

Performing Web Application and Database Attacks (4e)

Ethical Hacking, Fourth Edition - Lab 05

Student:

Isaiah Mosley

Email:

isaiahmosley80@gmail.com

Time on Task:

41 hours, 25 minutes

Progress:

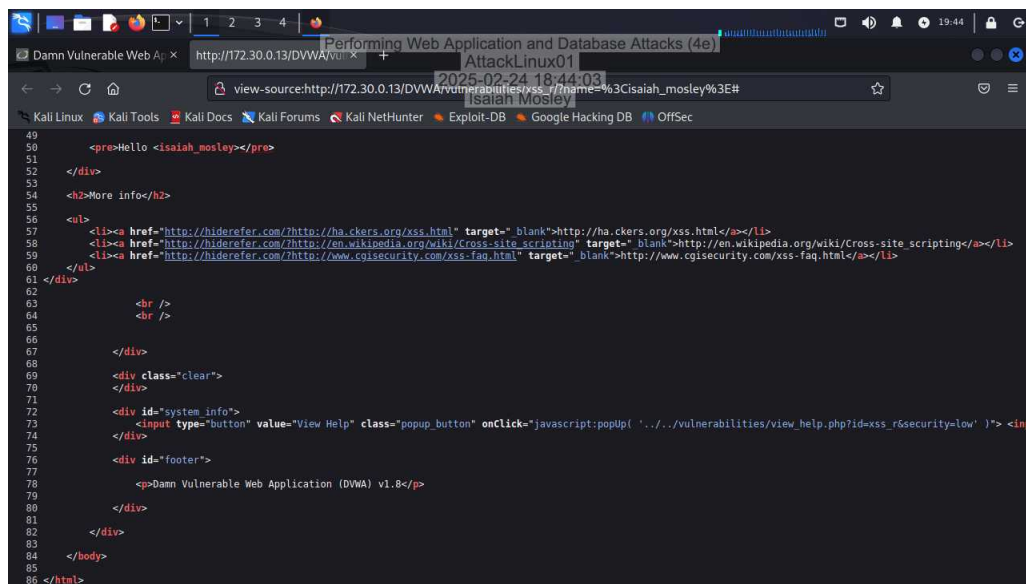
100%

Report Generated: Tuesday, December 2, 2025 at 1:23 PM

Hands-On Demonstration

Part 1: Demonstrate XSS Attacks Using DVWA

12. Make a screen capture showing the line with your name enclosed in < >.

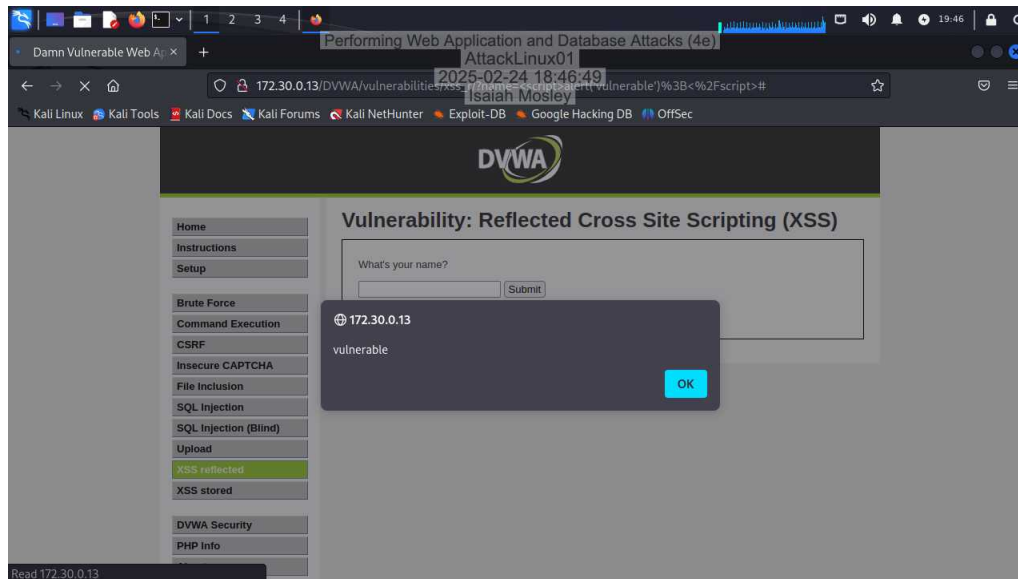


```
49 <pre>Hello <isaiah_mosley></pre>
50
51 </div>
52
53 <h2>More info</h2>
54
55 <ul>
56 <li><a href="http://hiderefer.com/?http://ha.ckers.org/xss.html" target=" blank">http://ha.ckers.org/xss.html</a></li>
