Udajuicer:

Threat Report

YOUR NAME:

Rahaf Ibrahim

9-11-2022

Section 1

Threat Assessment

1.1: Asset Inventory

Components and Functions

- ***Web server :*** *which handles basically HTTP protocols.*
- **Application server:** *manages a number of different protocols and is also responsible of the logic and the user-content interaction.*
- **Database:** *which considered as substantial asset for Udajuicer because it contain all data about the shop (products), admins, and the customers (names, addressee, credit cards numbers)*

1.1: Asset Inventory

Explanation of How A Request Goes from Client to Server

First, the customer visits the Udajuicer by sending an HTTP request to the web server then the client gets the response from the web server. Web server manages the request and gets responses. After that, the application server communicates with the database to bring the data. All The data travels back and forth between the server and its client until the end of the session.

1.2 Architecture Audit

Flaws

- *There is no firewall, we need web application firewall (WAF) to monitor and block the malicious traffic between the application (website Udajuicer) and the internet.*
- *There is no content delivery network (CDN) to provide a high availability and prevent distributed denial of service (DDoS) attack.*
- *In the architecture of Udajuicer the web server need load balancer to manage the traffic .*
- *No antivirus software.*

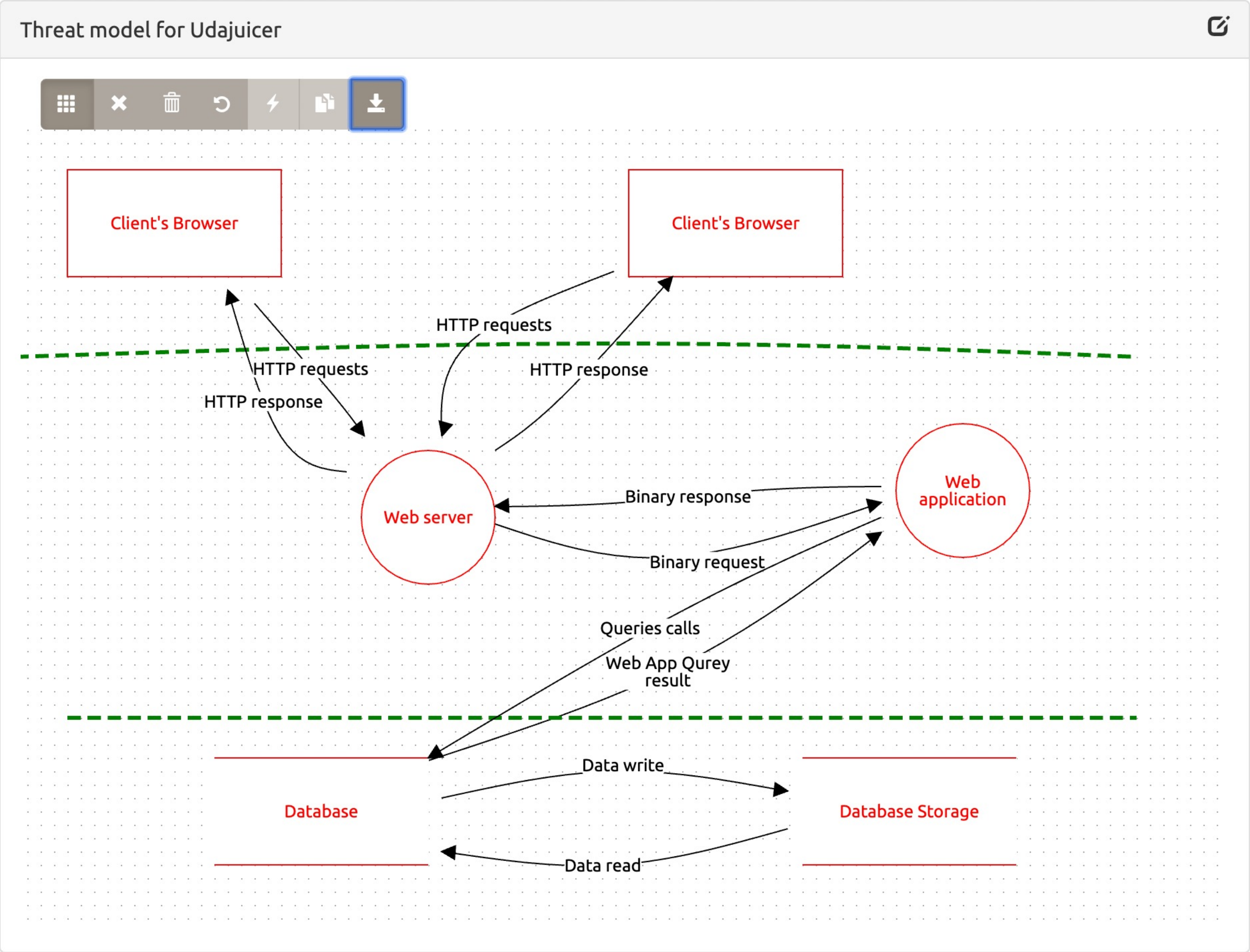
1.3 Threat Model Diagram

Using OWASP Threat Dragon, build a diagram showing the flow of data in the Juice Shop application and identify 3 possible threats to the Juice Shop. Make sure to include the following components:

- **Client**
- **Web Server**
- **Application Server**
- **Database**

1.3 Threat Model Diagram

Insert hreat Model Diagram Here:



Broken Authentication
Cross Site Scripting (XSS)
SQL Injection
Insufficient Logging & Monitoring

1.4 Threat Analysis

What Type of Attack Caused the Crash?

