



SECURITY ASSESSMENT

Juice Shop Vulnerabilities Report

Submitted to: Development Team
Security Analyst: Arwa AlQadheeb

Date of Testing: Dec 11, 2022
Date of Report Delivery: Dec 14, 2022

Table of Contents

Contents

- SECURITY ENGAGEMENT SUMMARY..... 2**
 - ENGAGEMENT OVERVIEW..... 2
 - SCOPE..... 2
 - EXECUTIVE RISK ANALYSIS 2
 - EXECUTIVE RECOMMENDATION..... 2
- SIGNIFICANT VULNERABILITY SUMMARY 3**
 - High Risk Vulnerabilities..... 3
 - Medium Risk Vulnerabilities 3
- SIGNIFICANT VULNERABILITY DETAIL..... 4**
 - SQL INJECTION 4
 - SECURITY MISCONFIGURATION 5
- SECURITY ANALYSIS METHODOLOGY 6**
 - ASSESSMENT TOOLSET SELECTION 6
 - ASSESSMENT METHODOLOGY DETAIL 6

Security Engagement Summary

Engagement Overview

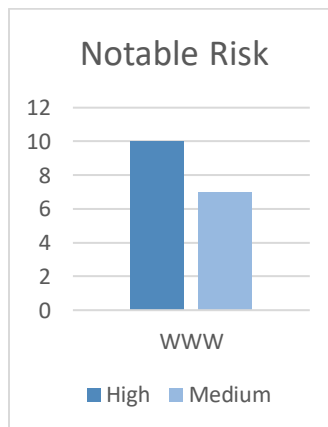
As part of the ongoing quarterly security assessment procedure and at the request of the development team, who is in charge of maintaining the legacy web-application (www) of Udajuicer, Arwa AlQadheeb completed the vulnerability assessment that is the topic of this report on December 14, 2022. In order to improve the overall security posture of the organization, this assessment is necessary to conduct.

Scope

The scope of this assessment is to analyze the risk the web-application (www) poses to the organization.

Executive Risk Analysis

A significant security weakness with HIGH risk level, referred to as SQL injection, in the way the web-application (www) interprets user input, making it easier to exploit and attack. Additionally, the web-application is developed improperly such that security misconfiguration in form of unhandled error with MEDUIM risk would facilitate further attacks.



Executive Recommendation

It is strongly suggested that security misconfiguration be handled as a priority and appropriately by restricting the amount of information shown to the user and making sure to thoroughly check every user-provided input to avoid the execution of any dangerous code.

Significant Vulnerability Summary

At the vulnerability identification stage, the first stage of vulnerability assessment process, we have scanned Udajuicer's web-application for vulnerabilities and we have detected several security vulnerabilities listed below, in descending order based on the risk they impose:

High Risk Vulnerabilities

- SQL Injection.

Medium Risk Vulnerabilities

- Security Misconfiguration.

