SECURITY ASSESSMENT

<< Vulnerabilities and Risk Analysis>>

Submitted to: << Udacity >>
Security Analyst: << Simon Chen >>

Date of Testing: << 6/5/21>
Date of Report Delivery: <<6/10/21>

Table of Contents

Contents

Security Engagement Summary

Engagement Overview

<<
Explain the engagement.

- 1) Who requested the engagement and why?

The stakeholders are the people that requested the rules of Engagement.
In the set-up phase, Analysts are to meet with Stakeholders to discuss the scope and rule of Engagement.
The stakeholders are Business owners and management in an organization.

- 2) What are the engagement's goals?

The goal of Engagement is to define how the assessment is to be executed.
Everything between the start to the end.
There is 7 steps in the rule of engagement: 1)Communication Plan 2) Meeting/Following Up Cadence
3) Emergency Contact 4) Report Deliverables 5) Scheduling 6) How to handle Evidence 7)Approvals/Permissions.

The Engagement's goal is to analyze security weakness in an application.
Given that purpose of a web application vulnerability assessment is to take stock of your system's overall security and
Identify any weaknesses. It is often recommended to conduct assessments, at least once a month to protect
Any existing and developing cyber threats.

- 3) Who is complete the engagement?
  I believe it's the Analyst's job to complete the Engagement because the analyst should develop a plan
  And the time it takes to execute the task . For Example) the analyst should develop a communication plan for alerts or Status updates. An example of that is: At the end of workers every shift, they should provide status updates to their supervisor.
- 4) How often is assessment completed?

>> The people that should assess your cyber security controls are people in the IT department.
You can choose people in IT department or take the recommended route of outsourcing cyber security audits to
Third party.
Assessments should be completed either monthly, quarterly, or bi-anually.
It is recommended that audits are performed at least twice a year.
Recurring Assessments like Cross Site Scripting(XSS) needs a frequency assessment, so that they can monitor and prevent threats.
When they are performing assessments, they can do vulnerability assessment or penetration testing.
These methods can help make the security controls more secure because they can actively monitor for
Cyber threats.

Scope

<<

In high-level terms, describe the scope of the engagement and why this scope is appropriate

>> The scope of the engagement is defined as what will be assessed.

The scope has 8 steps: 1) Inventory of Environment/Topology 2) Valuation of Identified resources

3) Estimation of Time 4) Policies 5) Regulatory Compliance 6) Business Processes

7) Existing Controls 8) Tool Selection

The scope is appropriate because the analyst have to discuss with the Stakeholders about the scope.

If they understand the scope, then they will have a strong plan.

Executive Risk Analysis

<<

Summarize the overall risk that the report indicates for the scope. (High | Medium | Low)

The overall risk that the report indicates for the scope is High.

Explain why this risk level was reported. Include a summary of vulnerabilities in discussion (Executive Summary) form.

>>

I would say that the risk level is high because part of the scope there is the valuation of identified resources.

Some of the Identified resources include : Game Server ,DLC Web sever.

In the Game Server, the risk level is high/ critical . In DLC Web Server, the risk level is high/critical.

Other servers : ERP Server, ERP DB Server, and LDAP Server.

ERP Server has high risk level. ERP DB Server has high/critical risk level .LDAP server has Medium/High.

I would say that the overall risk that the report indicates for the scope is High .

Executive Recommendation

<<

In discussion (Executive Summary) form, explain if remediation efforts are warranted. Describe at a high level how to best mitigate or remediate the highest-risk vulnerabilities Prioritize which vulnerability should be remediated first and why.

>>

1) Yes, I would say that remediation efforts are warranted because remediation is part of the

Vulnerability Assessment stage. If remediation is a part of the process, then it will make it more safe.

The best way to mitigate or remediate high-risk vulnerabilities is : 1) Risk Acceptance 2) Risk Reduction

3) Risk Transfer 4) Risk Avoidance.

The first strategy is Risk Acceptance, and in this strategy you can just accept the risk and do nothing.

The second strategy is Risk Reduction, in where you take measures to reduce the risk so that it can be at an acceptable level.

The third strategy is Risk Transfer. In this step, you transfer the risk to another person.

The third strategy is Risk Avoidance. In this step, you try to avoid risk.

You should prioritize vulnerability base on its risk level, so I would rank the risk and the higher the risk than the more

attention you should focus on the risk. The vulnerability would be: critical, high, medium, low.

I would focus my attention on critical as the most important because it’s the most dangerous, then I would consider high as my next urgent risk. Medium is third on that list, and I would consider low as the lowest priority.

Significant Vulnerability Summary

<<

Provide a list of the highlighted vulnerabilities in descending order of assessed risk

High | Medium | Low

>>

High Risk Vulnerabilities

- CVE-2021-3154(7.5 Base Score : High)

Medium Risk Vulnerabilities

- CVE -2021-3524 (6.5 Base Score: Medium)

Low Risk Vulnerabilities

- CVE-2020-16092 (3.8 Base Score : Low)

Significant Vulnerability Detail

<<

For each significant vulnerability assessed, provide a summary of the vulnerability.

Include a page-break between each vulnerability in this section.

>>

<< Vulnerability Name>>

<<RISK LEVEL HIGH | MEDIUM | LOW>>

<<

Vulnerability detail

- Provide the assessed risk level (High | Medium | Low) of the vulnerability.
- Discussion (Executive Summary) form, explain how the vulnerability was identified and validated.
- Provide evidence of validation (Screenshot, log excerpt, etc.)
- Discuss the probability of exploit/attack.
- Discuss who would be impacted if the attack was exploited (users-groups, departments, business-continuity/revenue)
- Discuss potential remediation

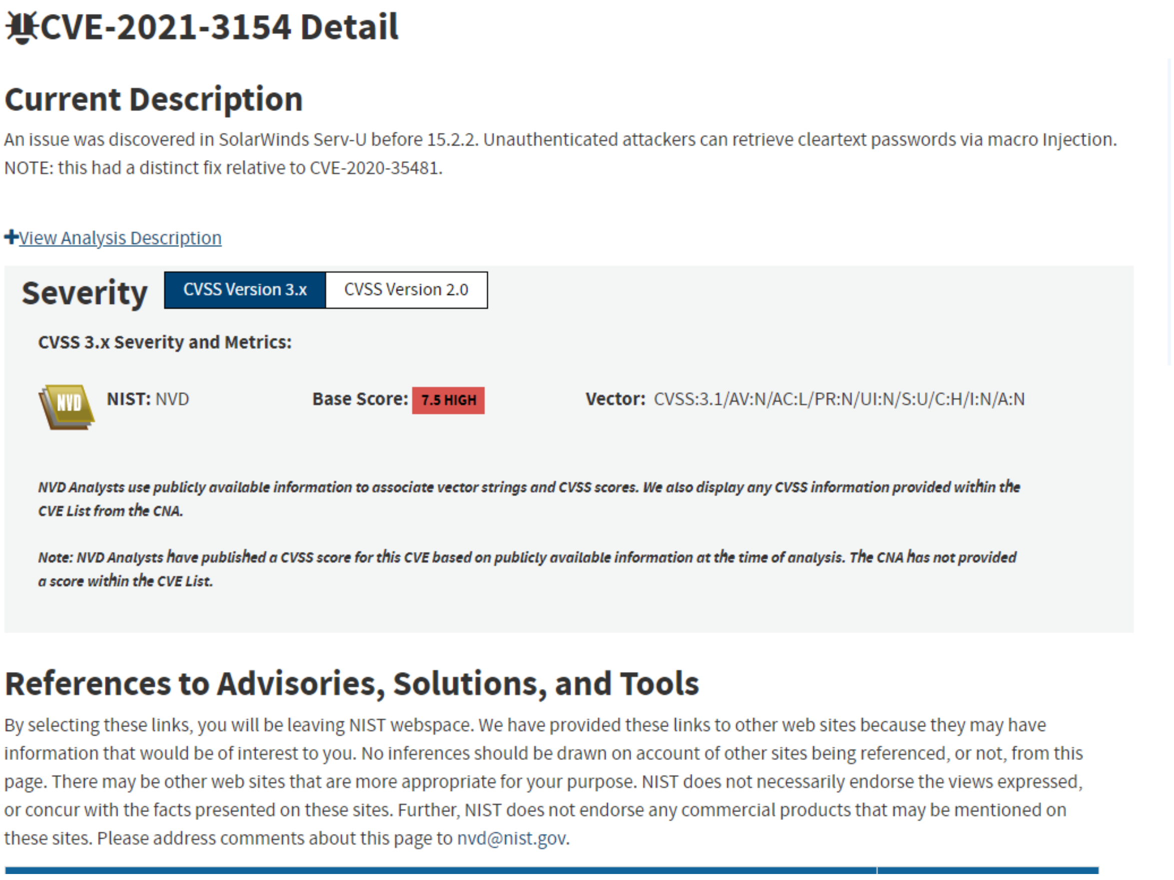
>> 1) The first Vulnerability that I analyzed was CVE-2021-3154 .

The risk level is High because the Base Score : 7.5 is considered high risk .

