SECURITY ASSESSMENT

Submitted to: Udajuicer
Security Analyst: Simone Canty

Date of Testing: 12/10/2022
Date of Report Delivery: 03/13/2023

Table of Contents

Contents

Security Engagement Summary

Engagement Overview

The Udajuicer's Development Team have requested a vulnerability assessment on the web-application to assess for security risk and vulnerabilities this application has on the organization's data integrity and continuity. The security analyst, Simone Canty, of the Information Security department will be conducting the vulnerability assessment.

Scope

A vulnerability assessment provides an organization with details on any security weakness in its organization. The assessment will give Udajuicer's a better understanding of its security flaws and overall risk, decreasing the likelihood that a cyber attack will breach their system. The development team and the security analyst have agreed the scope of the engagement would be the web application hosted on the provided virtual machine that will not require login. The booted virtual machine will reveal the IP address of the web application uniform resource locator (URL) on port HTTP (Hypertext Transfer Protocol) 3000. The vulnerability assessment will be taking place in an isolated environment called a sandbox environment that will not affect the running of the application or the daily operation of the organization. The web application tool used to perform this assessment was OWASP Zed Attack Proxy (ZAP), an open-source web application security scanner.

Regular vulnerability assessments are necessary for any organization, including Udajuicer. Information security is an ongoing process whether it be for a mobile app, web application, network, server, etc. It is necessary to incorporate automated scans that can help in reducing security problems and improve the company's security model.

Executive Risk Analysis

I am pleased to present the results of the vulnerability assessed commissioned by the Udajuicer's Development Team. This assessment was done remotely on November 14, 2022 by Simone Canty, Information Security Analyst.

The aim of the assessment was for Simone Canty to do a vulnerability assessment of the Udajuicer's web application, with a focus on identifying any vulnerabilities that would severely affect customer data and the application's operation and availability.

Although the organization has taken controls in properly securing and protecting its data and infrastructure, there were several issues identified which have the potential of be damaging to the organization including:

- I discovered that there was a high risk vulnerability in which an attacker uses code to exploit a database to gain access to valuable information or data.
- There was a medium risk vulnerability which involved an attacker being able to take over a user's session and perform further attacks.
- In addition, there was another medium risk vulnerability involving a misconfiguration of a web server allowing third-party domains (a group of users, workstations, computers, devices, printers, and database servers) to perform allowed tasks through the browsers of users.
- Two low risk vulnerabilities were revealed that can be exploited by attackers to execute malicious code on the web application.

- Another vulnerability considered low risk involves the missing Hypertext Transfer Protocol (HTTP) header in a web application that can increase the risk of the website to attacks.
- Lastly, there is a low risk vulnerability that can be exploited by an attacker to obtain information on the internet protocol (IP) addresses of a web application.

Overall, I believe Udajuicer has a solid base to build upon to continue to improve their infrastructure with the necessary remediation steps, and will have a strong security posture from an information security perspective.

Executive Recommendation

Given the information presented above, it is important to prioritize the vulnerability risks to remediate to lessen and/or prevent the vulnerabilities from being exploited. The risk level and description of the vulnerability will assess in prioritizing remedication as follows:

1. **Structured Query Language (SQL) Injection** should be remediated within two weeks. This is considered a high risk vulnerability.
2. **Cross-Domain JavaScript Source File Inclusion.** For this particular vulnerability, it is considered a low risk vulnerability. This means the vulnerability is unlikely to be exploited or cause significant damage. In addition, it may have a low impact on an organization if exploited. However, this vulnerability deals with an attacker's ability to execute malicious code on a web application, and should be mediated within one month.
3. **Web Browser Cross-Site Scripting (XSS) Protection Not Enabled.** Even though this is considered a low risk vulnerability, it should be mediated within one month. The reason is it has due with Cross Scripting (XSS), the ability of an attacker to send malicious link to a user and fool them by clicking on the link.
4. **Cross-Domain Misconfiguration.** This particular certificate should be remediated within a month due to it involves a misconfiguration of a web server allowing third-party domains (a group of users, workstations, computers, devices, printers, and database servers) to perform allowed tasks through the browsers of users. This is considered a medium risk vulnerability.
5. **X-Content-Type-Options Header Missing.** This is another low risk vulnerability that should be mediated within one month. This vulnerability involves the missing Hypertext Transfer Protocol (HTTP) header in a web application that can increase the risk of the website to attacks.
6. **Session ID in Uniform Resource Locator (URL) Rewrite.** This vulnerability allows an attacker being able to take over a user's session and perform further attacks. It is revealed to be a medium risk and should be remediated within 30-60 days.
7. **Private IP Disclosure.** This low risk vulnerability should be remediated within 30-60 days. This is the vulnerability that can be exploited by an attacker by obtaining information on the IP addresses.