Distributed Denial of Service (DDoS) attack.

What in the Logs Proves Your Theory?

A massive number of requests to the website Udajuicer all of them at the same time.

1.5 Threat Actor Analysis

Who is the Most Likely Threat Actor?

Script Kiddie

What Proves Your Theory?

Because the website does not have any protection method it was am easy target , Jjust kids want do something fun.

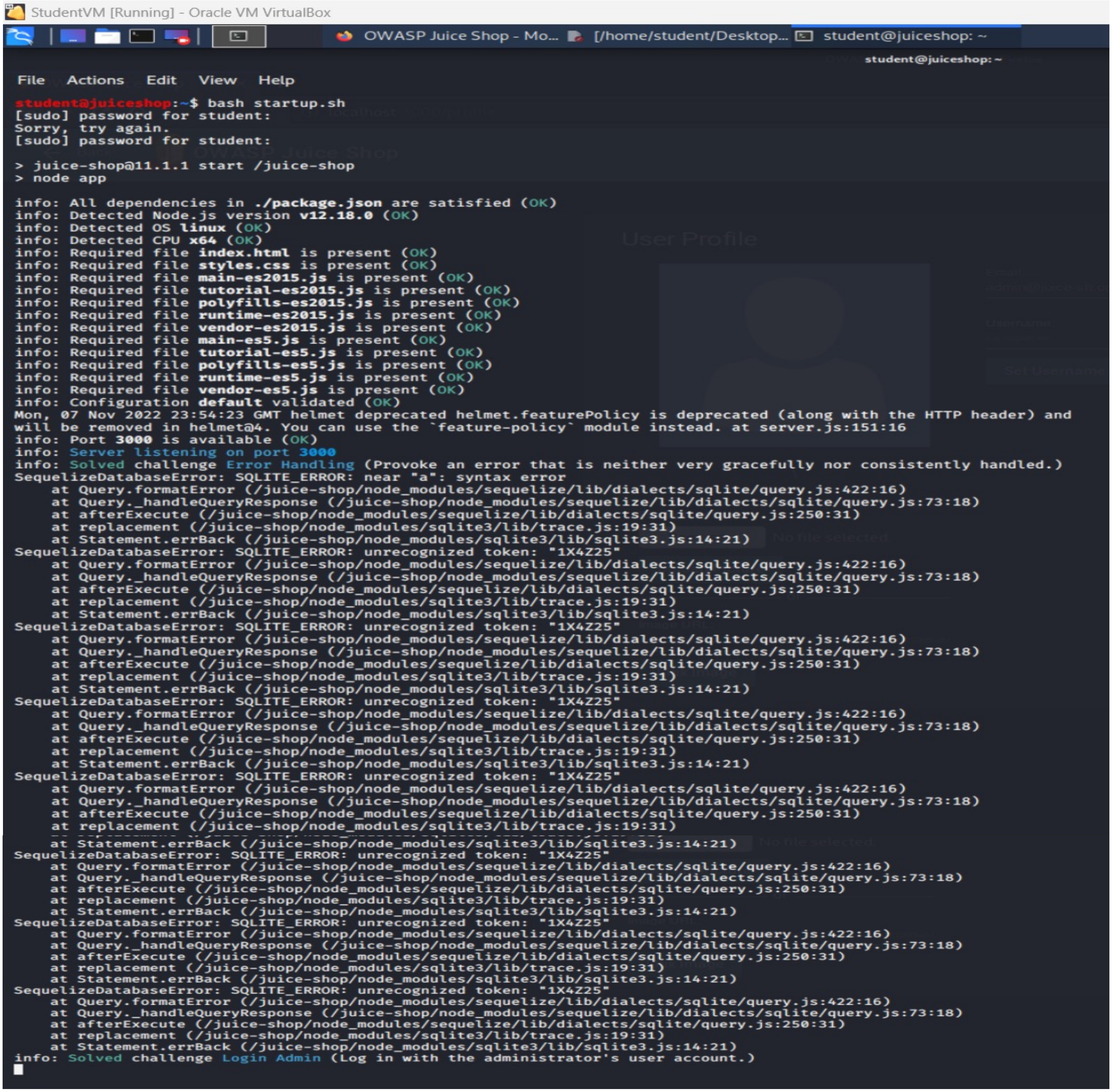
Section 2

Vulnerability Analysis

2.1 SQL Injection

Insert Screenshot of Your Commands Here:

bash startup.sh

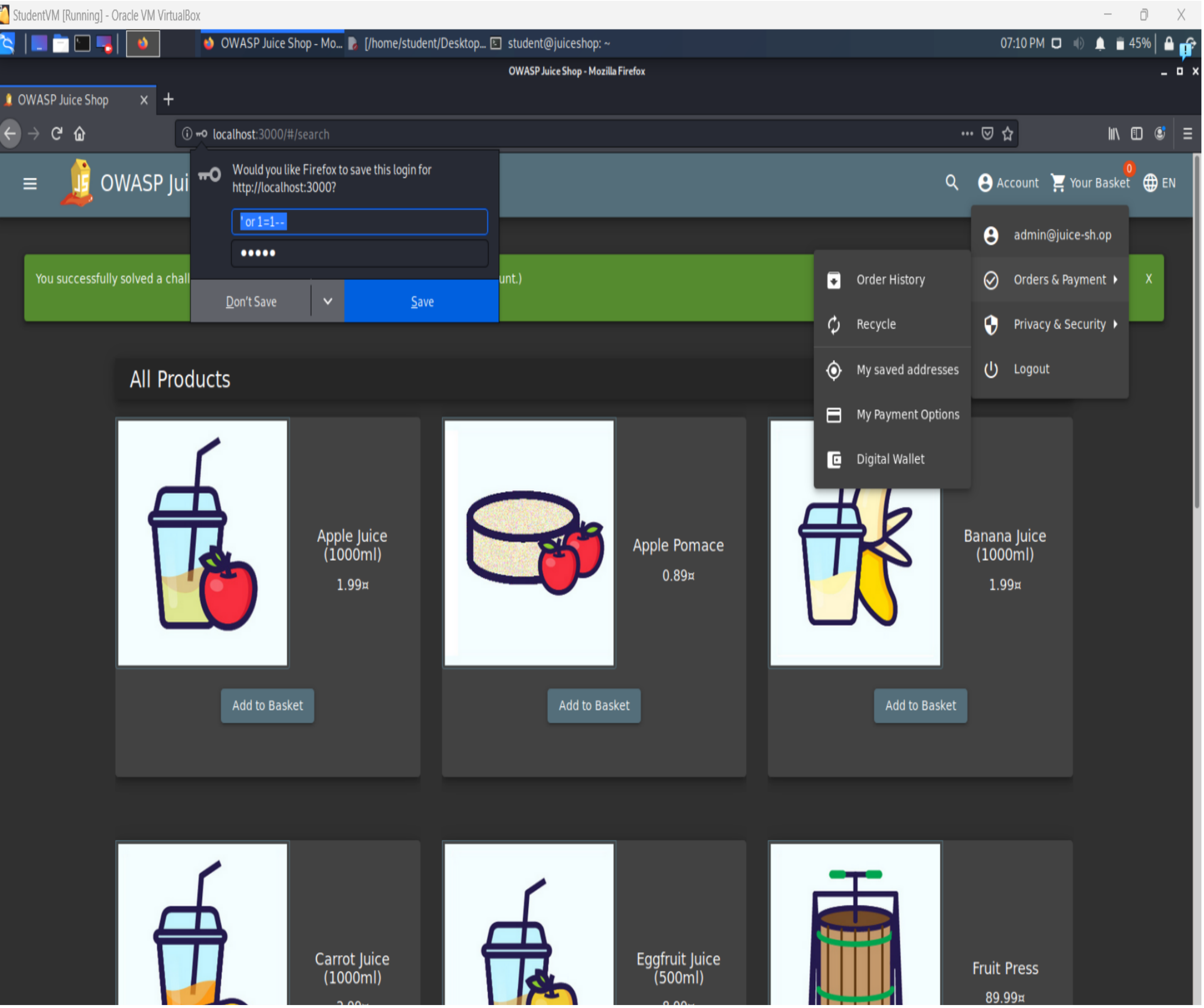


```
student@juiceshop:~$ bash startup.sh
[sudo] password for student:
Sorry, try again.
[sudo] password for student:

> 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)
Mon, 07 Nov 2022 23:54:23 GMT helmet deprecated helmet.featurePolicy is deprecated (along 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 Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)
SequelizeDatabaseError: SQLITE_ERROR: near "a": syntax error
    at Query.formatError (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:422:16)
    at Query._handleQueryResponse (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:73:18)
    at afterExecute (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:250:31)
    at replacement (/juice-shop/node_modules/sqlite3/lib/trace.js:19:31)
    at Statement.errBack (/juice-shop/node_modules/sqlite3/lib/sqlite3.js:14:21)
SequelizeDatabaseError: SQLITE_ERROR: unrecognized token: "1X4Z25"
    at Query.formatError (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:422:16)
    at Query._handleQueryResponse (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:73:18)
    at afterExecute (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:250:31)
    at replacement (/juice-shop/node_modules/sqlite3/lib/trace.js:19:31)
    at Statement.errBack (/juice-shop/node_modules/sqlite3/lib/sqlite3.js:14:21)
SequelizeDatabaseError: SQLITE_ERROR: unrecognized token: "1X4Z25"
    at Query.formatError (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:422:16)
    at Query._handleQueryResponse (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:73:18)
    at afterExecute (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:250:31)
    at replacement (/juice-shop/node_modules/sqlite3/lib/trace.js:19:31)
    at Statement.errBack (/juice-shop/node_modules/sqlite3/lib/sqlite3.js:14:21)
SequelizeDatabaseError: SQLITE_ERROR: unrecognized token: "1X4Z25"
    at Query.formatError (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:422:16)
    at Query._handleQueryResponse (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:73:18)
    at afterExecute (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:250:31)
    at replacement (/juice-shop/node_modules/sqlite3/lib/trace.js:19:31)
    at Statement.errBack (/juice-shop/node_modules/sqlite3/lib/sqlite3.js:14:21)
SequelizeDatabaseError: SQLITE_ERROR: unrecognized token: "1X4Z25"
    at Query.formatError (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:422:16)
    at Query._handleQueryResponse (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:73:18)
    at afterExecute (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:250:31)
    at replacement (/juice-shop/node_modules/sqlite3/lib/trace.js:19:31)
    at Statement.errBack (/juice-shop/node_modules/sqlite3/lib/sqlite3.js:14:21)
SequelizeDatabaseError: SQLITE_ERROR: unrecognized token: "1X4Z25"
    at Query.formatError (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:422:16)
    at Query._handleQueryResponse (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:73:18)
    at afterExecute (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:250:31)
    at replacement (/juice-shop/node_modules/sqlite3/lib/trace.js:19:31)
    at Statement.errBack (/juice-shop/node_modules/sqlite3/lib/sqlite3.js:14:21)
SequelizeDatabaseError: SQLITE_ERROR: unrecognized token: "1X4Z25"
    at Query.formatError (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:422:16)
    at Query._handleQueryResponse (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:73:18)
    at afterExecute (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:250:31)
    at replacement (/juice-shop/node_modules/sqlite3/lib/trace.js:19:31)
    at Statement.errBack (/juice-shop/node_modules/sqlite3/lib/sqlite3.js:14:21)
SequelizeDatabaseError: SQLITE_ERROR: unrecognized token: "1X4Z25"
    at Query.formatError (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:422:16)
    at Query._handleQueryResponse (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:73:18)
    at afterExecute (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:250:31)
    at replacement (/juice-shop/node_modules/sqlite3/lib/trace.js:19:31)
    at Statement.errBack (/juice-shop/node_modules/sqlite3/lib/sqlite3.js:14:21)
info: Solved challenge Login Admin (Log in with the administrator's user account.)
```

