SECURITY ASSESSMENT

<< Udajuicer Vulnerability Assessment>>

Submitted to: << Development team >>
Security Analyst: << Rahaf Ibrahim Aloufi >>

Date of Testing: << 30-11-2022>
Date of Report Delivery: <<8-12-2022>

Table of Contents

Contents

SECURITY ENGAGEMENT SUMMARY 2

ENGAGEMENT OVERVIEW 2

SCOPE 2

RISK ANALYSIS ..... **ERROR! BOOKMARK NOT DEFINED.**

RECOMMENDATION ..... **ERROR! BOOKMARK NOT DEFINED.**

SIGNIFICANT VULNERABILITY SUMMARY 3

High Risk Vulnerabilities 3

Medium Risk Vulnerabilities 3

Low Risk Vulnerabilities 3

SIGNIFICANT VULNERABILITY DETAIL 4

<< VULNERABILITY NAME>> 4

<< VULNERABILITY NAME>> 5

METHODOLOGY 6

ASSESSMENT TOOLSET SELECTION 6

ASSESSMENT METHODOLOGY DETAIL 7

Security Engagement Summary

Engagement Overview

Vulnerability assessment requested by development team because help them understand what security risk the web-application is posing to the organization, and what mitigations are possible to increase the security posture and reduce the risk to the organization. The goal of this engagement is to identify the vulnerability in the juice shop web-application. The security analyst and the information security management team are the ones who will work on the vulnerability scanning tasks. Vulnerability scan should be done at the first of every month because we need to be assured that all mitigation method has been taken and it is affected.

Scope

The scope of this engagement includes all individuals in information security team who assign to work with the vulnerability scanning. This assessment's scope is to make sure that the juice shop web-application which is an important business platform, is in compliance. Also to make sure to provide the security triad CIA which is confidentiality, integrity, and availability, to the website.

Executive Risk Analysis

This report indicates there is a high level of risk that the juice shop website faces. There are numerous different types of vulnerabilities found on the Juice Shop website. The reason for reporting this level of danger is that the juice shop website contains many dangerous vulnerabilities that a hacker can exploit to access the web-application resources of the juice shop and also threatens the security triad CIA (Confidentiality, integrity, and availability). After vulnerability scanning, it found seven vulnerabilities in the juice shop web application. Four of them are at a high-risk level, two of them are at a medium-risk level, and just one of them is at a low-risk level. As overall can be rank the website in risk level HIGH. So we need immediate remediation and mitigation to keep the web application server online.

Executive Recommendation

To address and mitigate the highest risk vulnerability, we need to shut down or disable the OpenSSH server on our juice web application. Because, ssh service port 22 which is used for remote login from one computer to another, is a threat to the web application. Also, the development security team should assign a dedicated SSH port to help eliminate noise on port 22. The development security team should also filter the SSH port on the Application Server firewall by configuring firewall policies. Also, one of the tasks of the development security team is to secure the ssh service using a login without a password. Finally, server packages for shh should always be kept up to date.

The mitigation plan for medium-risk vulnerabilities is based on encryption mechanisms. Therefore, the development security team is required to change the key. Dedicated information leakage as a risk assessment. As mentioned by Damian Miller, due to changes in the order, the client can obtain another public key from the server, which may trigger a key change warning. There are two recommended ways to do this, Certificate-Based Host Key Algorithms (recommended) and manually setting HostKeyAlgorithms.

As for the vulnerabilities with a low level of risk, Product Security companies do not consider this a security vulnerability. Therefore, there is no plan to mitigate this vulnerability.

Significant Vulnerability Summary

High Risk Vulnerabilities

- CVE-2020-15778 with CVSS 7.8 score. CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Medium Risk Vulnerabilities

- CVE-2020-14145 with CVSS 5.9 score. CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Low Risk Vulnerabilities

- CVE-2021-36368 with CVSS 3.7 score. CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

Significant Vulnerability Detail

CVE-2020-15778

RISK LEVEL HIGH

The risk level for this vulnerability is high because it has CVSS 7.8 score. The security vulnerability was verified by running many vulnerability scanning tools such as Nmap, Nessus, and others (details come in the methodology part). A hacker can exploit this vulnerability by using port 22 and ssh to remotely access the server and threaten its security, steal client data and gain administrator privileges.

This exploitation will affect the continuity of the web application because it is likely that the hacker will perform DDOS attacks and prevent the service from the server. Also, it may affect the revenue of the store due to unavailability, and the reputation of the juice store may also be affected, and users feel the danger of adding their credit cards and personal information. By adding the command as part of the filename being copied on the server, an attacker with the ability to scp files to a remote server might execute arbitrary commands on the server. With the user whose credentials the files were copied to the remote server, this command is executed. Data integrity and confidentiality, as well as system availability, are the areas that are most at risk from this vulnerability.

To discuss the possibility of an exploit for CVE-2020-15778, we need to know the exploit method. As we mentioned earlier, this vulnerability exploits the open SSH and Port 22 service, and thus the possibility of its occurrence is related to the availability of this port. We can summarize the probability of exploiting this vulnerability with a direct relationship with the more open the SSH and Port 22 service, the greater the risk probability.

To mitigate this vulnerability, we recommend that you close port 22 ssh service. Filter the SSH port on your firewall by configuring the firewall policies. Secure the ssh service by using Passwordless Login. Finally, always keep the server packages for shh updated.

CVE-2020-14145

RISK LEVEL MEDIUM

The risk level for this vulnerability is medium because it has CVSS 5.9 score. The security vulnerability was verified by running many vulnerability scanning tools such as Nmap, Nessus, and others (details come in the methodology part). The flaw in OpenSSH versions 5.7 to 8.3 can be exploited. Through this vulnerability, a hacker can initiate man-in-the-middle attacks by targeting initial connection attempts since there is no host key for the server that is cached by the client.

The overall evaluation of the risks of the Cve-2020-14145 security vulnerability can be calculated by setting the risk Impact and the risk likelihood. To determine the possibility of this exploitation, we need to know the method of exploitation, this weakness benefits from a flaw in some OpenSSH versions to perform an attack in the middle. Therefore, if the server contains OpenSSH versions from 5.7 to 8.3, the possibility of exploiting this weakness is high, but if not, it will be low. To calculate the Impact of this exploitation, it affects the confidentiality of the customer's data and obtaining the credential of the admin. Therefore, the general evaluation of the risks of the CVE-2020-14145 security vulnerability is medium. Because just affect some of OpenSSH versions. To prevent any chance of a man-in-the-middle attack, always connect to SSH servers using verified host keys. Also, keep OpenSSL upgrade to the latest version.

Methodology

To check for security vulnerabilities in the web application, we must first specify the IP address of the server, which is 10.0.2.4. After that, a scan can be made to search for security vulnerabilities. In this report, several tools were used to detect security vulnerabilities. One of these tools is Nmap The command "nmap 10.0.2.4 -sV --script=vulners' was used in the command line screen (CLI). Indeed "script=vulners" was used after the archive file was downloaded and then the archive was opened using "unzip master.zip".

Also, the Nessus tool was used to search for more vulnerabilities, and this happened after the Nessus tool was downloaded and installed from the Tenable site and an activation code was obtained. After downloading all the plugins, a new scan was created and the IP address of the juice shop web application was determined, which is (10.0.2 .4.) However, no observable vulnerabilities were found unlike when Nmap was used.

Through the Nmap tool, seven security vulnerabilities were obtained in the juice shop server. Four of them are at high risk and are CVE-2020-15778, CVE-2020-12062, CVE-2021-28041, and CVE-2021-41617. These are security vulnerabilities that exploit the SSH service on Port 22 to access the server and log in remotely. To address and mitigate the effects of this vulnerability, the OpenSSH server on the juice web application must be closed or disabled. Also, you should assign a dedicated SSH port to help eliminate noise on port 22. SSH port filtering on your firewall by configuring firewall policies. Secure your ssh service using passwordless login. Finally, always keep the server packages for shh up to date. Two of the seven are at medium risk, CVE-2020-14145, and CVE-2016-20012. This vulnerability exploits an SSH server and allows an attacker to gain remote access to the server and try the username and public key known to the SSH server to obtain a valid login session. To mitigate this vulnerability, we recommend that the client obtain another public key from the server, which may trigger a key change warning. Most SSH servers have different keys (RSA, elliptical curve, ...) and the server will respond with your preferred algorithm. There are two recommended ways to do this, Certificate-Based Host Key Algorithms (recommended) and manually setting HostKeyAlgorithms. To prevent any chance of a man-in-the-middle attack, always connect to SSH servers using verified host keys.