Significant Vulnerability Summary

Risk Level	Number of Alerts
High	1
Medium	2
Low	4

Significant Vulnerability Detail

High (Medium) **SQL Injection**

- The chance of this vulnerability being exploited is high.
- This vulnerability if exploited can affect clients, an organization's sensitive data, and databases
- Structured Query Language (SQL) injection can happen if the client data is not validated, sanitized, or filtered.
- The SQL or command contains the malicious code that an attacker can use to infiltrate to view and/or modify a database.
- The remediation involves
    - Use LIMIT and other SQL controls within queries to prevent mass disclosure of records in case of SQL injection.
    - Use positive server-side input validation. This is not a complete defense as many applications require special characters, such as text areas or APIs for mobile applications.
    - The preferred option is to use a safe API, which avoids using the interpreter entirely, provides a parameterized interface, or migrates to Object Relational Mapping Tools (ORMs).

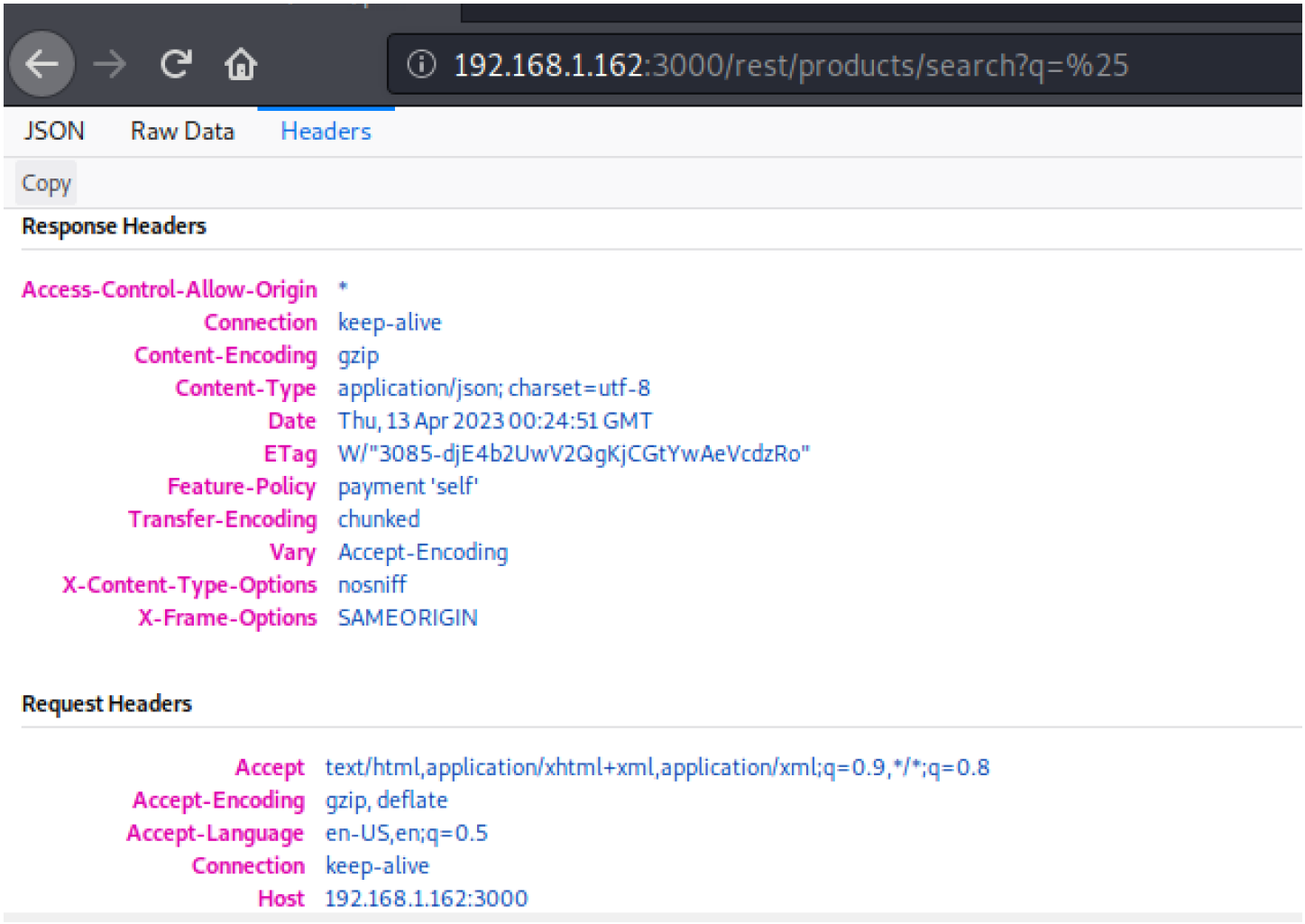


Figure 2
Validation of SQL Injection

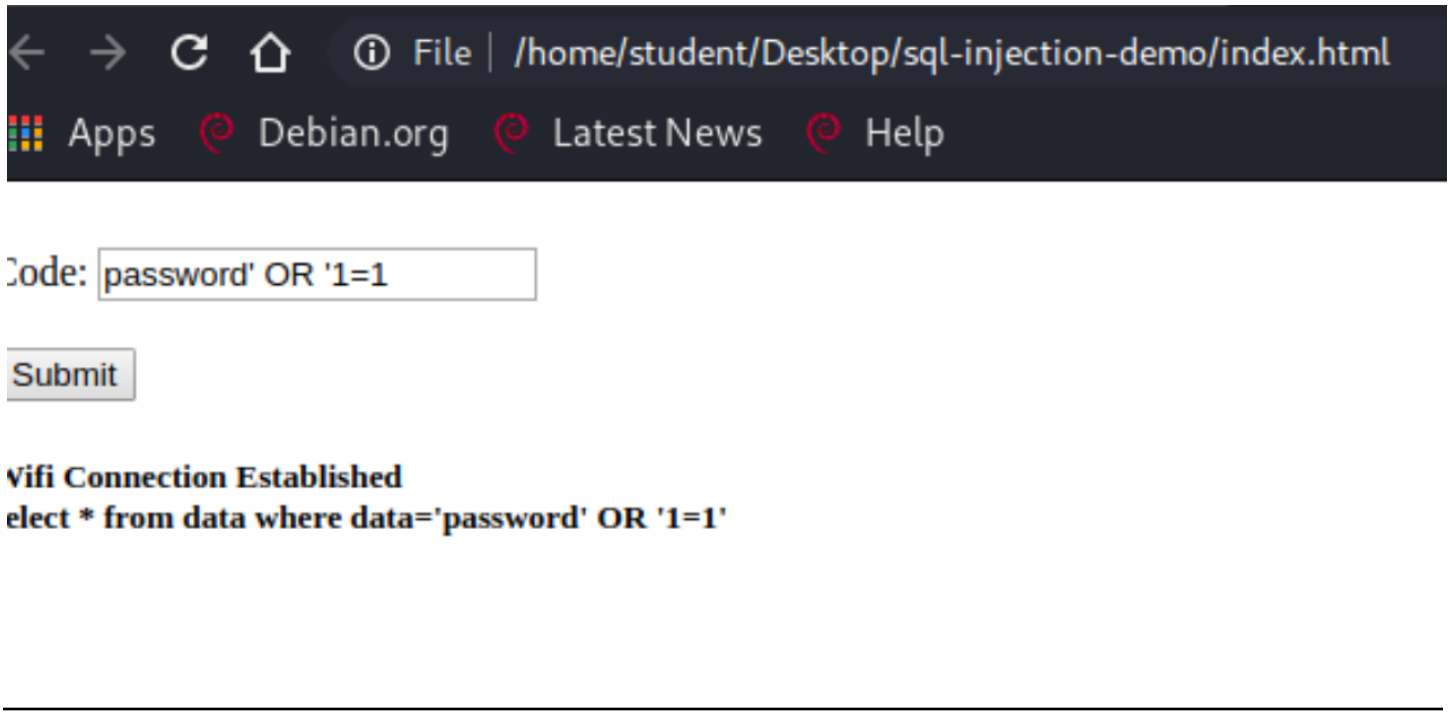


Figure 3
Validation of SQL Injection

Medium (High) Session ID in URL Rewrite

- This risk is considered medium risk.