57 <li><a href="http://hiderefer.com/?http://en.wikipedia.org/wiki/Cross-site_scripting" target=" blank">http://en.wikipedia.org/wiki/Cross-site_scripting</a></li>
58 <li><a href="http://hiderefer.com/?http://www.cgisecurity.com/xss-faq.html" target=" blank">http://www.cgisecurity.com/xss-faq.html</a></li>
59 </ul>
60 </div>
61
62 <br />
63 <br />
64
65 </div>
66
67 <div class="clear">
68 </div>
69
70 <div id="system_info">
71 <input type="button" value="View Help" class="popup_button" onClick="javascript:popup(' ../../vulnerabilities/view_help.php?id=xss_rsecurity=low' )"> <img
72 </div>
73
74 <div id="footer">
75
76 <p>Damn Vulnerable Web Application (DVWA) v1.8</p>
77
78 </div>
79
80 </div>
81
82 </div>
83
84 </body>
85
86 </html>
```

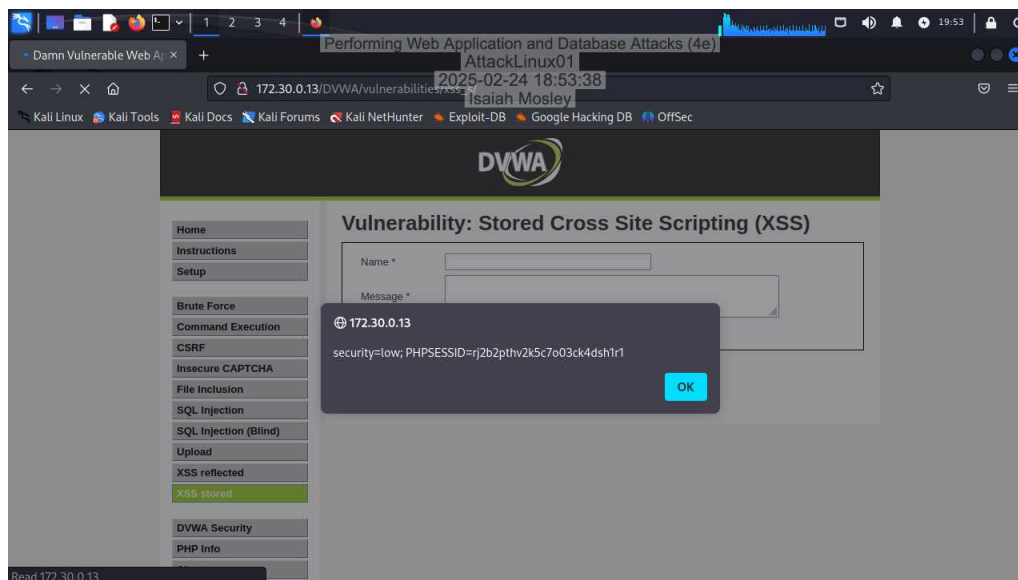
Performing Web Application and Database Attacks (4e)

