<COMPANY> Web Application VAPT Report

Table Of Contents

1 <COMPANY> Web Application VAPT Report	3
1.1 Introduction	3
1.2 Confidentiality	3
1.3 Scope	3
2 Executive Summary	4
2.1 Recommendation	4
3 Finding Severity Ratings	5
3.1 Risk Factors	5
4 Vulnerabilities Summary	6
5 Critical Severity Vulnerabilities	7
5.1 SQL Injection	7
5.2 Cross-Site Scripting (XSS)	10
6 Medium Severity Vulnerabilities	11
6.1 Absence of Brute-Force Lockout Mechanism	11
7 Appendix	12
7. 1 Lorem ipsum dolor sit amet, consec	12

1 <COMPANY> Web Application VAPT Report

REMOVE THIS DESCRIPTION PROPERTY FROM JSON IF IT IS NOT NEEDED.

NOTE	ONLY TWO COLS SUPPORTED: REMOVE THIS ROW FROM JSON
Version	1.0
Date	29th April 2024
Author	Safeer S

1.1 Introduction

Subject of this document is summary of penetration test performed against web applications owned by <COMPANY> company. Test was conducted according to rules of engagement defined and approved at the beginning by both parties – customer and contractor. Black-box pentesting assignment was requested.

Black-box penetration test classification means that penetration tester has no internal knowledge about target system architecture. He/she can use information commonly available on the Internet. More data can be collected during reconnaissance phase based on observation of target system behavior. Black-box penetration test results gives overview of vulnerabilities exploitable from outside the company network. It shows how unauthenticated actor can take advantage of weaknesses existing in tested web application.

1.2 Confidentiality

This document contains confidential and proprietary information solely intended for internal use within <COMPANY>. Any unauthorized disclosure, transmission, duplication, or use of this information, in whole or in part, for purposes other than its intended use, is strictly prohibited. Unauthorized use or disclosure of this information without explicit written permission from <COMPANY> is in violation of confidentiality agreements and may result in legal action. Please ensure that this information is handled with the utmost confidentiality and only shared with authorized personnel within <COMPANY>.

1.3 Scope

To perform a Black Box Web Application Penetration Test against the web applications of the organization named <COMPANY>.

- www.<COMPANY>.exam
- me.<COMPANY>.exam
- blog.<COMPANY>.exam

2 Executive Summary

Performed a Web Application Penetration Test for <COMPANY> to evaluate its defensive posture, identify vulnerabilities, assess their severity, and offer remediation steps. Identified critical vulnerabilities posing a significant risk of compromise by external attackers, including the ability to inject arbitrary database commands, potentially leading to unauthorized access and data exfiltration. Another critical vulnerability allows attackers to obtain a reverse shell, compromising <COMPANY>'s servers.

2.1 Recommendation

We recommend promptly patching the vulnerabilities identified during the testing to prevent potential exploitation by attackers in the future. It's essential to note that these systems necessitate frequent patching. Once patched, they should be included in a regular patch program to address any additional vulnerabilities that may emerge at a later date. By maintaining a proactive approach to patch management, <COMPANY> can significantly enhance the security posture of its systems and mitigate the risk of potential cyber threats.

3 Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

NOTE	ONLY TWO COLS SUPPORTED: REMOVE THIS ROW FROM JSON
Severity	**Definition**
Critical	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately
High	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible
Medium	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

3.1 Risk Factors

Likelihood: It measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact: It measures the potential vulnerability’s effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss

4 Vulnerabilities Summary

Severity	Vulnerability
Critical	SQL Injection
Critical	Cross-Site Scripting (XSS)
Medium	Absence of Brute-Force Lockout Mechanism