- This vulnerability if exploited will affect the client's sensitive data, organization's data and functionality of data.
- The session id is an identifier that is generated by a web application server to maintain the user's session.
- Session identifiers are typically passed between the client and the server in various ways, such as cookies or hidden form fields. However, some web applications may use the session ID as a parameter in the URL.
- When the session ID is in the URL, it can be used by attackers to use such techniques like sniffing and cross-scripting to hijack a user's session.
- Remediation include:
  - Putting the session ID in a cookie.
  - Using hidden form fields to store session IDs.

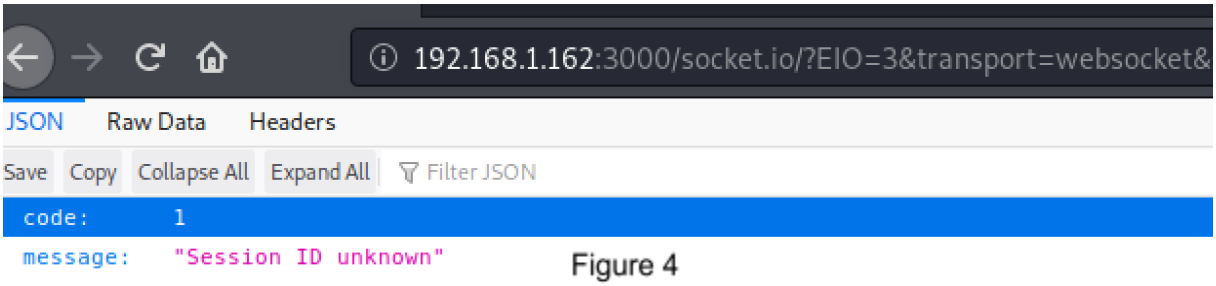


Figure 4
Validation of Session ID

Medium (Medium) Cross-Domain (COR) Misconfiguration

- This vulnerability is considered medium.
- This vulnerability when exploited will affect an user's and organization's data
- A cross-domain misconfiguration can leave a website at risk for a third party sites to request through authenticated users to obtained data like credit card or login information
- To mediate this risk:
    - Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove
      all COR headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