2) The vulnerability was identified by I went to the cve.mitre.org . I went on that website, so that I can analyze vulnerability because on that website it gives you the vulnerability and it also gives you the risk score. It will tell you if the vulnerability is: critical, high , medium, or low

The vulnerability was identified because I went on the website I mentioned above, and it was validated by I saw the risk score next to the vulnerability

3) Screenshot.



CVE-2021-3154 Detail

Current Description

An issue was discovered in SolarWinds Serv-U before 15.2.2. Unauthenticated attackers can retrieve cleartext passwords via macro Injection. NOTE: this had a distinct fix relative to CVE-2020-35481.

+View Analysis Description

Severity

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 7.5 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

---

4) The CVE-2021-3154 Vulnerability is a vulnerability where Unauthenticated attackers can retrieve cleartext passwords via macro Injection. The probability would be high risk because cleartext passwords are stolen.

5) If the attack was exploited, I believe that it would affect businesses because if cleartext passwords are stolen, then unauthorized users can gain access, and it would give permission to unauthorized users.

6) The potential remediation is that they should install applications that encrypt cleartext passwords, so that it would be hard to decipher.

<< Vulnerability Name>>

<<RISK LEVEL HIGH | MEDIUM | LOW>>

<<

Vulnerability detail

- Provide the assessed risk level (High | Medium | Low) of the vulnerability.
- Discussion (Executive Summary) form, explain how the vulnerability was identified and validated.
- Provide evidence of validation (Screenshot, log excerpt, etc.)
- Discuss the probability of exploit/attack.
- Discuss who would be impacted if the attack was exploited (users-groups, departments, business-continuity/revenue)
- Discuss potential remediation

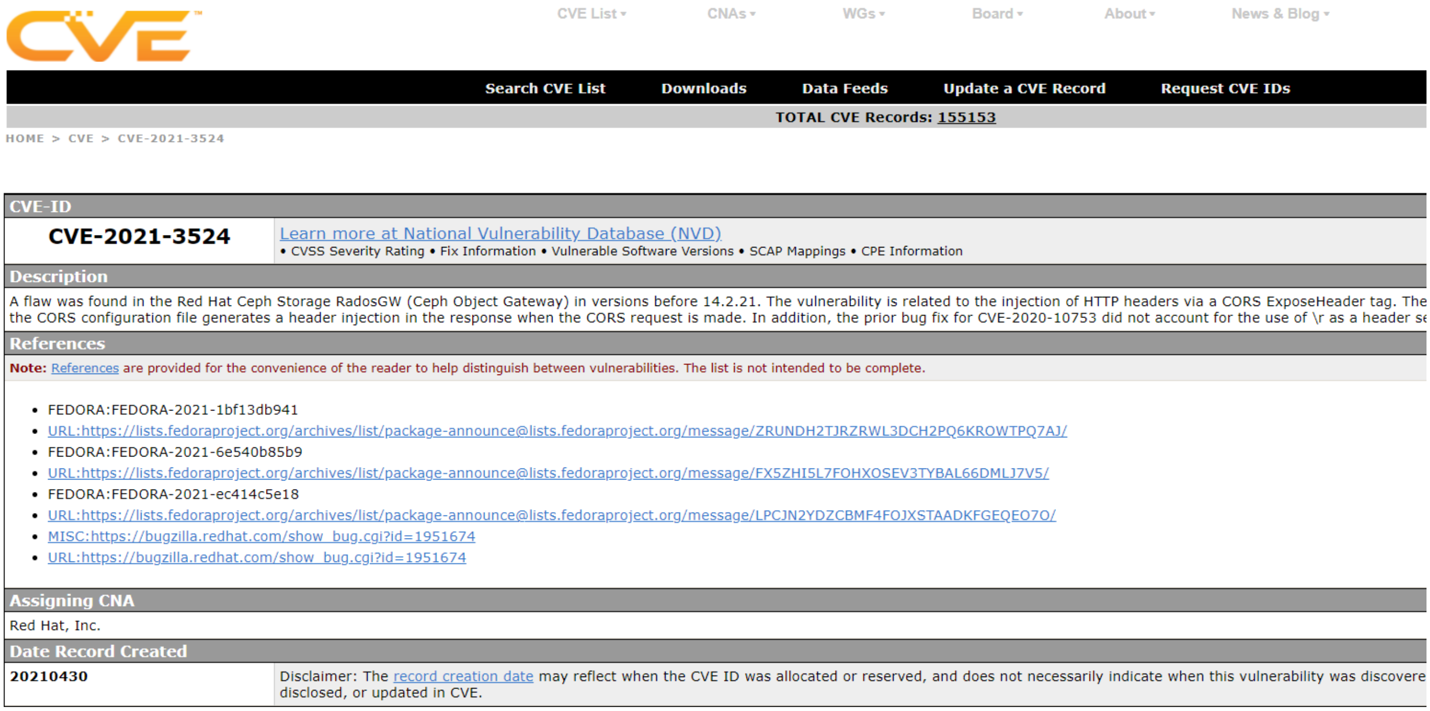
>> 1. For the CVE -2021-3524 vulnerability, it is a vulnerability that has medium risk.

It is medium risk because the base score is 6.5, and that is considered medium risk.

2.The vulnerability was identified by I went to the website cve.mitre.org , so that I can analyze the vulnerabilities.

It was validated by I went on the website, and I chose CVE-2021-3524 vulnerability, and next to it there is a Base Score: 6.5 and 6.5 is considered to be medium risk.

3. Screenshot below.



TOTAL CVE Records: 155153

HOME > CVE > CVE-2021-3524

CVE-ID

CVE-2021-3524

Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A flaw was found in the Red Hat Ceph Storage RadosGW (Ceph Object Gateway) in versions before 14.2.21. The vulnerability is related to the injection of HTTP headers via a CORS ExposeHeader tag. The
the CORS configuration file generates a header injection in the response when the CORS request is made. In addition, the prior bug fix for CVE-2020-10753 did not account for the use of \r as a header se

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- FEDORA:FEDORA-2021-1bf13db941
- URL:https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/ZRUNDH2TJRZRWL3DCH2PQ6KROWTPQ7AJ/
- FEDORA:FEDORA-2021-6e540b85b9
- URL:https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/FX5ZHI5L7FOHXOSEV3TYBAL66DMLJ7V5/
- FEDORA:FEDORA-2021-ec414c5e18
- URL:https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/LPCJN2YDZCBMF4FOJXSTAADKFGEQEO7O/
- MISC:https://bugzilla.redhat.com/show_bug.cgi?id=1951674
- URL:https://bugzilla.redhat.com/show_bug.cgi?id=1951674

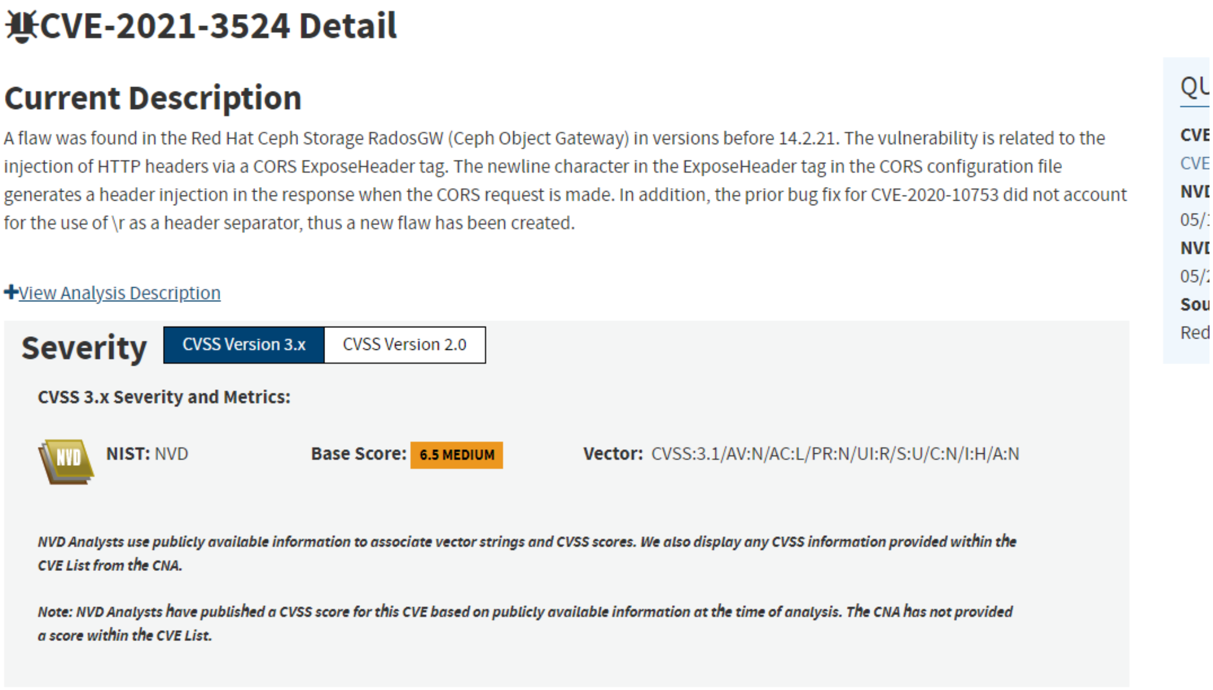
Assigning CNA

Red Hat, Inc.