5 Critical Severity Vulnerabilities

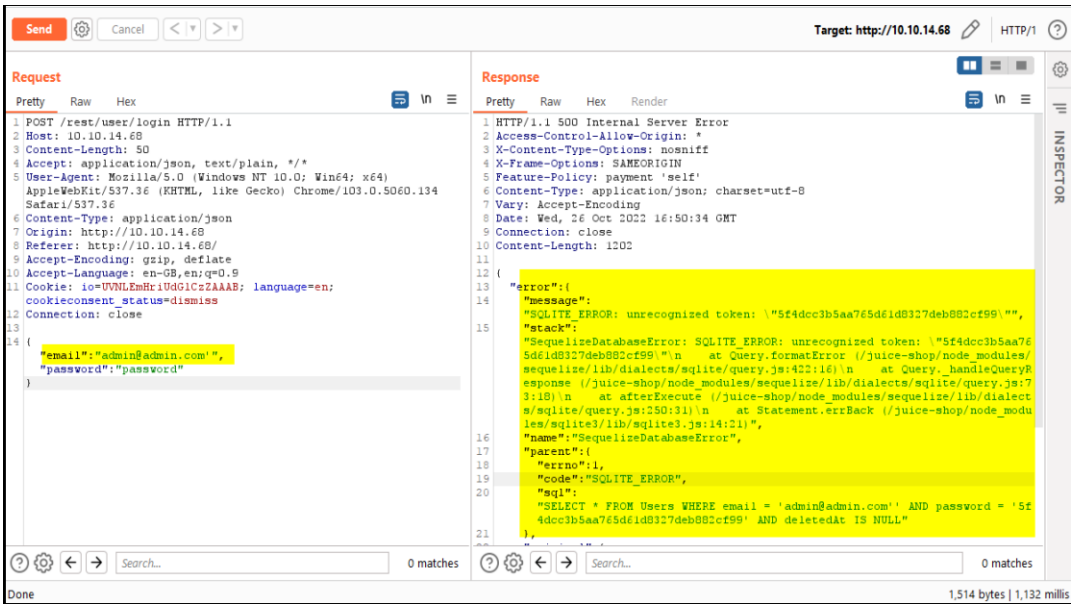
5.1 SQL Injection

Description	SQL Injection occurs when untrusted user inputs are incorrectly sanitized and directly incorporated into SQL queries, allowing attackers to manipulate the database.
Severity	Critical
Impact	If exploited, SQL Injection vulnerabilities could lead to unauthorized access to sensitive data, data manipulation, or even database compromise.
System	juice.<COMPANY>.com, webgoat.<COMPANY>.com
Recommendation	To mitigate this vulnerability, use parameterized queries or prepared statements to interact with the database. Implement input validation and proper escaping of user inputs.

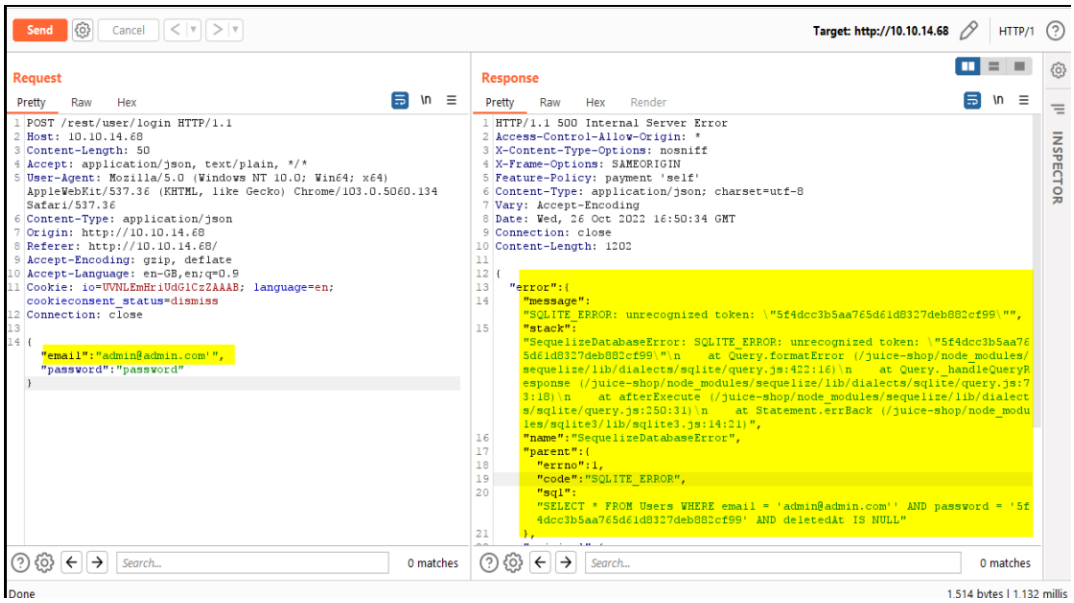
Evidence of the defect:

juice.<COMPANY>.com - Login

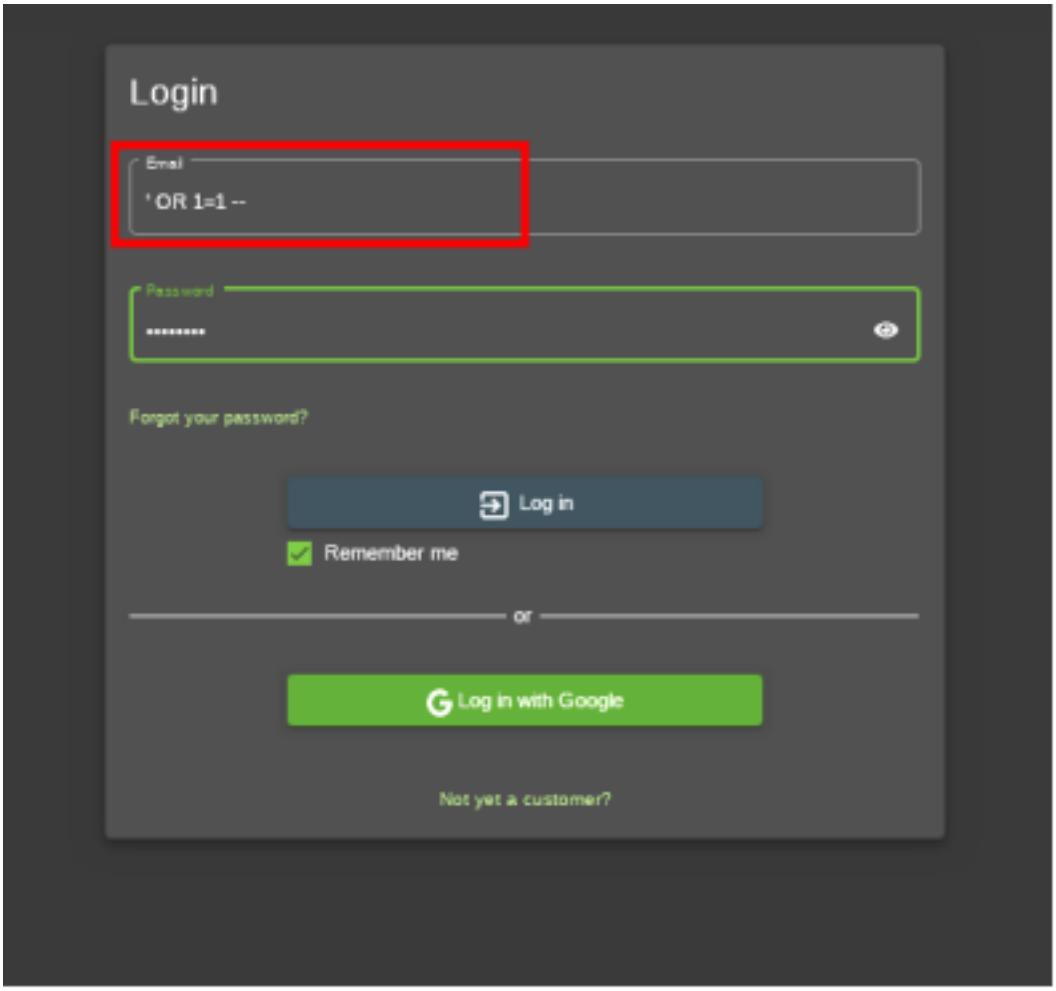
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Suspendisse potenti nullam ac tortor vitae. Mi quis hendrerit dolor magna eget est.
Lorem ipsum dolor sit amet, consectetur adipiscing elit



Molestie nunc non blandit massa enim. Risus feugiat in ante metus dictum at tempor commodo.



