Cyber Security Internship Report – Task 3

Name: Kabsha Farooq

University: University of Engineering and Technology, Taxila

Department: Telecommunication Engineering

Internship Organization: Digital Empowerment Network

Task Title: Injection and Input Validation Exploitation

Task No.: 3

Date Completed: [Enter Date]

# Task Overview

In Task 3 of my cybersecurity internship, I tested for common web application vulnerabilities on OWASP Juice Shop by performing SQL injection and input validation testing such as Cross-Site Scripting (XSS).

# Tools Used

• Web Browser (Chrome)  
• OWASP Juice Shop (https://juice-shop.herokuapp.com)

# Steps Performed

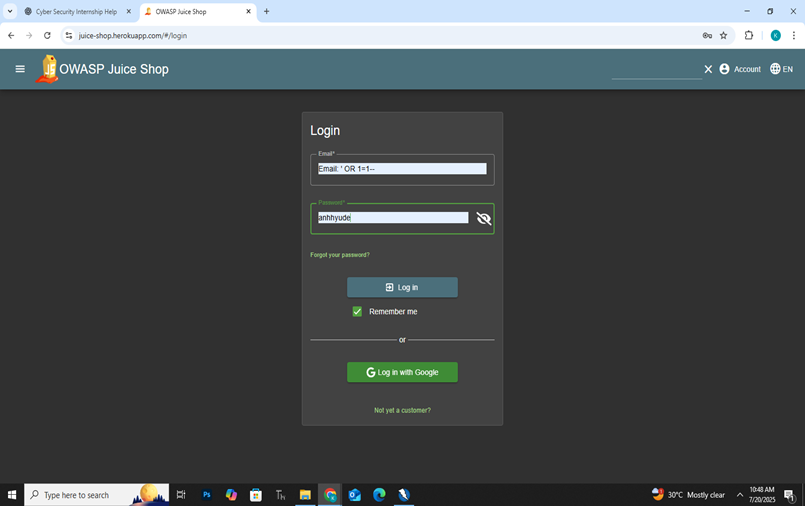
1. Visited the Juice Shop login page.
2. Tested SQL Injection using the payload: ' OR 1=1-- in the email field.
3. Successfully bypassed login validation and accessed the user dashboard.
4. Attempted Cross-Site Scripting (XSS) by entering <script>alert('XSS')</script> into the feedback form.
5. Observed that the input was stored as plain text — the script was not executed, indicating partial validation.
6. Captured relevant screenshots of inputs and results for documentation.

# Findings

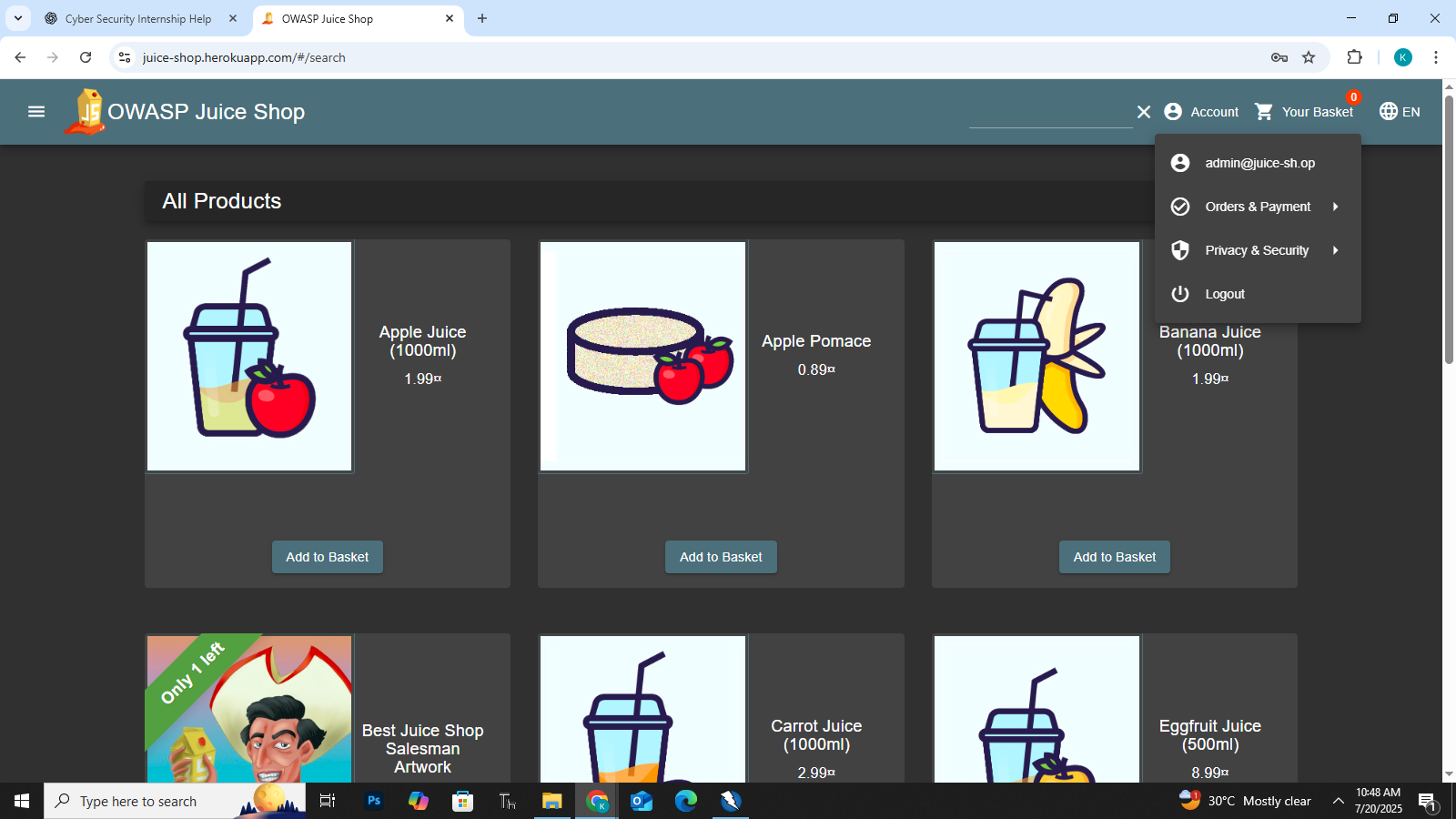
• SQL Injection vulnerability was present in the login form. The application failed to sanitize input, allowing bypass of authentication.  
• XSS input was stored but not executed. This shows the application uses partial input validation.  
• These vulnerabilities highlight weak or missing server-side validation and the need for stronger sanitization and escaping techniques.