Ethical Hacking, Fourth Edition - Lab 05

15. Make a screen capture showing the popup.

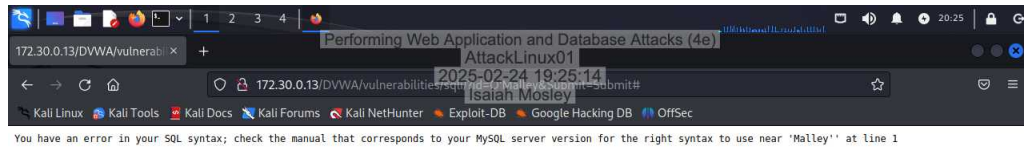


22. Make a screen capture showing the popup.

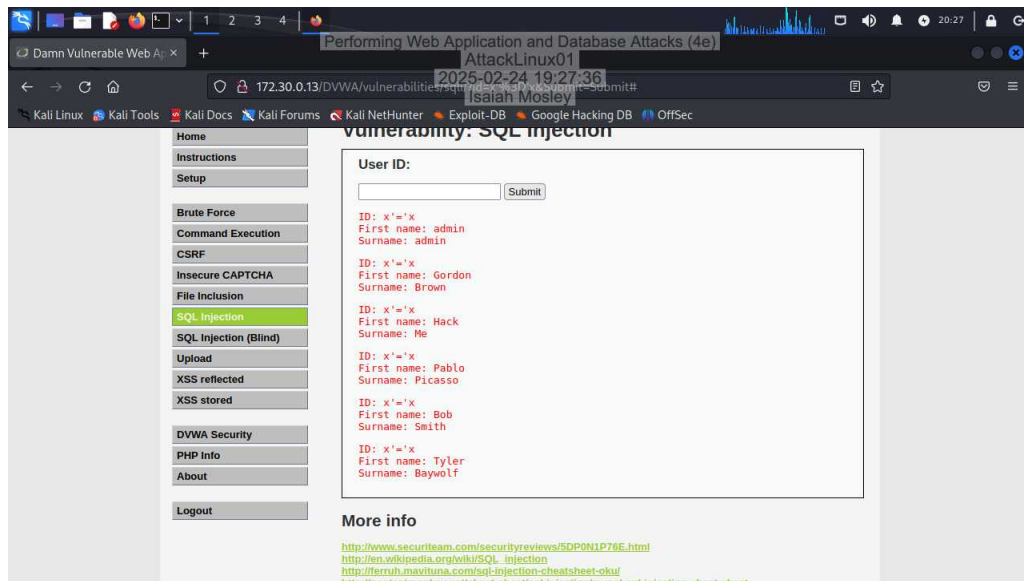


Part 2: Demonstrate SQL Injection Attacks Using DVWA

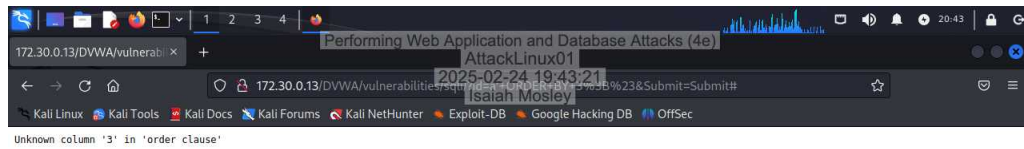
4. Make a screen capture showing the **SQL syntax error**.



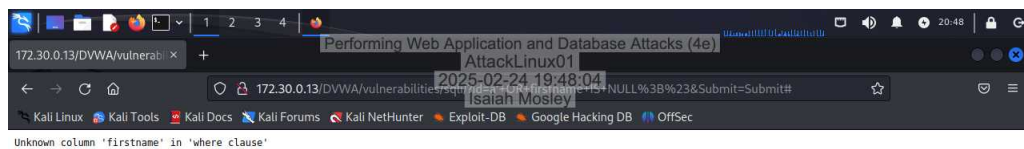
9. Make a screen capture showing the results of the query.