Semper quis lectus nulla at volutpat diam ut venenatis tellus. Tincidunt vitae semper quis lectus nulla



webgoat.<COMPANY>.com - Challenge

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Suspendisse potenti nullam ac tortor vitae. Mi quis hendrerit dolor magna eget est.

Neque viverra justo nec ultrices dui sapien eget. Porttitor massa id neque aliquam vestibulum

```
PUT /WebGoat/SqlInjectionAdvanced/challenge HTTP/1.1
Host: 192.168.56.104:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.56.104:8080/WebGoat/start.mvc
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 106
Connection: close
Cookie: JSESSIONID=mPxOky49RpzIz9VuHX_u2pO6xFoxDXXgxmq3DojW; WEBWOLFSESSION=9zfdVIu-KwWdxIwoOoyUHygGfAXpa8lq0zebKHV6

username_reg=newuser'+AND+substring(database_version(),1,1)='§2§&email_reg=email%40email.com&password_reg=1234&
confirm_password_reg=1234
```

Id velit ut tortor pretium viverra. Pharetra diam sit amet nisl suscipit adipiscing bibendum. Consectetur libero id faucibus nisl.

```
HTTP/1.1 200 OK
Connection: close
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Content-Type: application/json
Date: Sun, 06 Sep 2020 15:26:12 GMT

{
  "lessonCompleted":false,
  "feedback":"User newuser' AND substring(database_version(),1,1)='2 already exists please try to register with a different username.",
  "output":null,
  "assignment":"SqlInjectionChallenge",
  "attemptWasMade":true
}
```

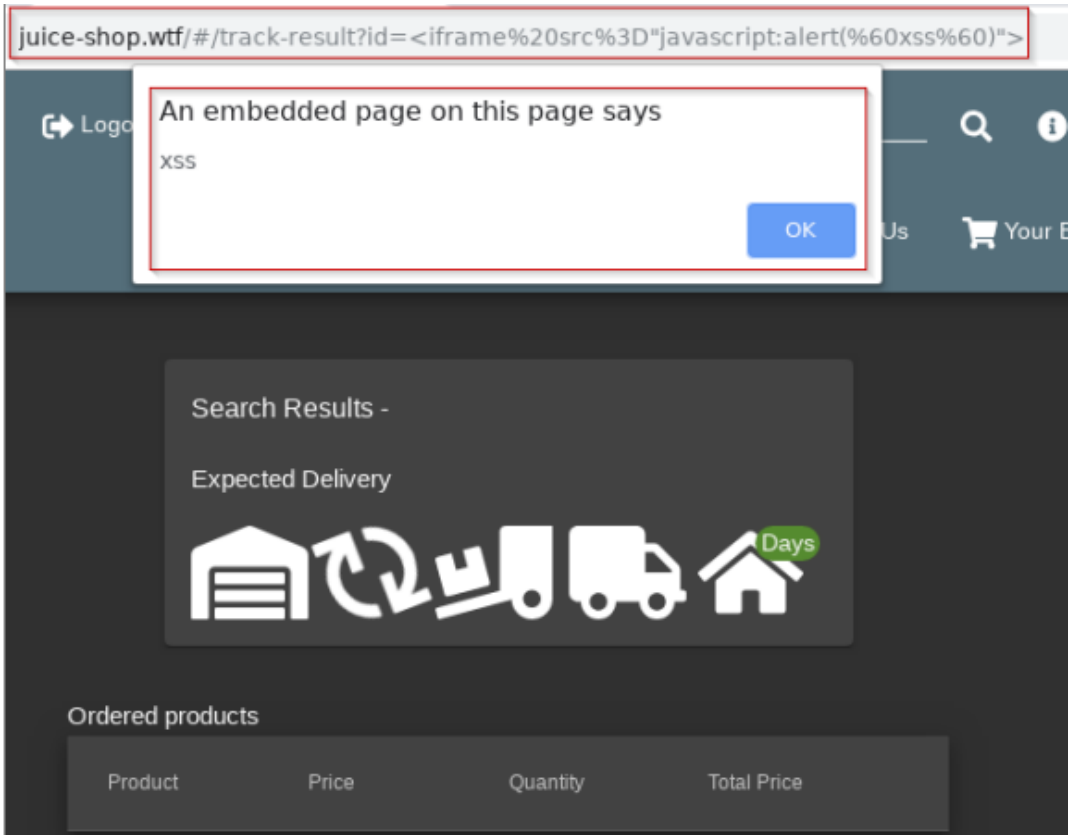
5.2 Cross-Site Scripting (XSS)