2.1 SQL Injection



localhost:3000/#/search

Would you like Firefox to save this login for http://localhost:3000?

' or 1=1--

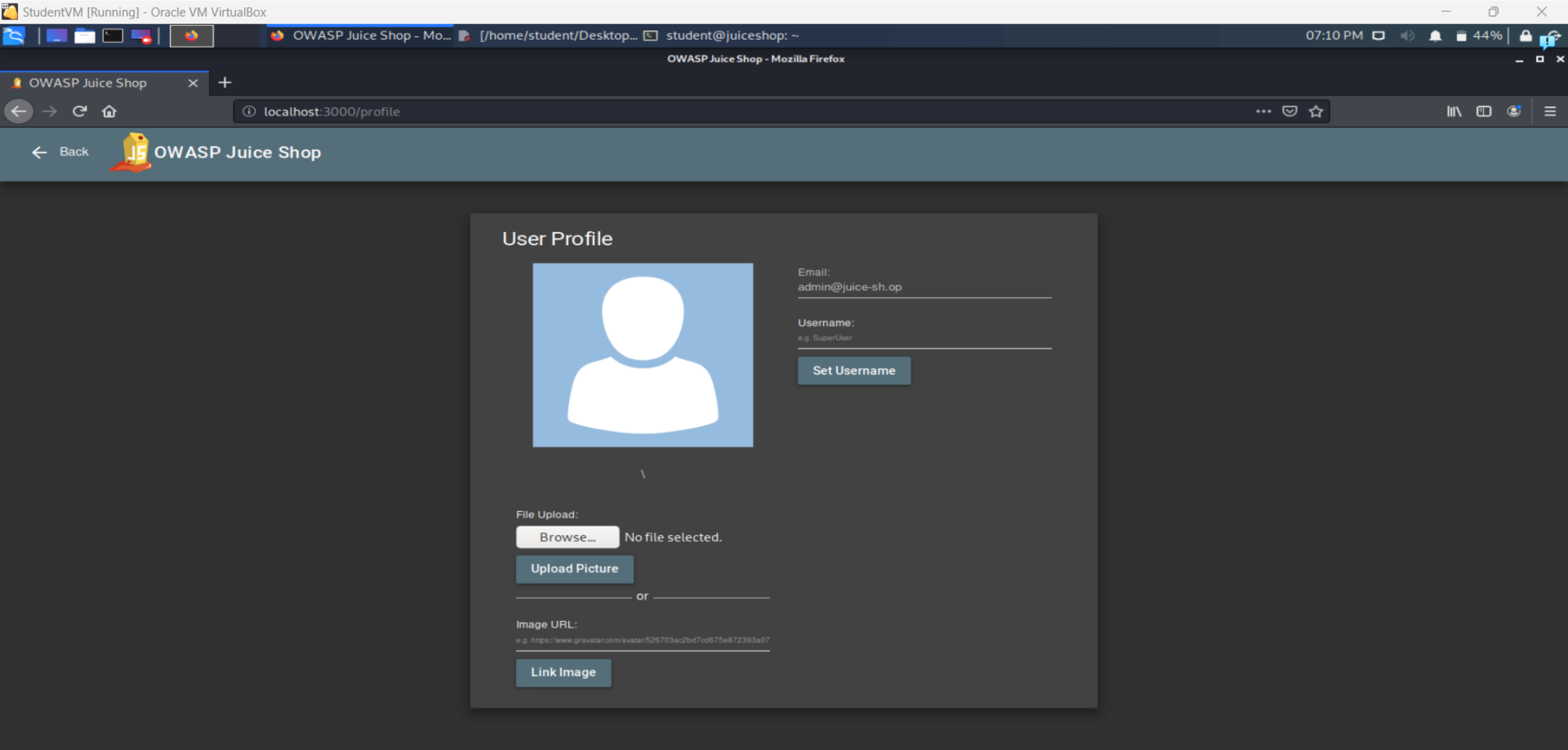
•••••

You successfully solved a chall unt.)

admin@juice-sh.op