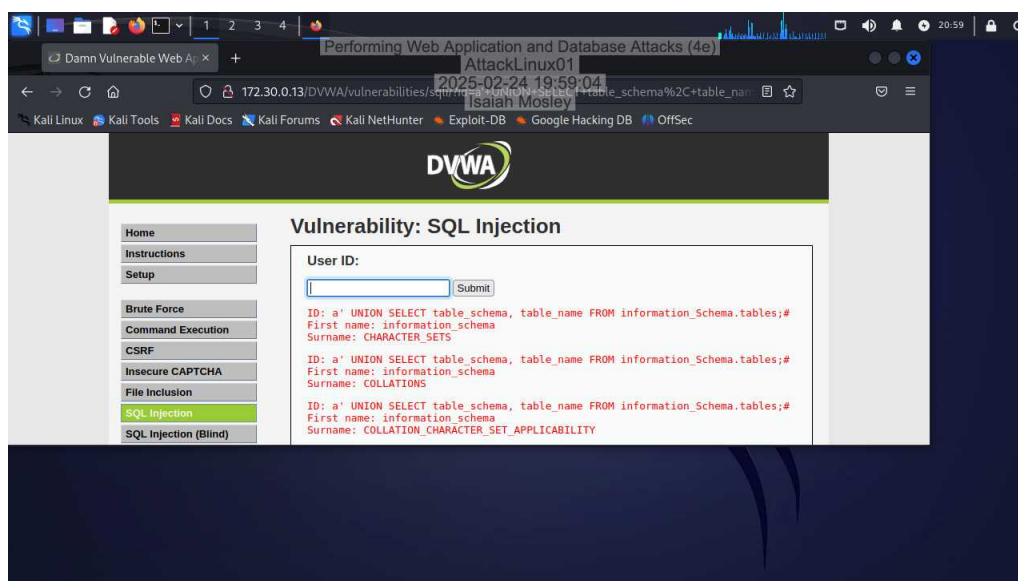
13. **Make a screen capture** showing the error page for ORDER BY 3.



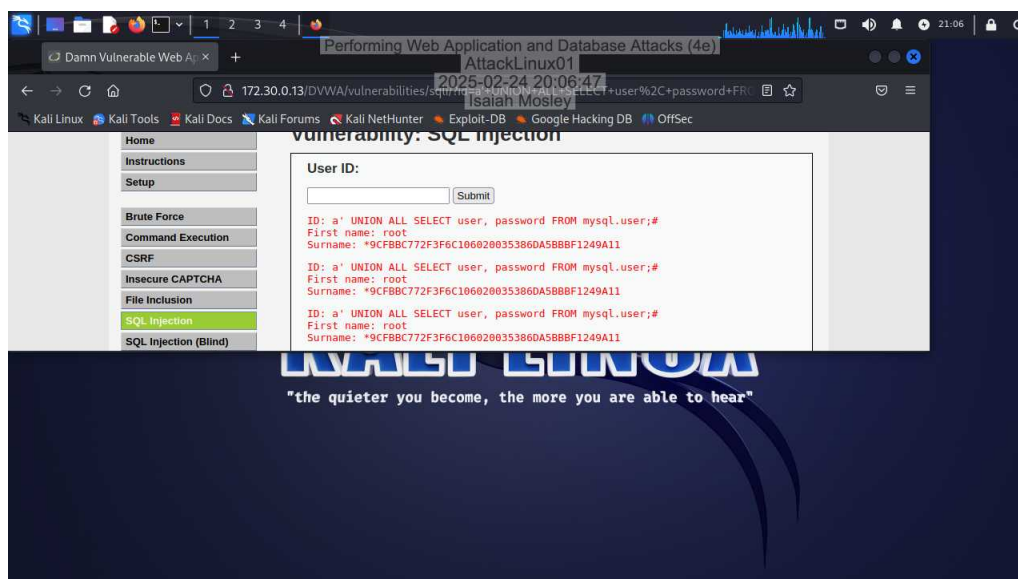
16. **Make a screen capture** showing the error page for the firstname field.