Date Record Created

20210430

Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovere
disclosed, or updated in CVE.



CVE-2021-3524 Detail

Current Description

A flaw was found in the Red Hat Ceph Storage RadosGW (Ceph Object Gateway) in versions before 14.2.21. The vulnerability is related to the injection of HTTP headers via a CORS ExposeHeader tag. The newline character in the ExposeHeader tag in the CORS configuration file generates a header injection in the response when the CORS request is made. In addition, the prior bug fix for CVE-2020-10753 did not account for the use of \r as a header separator, thus a new flaw has been created.

+View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 6.5 MEDIUM **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

4) The CVE-2021-3524 vulnerability is a vulnerability is related to injections of HTTP headers.
I would say that it is dangerous risk, and it should be prevented if possible.
I believe the probability of exploit is medium.

5) I would say that the people that would be affected is departments.
Since this attack affects HTTP Headers, I believe it will affect Programmers/Software Engineer Department and IT Department.

6) The possible remediation is that they should install a software application that constantly monitors the computer for threats.

<< Vulnerability Name>>

<<RISK LEVEL HIGH | MEDIUM | LOW>>

<<

Vulnerability detail

- Provide the assessed risk level (High | Medium | Low) of the vulnerability.
- Discussion (Executive Summary) form, explain how the vulnerability was identified and validated.
- Provide evidence of validation (Screenshot, log excerpt, etc.)
- Discuss the probability of exploit/attack.
- Discuss who would be impacted if the attack was exploited (users-groups, departments, business-continuity/revenue)
- Discuss potential remediation

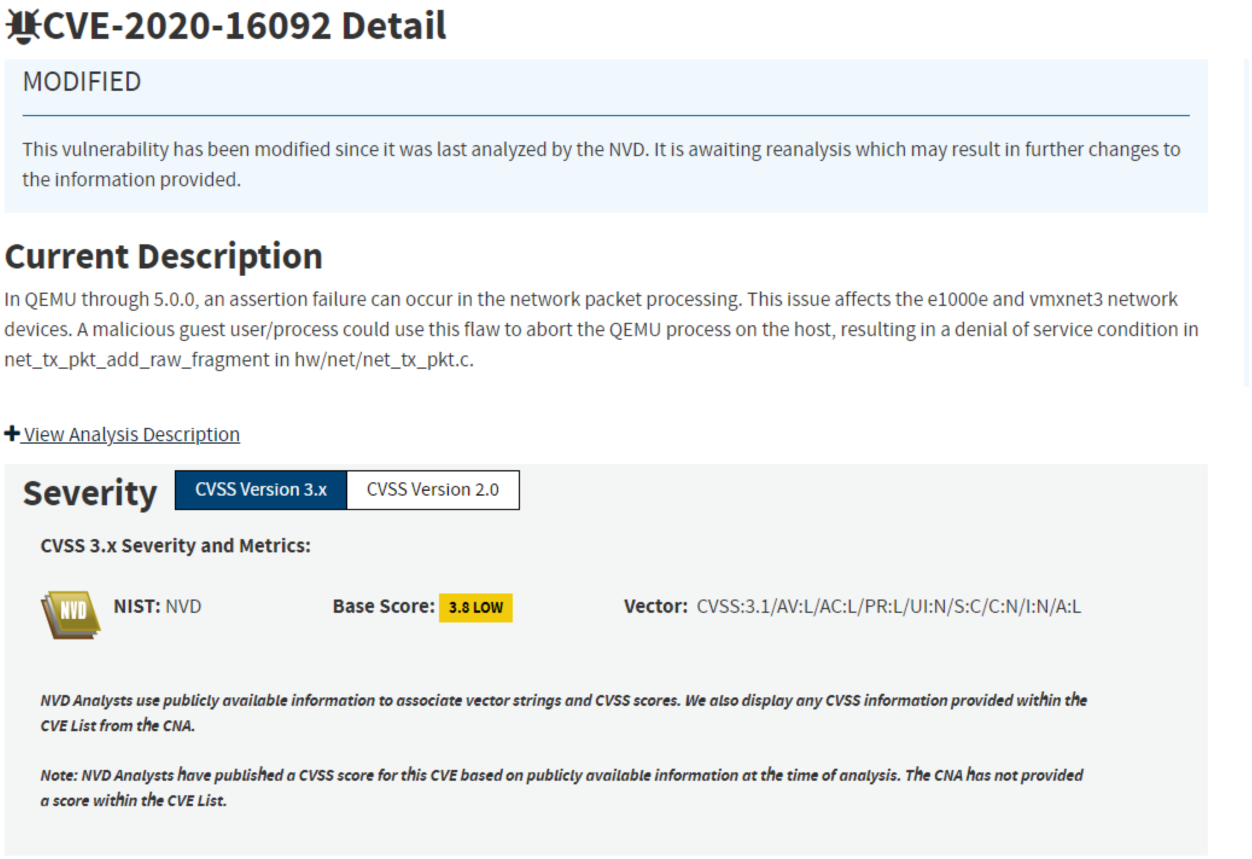
>> 1) For the CVE-2020-16092 vulnerability, the risk level is low risk.

It is low risk because the base score : 3.8 , and it is considered low risk.

2) The vulnerability was identified by I went to the website cve.mitre.org ,and I was browsing for vulnerabilities.

I chose CVE-2020-16092 vulnerability, then I analyzed the vulnerability.

3) Screenshot. On the next page.



CVE-2020-16092 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

In QEMU through 5.0.0, an assertion failure can occur in the network packet processing. This issue affects the e1000e and vmxnet3 network devices. A malicious guest user/process could use this flaw to abort the QEMU process on the host, resulting in a denial of service condition in net_tx_pkt_add_raw_fragment in hw/net/net_tx_pkt.c.

Severity

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 3.8 LOW **Vector:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:L

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

4) The probability of the attack is low because it is low risk.

5) For the CVE-2020-16092 vulnerability, it is a vulnerability where a malicious guest can use a flaw that can abort the QEMU on the host, that can result in Denial of Service(DOS) Condition.

I would say that the people that would be affected would be business and departments.

The Denial of Service(DOS) attack can affect business by the unauthorized users can flood the network, and cause the company's network to crash resulting in where employees of company can be without work because it will take time to fix the nextwork.

It would affect the IT department because if an unauthorized users uses DOS attack, it can cause the IT personnel to immediately remediate the Dos attack.

6.) The potential remediation is that you can build a firewall, so that the firewall can mitigate potential threats. The Firewall is a good mitigation strategy against Dos attacks because it can filter incoming/outgoing traffic.

Methodology

<<

The remainder of the report is intended for technical practitioners, other security analysts, engineers, developers, and systems-administrators. Use of technical terms is appropriate.

The assessment methodology will be the longest single section of this report. It is written in a mostly chronological order starting with tool selection, followed be execution of tools, analysis of output, and validation of significant vulnerabilities.

Any significant vulnerabilities should be referenced in the earlier Significant Vulnerabilities Summary and Detail section, as well as discussed in the Risk Analysis and potentially in the Recommendation portions of this report.

>>

Assessment Toolset Selection

<<

Provide a list of tools used during the vulnerability assessment and validation.

>> 1) Common Vulnerability and Exposures (CVE)

2) National Vulnerability Database(NVD)

3) Common Vulnerability Scoring System(CVSS)

4) OWASP Juice Shop

5) OWASP ZAP Tool

Assessment Methodology Detail

<<

Include evidence of the vulnerability assessment tool execution and sample output.

As tools are used, include either screenshots or specific command-line instructions.

Analysis of the tool output may identify significant vulnerabilities. Vulnerabilities that are considered significant should be validated manually. The process of manual validation is documented. The process documentation may include screenshots, tool commands. The process documentation should include evidence if the significant vulnerability is valid.

The methodology should include sufficient detail for a technical practitioner to arrive at the same risk conclusions as you present in earlier sections of the report.

>>

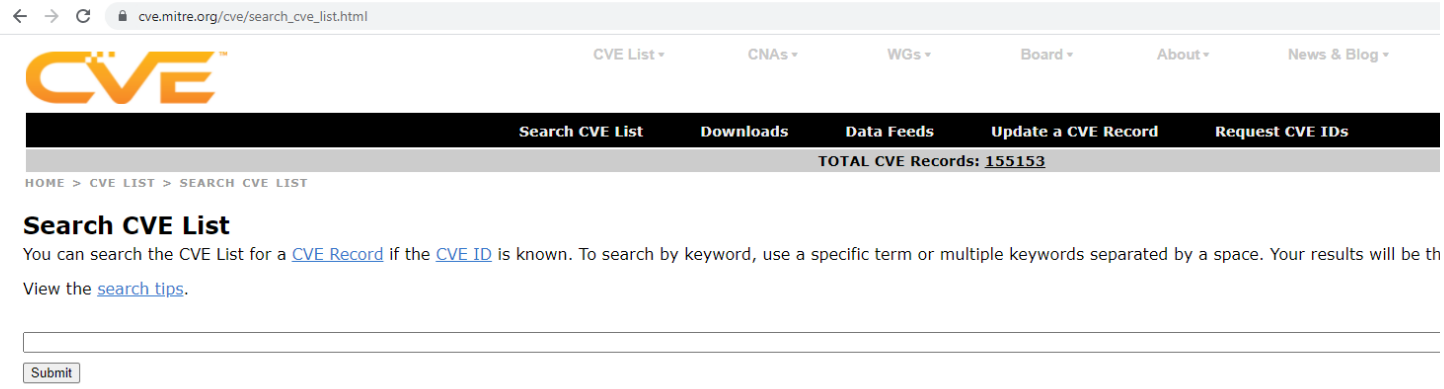
1) The first tool that I used is : CVE.

