localhost:3000/socket.io/?EIO=3&transp...	400	Bad Request	3 ms	153 bytes	41 bytes
1,821	3/18/21, 4:00:16 PM	3/18/21, 4:00:16 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	200	OK	3 ms	246 bytes	103 bytes
1,822	3/18/21, 4:00:16 PM	3/18/21, 4:00:16 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	101	Switching ...	2 ms	129 bytes	0 bytes
1,823	3/18/21, 4:00:34 PM	3/18/21, 4:00:34 PM	POST	http://localhost:3000/socket.io/?EIO=3&transp...	400	Bad Request	2 ms	153 bytes	41 bytes
1,824	3/18/21, 4:00:35 PM	3/18/21, 4:00:35 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	200	OK	3 ms	246 bytes	103 bytes
1,825	3/18/21, 4:00:35 PM	3/18/21, 4:00:35 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	101	Switching ...	2 ms	129 bytes	0 bytes
1,826	3/18/21, 4:00:36 PM	3/18/21, 4:00:36 PM	POST	http://localhost:3000/socket.io/?EIO=3&transp...	400	Bad Request	2 ms	153 bytes	41 bytes
1,827	3/18/21, 4:00:37 PM	3/18/21, 4:00:37 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	200	OK	4 ms	246 bytes	103 bytes
1,828	3/18/21, 4:00:37 PM	3/18/21, 4:00:37 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	101	Switching ...	8 ms	129 bytes	0 bytes
1,829	3/18/21, 4:00:55 PM	3/18/21, 4:00:55 PM	POST	http://localhost:3000/socket.io/?EIO=3&transp...	400	Bad Request	8 ms	153 bytes	41 bytes
1,830	3/18/21, 4:00:56 PM	3/18/21, 4:00:56 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	200	OK	6 ms	246 bytes	103 bytes
1,831	3/18/21, 4:00:56 PM	3/18/21, 4:00:56 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	101	Switching ...	1 ms	129 bytes	0 bytes
1,832	3/18/21, 4:00:57 PM	3/18/21, 4:00:57 PM	POST	http://localhost:3000/socket.io/?EIO=3&transp...	400	Bad Request	2 ms	153 bytes	41 bytes
1,833	3/18/21, 4:00:58 PM	3/18/21, 4:00:58 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	200	OK	3 ms	246 bytes	103 bytes
1,834	3/18/21, 4:00:58 PM	3/18/21, 4:00:58 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	101	Switching ...	5 ms	129 bytes	0 bytes
1,835	3/18/21, 4:23:10 PM	3/18/21, 4:23:10 PM	POST	http://localhost:3000/socket.io/?EIO=3&transp...	400	Bad Request	2 ms	153 bytes	41 bytes
1,836	3/18/21, 4:23:11 PM	3/18/21, 4:23:11 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	200	OK	4 ms	246 bytes	103 bytes
1,837	3/18/21, 4:23:11 PM	3/18/21, 4:23:11 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	101	Switching ...	2 ms	129 bytes	0 bytes
1,838	3/18/21, 4:23:12 PM	3/18/21, 4:23:12 PM	POST	http://localhost:3000/socket.io/?EIO=3&transp...	400	Bad Request	3 ms	153 bytes	41 bytes
1,839	3/18/21, 4:23:13 PM	3/18/21, 4:23:13 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	200	OK	4 ms	246 bytes	103 bytes
1,840	3/18/21, 4:23:13 PM	3/18/21, 4:23:13 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	101	Switching ...	2 ms	129 bytes	0 bytes
1,841	3/18/21, 4:23:31 PM	3/18/21, 4:23:31 PM	POST	http://localhost:3000/socket.io/?EIO=3&transp...	400	Bad Request	3 ms	153 bytes	41 bytes
1,842	3/18/21, 4:23:32 PM	3/18/21, 4:23:32 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	200	OK	5 ms	246 bytes	103 bytes
1,843	3/18/21, 4:23:32 PM	3/18/21, 4:23:32 PM	GET	http://localhost:3000/socket.io/?EIO=3&transp...	101	Switching ...	3 ms	129 bytes	0 bytes
1,844	3/18/21, 4:23:33 PM	3/18/21, 4:23:33 PM	POST	http://localhost:3000/socket.io/?EIO=3&transp...	400	Bad Request	3 ms	153 bytes	41 bytes

erts 0 1 1 2 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

This concluded the vulnerability assessment methodology portion of this report.