# Screenshots

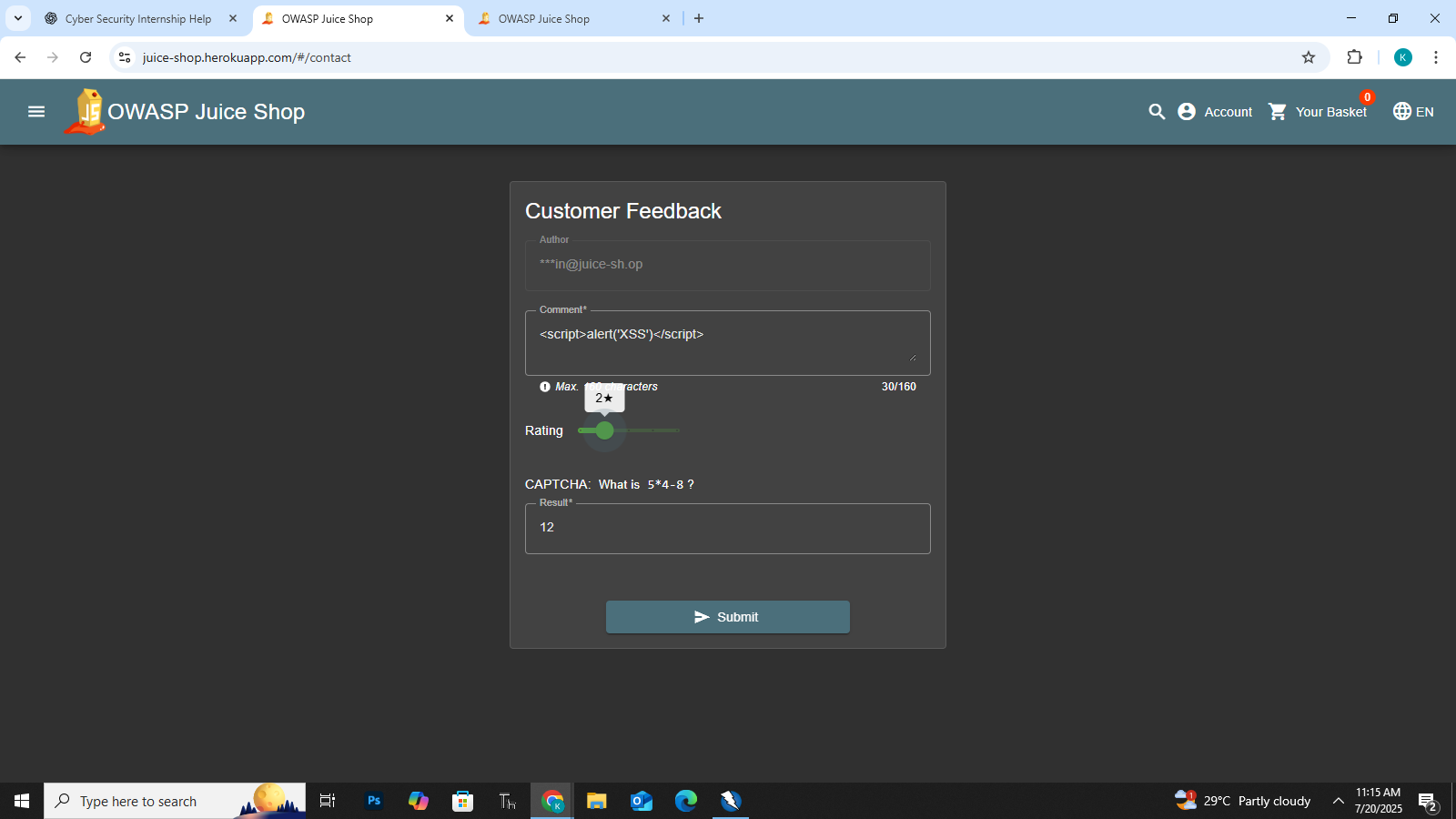
1. task3-sql-input.png – SQL Injection input in login form