I used the CVE to help me find vulnerabilities and their risk scores.

The CVE website was easy to use because I just went to the website cve.mitre.org ,

Then I would enter the CVE and pressed search. It would then give me the CVE information that I need.

Look on next page for screenshot.



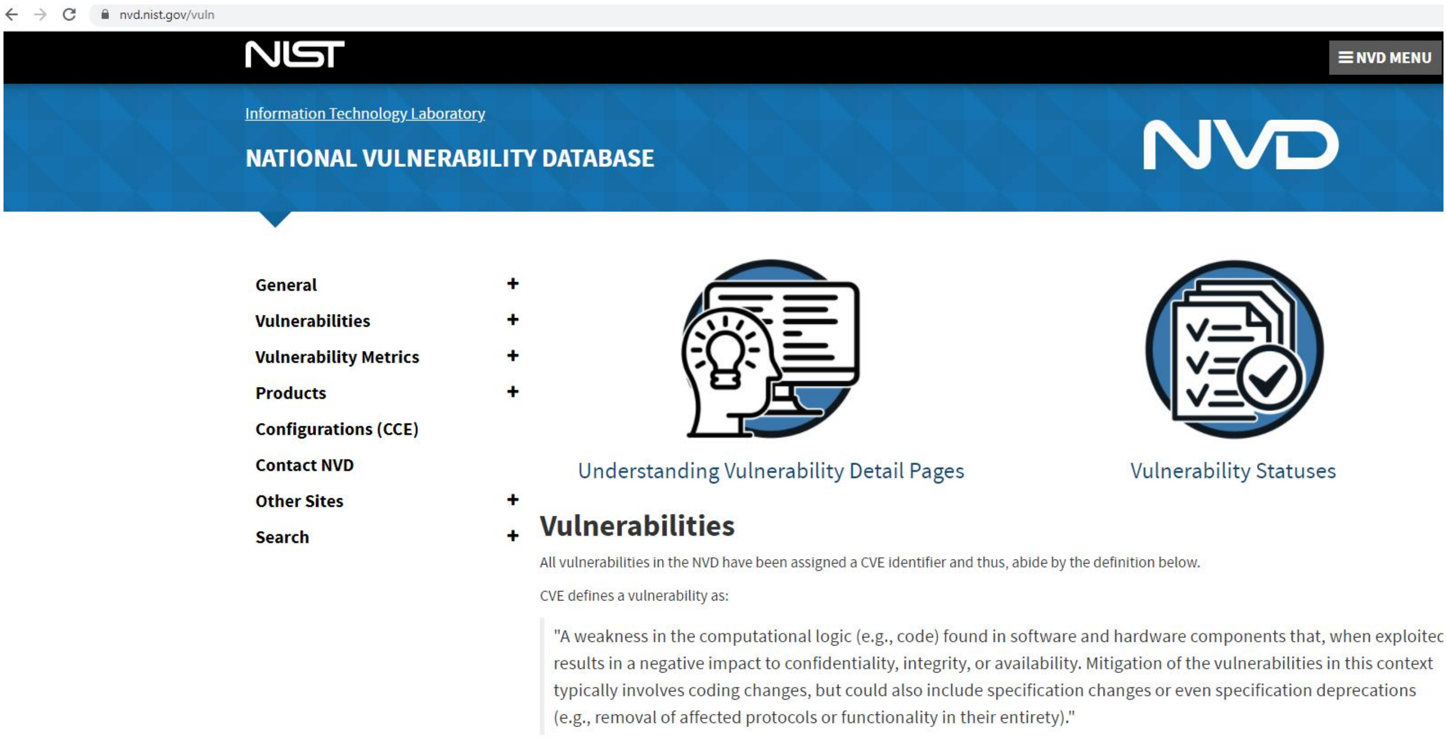
Search CVE List

You can search the CVE List for a CVE Record if the CVE ID is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be th

View the search tips.

This concluded the vulnerability assessment methodology portion of this report.

2) The next tool that I used is : NVD.
I used this tool to help me learn more about vulnerability because
NVD is a vulnerability Database.



Vulnerabilities

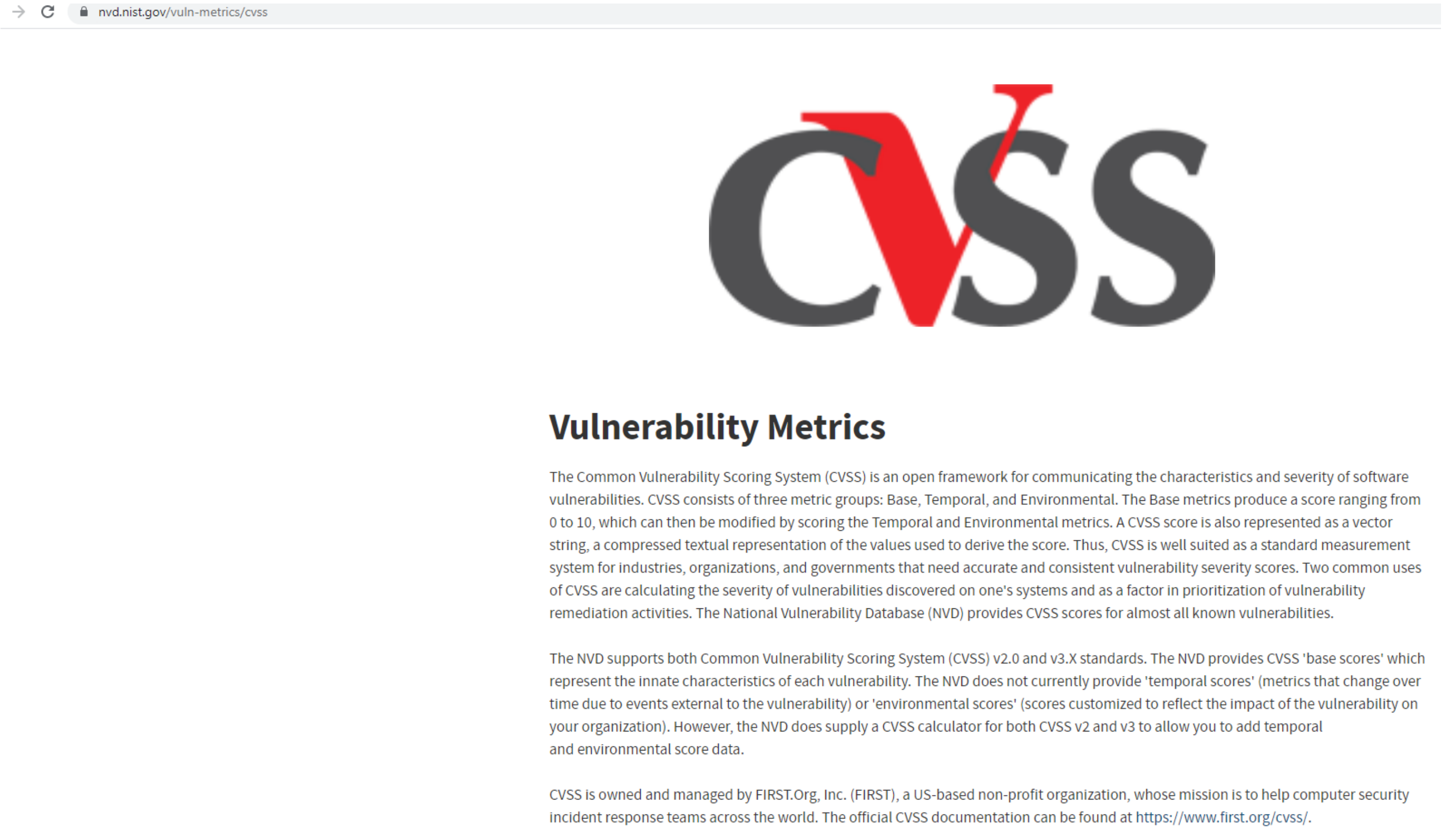
All vulnerabilities in the NVD have been assigned a CVE identifier and thus, abide by the definition below.

CVE defines a vulnerability as:

> "A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploitec results in a negative impact to confidentiality, integrity, or availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety)."

3) The third tool that I used is : Common Vulnerability Scoring System(CVSS).

I used this online tool, so that I can learn about what is CVSS and how it worked.