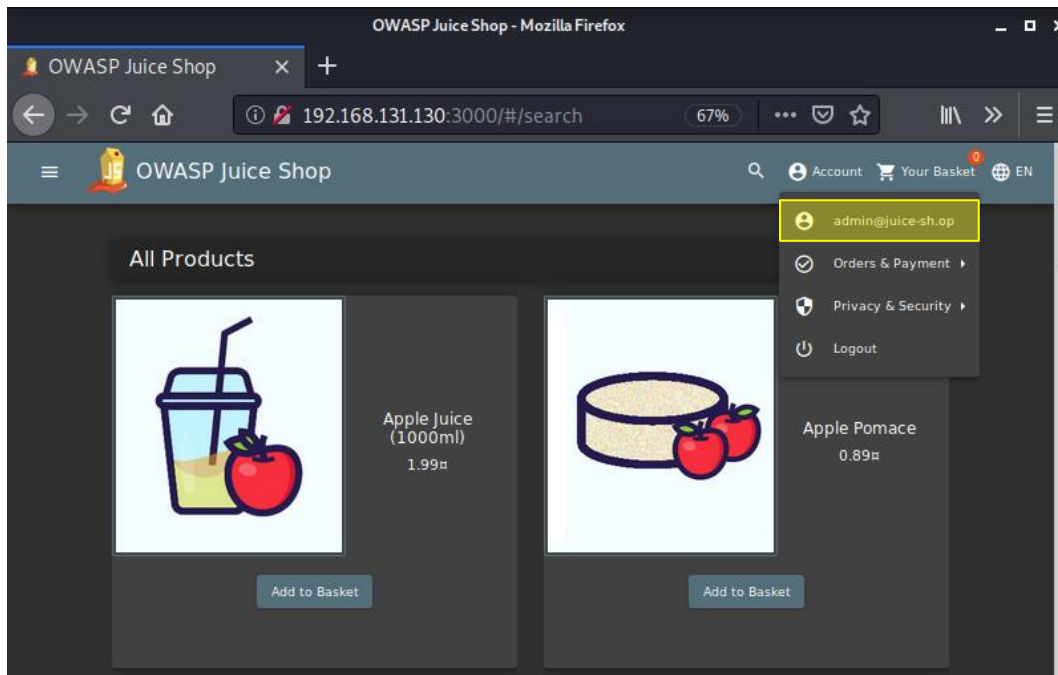
Significant Vulnerability Detail

SQL Injection

HIGH

SQL injection is a widespread vulnerability found on different web-applications, so do on our Juice Shop web-application, and has been rated as one of [Open-Source Web-application Project \(OWASP\) Top 10](#). The exploitation of SQL injection is somehow effortless and does not require that much of a skill from an attacker due to the various resources and tools out there in the wild that can aid with such vulnerability.

We have assessed this vulnerability as **HIGH** risk based on the qualitative analysis of two factors: the likelihood that concerns the probability of the vulnerability getting exploited, and the impact which comprises the consequences resulted from the vulnerability misuse. Based on what have been observed, SQL injection was easily detected and easily exploited using a vulnerability scanning tool where an attempt to login as administrator was successful (refer to the below screenshot).



Since SQL injection is a well-known vulnerability, it will probably be the first vulnerability to look for in a web-application. In other words, it is *almost assured* that during malicious reconnaissance, any adversary with minimum skill-level would catch the security flaw that revealed the database reside in the background, and then would easily use any scanning tool with fuzzing technique to leverage the improper input validation and inject malicious SQL query to the web-application then gain unauthorized access to its internal component.

On the other hand, the consequences of a successful SQL injection attempt can be the source of *multiple severe effects* ranging from accessing the database, associated with the Juice Shop web-application, with admin privilege to issuing commands to the hosted system. Hence, it is determined that the overall risk imposed by the SQL injection is **HIGH**, implying that organization as a whole and specific departments, in particular IT and Sales and Marketing departments can suffer from several negative outcomes. This may include loss of customer trust, reputational damage, lack of productivity, or disciplinary penalties/fees. In addition, the negative impact would extend to cover customers if their Personally Identifiable Information (PII) was disclosed by unauthorized individual. Nevertheless, the ability to mitigate the potential risk of SQL injection depends on implementing the appropriate controls such as:

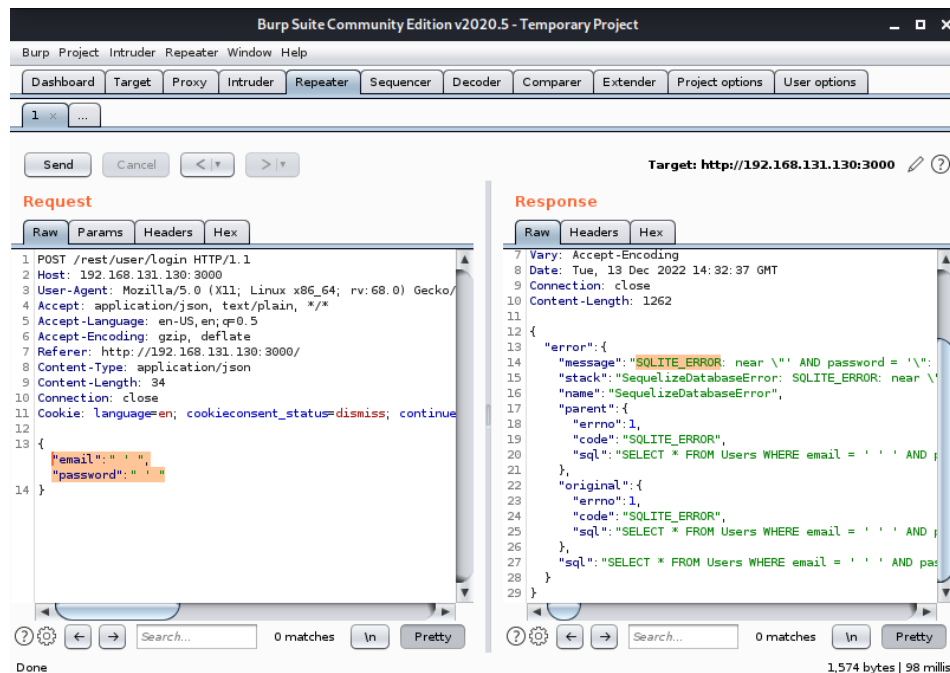
1. Input validation, sanitization, and escaping must be in place since user input cannot be trusted.
2. Parametrized queries including prepared statements to prevent malicious SQL queries execution.