20. Make a screen capture showing the **first 3 results** of the query.



23. Make a screen capture showing the **first few results** of the query.

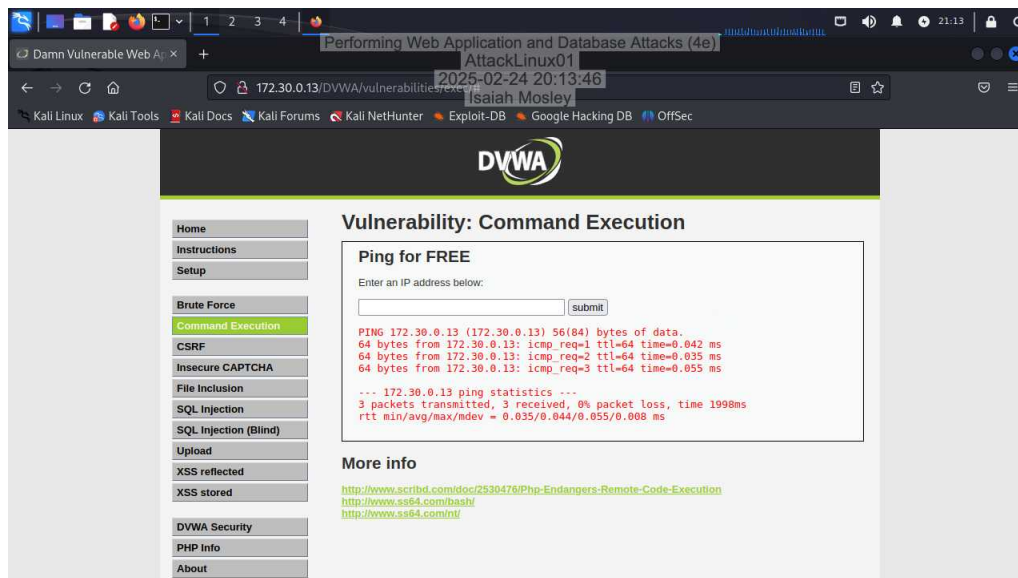


Part 3: Command Execution

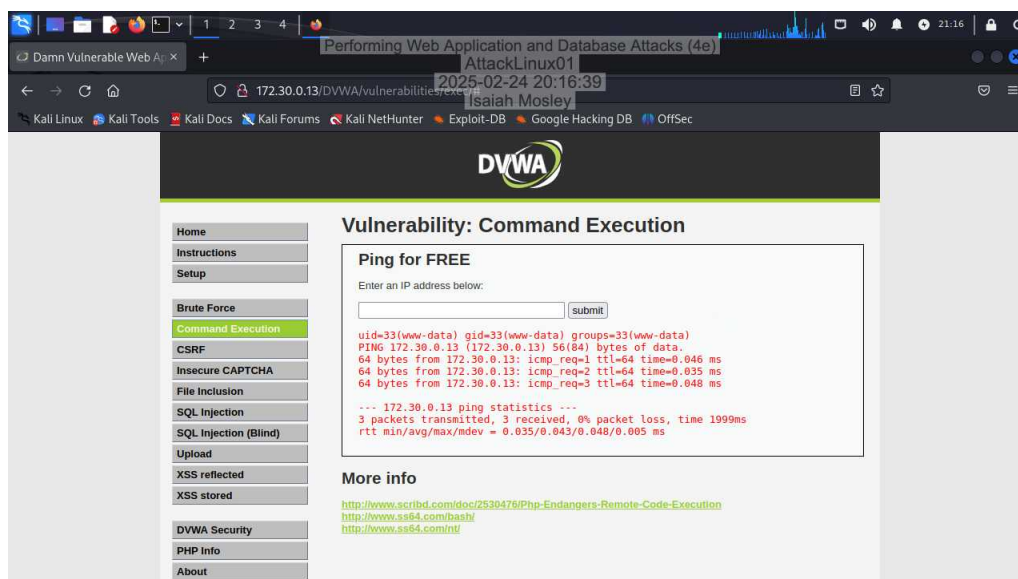
Performing Web Application and Database Attacks (4e)