2.1 SQL Injection

Insert Screenshot of Account Settings Showing You as Admin Here:



User Profile

Email:
admin@juice-sh.op

Username:
e.g. SuperUser

Set Username

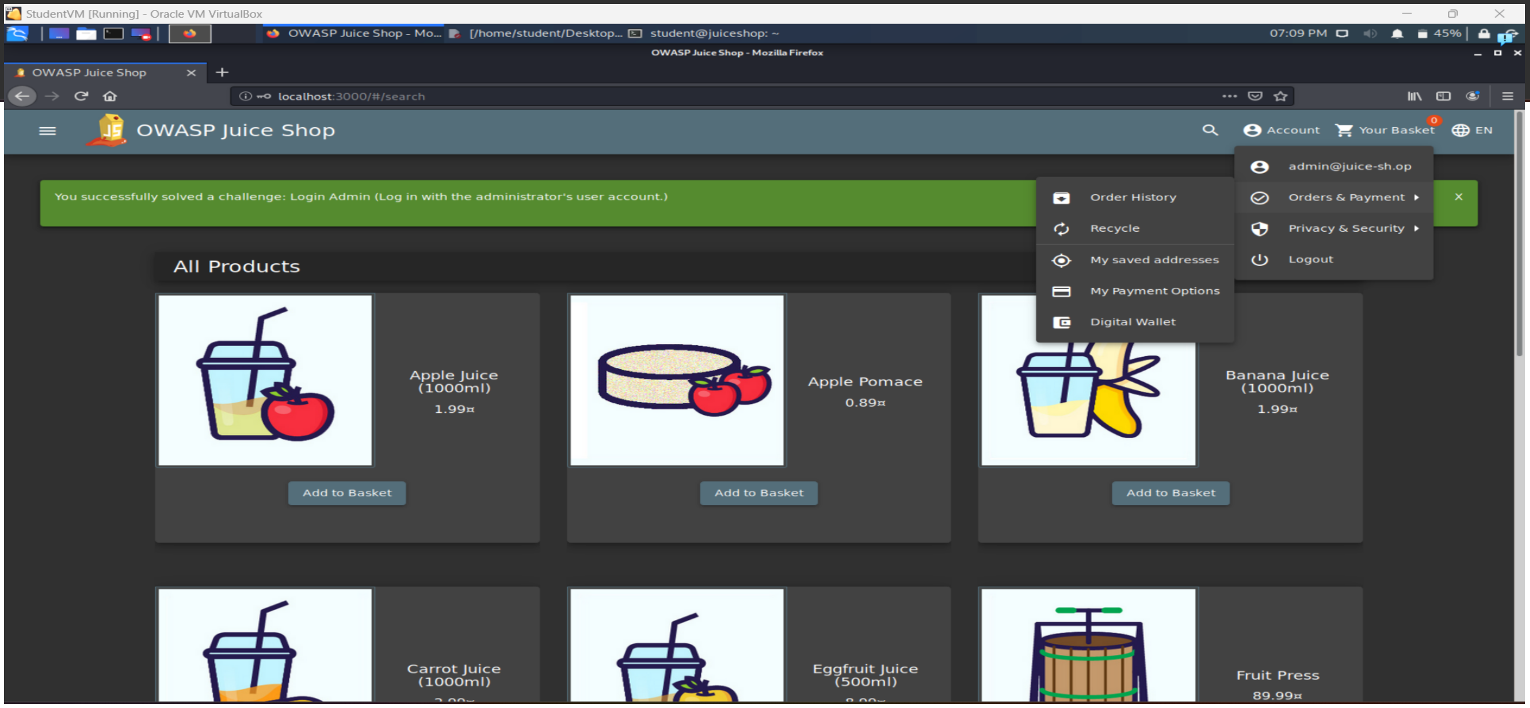
File Upload:
Browse... No file selected.