The latest vulnerability discovered by the Nmap tool is CVE-2021-36368, which has a low severity stage. Before version 8.9, OpenSSH had a problem. If a server has been silently modified by an attacker to support the None authentication option and a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, the user cannot tell whether FIDO authentication will confirm that the user wishes to connect to that server or that the user wishes to permit that server to connect to another server on the user's behalf. Red Hat Product Security does not consider this a security vulnerability. Therefore we do not recommend any mitigation and remediation methods

Also, through the Nikto tool, URL links have been accessed so that the hacker can access, manipulate and steal the data inside, and this threatens the security triad of the web application.

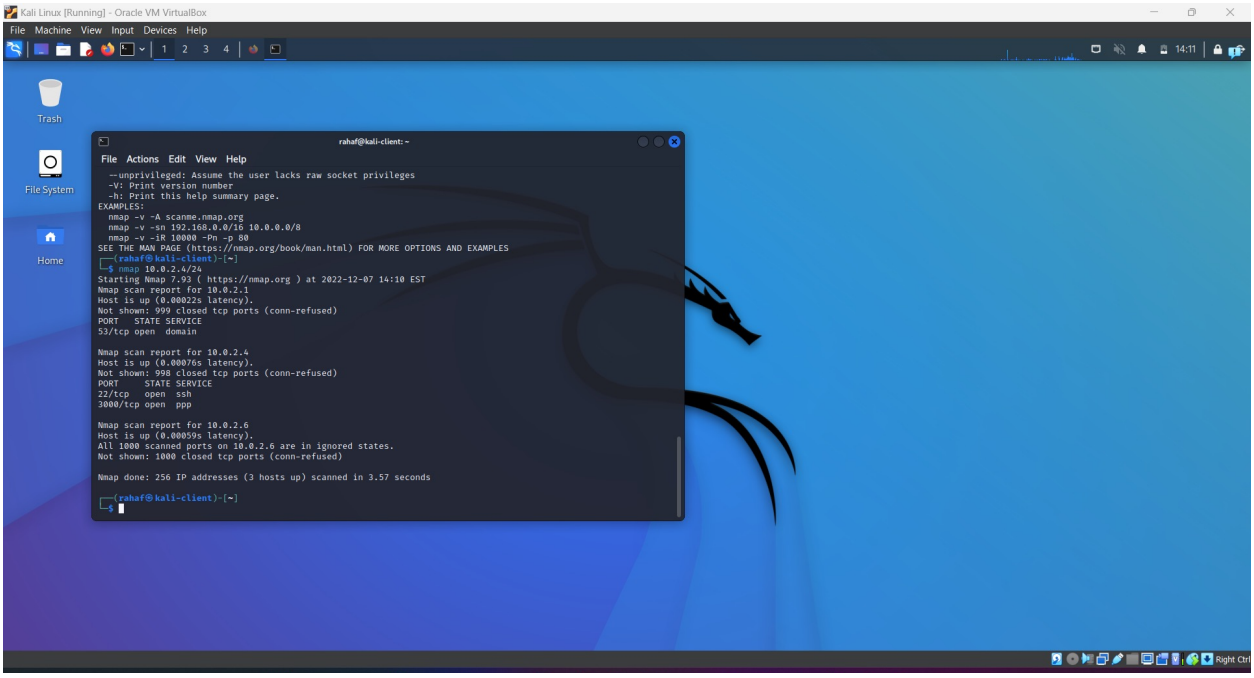
The exploitation of security vulnerabilities can occur for a wide variety of organizations. The hacker targets companies that have a lot to lose. Small enterprises may also be targeted to damage their resources. The security development department must embrace cyber security policies to identify, prevent, detect and mitigate attacks. Include policies to recover if an attack occurs. The security development team must also assess its system and its sensitivity to a potential data breach. It must be taken into account that attacks do not come only from outside intruders, they may be from within, intentionally or unintentionally. Therefore, the security department in “Udajuicer” must raise awareness and develop policies to limit the exploitation of security vulnerabilities, such as keeping systems updated to the latest update. Cyberattacks cannot be stopped, and as technology develops, their frequency and expense increase annually. The best practice of action for any size of business is to create security mechanisms and a breach response strategy. For the web application to continue to function Udajuicer, a continuity plan must be defined. First, according to CVE-2020-15778, for continuity, port 22 of the SSH service must be kept closed or disabled. As for CVE-2020-14145, for continuity, you must keep OpenSSH updated to the latest version. And change the client's key to get another public key from the server.