Ethical Hacking, Fourth Edition - Lab 05

4. Make a screen capture showing the results of the command injection.



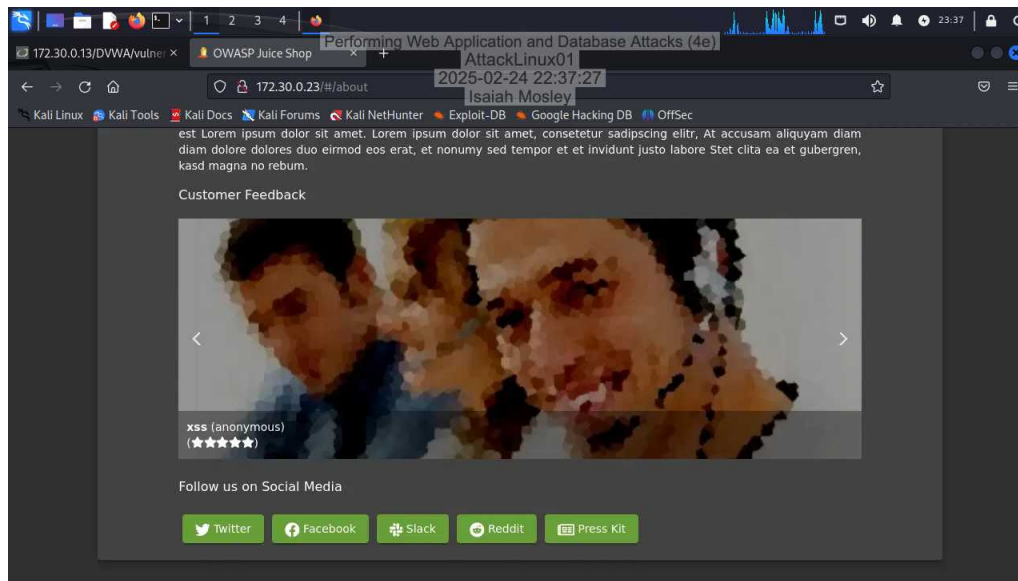
6. Make a screen capture showing the results of the command injection.