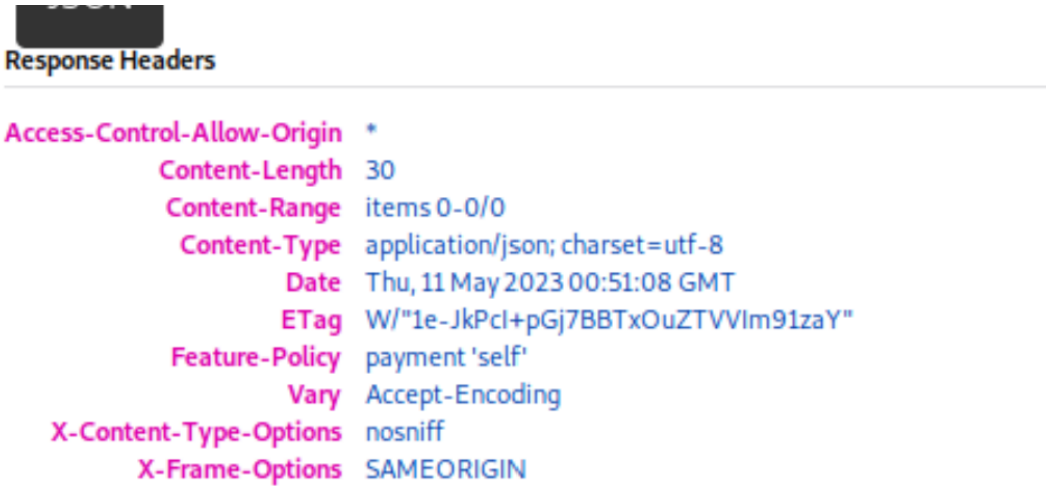


Figure 5
Validation of Cross-Domain Misconfiguration

Low (Medium) Cross-Domain JavaScript Source File Inclusion

- The vulnerability is low risk.
- This vulnerability can affect a user and an organization.
- This vulnerability can be exploited by attackers to execute malicious code on your web application. This vulnerability occurs when your web application loads JavaScript files from an external domain without proper validation, allowing an attacker to inject their own code and potentially take control of the application.
- The remediation is to ensure Javascript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

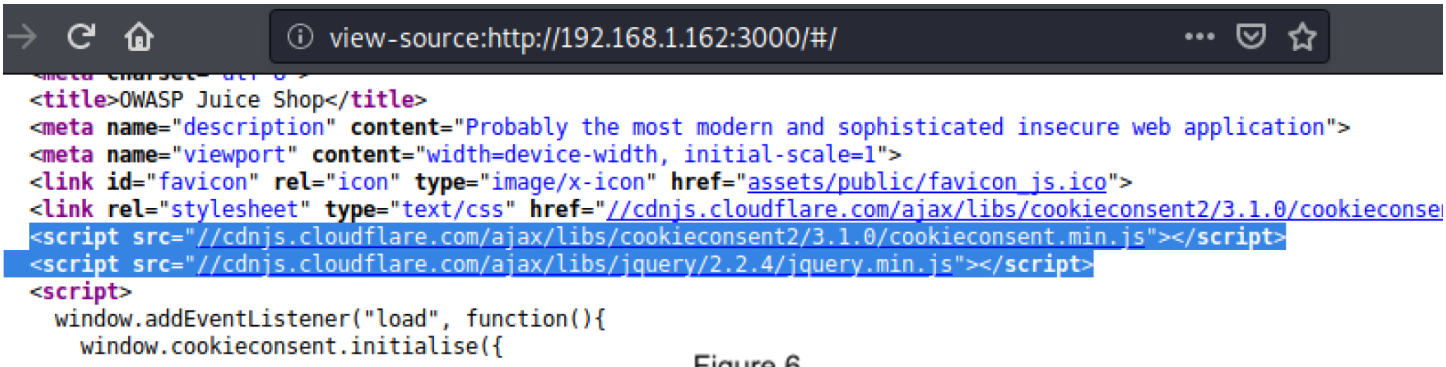


Figure 6
Validation of Cross-Domain JavaScript Soure File Inclusion

Low(Medium) X-Content-Type-Options Header Missing

- The vulnerability is considered low risk
- The vulnerability can affect users and an organization's network.
- X-Content-Type-Options Header is a Hypertext Transport Protocol (HTTP) response header that is used to protect web browsers from Multipurpose Internet Mail Extensions (MIME). MIME lets users exchange data, files, audio, and videos over email.
- When this header is missing, this increases the risk for sniffing attacks,where an attacker may try to exploit the browser's sniffing behavior to trick it into interpreting content in unintended ways.
- The solution is to ensure that the application/web server sets the Content-Type header appropriately, and it sets the X-Content-Type-Options header to 'nosniff' for all web pages.