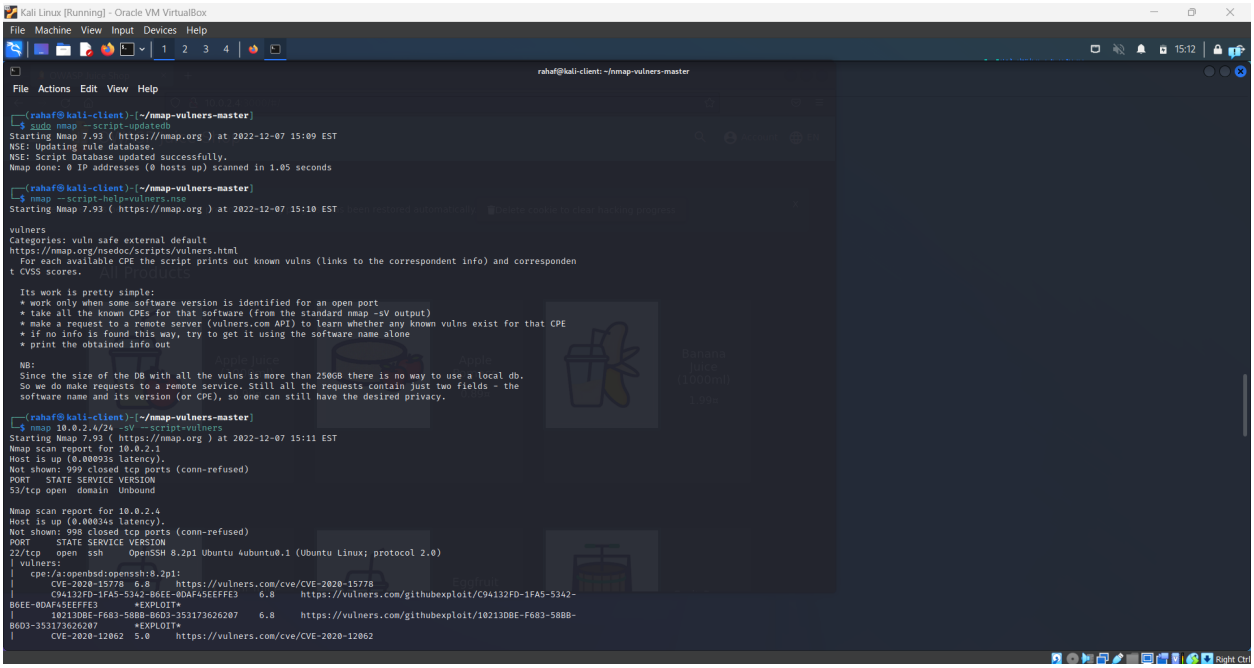
Assessment Toolset Selection

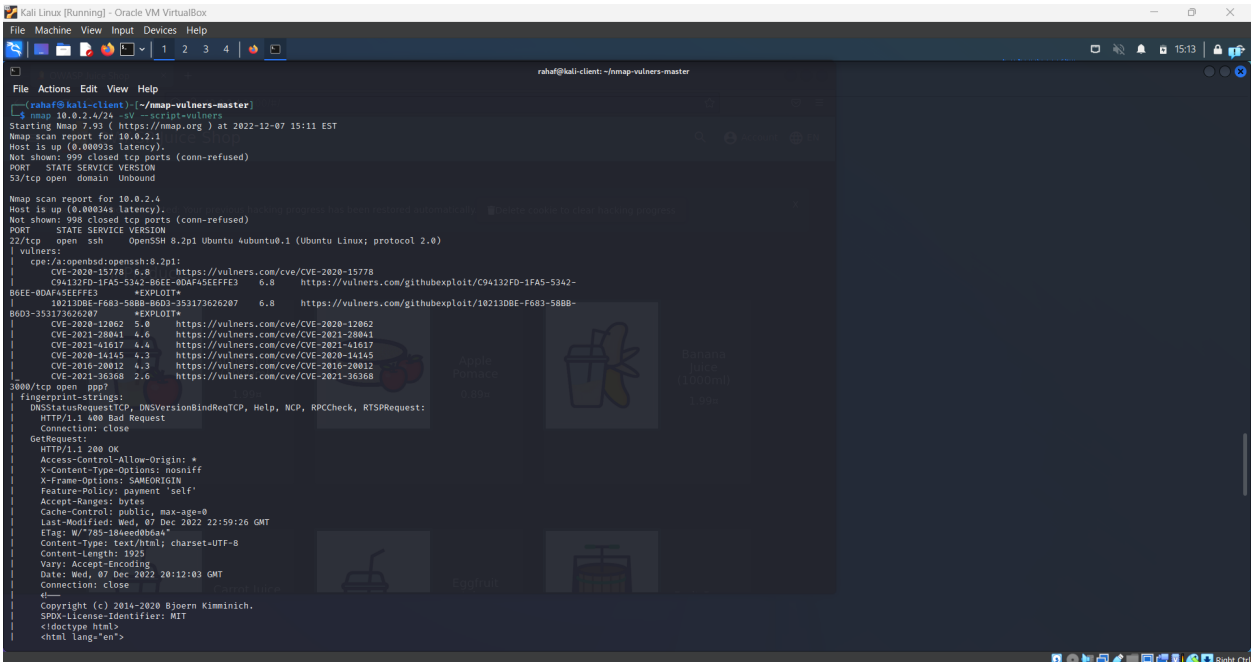
List of tools used during the vulnerability assessment and validation.