Description	Cross-Site Scripting (XSS) occurs when untrusted user inputs are incorrectly validated or not properly encoded in web applications, allowing attackers to inject malicious scripts into web pages viewed by other users.
Severity	Critical
Impact	If exploited, XSS vulnerabilities could lead to unauthorized access to sensitive data, session hijacking, defacement of web pages, or execution of arbitrary code in the context of the victim's browser.
System	juice.<COMPANY>.com
Recommendation	To mitigate this vulnerability, ensure proper input validation, output encoding, and validation of HTML content. Implement Content Security Policy (CSP) headers to restrict the execution of scripts from unauthorized sources.

Evidence of the defect:

juice.<COMPANY>.com - Login

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Suspendisse potenti nullam ac tortor vitae. Mi quis hendrerit dolor magna eget est.
Lorem ipsum dolor sit amet, consectetur adipiscing elit



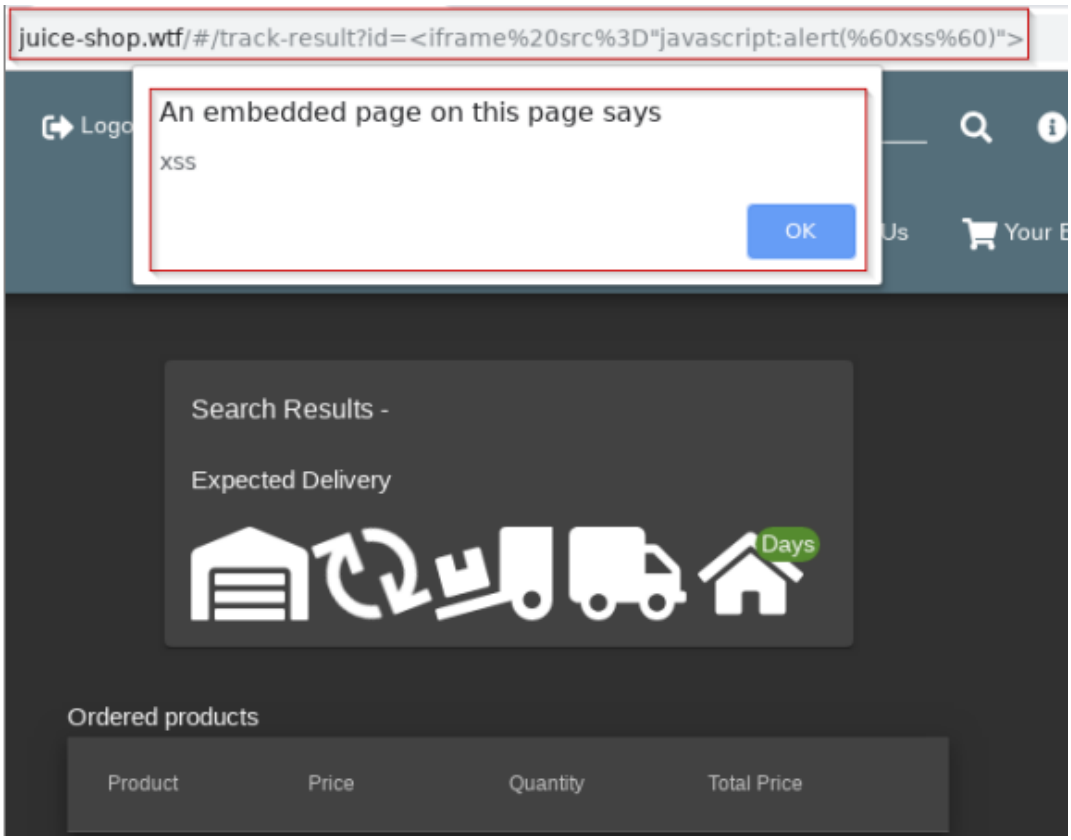
6 Medium Severity Vulnerabilities

6.1 Absence of Brute-Force Lockout Mechanism

Description	The absence of a brute-force lockout mechanism allows attackers to repeatedly attempt to guess user credentials or access sensitive areas of a system without any restrictions. This increases the risk of successful unauthorized access.
Severity	Medium