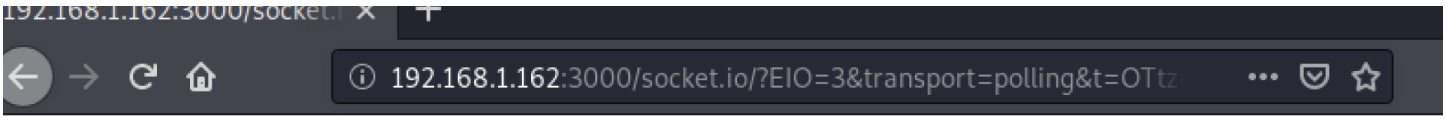


Figure 7
Validation of X-Content-Type-Option Header Missing

Low (Medium) Web Browser XSS Protection Enabled

- This vulnerability is considered low risk.
- Web Browser Cross-Site Scripting (XSS) protection is a security mechanism that web browsers use to detect and prevent cross-site scripting attacks. Cross-site scripting is a type of vulnerability where an attacker injects malicious scripts into web pages viewed by other users.
- This vulnerability can affect users and the operation of an organization.
- The solution to prevent this from happening is to ensure the web browser XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.

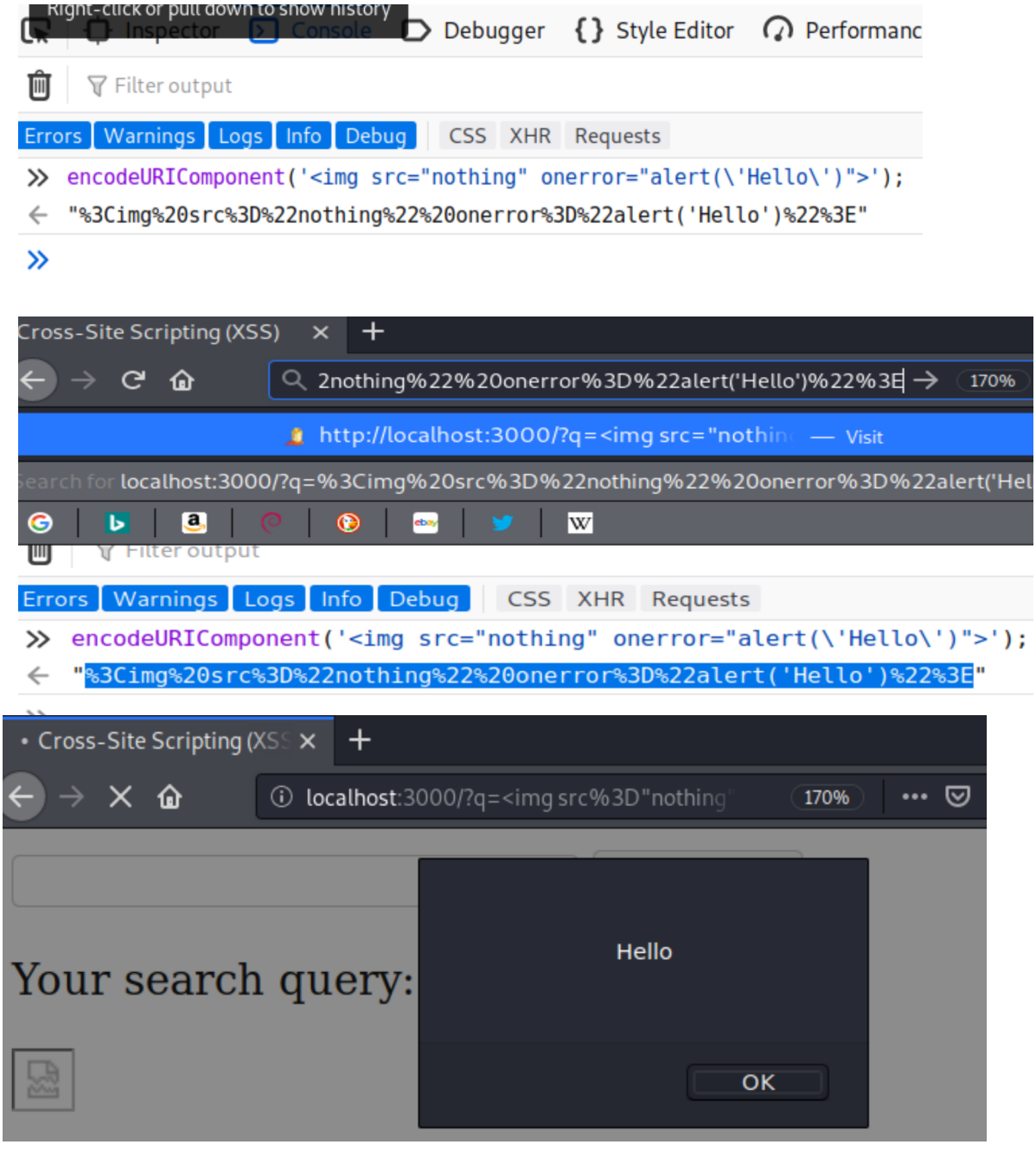


Figure 8
Validation of Cross-Site Scripting

Low (Medium) Private IP Disclosure

- This vulnerability is considered low risk.
- Private Internet Protocol (IP) Disclosure is a vulnerability where a server discloses the IP addresses of its users. This disclosure can leak information about the organization/company's internal network.
- An attacker can gain further information of its users by using the leaked IP addresses.
- If exploited, this can have an impact on the user/client/customer's sensitive data, an organization's internal network as well as its confidentiality, integrity, and availability.
- The mitigation for this type of vulnerability is:
    - Do not disclose the internal IP addresses.
    - Hide the private IPs in error messages.
    - Use innocuous identifiers for passing information

```
//demo.owasp-juice.shop"},{"uri":"http://demo.owasp-juice.shop"},{"uri":"https://juice-shop.herokuapp.com"},{"uri":"http://juice-
shop.herokuapp.com"},{"uri":"https://preview.owasp-juice.shop"},{"uri":"http://preview.owasp-juice.shop"},{"uri":"https://juice-sh
staging.herokuapp.com"},{"uri":"http://juice-shop-staging.herokuapp.com"},{"uri":"http://juice-shop.wtf"},{"uri":"http:
//localhost:3000","proxy":"http://local3000.owasp-juice.shop"},{"uri":"http://127.0.0.1:3000","proxy":"http://local3000.owasp-
juice.shop"},{"uri":"http://localhost:4200","proxy":"http://local4200.owasp-juice.shop"},{"uri":"http:
//127.0.0.1:4200","proxy":"http://local4200.owasp-juice.shop"},{"uri":"http://192.168.99.100:3000","proxy":"http://localmac.owasp-
juice.shop"},{"uri":"http://penguin.termina.linux.test:3000","proxy":"http://localchromeos.owasp-juice.shop"}]}},"challenges":
{"showSolvedNotifications":true,"showHints":true,"restrictToTutorialsFirst":false,"overwriteUrlForProductTamperingChallenge":"http