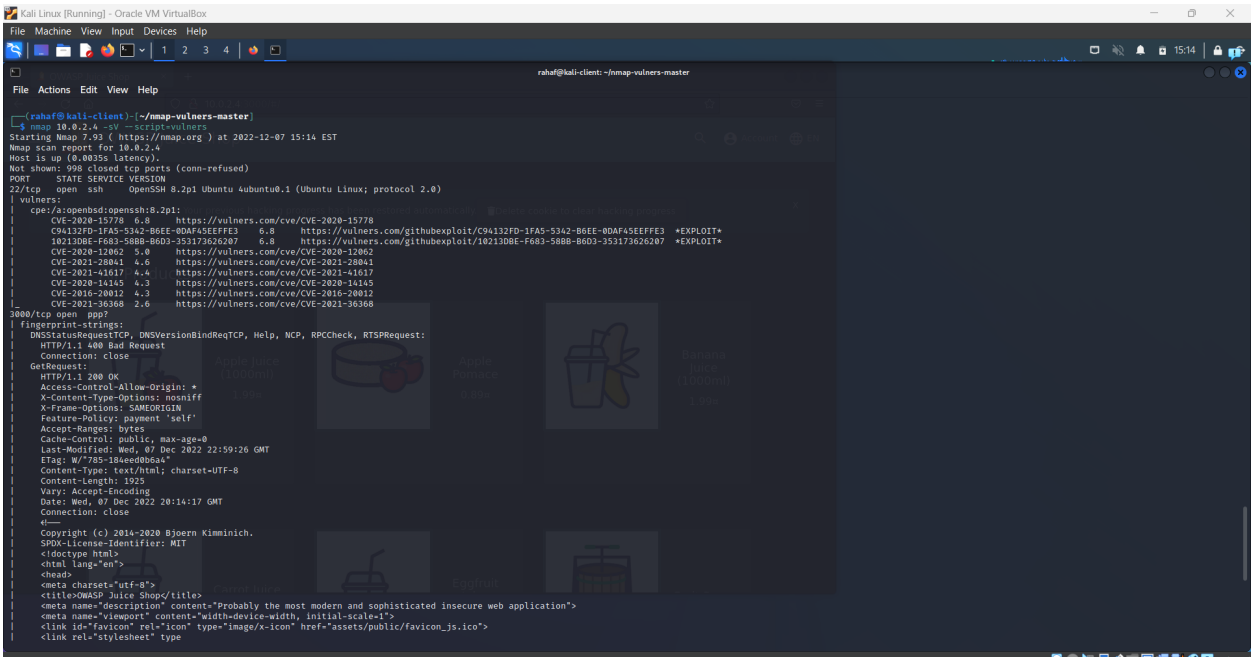
- Nmap
- Nessus
- Nikto
- OWASP ZAP

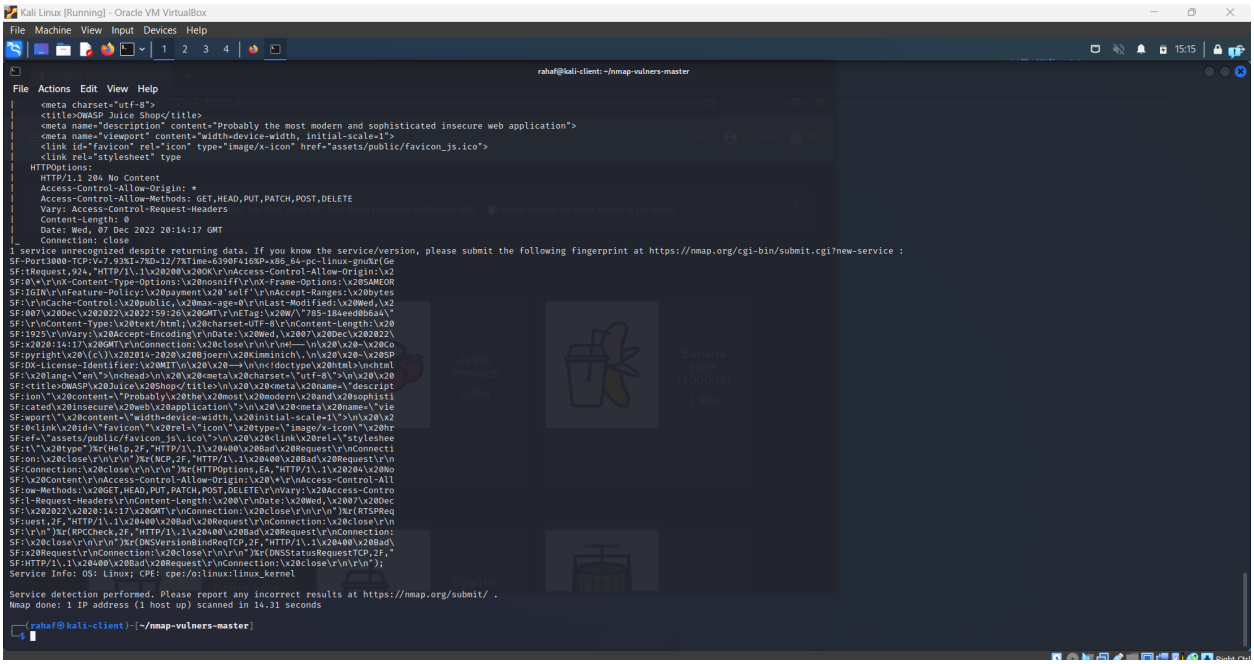
Assessment Methodology Detail

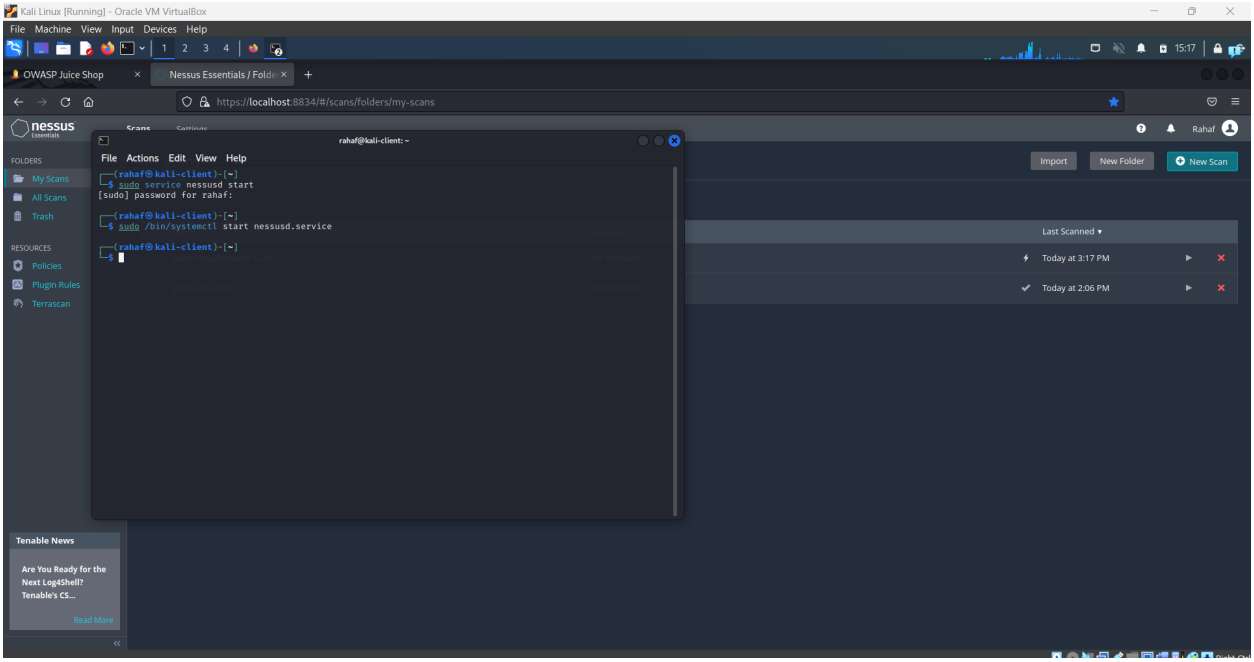


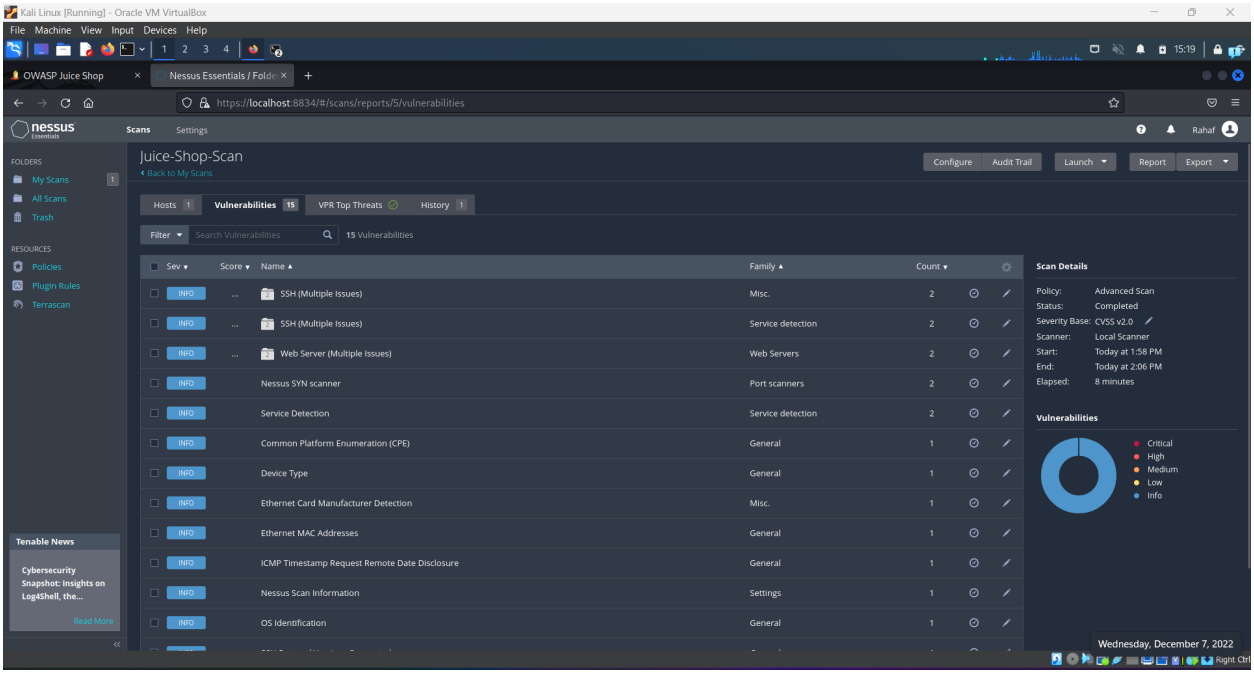


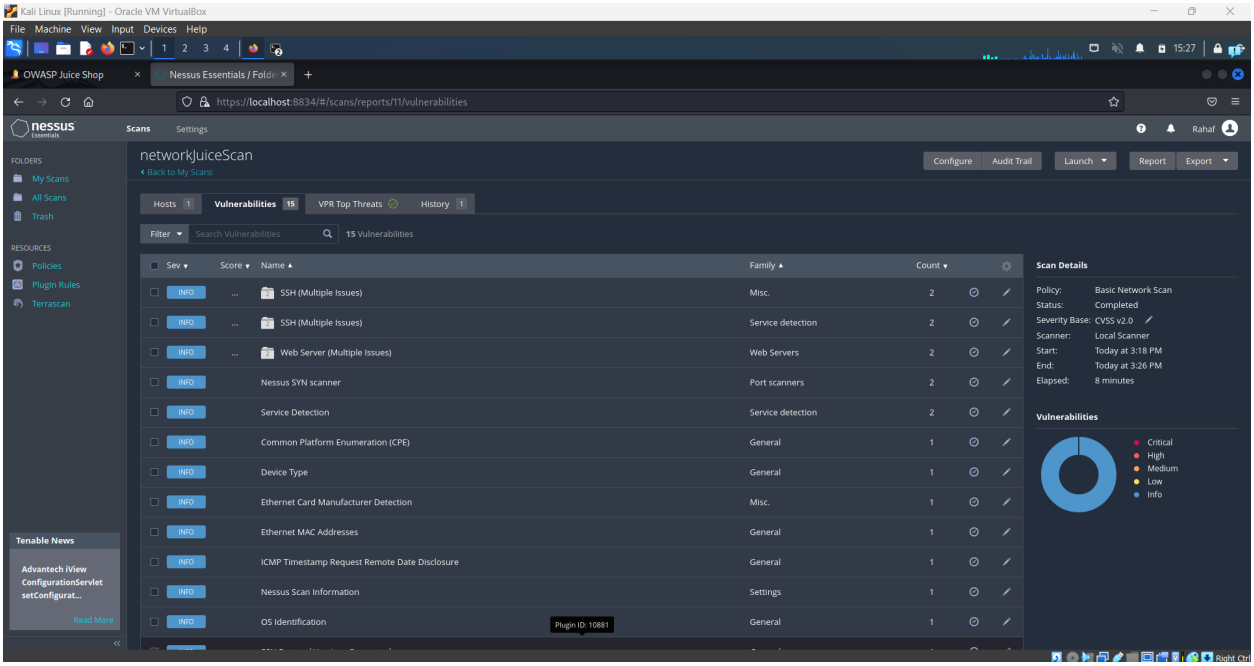

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
rahaf@kali-client: ~/nmap-vulners-master
File Actions Edit View Help
(rahaf㉿kali-client)-[~/nmap-vulners-master]
$ nmap 10.0.2.4/24 -sV --script=vulners
Starting Nmap 7.93 (https://nmap.org) at 2022-12-07 15:11 EST
Nmap scan report for 10.0.2.1
Host is up (0.00093s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
53/tcp open domain Unbound
Nmap scan report for 10.0.2.4
Host is up (0.00034s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| vulners:
| cpe:/a:openbsd:openssh:8.2p1:
| CVE-2020-15778 6.8 https://vulners.com/cve/CVE-2020-15778
| C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 6.8 https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 *EXPLOIT*
| 10213DBE-F683-588B-B6D3-353173626207 6.8 https://vulners.com/githubexploit/10213DBE-F683-588B-B6D3-353173626207 *EXPLOIT*
| CVE-2020-12062 5.0 https://vulners.com/cve/CVE-2020-12062
| CVE-2021-28041 4.6 https://vulners.com/cve/CVE-2021-28041
| CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617
| CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145
| CVE-2016-20012 4.3 https://vulners.com/cve/CVE-2016-20012
|_ CVE-2021-36368 2.6 https://vulners.com/cve/CVE-2021-36368
3000/tcp open ppp?
| fingerprint-strings:
| DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, NCP, RPCCheck, RTSPRequest:
| HTTP/1.1 400 Bad Request
| Connection: close
| GetRequest:
| 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: Wed, 07 Dec 2022 22:59:26 GMT
| ETag: W/"785-184eed0b6a4"
| Content-Type: text/html; charset=UTF-8
| Content-Length: 1925
| Vary: Accept-Encoding
| Date: Wed, 07 Dec 2022 20:12:03 GMT
| Connection: close
| <!--
| Copyright (c) 2014-2020 Bjoern Kimminich.
| SPDX-License-Identifier: MIT
| <!doctype html>
| <html lang="en">
15:13