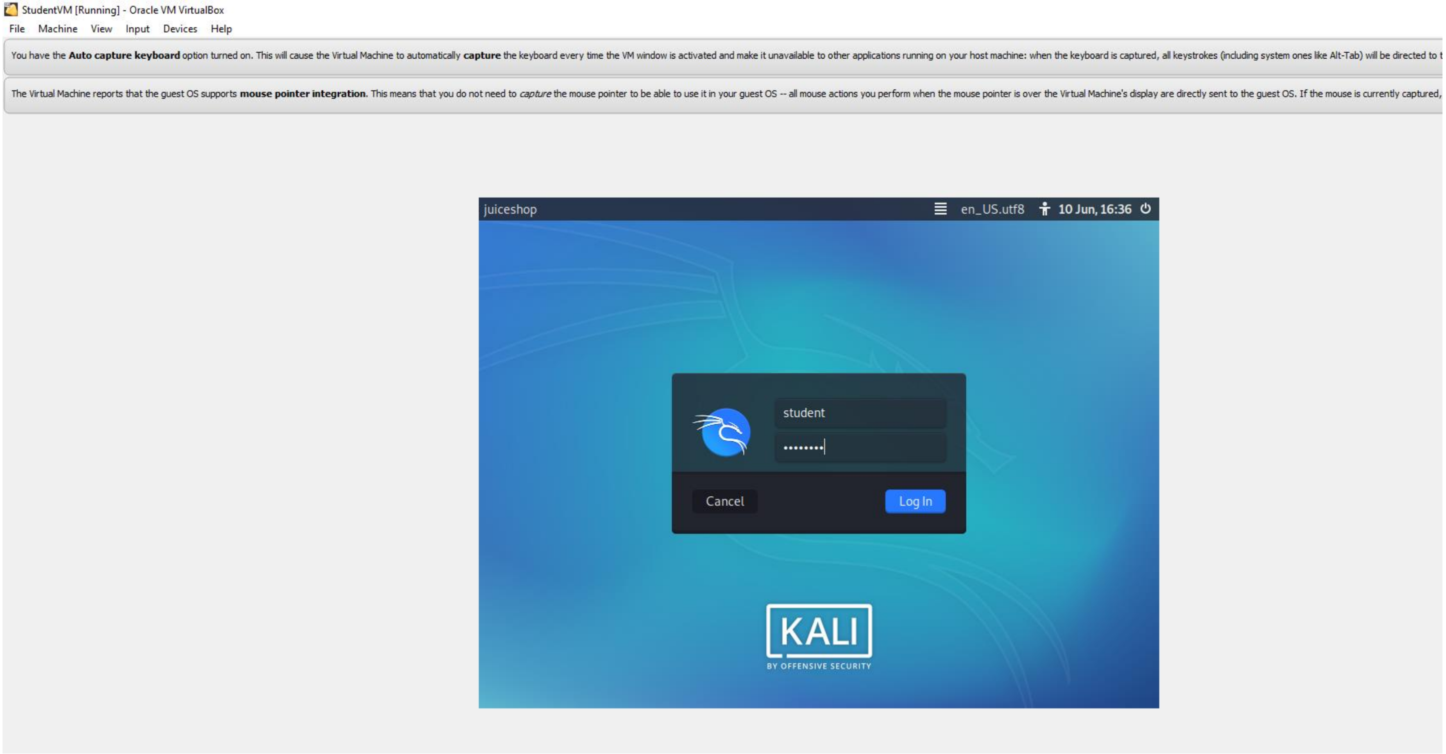
Vulnerability Metrics

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability severity scores. Two common uses of CVSS are calculating the severity of vulnerabilities discovered on one's systems and as a factor in prioritization of vulnerability remediation activities. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

The NVD supports both Common Vulnerability Scoring System (CVSS) v2.0 and v3.X standards. The NVD provides CVSS 'base scores' which represent the innate characteristics of each vulnerability. The NVD does not currently provide 'temporal scores' (metrics that change over time due to events external to the vulnerability) or 'environmental scores' (scores customized to reflect the impact of the vulnerability on your organization). However, the NVD does supply a CVSS calculator for both CVSS v2 and v3 to allow you to add temporal and environmental score data.

CVSS is owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to help computer security incident response teams across the world. The official CVSS documentation can be found at https://www.first.org/cvss/.

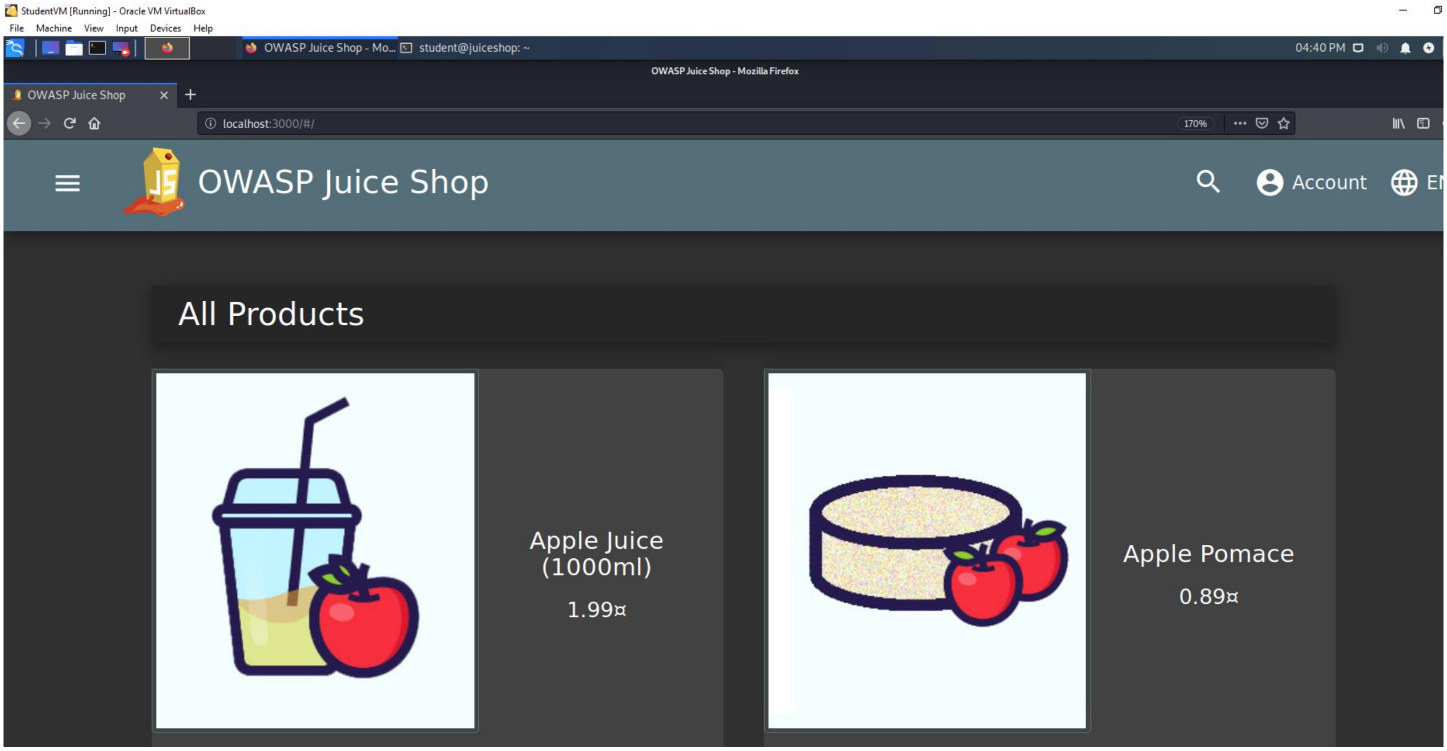
4)


StudentVM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
juiceshop
en_US.utf8
10 Jun, 16:36
Cancel
Log In
KALI
BY OFFENSIVE SECURITY

You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is activated and make it unavailable to other applications running on your host machine: when the keyboard is captured, all keystrokes (including system ones like Alt-Tab) will be directed to t

The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual Machine's display are directly sent to the guest OS. If the mouse is currently captured,