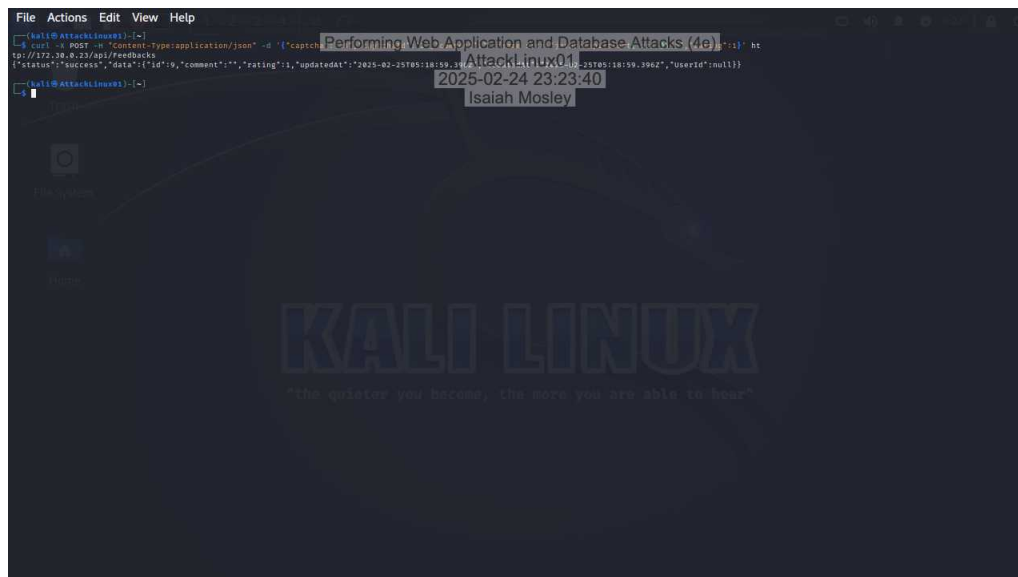
Applied Learning

Part 1: Perform a Stored XSS Attack on the Juice Shop

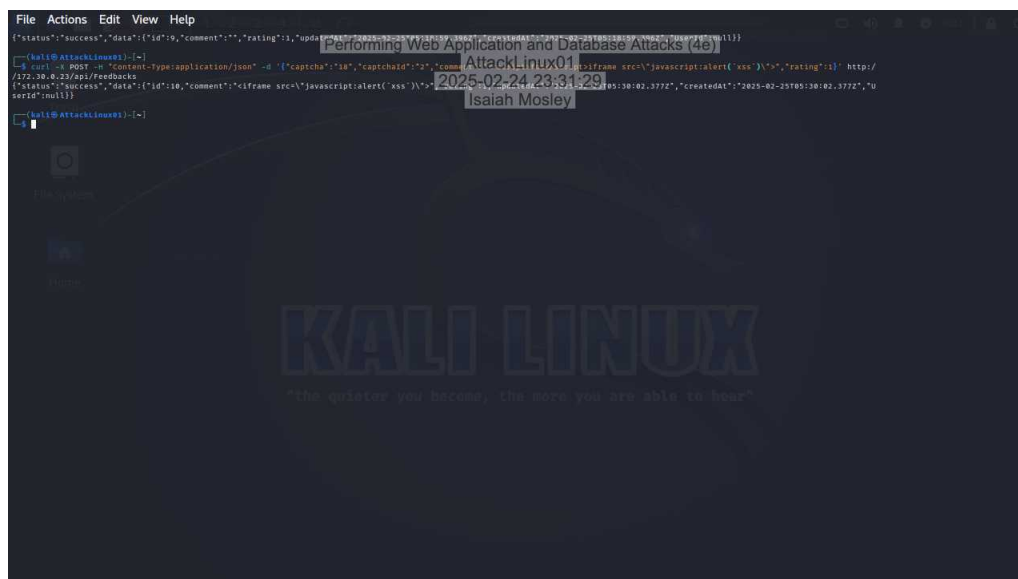
7. Make a screen capture of the page showing your comment.



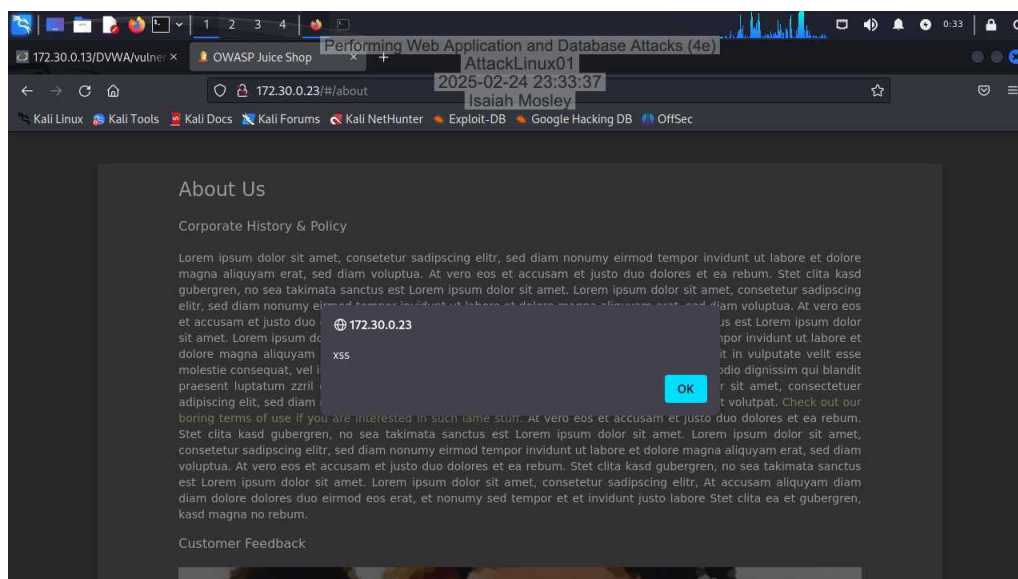
12. Make a screen capture showing the successful addition of Feedback but with an empty result.