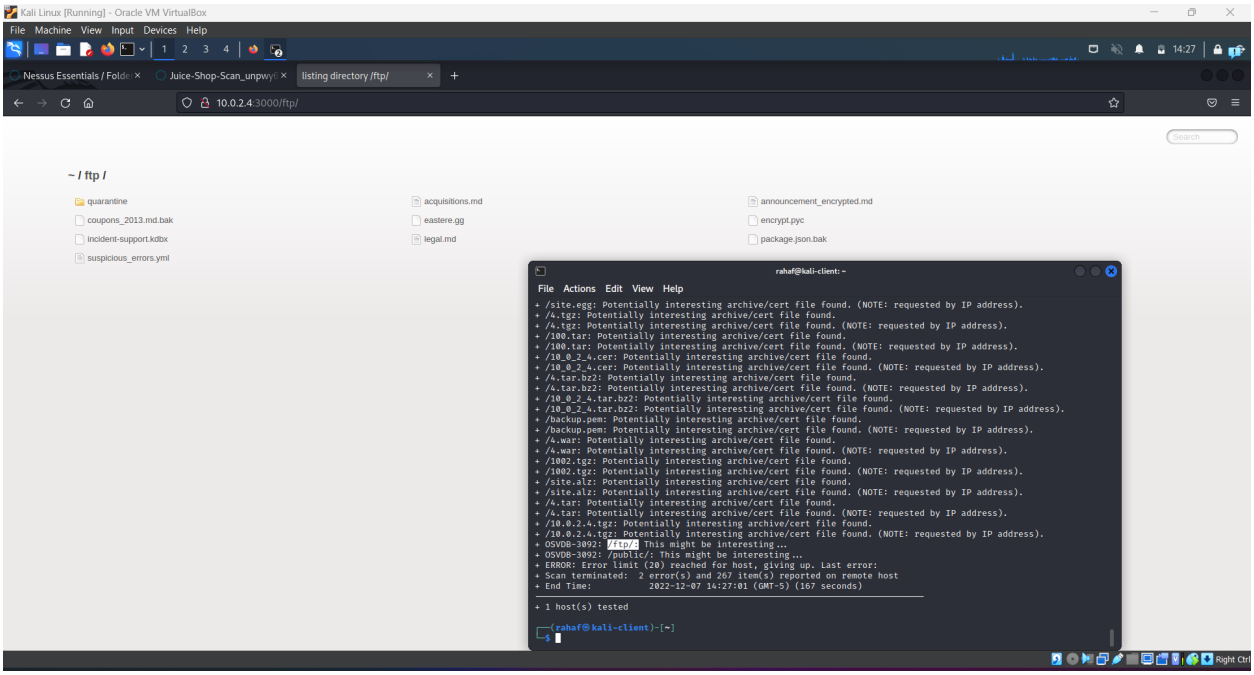

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
rahaf@kali-client: ~/nmap-vulners-master
File Actions Edit View Help
(rahaf㉿kali-client)-[~/nmap-vulners-master]
$ nmap 10.0.2.4 -sV --script=vulners
Starting Nmap 7.93 (https://nmap.org) at 2022-12-07 15:14 EST
Nmap scan report for 10.0.2.4
Host is up (0.0035s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| vulners:
| cpe:/a:openbsd:openssh:8.2p1:
| CVE-2020-15778 6.8 https://vulners.com/cve/CVE-2020-15778
| C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 6.8 https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 *EXPLOIT*
| 10213DBE-F683-588B-B6D3-353173626207 6.8 https://vulners.com/githubexploit/10213DBE-F683-588B-B6D3-353173626207 *EXPLOIT*
| CVE-2020-12062 5.0 https://vulners.com/cve/CVE-2020-12062
| CVE-2021-28041 4.6 https://vulners.com/cve/CVE-2021-28041
| CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617
| CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145
| CVE-2016-20012 4.3 https://vulners.com/cve/CVE-2016-20012
|_ CVE-2021-36368 2.6 https://vulners.com/cve/CVE-2021-36368
3000/tcp open ppp?
| fingerprint-strings:
| DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, NCP, RPCCheck, RTSPRequest:
| HTTP/1.1 400 Bad Request
| Connection: close
| GetRequest:
| 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: Wed, 07 Dec 2022 22:59:26 GMT
| ETag: W/"785-184eed0b6a4"
| Content-Type: text/html; charset=UTF-8
| Content-Length: 1925
| Vary: Accept-Encoding
| Date: Wed, 07 Dec 2022 20:14:17 GMT
| Connection: close
| <!--
| 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
15:14

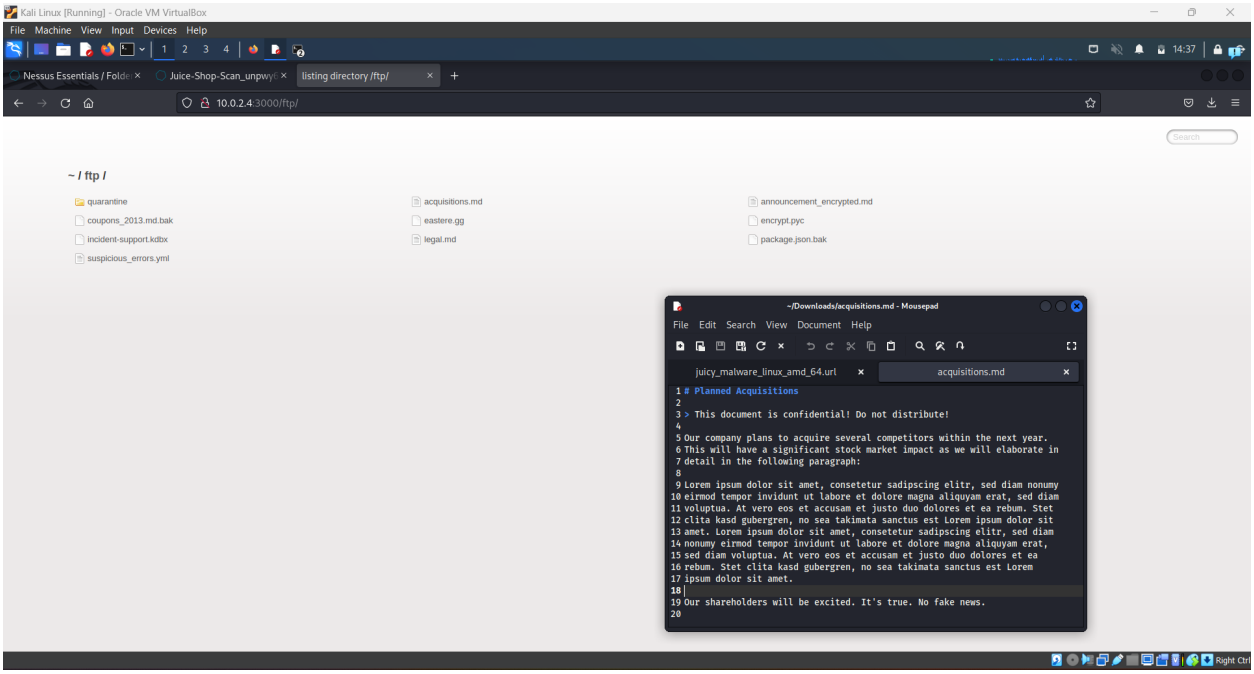

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
rahaf@kali-client: ~/nmap-vulners-master
File Actions Edit View Help
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.31 seconds
(rahaf㉿kali-client)-[~/nmap-vulners-master]