//owasp.slack.com","xssBonusPayload":"<iframe width=\"100%\" height=\"166\" scrolling=\"no\" frameborder=\"no\" allow=\"autoplay\"
src=\"https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto_play=true&
hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true
\"></iframe>","safetyOverride":false},"hackingInstructor":{"isEnabled":true,"avatarImage":"JuicyBot_MedicalMask.png"},"products":
[{"name":"Apple Juice (1000ml)","price":1.99,"deluxePrice":0.99,"limitPerUser":5,"description":"The all-time
classic.","image":"apple_juice.jpg","reviews":[{"text":"One of my favorites!","author":"admin"}]},{"name":"Orange Juice
(1000ml)","description":"Made from oranges hand-picked by Uncle
Dittmeyer.","price":2.99,"deluxePrice":2.49,"image":"orange_juice.jpg","reviews":[{"text":"y0ur f1r3wall needs m0r3
musc13","author":"uvogin"}]},{"name":"Eggfruit Juice (500ml)","description":"Now with even more exotic
flavour.","price":8.99,"image":"eggfruit_juice.jpg","reviews":[{"text":"I bought it, would buy again. 5/7","author":"admin"}]},
{"name":"Raspberry Juice (1000ml)","description":"Made from blended Raspberry Pi, water and
sugar.","price":4.99,"image":"raspberry_juice.jpg"},{"name":"Lemon Juice (500ml)","description":"Sour but full of
vitamins.","price":2.99,"deluxePrice":1.99,"limitPerUser":5,"image":"lemon_juice.jpg"},{"name":"Banana Juice
(1000ml)","description":"Monkeys love it the most.","price":1.99,"image":"banana_juice.jpg","reviews":[{"text":"Fry liked it
```


Figure 9
Validation of Private IP Disclosure

Methodology

Assessment Tool set Selection

In order to provide a thorough security assessment, the use of vulnerability data from a variety of sources were used to move our assessment model. Several assessment tools were used

Tools Used

- Oracle VM Virtual Box Manager
- Kali Linux
- OVA/Web Server
- Student VM
- Firefox Web Browser
- OWASP Zed Attack Proxy (ZAP)

Assessment Methodology Detail

The methodology for the assessment is as follows:

1. Use Oracle VM Virtual Box and downloading the OVA, I changed the settings under the Network tab and choose Advance as indicated below:

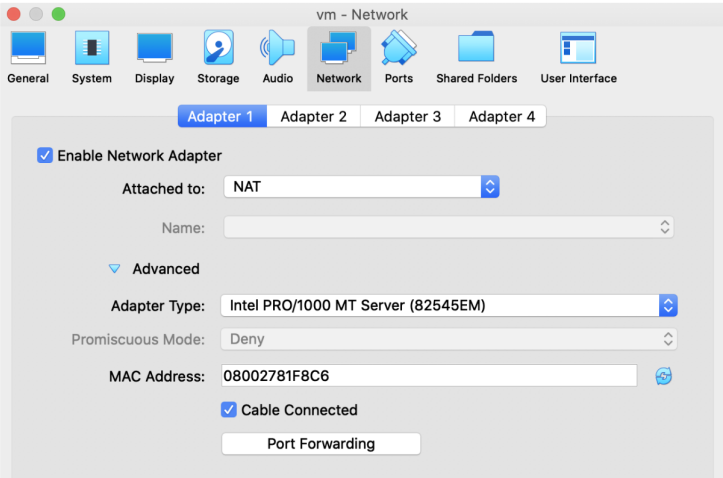


Figure 10
Setting up the VM

2. The correct port is 3000 and should be changed as follows:

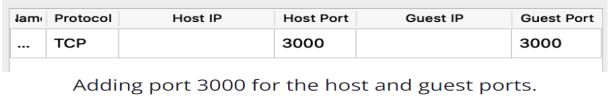


Figure 11
Adding port 3000 to Host and Guest ports

2. When you run the OVA, you will be given a web server IP address. For this vulnerability assessment, the IP address given was 192.168.1.162:3000 and was used to access the Juice Shop application within Kali Linux.