student
••••••••

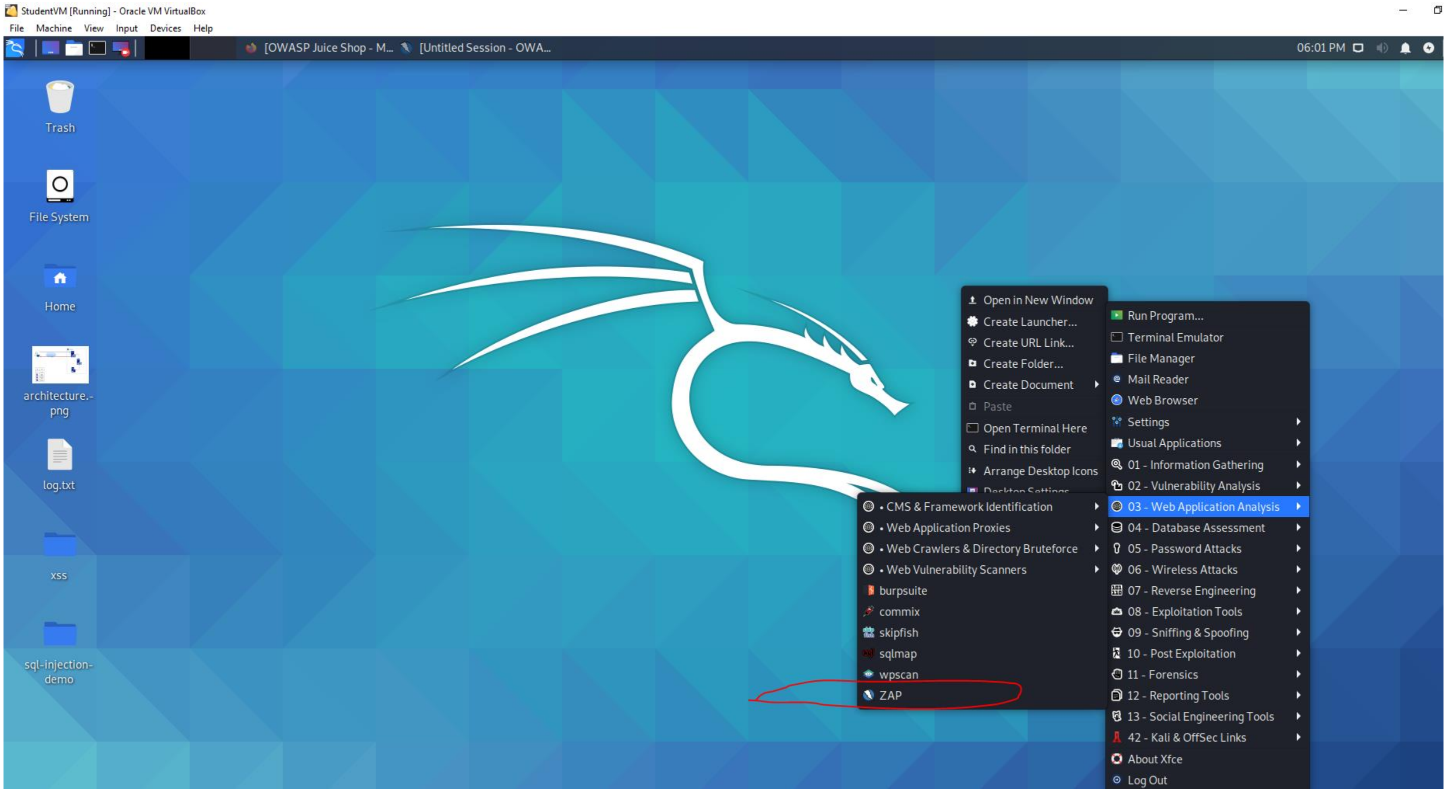


I would also consider OWASP Juice shop as a tool that I have used because I would use the OWASP ZAP TOOL so that I input localhost:3000 as the website address .

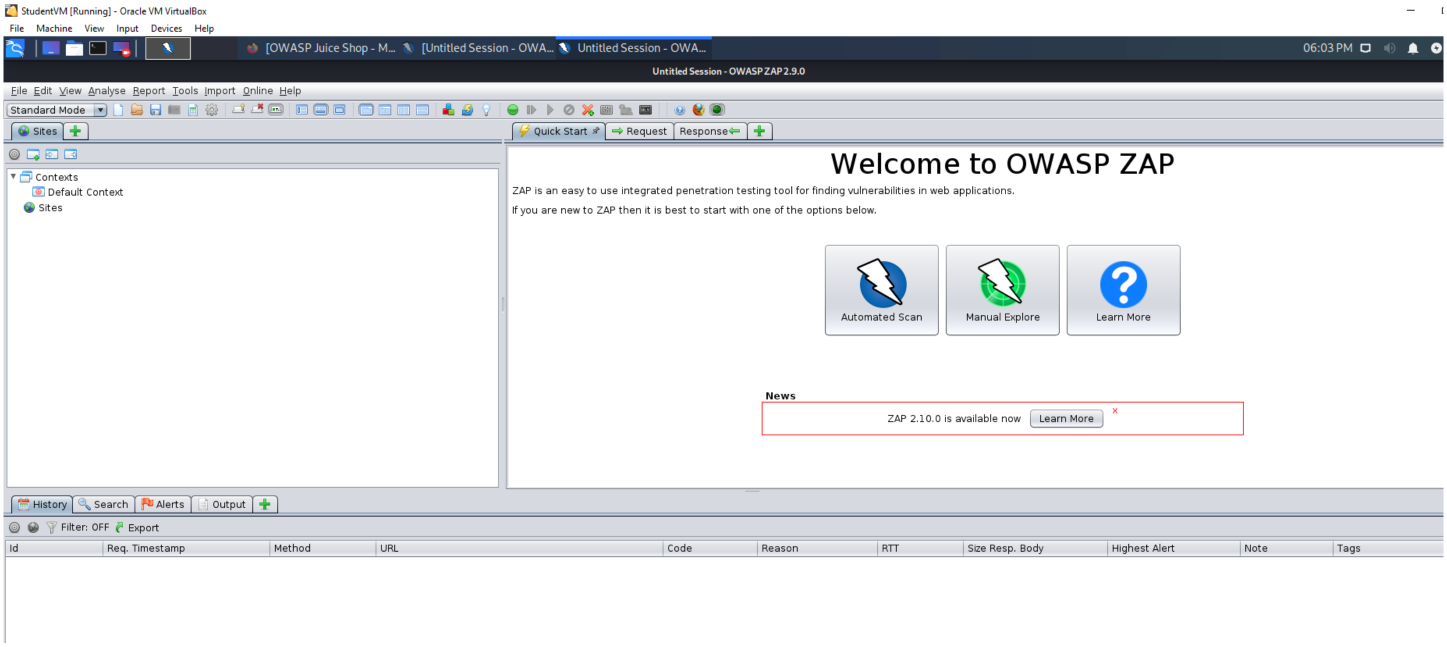
I needed to find vulnerabilities on the OSWAP Juice SHOP.

I would analyze the security threats on the OWASP ZAP TOOL.

5)



My next tool that I used is the OSWAP ZAP TOOL. I find it an easy process. First I right click, then I press on web Application Analysis, then I click on ZAP .

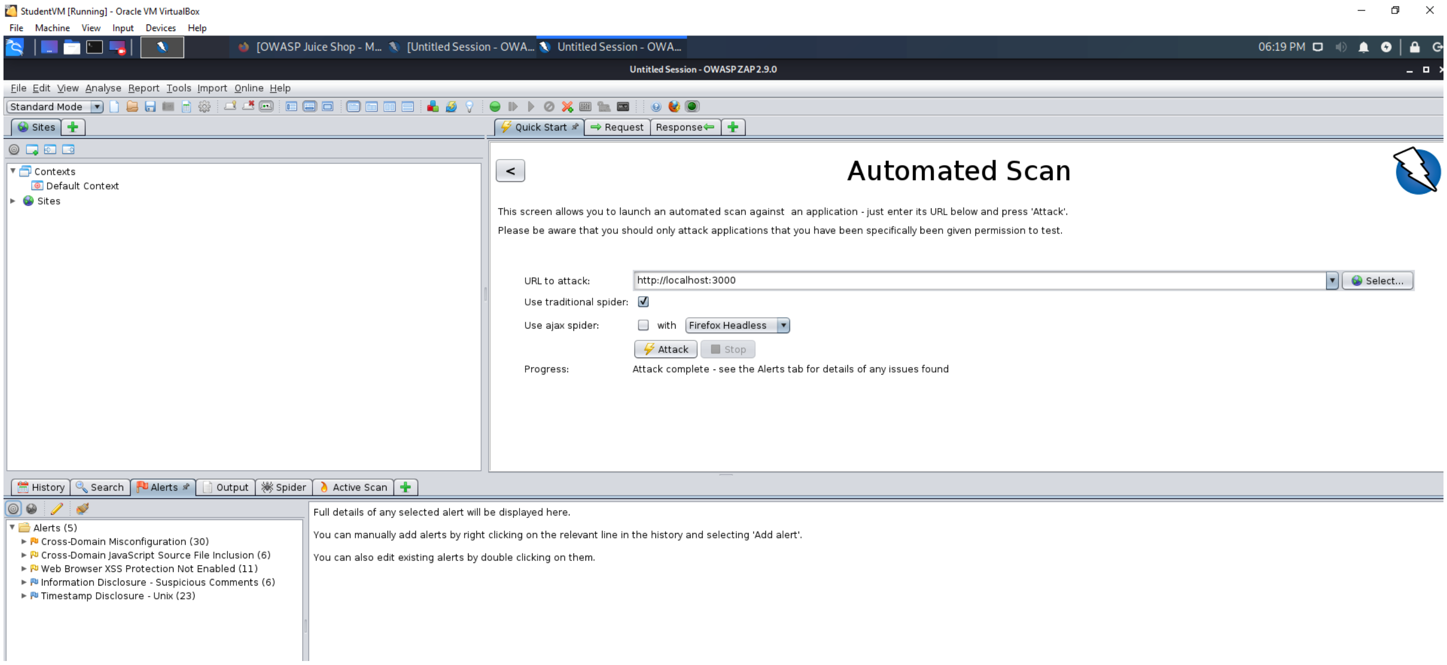


Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

ZAP 2.10.0 is available now



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://localhost:3000

Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Progress: Attack complete - see the Alerts tab for details of any issues found