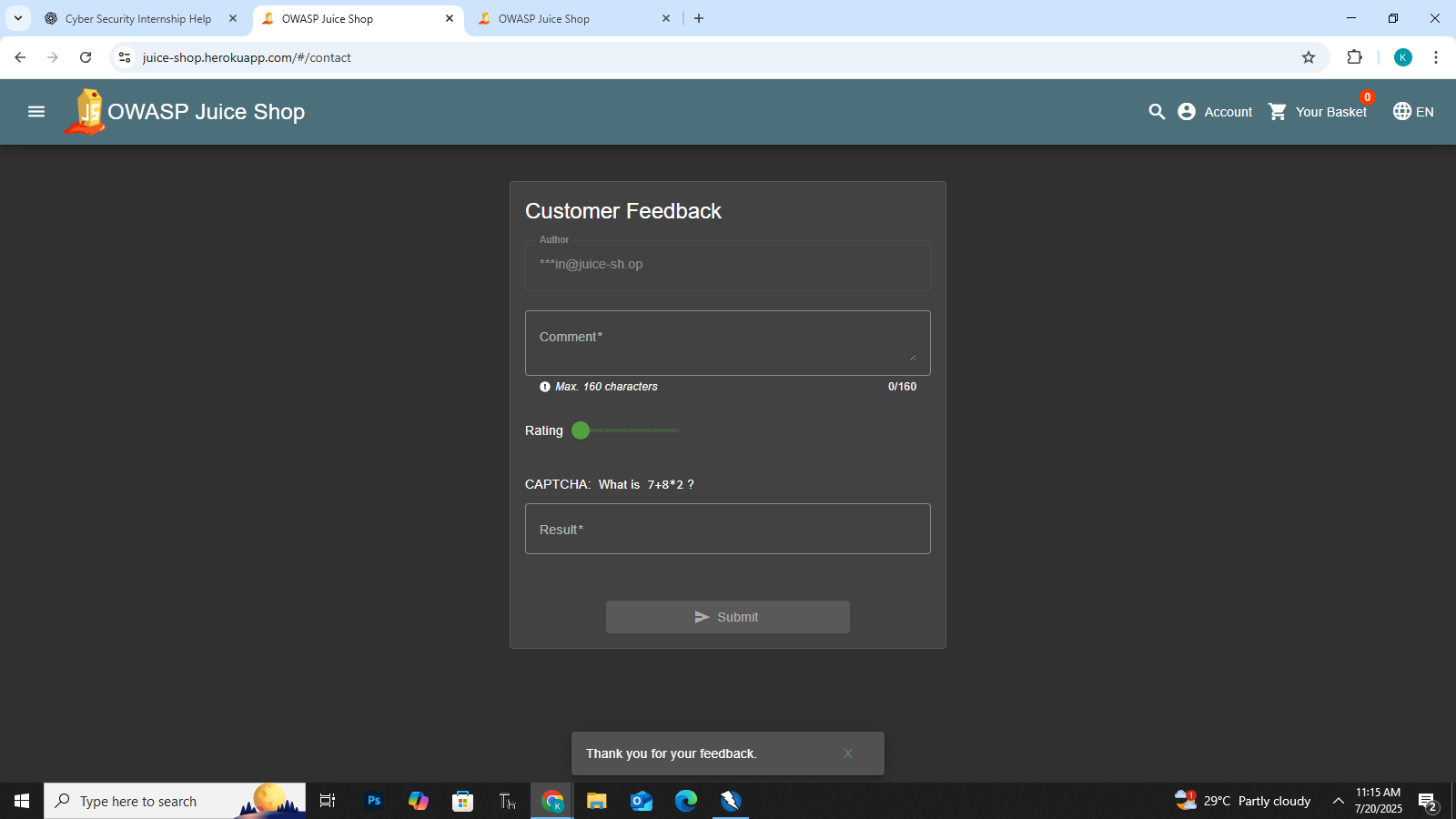
1. task3-loggedin.png – Logged-in dashboard after injection



1. task3-xss-input.png – XSS payload entered in feedback form



1. task3-xss-output.png – Displayed output (non-executed script)



# Conclusion

This task helped me understand practical exploitation of input validation flaws in web applications. By testing SQL Injection and XSS, I learned how poorly filtered inputs can lead to serious vulnerabilities.