Security Misconfiguration

MEDIUM

Security Misconfiguration placed 5th on OWASP Top 10 with over 208k occurrences of a Common Weakness Enumeration (CWE) in this risk category, which implies that a considerable number of web-application were flawed with this vulnerability. The exploitation of security misconfiguration can vary in complexity depending on the skill level of the adversary and the design of the web-application.

We have assessed this vulnerability as **MEDIUM** risk based on the same qualitative methodology which have been used to evaluate the previously mentioned significant **vulnerability**. Based on what has been reported by the scanning tool, security misconfiguration was quickly found during the first simulated attack against the web-application. In addition, it was readily abusable to carry out further exploitation of other vulnerabilities such that a mishandled error was detected during a failed login attempt (refer to the blow screenshot).



In this scenario, the security misconfiguration appeared in form of an unhandled error which led to revealing useful information that an adversary can use to initiate a more harmful attack. It must bring to attention that security misconfigurations are unavoidable in any system at any scale, therefore, it is *highly likely* that an adversary might spend a little more time and effort to dig for security flaws during reconnaissance to gather as much information as possible about the target and leverage what has been gathered to launch more sophisticated attacks or identify injection weaknesses as in the Juice Shop web-application.

On the other hand, if security misconfiguration was overlooked, it can cause *significant effects* ranging from sensitive data exposure to server or web-application takeover. Hence, it is determined that the overall risk imposed by the security configuration is **MEDIUM**, indicating that the organization may experience a variety of negative impacts including operations disruption within IT department, revenue loss within Sales and Marketing department, and massive data breach that must be addressed without delay by Incident Response team. Also, such vulnerability would impact the confidentiality of customers' data. However, this vulnerability can be either remediated or mitigated using the proper safeguards such as:

1. Error responses must be designed to assist the user without disclosing unnecessary internal information.
2. Intrusion detection system could be helpful with tracking repeated failed attempts and generating alerts.
3. IT incident response plan must be in place to ensure business continuity in case of a security incident occur.