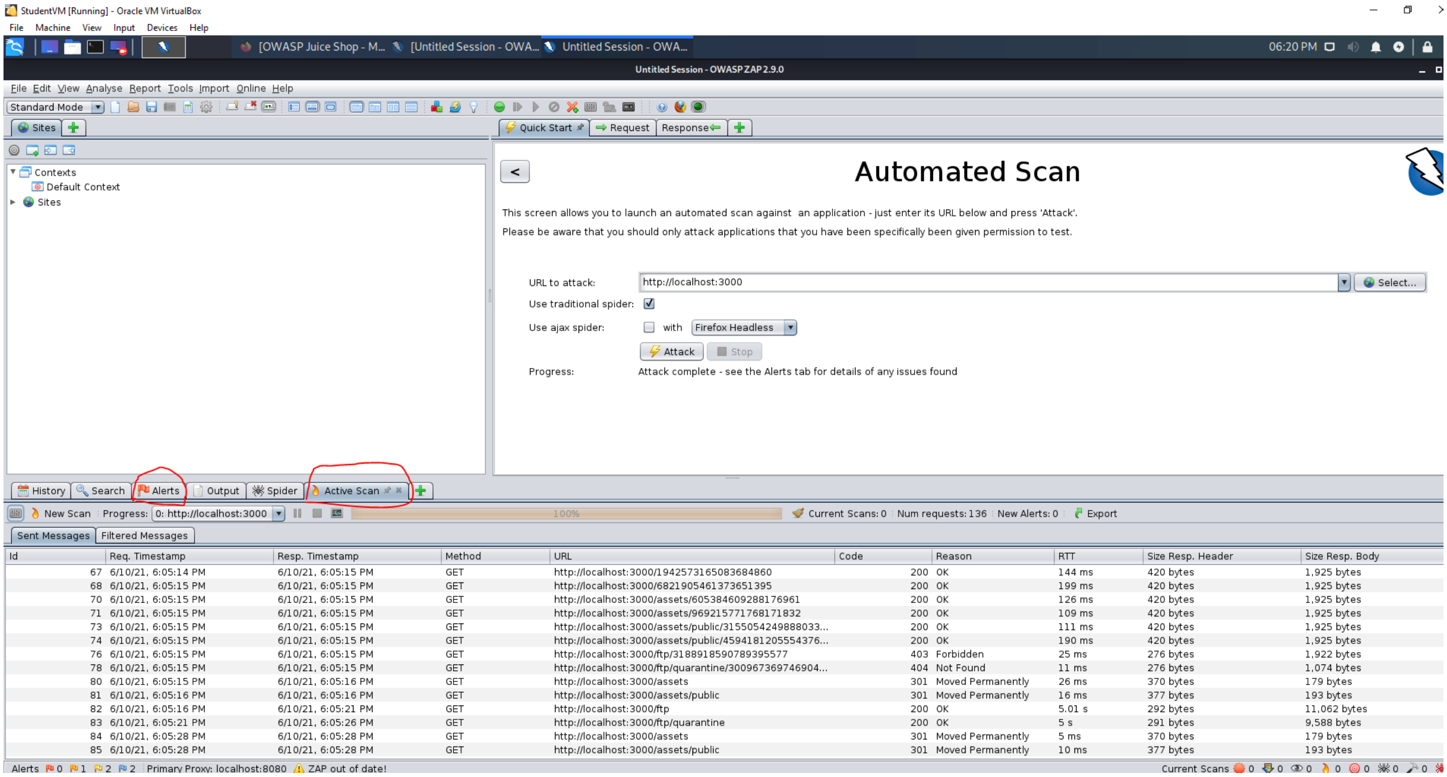
- Alerts (5)
  - Cross-Domain Misconfiguration (30)
  - Cross-Domain JavaScript Source File Inclusion (6)
  - Web Browser XSS Protection Not Enabled (11)
  - Information Disclosure - Suspicious Comments (6)
  - Timestamp Disclosure - Unix (23)

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

StudentVM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[OWASP Juice Shop - M... [Untitled Session - OWA... Untitled Session - OWA...
06:19 PM
Untitled Session - OWASP ZAP 2.9.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
Select...
Attack
Stop
History
Search
Alerts
Output
Spider
Active Scan



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://localhost:3000

Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Progress: Attack complete - see the Alerts tab for details of any issues found

New Scan | Progress: 0: http://localhost:3000 | 100% | Current Scans: 0 | Num requests: 136 | New Alerts: 0 | Export

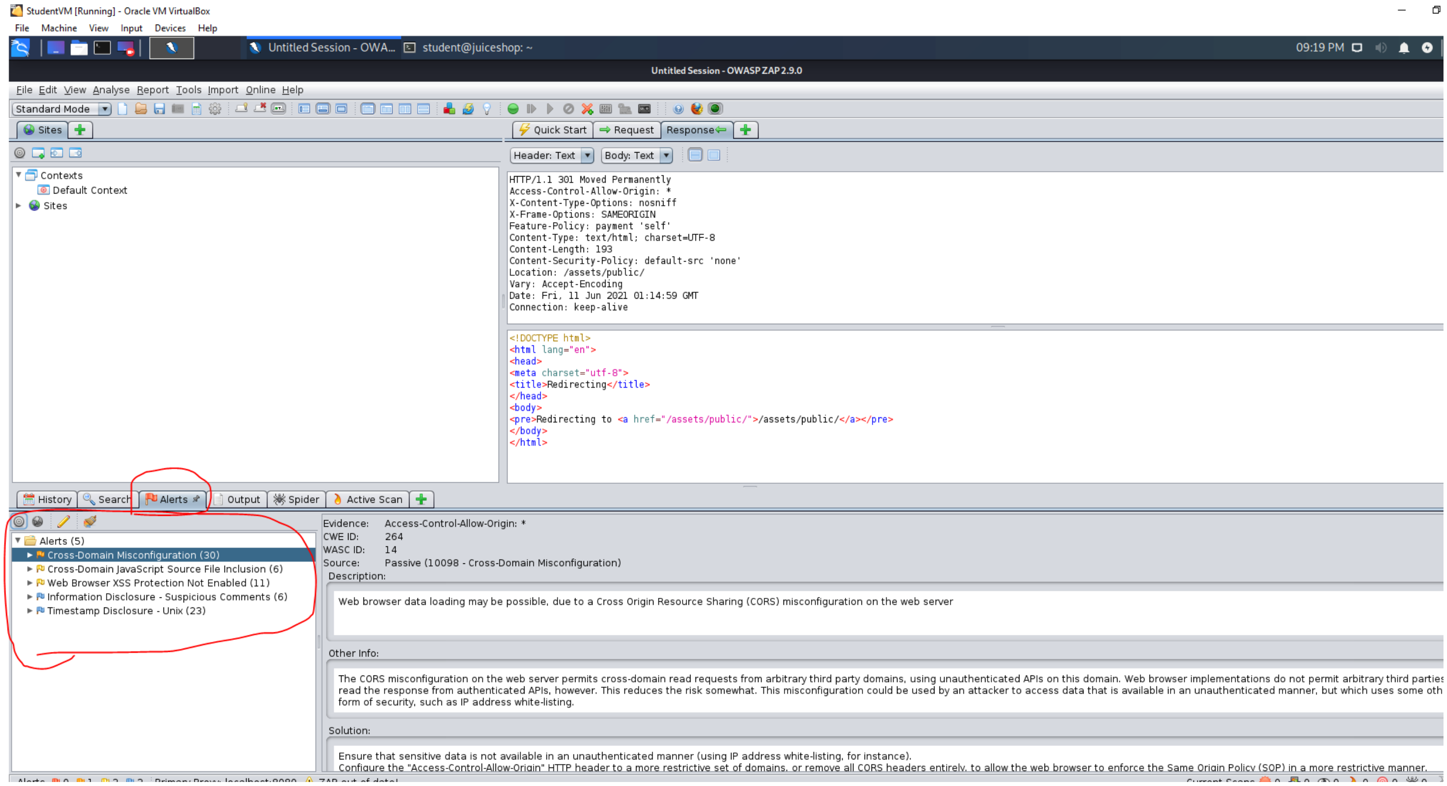
Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
67	6/10/21, 6:05:14 PM	6/10/21, 6:05:15 PM	GET	http://localhost:3000/1942573165083684860	200	OK	144 ms	420 bytes	1,925 bytes
68	6/10/21, 6:05:15 PM	6/10/21, 6:05:15 PM	GET	http://localhost:3000/6821905461373651395	200	OK	199 ms	420 bytes	1,925 bytes
70	6/10/21, 6:05:15 PM	6/10/21, 6:05:15 PM	GET	http://localhost:3000/assets/6053846092881 76961	200	OK	126 ms	420 bytes	1,925 bytes
71	6/10/21, 6:05:15 PM	6/10/21, 6:05:15 PM	GET	http://localhost:3000/assets/9692157717681 71832	200	OK	109 ms	420 bytes	1,925 bytes
73	6/10/21, 6:05:15 PM	6/10/21, 6:05:15 PM	GET	http://localhost:3000/assets/public/3155054249888033...	200	OK	111 ms	420 bytes	1,925 bytes
74	6/10/21, 6:05:15 PM	6/10/21, 6:05:15 PM	GET	http://localhost:3000/assets/public/4594181205554376...	200	OK	190 ms	420 bytes	1,925 bytes
76	6/10/21, 6:05:15 PM	6/10/21, 6:05:15 PM	GET	http://localhost:3000/ftp/3188918590789395577	403	Forbidden	25 ms	276 bytes	1,922 bytes
78	6/10/21, 6:05:15 PM	6/10/21, 6:05:15 PM	GET	http://localhost:3000/ftp/quarantine/300967369746904...	404	Not Found	11 ms	276 bytes	1,074 bytes
80	6/10/21, 6:05:15 PM	6/10/21, 6:05:16 PM	GET	http://localhost:3000/assets	301	Moved Permanently	26 ms	370 bytes	179 bytes
81	6/10/21, 6:05:16 PM	6/10/21, 6:05:16 PM	GET	http://localhost:3000/assets/public	301	Moved Permanently	16 ms	377 bytes	193 bytes
82	6/10/21, 6:05:16 PM	6/10/21, 6:05:21 PM	GET	http://localhost:3000/ftp	200	OK	5.01 s	292 bytes	11,062 bytes
83	6/10/21, 6:05:21 PM	6/10/21, 6:05:26 PM	GET	http://localhost:3000/ftp/quarantine	200	OK	5 s	291 bytes	9,588 bytes
84	6/10/21, 6:05:28 PM	6/10/21, 6:05:28 PM	GET	http://localhost:3000/assets	301	Moved Permanently	5 ms	370 bytes	179 bytes
85	6/10/21, 6:05:28 PM	6/10/21, 6:05:28 PM	GET	http://localhost:3000/assets/public	301	Moved Permanently	10 ms	377 bytes	193 bytes