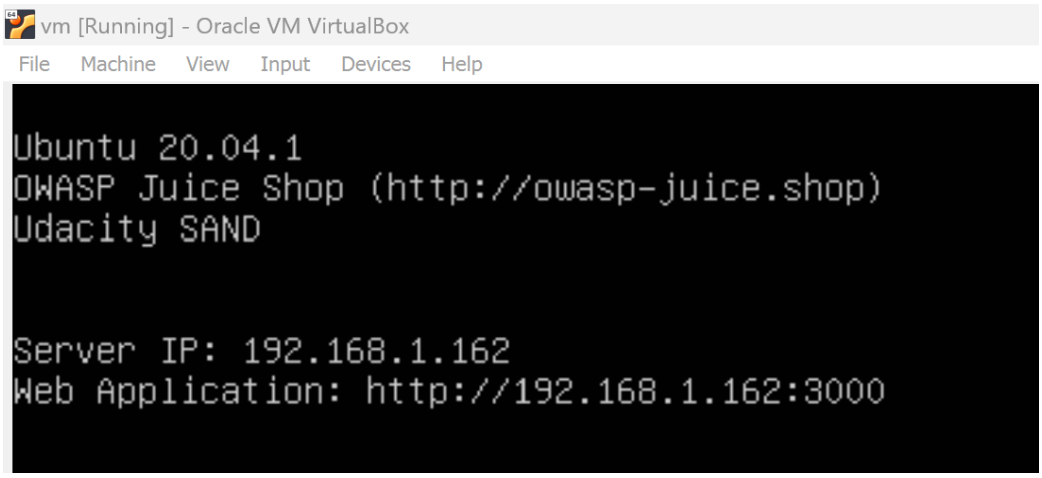


Figure 12
Web Application IP Address

3. Within the Oracle VM, start the Student VM and log into Kali Linux using the following:

- student
- Password: Abcdef1!

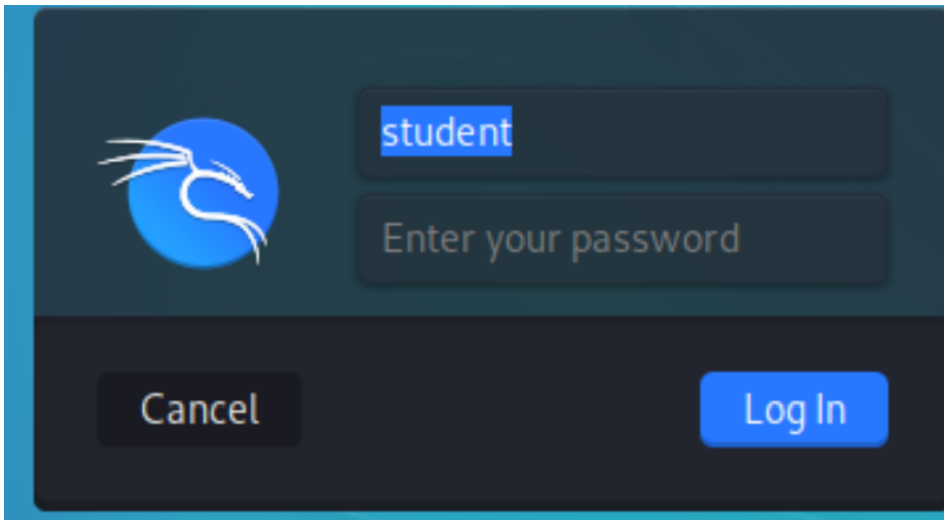


Figure 13
Login of Kali Linux

4. Once logged into Kali Linux, go to Mozilla Firefox web browser and place the IP address: 192.168.1.162:3000 into the search bar. The Juice Shop should be present as indicated below:

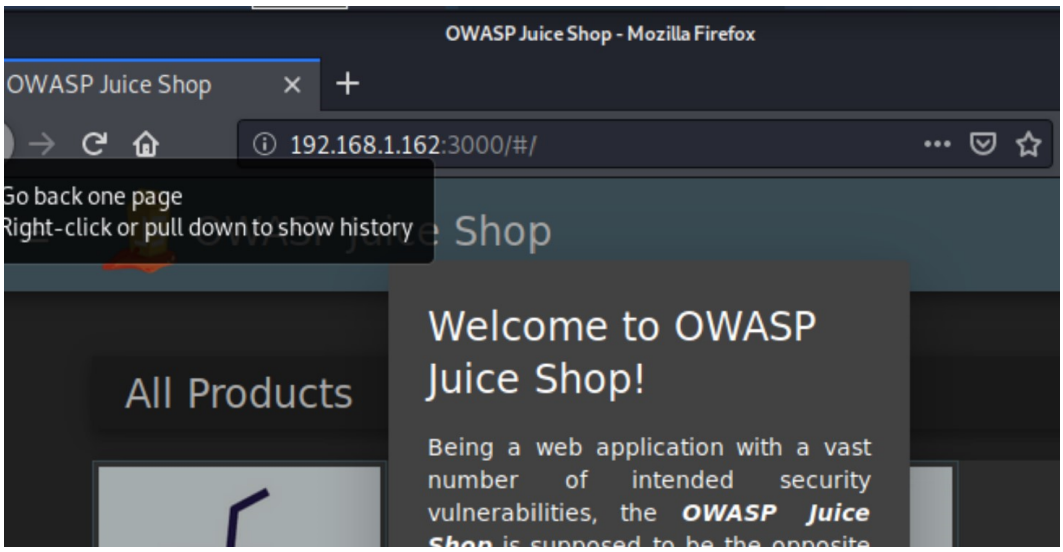
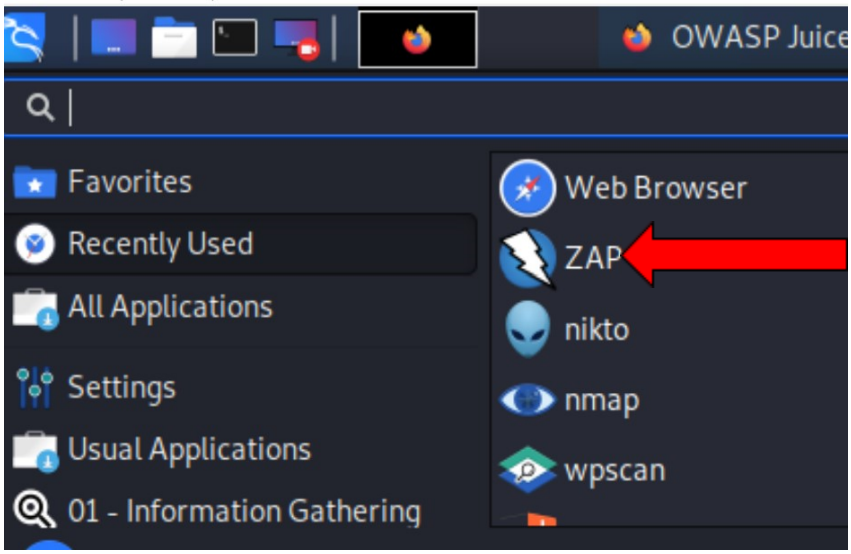
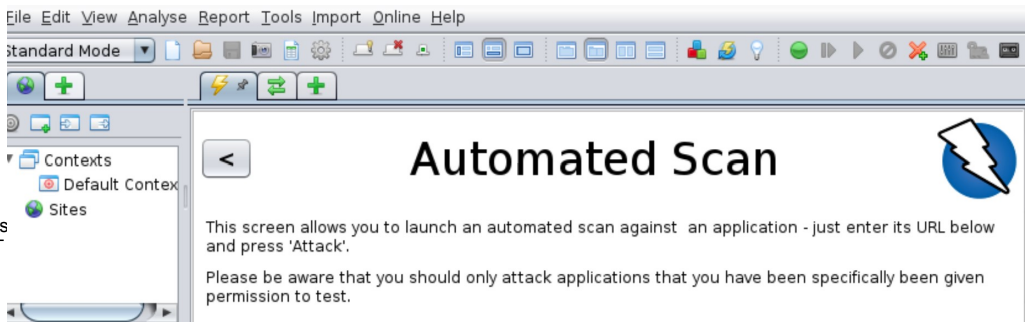


Figure 14
Web Application

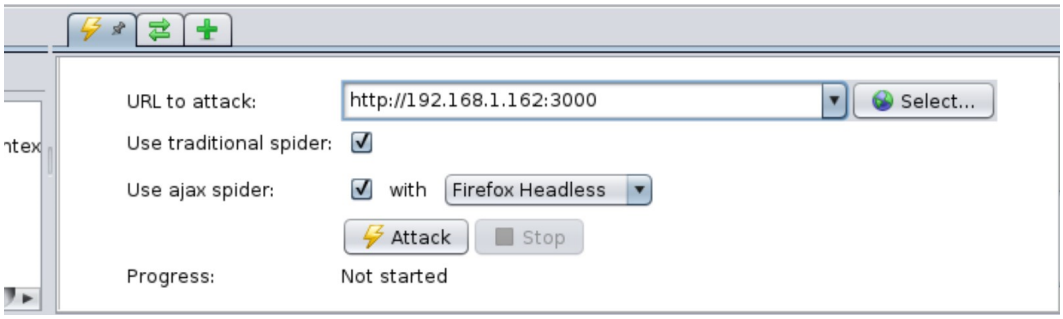
5. To perform the web application vulnerability scan of the website, I used the OWASP ZAP which is installed in Kali Linux.



6. Open OWASP ZAP and click on Automated Scan



7. Fill in the areas as such and click on the Attack button.



8. The results of the scan will appear on the bottom under Alerts. Each vulnerability alert will provide information on the vulnerability.