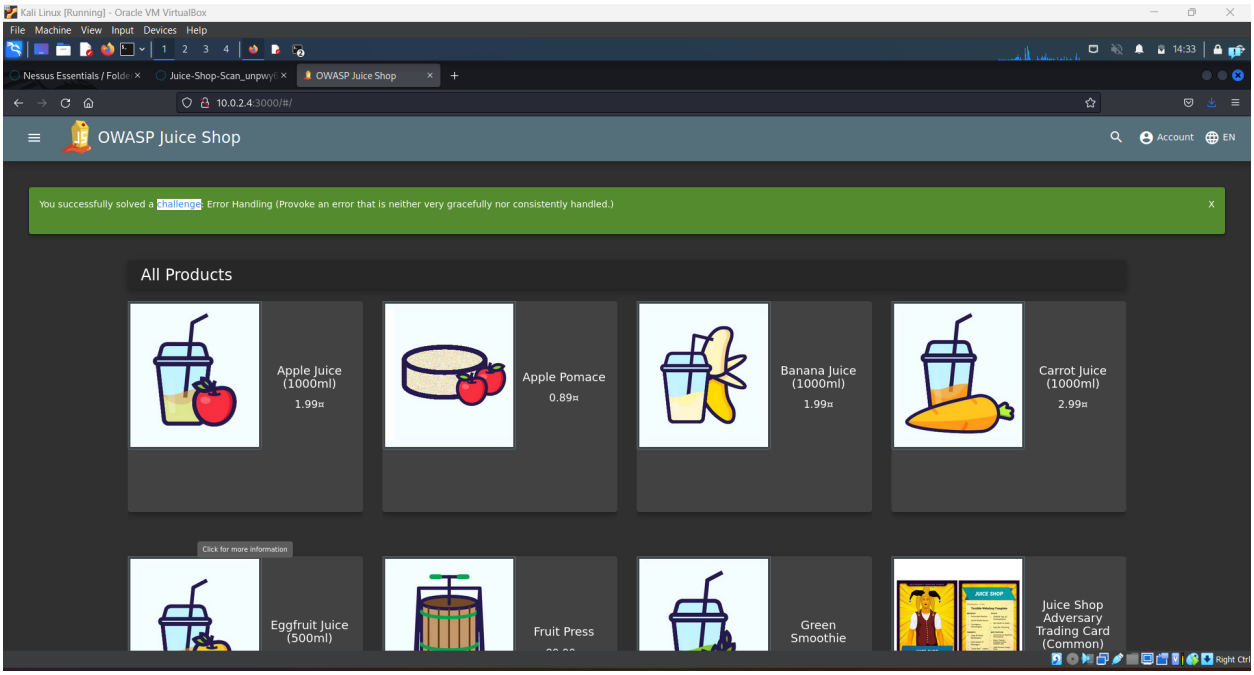

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
OWASP Juice Shop
Nessus Essentials / Folde
https://localhost:8834/#/scans/folders/my-scans
nessus
Rahaf
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Import
New Folder
New Scan
Last Scanned
Today at 3:17 PM
Today at 2:06 PM
rahaf@kali-client: ~
File Actions Edit View Help
(rahaf㉿kali-client)-[~]
$ sudo service nessusd start
[sudo] password for rahaf:
(rahaf㉿kali-client)-[~]
$ sudo /bin/systemctl start nessusd.service
(rahaf㉿kali-client)-[~]
$
Tenable News
Are You Ready for the Next Log4Shell? Tenable's CS...
Read More

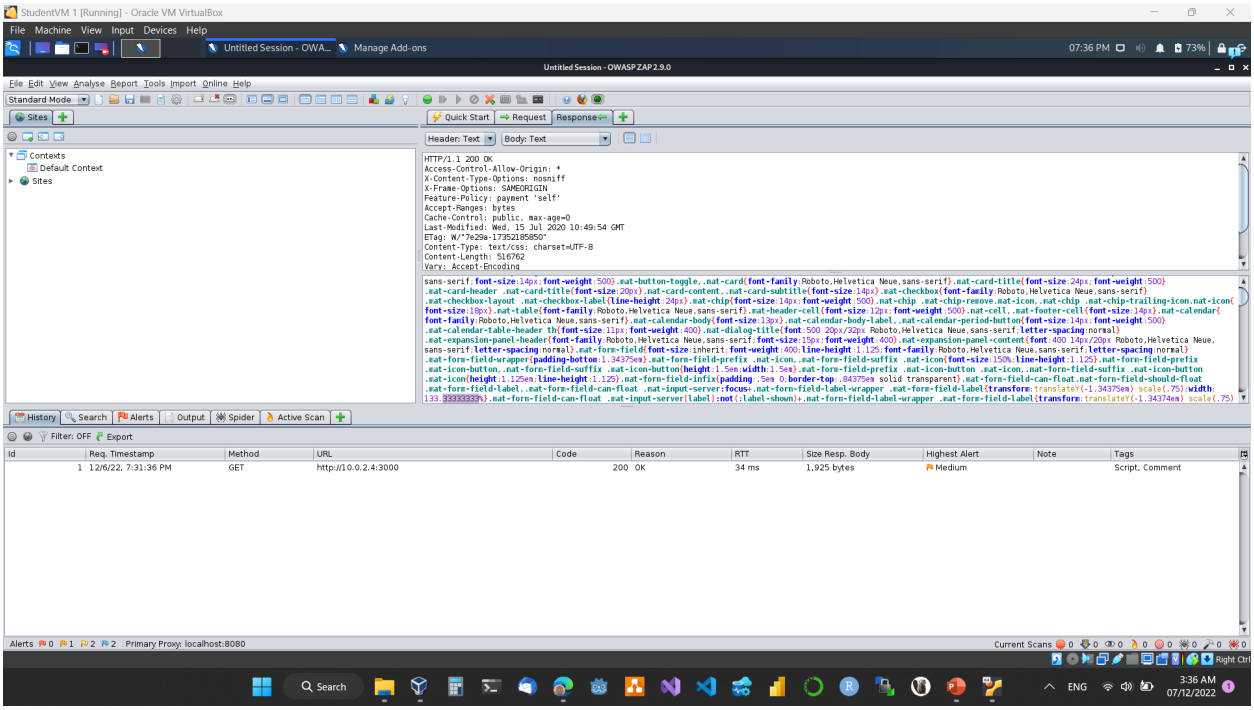

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
OWASP Juice Shop
Nessus Essentials / Folde
https://localhost:8834/#/scans/reports/5/vulnerabilities
nessus Essentials
Scans
Settings
Rahaf
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Cybersecurity Snapshot: Insights on Log4Shell, the...
Read More
Juice-Shop-Scan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 15
VPR Top Threats
History 1
Filter
Search Vulnerabilities
15 Vulnerabilities
Sev
Score
Name
Family
Count
INFO
SSH (Multiple Issues)
Misc.
2
SSH (Multiple Issues)
Service detection
2
Web Server (Multiple Issues)
Web Servers
2
Nessus SYN scanner
Port scanners
2
Service Detection
Service detection
2
Common Platform Enumeration (CPE)
General
1
Device Type
General
1
Ethernet Card Manufacturer Detection
Misc.
1
Ethernet MAC Addresses
General
1
ICMP Timestamp Request Remote Date Disclosure
General
1
Nessus Scan Information
Settings
1
OS Identification
General
1
Scan Details
Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v2.0
Scanner: Local Scanner
Start: Today at 1:58 PM
End: Today at 2:06 PM
Elapsed: 8 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Wednesday, December 7, 2022
Right Ctrl