Upload Picture

or

Image URL:
e.g. https://www.gravatar.com/avatar/526703ad2bd7cd675e872393a07

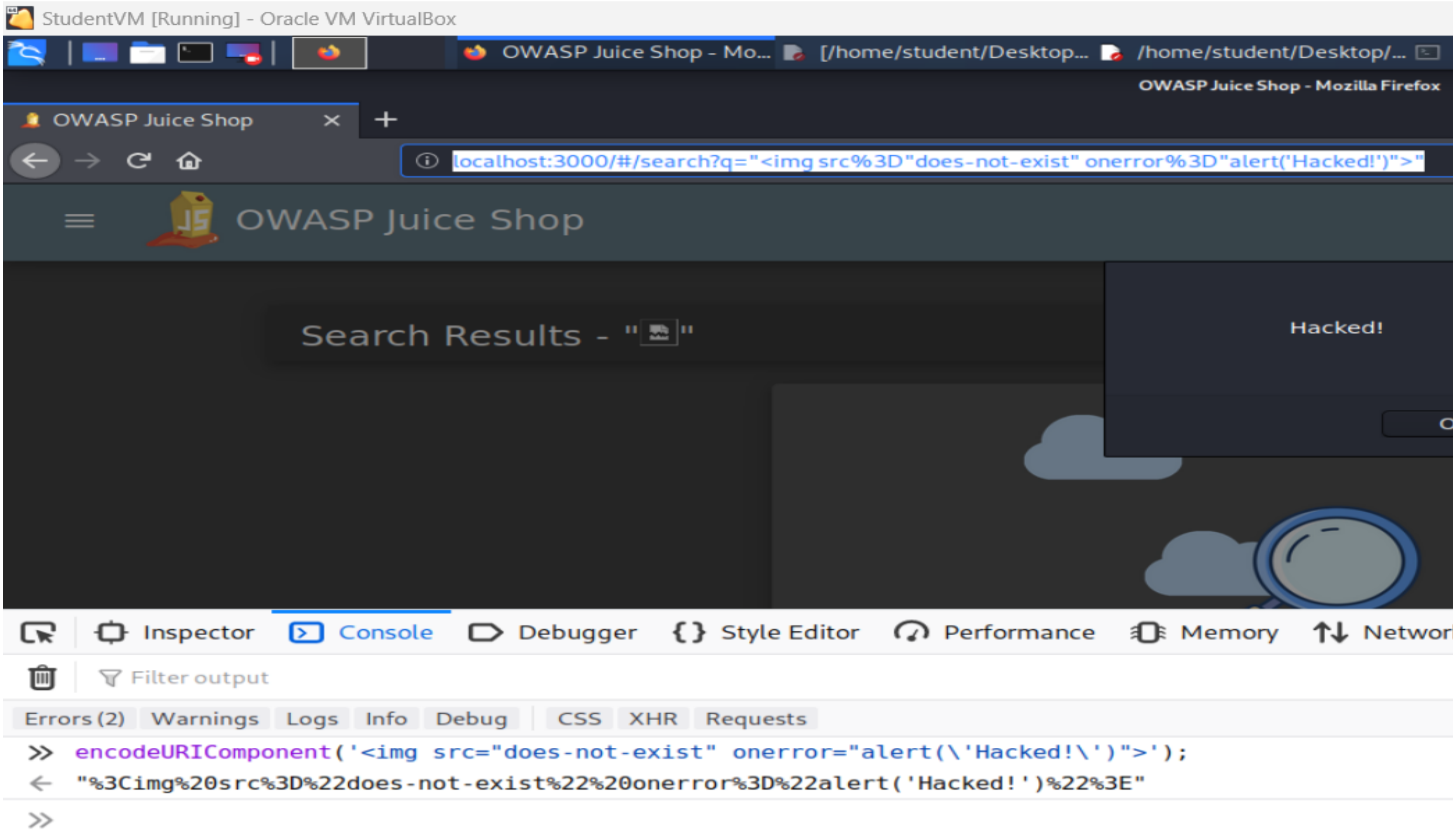
Link Image



You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

2.2 XSS

Insert Screenshot of Your Commands Here:

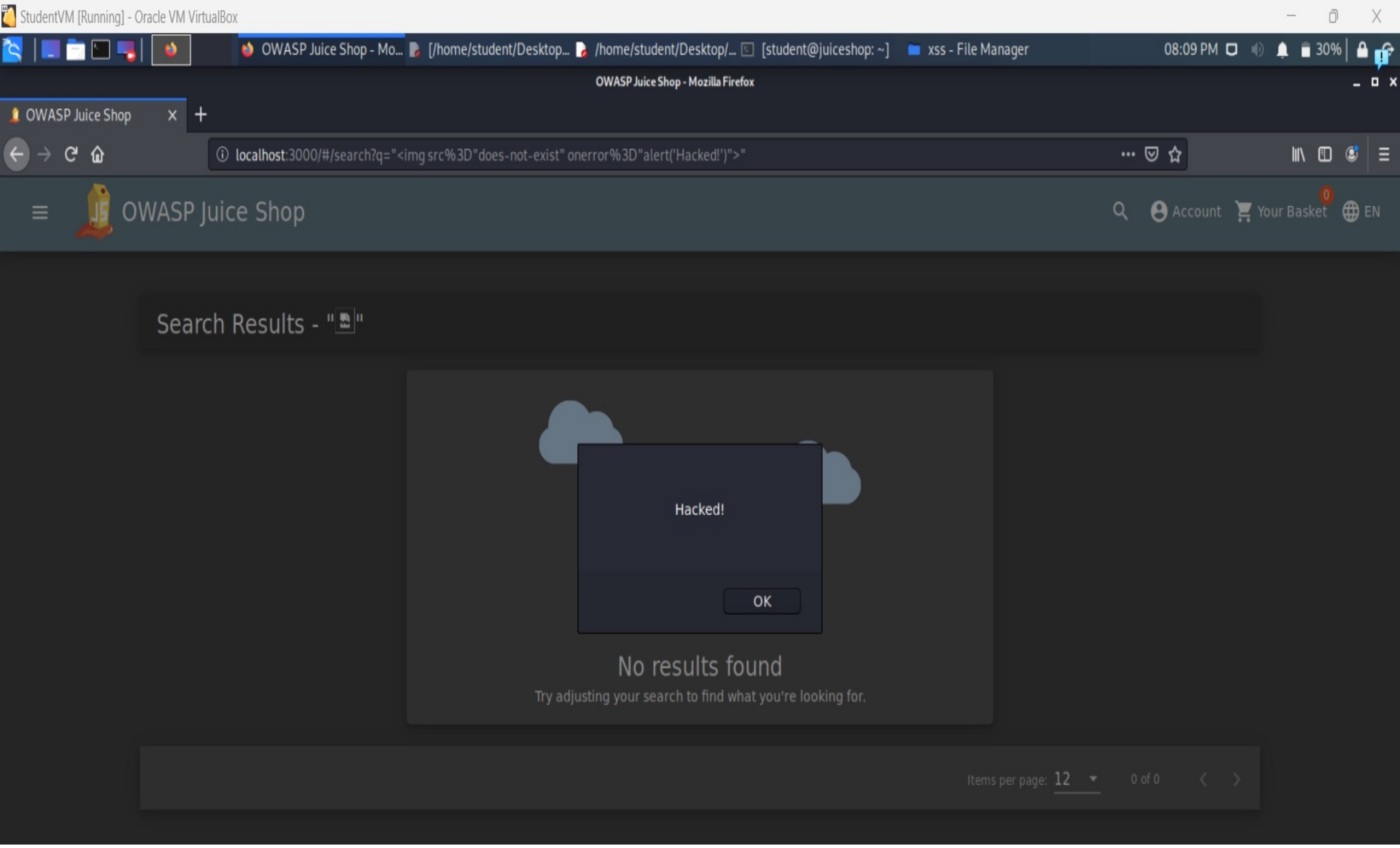


```
localhost:3000/#/search?q="<img src%3D"does-not-exist" onerror%3D"alert('Hacked!')">"
```

```
>> encodeURIComponent('<img src="does-not-exist" onerror="alert(\'Hacked!\')">');
← "%3Cimg%20src%3D%22does-not-exist%22%20onerror%3D%22alert('Hacked!')%22%3E"
>>
```

2.2 XSS

Insert Screenshot of `alert()` popup saying "Hacked!" Here:



localhost:3000/#/search?q="<img src%3D"does-not-exist" onerror%3D"alert('Hacked!')">"

Search Results - ""

Hacked!

No results found

Try adjusting your search to find what you're looking for.

Section 3

Risk Analysis

3.1 Scoring Risks

Risk	**Score** ***(1 is most dangerous, 4 is least dangerous)***
Distributed Denial of Service (DDoS) attack.	1
SQL Injection	1
XSS Vulnerability	1
Insecure Architecture	2

3.2 Risk Rationale

Why Did You Choose That Ranking?