Alerts 0 1 2 2 Primary Proxy: localhost:8080 ZAP out of date!

StudentVM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[OWASP Juice Shop - M... [Untitled Session - OWA... Untitled Session - OWA...
06:20 PM
Untitled Session - OWASP ZAP 2.9.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
Select...
Attack
Stop
History
Search
Alerts
Output
Spider
Active Scan
Sent Messages
Filtered Messages
Current Scans 0 0 0 0 0 0 0

The next step is that I am on the OWASP ZAP Tool. I would use this tool to help me scan for vulnerabilities for the OSWAP Juice Shop website. First, I would click on the automated Scan button, then on the URL to attack Next to it I would input the web address, so in this case I wanted to type http://localhost:3000 . I would do this because I wanted to scan for vulnerabilities for the OSWAP Juice Shop website.

I would then browse to the bottom and check the alerts and active scan tabs, to learn more about the vulnerabilities.


StudentVM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Untitled Session - OWA...
student@juiceshop: ~
09:19 PM
Untitled Session - OWASP ZAP 2.9.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Text
Contexts
Default Context
Sites
History
Search
Alerts
Output
Spider
Active Scan

```
HTTP/1.1 301 Moved Permanently
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Type: text/html; charset=UTF-8
Content-Length: 193
Content-Security-Policy: default-src 'none'
Location: /assets/public/
Vary: Accept-Encoding
Date: Fri, 11 Jun 2021 01:14:59 GMT
Connection: keep-alive
```

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Redirecting</title>
</head>
<body>
<pre>Redirecting to <a href="/assets/public/">/assets/public/</a></pre>
</body>
</html>
```

Alerts (5)
- Cross-Domain Misconfiguration (30)
- Cross-Domain JavaScript Source File Inclusion (6)
- Web Browser XSS Protection Not Enabled (11)
- Information Disclosure - Suspicious Comments (6)
- Timestamp Disclosure - Unix (23)

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 read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some oth form of security, such as IP address white-listing.

Solution:

Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

I have used the OWASP ZAP Tool to help me search for vulnerabilities on the OWASP Juice shop website.

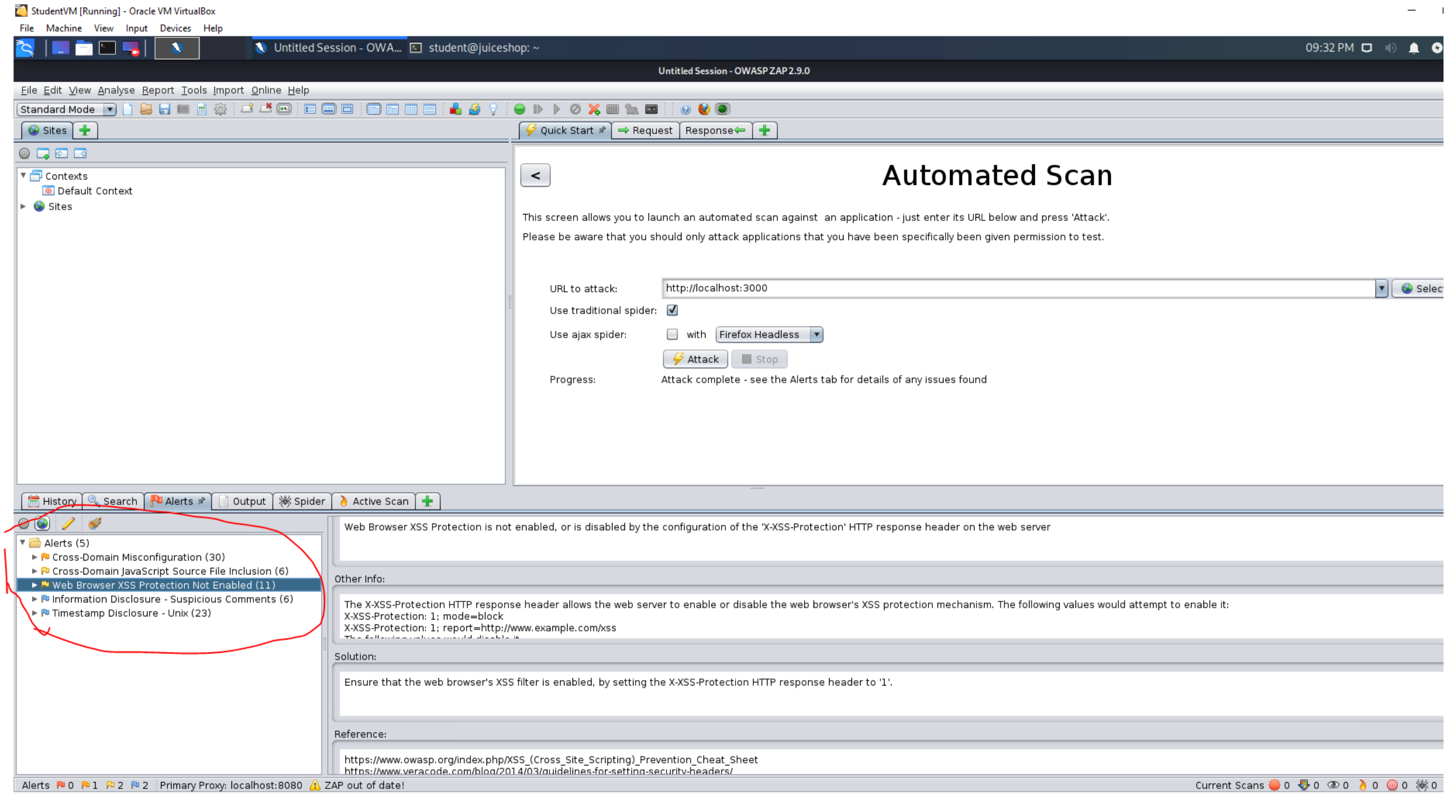
I have found these vulnerabilities by first going to the OWASP ZAP Tool , I opened it then I went to automated scan and I typed: localhost:3000 . I clicked on the attack button, and it launch the search.

The next step is that I scrolled down, and went to the alerts tab . I browsed and I would find several vulnerabilities.

The first vulnerability is : Cross Domain Configuration.

The Cross Domain Configuration vulnerability is defined as a vulnerability where misconfiguration could used by an attacker to access data in an unauthenticated Manner.

The solution to mitigate Cross Domain Configuration is ensure sensitive data is not available in an unauthenticated manner.



StudentVM [Running] - Oracle VM VirtualBox

Untitled Session - OWASP ZAP 2.9.0

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://localhost:3000
Use traditional spider: ☑
Use ajax spider: ☐ with Firefox Headless
Progress: Attack complete - see the Alerts tab for details of any issues found

Alerts (5)
- Cross-Domain Misconfiguration (30)
- Cross-Domain JavaScript Source File Inclusion (6)
- Web Browser XSS Protection Not Enabled (11)
- Information Disclosure - Suspicious Comments (6)
- Timestamp Disclosure - Unix (23)

Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server

Other Info:

```
The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it:
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; report=http://www.example.com/xss
```

Solution:

Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.

Reference:

https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
https://www.veracode.com/blog/2014/03/guidelines-for-setting-security-headers/

Alerts 0 1 2 2 Primary Proxy: localhost:8080 ZAP out of date! Current Scans 0 0 0 0 0 0

The next vulnerability that I have discovered by using the OWASP ZAP Tool is : Web Browser XSS Not enabled.

I have found this vulnerability by going to OWASP ZAP TOOL, then I went on the automated scan.

Next to the URL to attack : I typed in http://localhost:3000 . Then I clicked on the attack button, next I would scroll to the bottom and click the alerts tab. I have found that one of the vulnerability that I have discovered is Web Browser XSS .

The Web Browser XSS vulnerability is defined as HTTP response headers allows the web server to enable or disable

By the configuration.

The solution to mitigate is to ensure that the web browser’s XSS filter is enabled.