Impact	Without a brute-force lockout mechanism, attackers can launch automated attacks to guess passwords or gain unauthorized access to accounts, potentially leading to data breaches, identity theft, or unauthorized transactions.
System	juice.<COMPANY>.com
Recommendation	To mitigate this vulnerability, implement a mechanism that limits the number of login attempts within a certain timeframe. This could include temporarily locking user accounts or introducing CAPTCHA challenges after multiple failed login attempts. Additionally, enforce strong password policies to make it more difficult for attackers to guess passwords.

Evidence of the defect:

juice.<COMPANY>.com
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Suspendisse potenti nullam ac tortor vitae. Mi quis hendrerit dolor magna eget est.
Lorem ipsum dolor sit amet, consectetur adipiscing elit



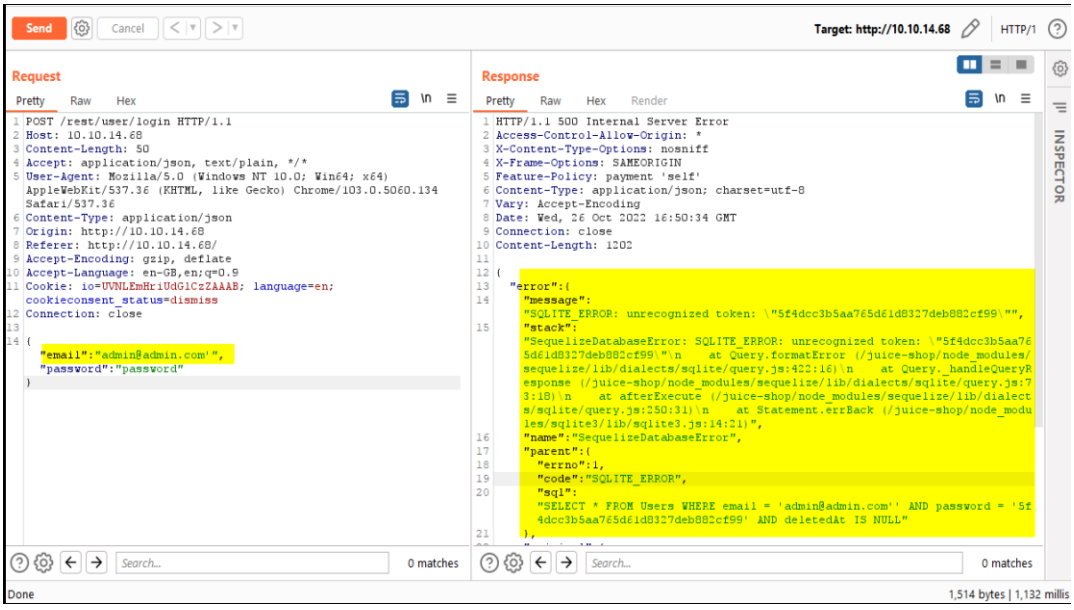
7 Appendix

7. 1 Lorem ipsum dolor sit amet, consec

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Suspendisse potenti nullam ac tortor vitae. Mi quis hendrerit dolor magna eget est.

Evidence of the defect:

Lorem ipsum dolor
Id velit ut tortor pretium viverra. Pharetra diam sit amet nisl suscipit adipiscing bibendum. Consectetur libero id faucibus nisl
Suspendisse potenti nullam ac tortor vitae. Mi quis hendrerit dolor magna eget est



Lorem ipsum dolor sit amet