First, we need to solve the problem that makes ***Distributed Denial of Service (DDoS)*** *attacks happened. Because DDoS attacks affect the availability of the Udajuicer website. which is one of the elements of CIA triad.*

Second, ***SQL Injection*** *because when occurring the attacker gets full access to the database he can alter, insert or delete. That affects the CIA triad, confidentiality, integrity, and authenticity of the data. Attacker can compromise the users' information, and steal the*

Third, ***XSS Vulnerability*** *because it compromises confidentiality and integrity causing a series of risks that can affect the whole Udajuicer website, compromise the users' information, and steal the credentials of the admin.*

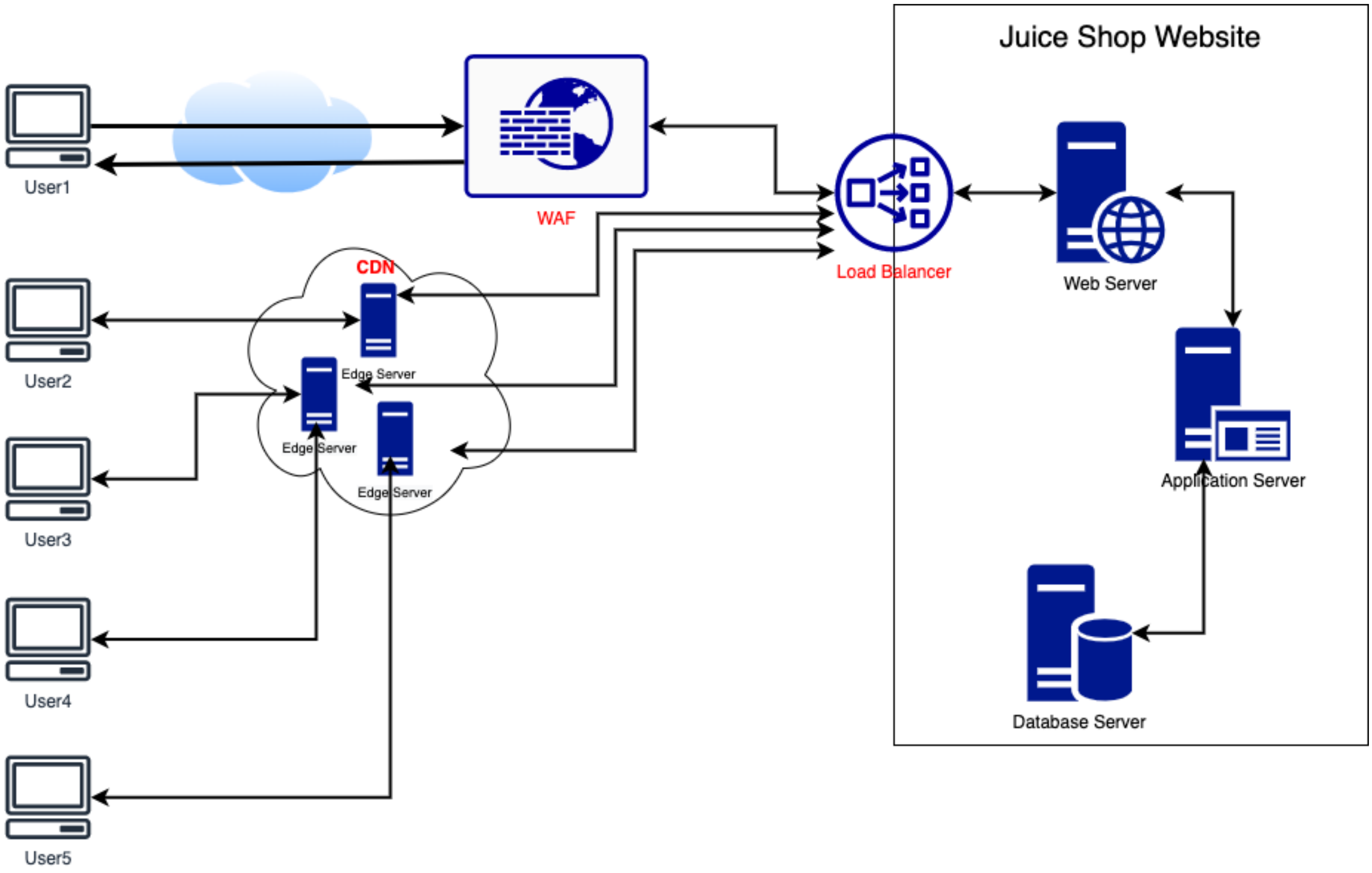
Fourth, ***Insecure Architecture*** *has less priority because it doesn't compromise CIA triad directly to the endanger.*

Section 4

Mitigation Plan

4.1 Secure Architecture

Insert Image of Your Secure Architecture Here:



4.2 Mystery Attack Mitigation

What is Your Mitigation Plan?

As I security analyst, I suggest some methods to prevent any further attack of the type of DDoS. First, we should implement a content delivery network (CDN) to cached content to the edge servers to manage the requests if a DDoS attack happened and the main server is overloaded. Second, we need a firewall to monitor and manage in and out traffic and set the rules on the firewall to prevent the server from overloading and crashing.

4.3 SQL Injection Mitigation

What is Your Mitigation Plan?

To mitigate SQL injection attacks we should take into account user input, so we need Input sanitization, input validation, prepared statements with parameterized queries, and escaping. To make sure no malicious queries are entered in the input field.

4.4 XSS Mitigation

What is Your Mitigation Plan?

To mitigate XSS attacks we should take into account user input, so we need Input sanitization, input validation and escaping. To make sure no malicious code is entered in the input field.