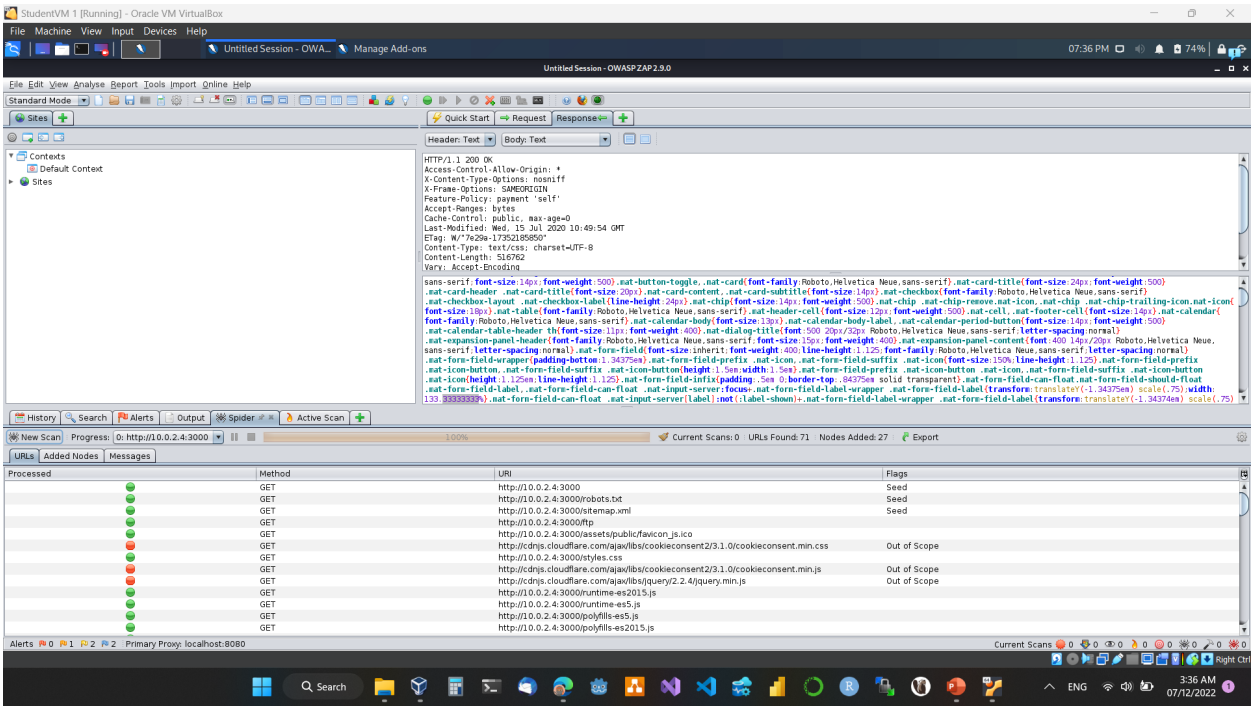

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
OWASP Juice Shop
Nessus Essentials / Folde
https://localhost:8834/#/scans/reports/11/vulnerabilities
nessus Essentials
Scans
Settings
Rahaf
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Advantech iView ConfigurationServlet setConfigurat...
Read More
networkJuiceScan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 15
VPR Top Threats
History 1
Filter
Search Vulnerabilities
15 Vulnerabilities
Sev
Score
Name
Family
Count
INFO
SSH (Multiple Issues)
Misc.
2
SSH (Multiple Issues)
Service detection
2
Web Server (Multiple Issues)
Web Servers
2
Nessus SYN scanner
Port scanners
2
Service Detection
Service detection
2
Common Platform Enumeration (CPE)
General
1
Device Type
General
1
Ethernet Card Manufacturer Detection
Misc.
1
Ethernet MAC Addresses
General
1
ICMP Timestamp Request Remote Date Disclosure
General
1
Nessus Scan Information
Settings
1
OS Identification
General
1
Plugin ID: 10881
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v2.0
Scanner: Local Scanner
Start: Today at 3:18 PM
End: Today at 3:26 PM
Elapsed: 8 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Right Ctrl

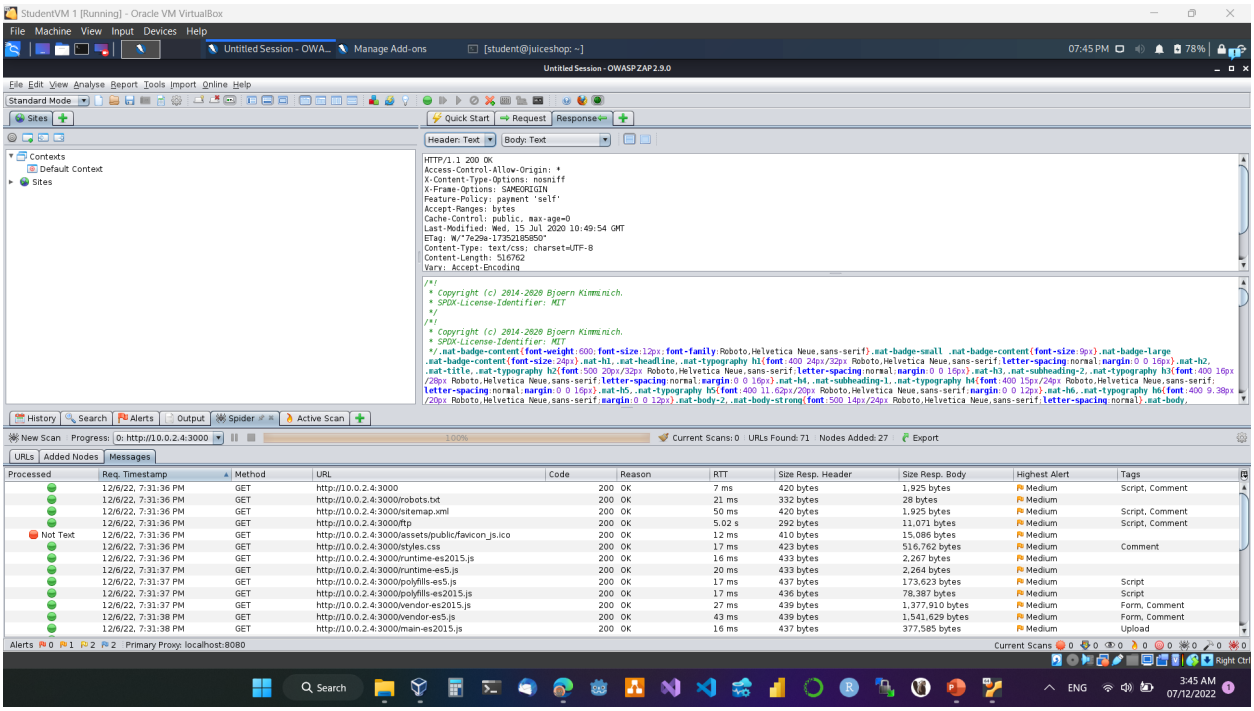

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
listing directory /ftp/
10.0.2.4:3000/ftp/
~ / ftp /
quarantine
coupons_2013.md.bak
incident-support.kdbx
suspicious_errors.yml
acquisitions.md
eastere.gg
legal.md
announcement_encrypted.md
encrypt.pyc
package.json.bak
rahaf@kali-client: ~
File Actions Edit View Help
+ /site.egg: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /4.tgz: Potentially interesting archive/cert file found.
+ /4.tgz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /100.tar: Potentially interesting archive/cert file found.
+ /100.tar: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /10_0_2_4.cer: Potentially interesting archive/cert file found.
+ /10_0_2_4.cer: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /4.tar.bz2: Potentially interesting archive/cert file found.
+ /4.tar.bz2: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /10_0_2_4.tar.bz2: Potentially interesting archive/cert file found.
+ /10_0_2_4.tar.bz2: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /backup.pem: Potentially interesting archive/cert file found.
+ /backup.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /4.war: Potentially interesting archive/cert file found.
+ /4.war: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /1002.tgz: Potentially interesting archive/cert file found.
+ /1002.tgz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /site.alz: Potentially interesting archive/cert file found.
+ /site.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /4.tar: Potentially interesting archive/cert file found.
+ /4.tar: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /10.0.2.4.tgz: Potentially interesting archive/cert file found.
+ /10.0.2.4.tgz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ OSVDB-3092: /ftp/: This might be interesting...
+ OSVDB-3092: /public/: This might be interesting...
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 2 error(s) and 267 item(s) reported on remote host
+ End Time: 2022-12-07 14:27:01 (GMT-5) (167 seconds)
+ 1 host(s) tested
(rahaf㉿kali-client)-[~]
$