Security Analysis Methodology

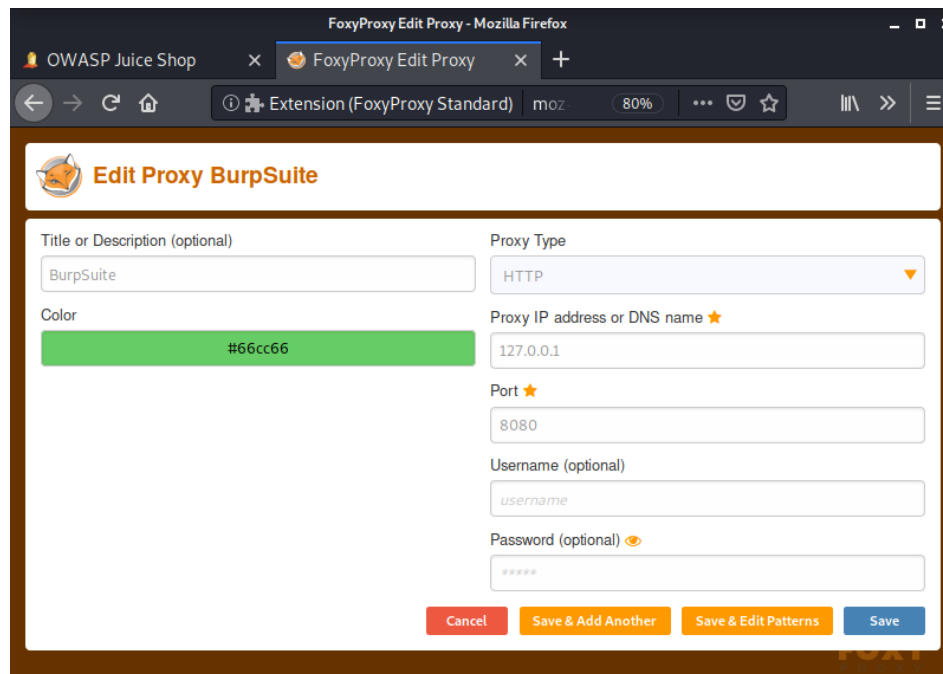
Assessment Toolset Selection

For the purpose of this assessment, the below tools were used to detect and validate the vulnerabilities mentioned in the [Significant Vulnerability Detail](#) section:

1. Firefox Web Browser.
2. Foxy Proxy Standard (Add-on Extension): an advanced proxy management tool that simplifies configuring browsers to access proxy-servers, offering more features than other proxy-plugins. For more information, please visit [here](#).
3. Burp Suite: an integrated platform developed by Portswigger for performing security testing of web-applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, to finding and exploiting security vulnerabilities. For more information, please visit [here](#).

Assessment Methodology Detail

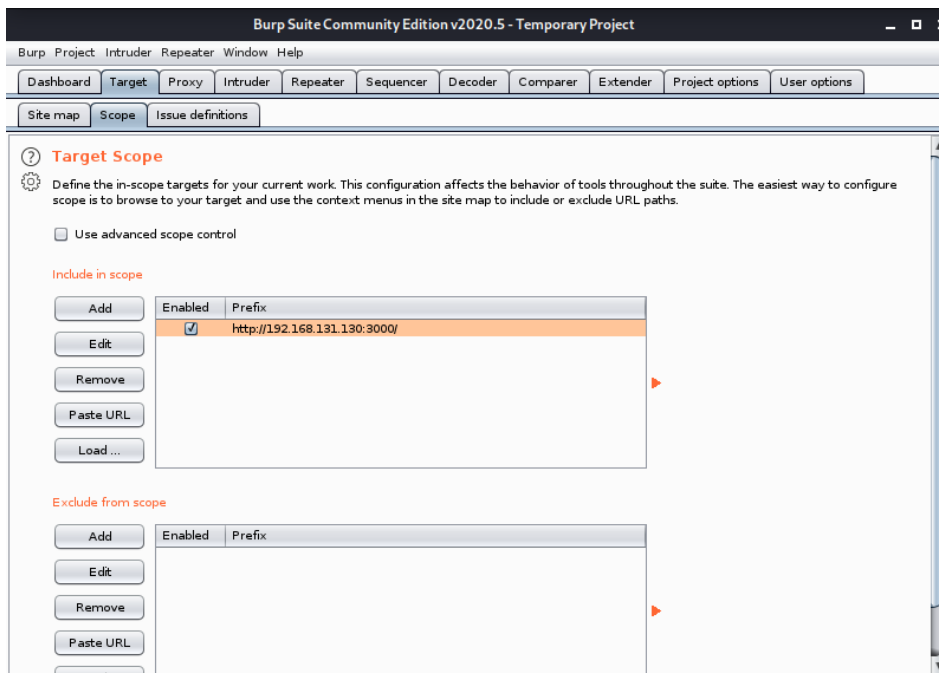
For effective vulnerability scanning, the below configuration must be made for both Foxy Proxy extension and Burp Suite.



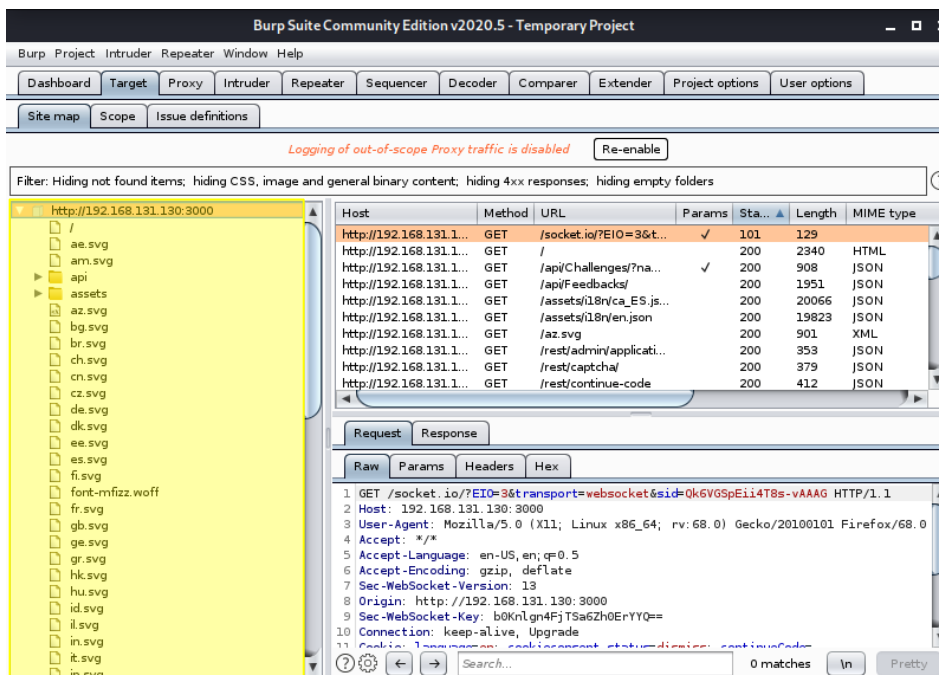
The screenshot shows the 'FoxyProxy Edit Proxy - Mozilla Firefox' window. The browser's address bar shows 'OWASP Juice Shop' and 'FoxyProxy Edit Proxy'. The extension 'Extension (FoxyProxy Standard)' is active. The main content area is titled 'Edit Proxy BurpSuite'. It contains a form with the following fields:

- Title or Description (optional):** BurpSuite
- Color:** #66cc66
- Proxy Type:** HTTP
- Proxy IP address or DNS name:** 127.0.0.1
- Port:** 8080
- Username (optional):** username
- Password (optional):** *****

At the bottom of the form, there are four buttons: 'Cancel', 'Save & Add Another', 'Save & Edit Patterns', and 'Save'.