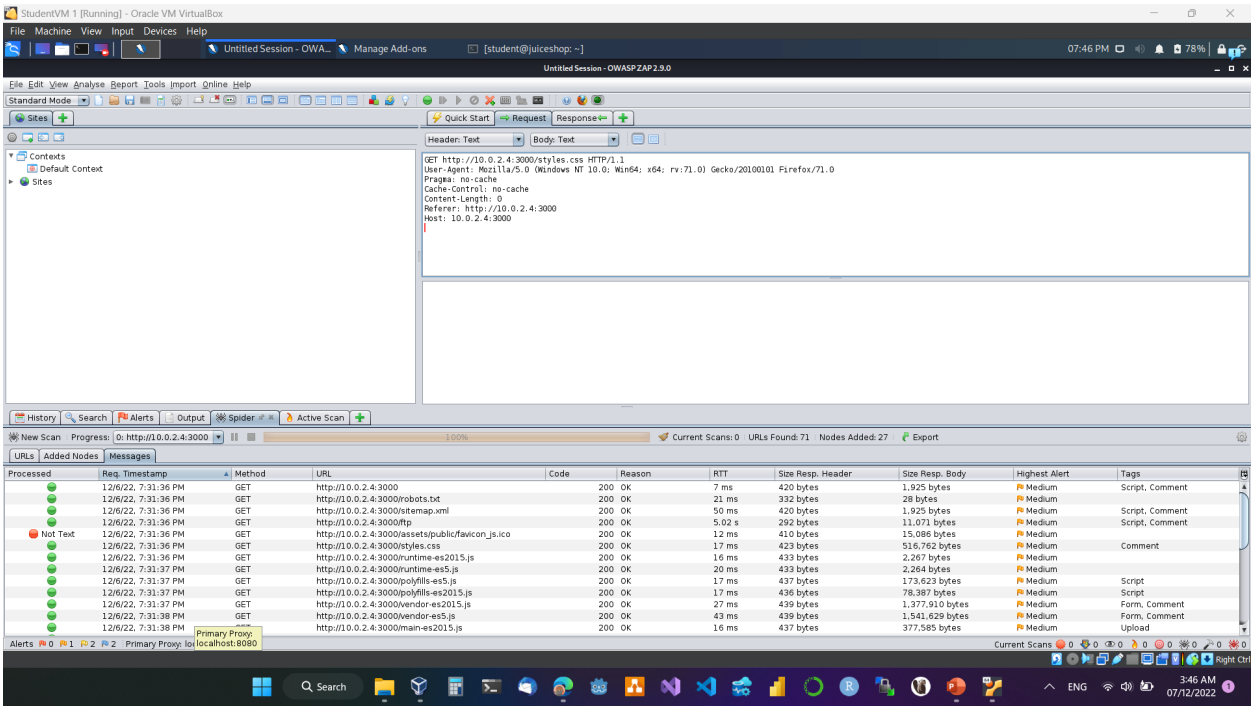

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
listing directory /ftp/
10.0.2.4:3000/ftp/
~ / ftp /
quarantine
coupons_2013.md.bak
incident-support.kdbx
suspicious_errors.yml
acquisitions.md
eastere.gg
legal.md
announcement_encrypted.md
encrypt.pyc
package.json.bak
~/Downloads/acquisitions.md - Mousepad
File Edit Search View Document Help
juicy_malware_linux_amd_64.url
acquisitions.md
Planned Acquisitions
> This document is confidential! Do not distribute!
Our company plans to acquire several competitors within the next year.
This will have a significant stock market impact as we will elaborate in
detail in the following paragraph:
Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy
eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam
voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet
clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit
amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam
nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat,
sed diam voluptua. At vero eos et accusam et justo duo dolores et ea
rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem
ipsum dolor sit amet.
Our shareholders will be excited. It's true. No fake news.


Kali Linux [Running] - Oracle VM VirtualBox
OWASP Juice Shop
You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)
All Products
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤
Banana Juice (1000ml)
1.99¤
Carrot Juice (1000ml)
2.99¤
Eggfruit Juice (500ml)
Fruit Press
Green Smoothie
Juice Shop Adversary Trading Card (Common)


StudentVM 1 [Running] - Oracle VM VirtualBox
Untitled Session - OWASP ZAP 2.9.0


StudentVM 1 [Running] - Oracle VM VirtualBox
Untitled Session - OWASP ZAP 2.9.0
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: Wed, 15 Jul 2020 10:49:54 GMT
ETag: W/"7e29a-17352185850"
Content-Type: text/css; charset=UTF-8
Content-Length: 516762
Vary: Accept-Encoding
Processed
Method
URI
Flags
GET http://10.0.2.4:3000 Seed
GET http://10.0.2.4:3000/robots.txt Seed
GET http://10.0.2.4:3000/sitemap.xml Seed
GET http://10.0.2.4:3000/ftp
GET http://10.0.2.4:3000/assets/public/favicon_js.ico
GET http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css Out of Scope
GET http://10.0.2.4:3000/styles.css
GET http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js Out of Scope
GET http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js Out of Scope
GET http://10.0.2.4:3000/runtime-es2015.js
GET http://10.0.2.4:3000/runtime-es5.js
GET http://10.0.2.4:3000/polyfills-es5.js
GET http://10.0.2.4:3000/polyfills-es2015.js


StudentVM 1 [Running] - Oracle VM VirtualBox
Untitled Session - OWASP ZAP 2.9.0
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: Wed, 15 Jul 2020 10:49:54 GMT
ETag: W/"7e29a-17352185850"
Content-Type: text/css; charset=UTF-8
Content-Length: 516762
Vary: Accept-Encoding
Processed
Req. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
Highest Alert
Tags
12/6/22, 7:31:36 PM GET http://10.0.2.4:3000 200 OK 7 ms 420 bytes 1,925 bytes Medium Script, Comment
12/6/22, 7:31:36 PM GET http://10.0.2.4:3000/robots.txt 200 OK 21 ms 332 bytes 28 bytes Medium
12/6/22, 7:31:36 PM GET http://10.0.2.4:3000/sitemap.xml 200 OK 50 ms 420 bytes 1,925 bytes Medium Script, Comment
12/6/22, 7:31:36 PM GET http://10.0.2.4:3000/ftp 200 OK 5.02 s 292 bytes 11,071 bytes Medium Script, Comment
Not Text 12/6/22, 7:31:36 PM GET http://10.0.2.4:3000/assets/public/favicon_js.ico 200 OK 12 ms 410 bytes 15,086 bytes Medium
12/6/22, 7:31:36 PM GET http://10.0.2.4:3000/styles.css 200 OK 17 ms 423 bytes 516,762 bytes Medium Comment
12/6/22, 7:31:36 PM GET http://10.0.2.4:3000/runtime-es2015.js 200 OK 16 ms 433 bytes 2,267 bytes Medium
12/6/22, 7:31:37 PM GET http://10.0.2.4:3000/runtime-es5.js 200 OK 20 ms 433 bytes 2,264 bytes Medium
12/6/22, 7:31:37 PM GET http://10.0.2.4:3000/polyfills-es5.js 200 OK 17 ms 437 bytes 173,623 bytes Medium Script
12/6/22, 7:31:37 PM GET http://10.0.2.4:3000/polyfills-es2015.js 200 OK 17 ms 436 bytes 78,387 bytes Medium Script
12/6/22, 7:31:37 PM GET http://10.0.2.4:3000/vendor-es2015.js 200 OK 27 ms 439 bytes 1,377,910 bytes Medium Form, Comment
12/6/22, 7:31:38 PM GET http://10.0.2.4:3000/vendor-es5.js 200 OK 43 ms 439 bytes 1,541,629 bytes Medium Form, Comment
12/6/22, 7:31:38 PM GET http://10.0.2.4:3000/main-es2015.js 200 OK 16 ms 437 bytes 377,585 bytes Medium Upload



>>

This concluded the vulnerability assessment methodology portion of this report.