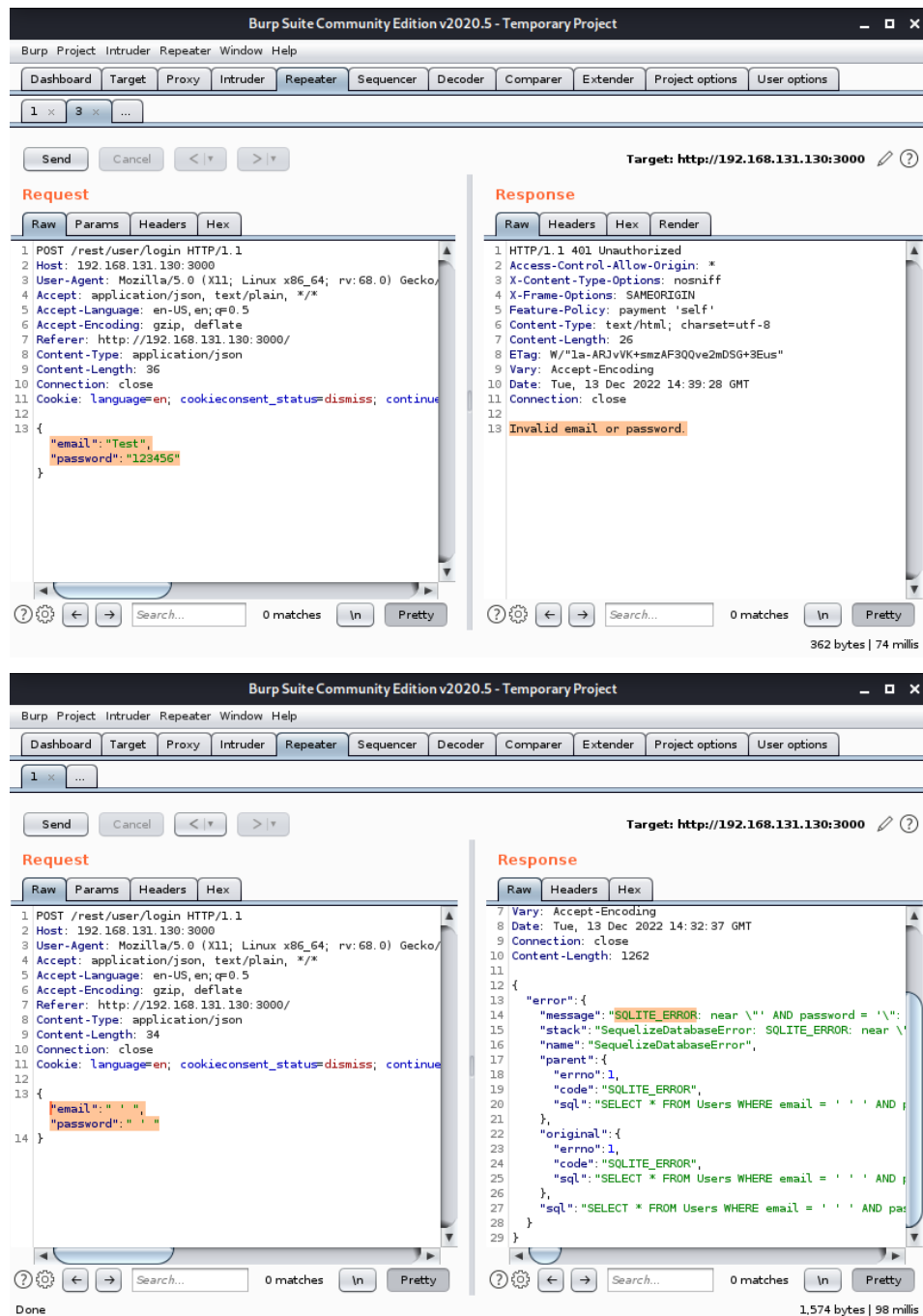


After the necessary configuration have been applied for both Foxy Proxy and Burp Suite, we have generated a site map for our target 192.168.131.130:3000



As part of the penetration testing, we tried to login to the online shop with random credentials to examine the HTTP Request and Response and to investigate the application behavior toward unexpected input by sending the login HTTP Request back to the web-application but with the below input using Burp Suite Repeater:

```
{
  "email": " ' ",
  "password": " ' "
}
```

The highlighted error in the Response tab indicates our first identified vulnerability that is security misconfiguration (i.e., mishandled error) which has revealed that the database in the background is an SQLite database. From this piece of information, an assumption was made that the web-application might be vulnerable to SQL injection attacks.

As an attempt to prove SQL injection assumption, the Burp Suite Sniper attack comes in handy which will run through a list of values in the payload and try them one at a time. The same HTTP Request for the failed login attempt was used but this time with Burp Suite Intruder. On the Position tab, the attack type must be specified, and the desirable positions must be selected as shown below. In addition, a common wordlist was used as the payload and can be found [here](#).

NOTE: make sure to *uncheck* URL-encodes these characters option in the Payload Encoding section.

Intruder attack 5

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Position	Payload	Status	Error	Timeo...	Length	Comment
45	1	a'	500			1599	
46	1	admin' or '	401			362	
47	1	' and 1=(if(load_file(char...	500			1733	
48	1	' and 1 in (select var from ...	500			1626	
49	1	anything' OR 'x'='x	401			362	
50	1	"a'" or 1=1--"	500			1531	
51	1	a' or 1=1--	200			1170	
52	1	"a'" or 3=3--"	500			1531	
53	1	a' or 3=3--	200			1170	
54	1	a' or 'a' = 'a	401			362	
55	1	'%20OR	401			362	
56	1	as	401			362	
57	1	asc	401			362	

Request Response

Raw Params Headers Hex

```

Content-Type: application/json
Content-Length: 43
Connection: close
Cookie: language=en; cookieconsent_status=dismiss; continueCode=L5w0ojDeg790nz06aB4Z8ERHvyJr0XYAq9pw5xYVWmkj2P1LXU
{
  "email": "a' or 3=3--",
  "password": "123456"
}

```

108 of 386

For additional validation, the same values within the successful HTTP Request were used to login to Juice Shop manually. As a result, login to administrator account was made successfully.

OWASP Juice Shop - Mozilla Firefox

OWASP Juice Shop

192.168.131.130:3000/#/login

67%

Account EN

Login

Email

a' or 3=3--

Password

123456

Forgot your password?

Log in

☐ Remember me

Not yet a customer?