14. Make a screen capture showing the successful addition of the feedback.

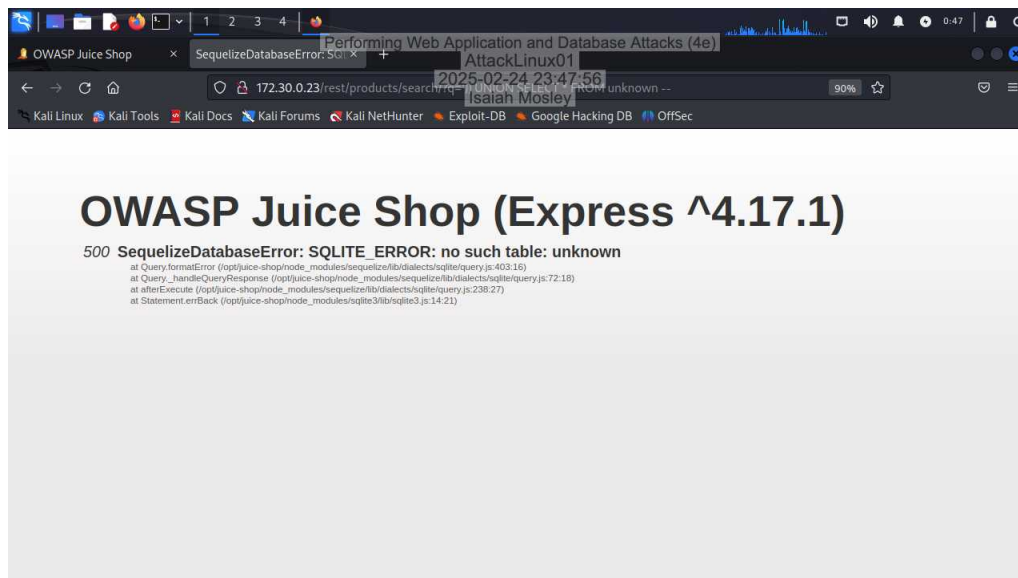


17. Make a screen capture showing the XSS alert.

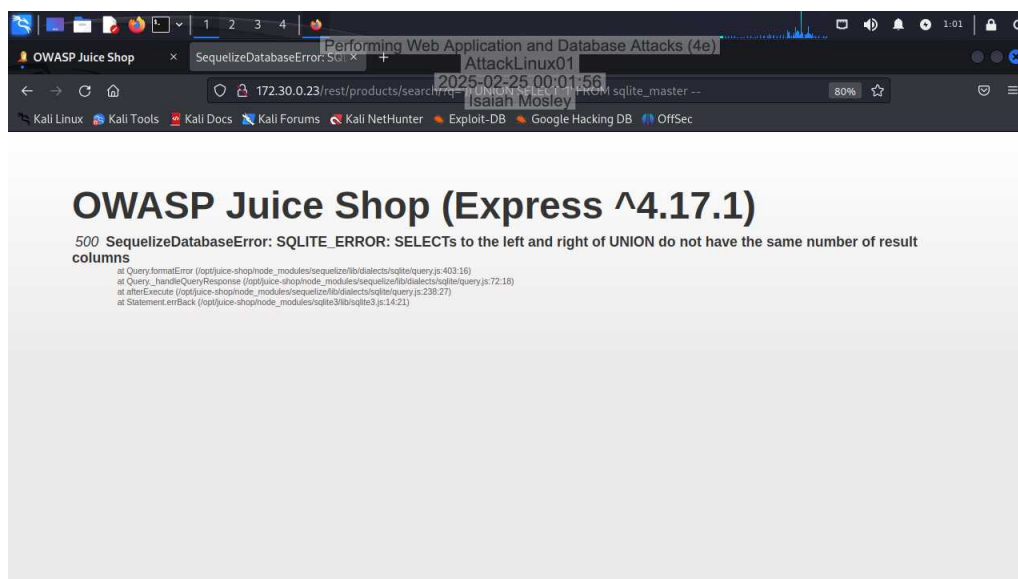


Part 2: Perform an SQL Injections Attack on the Juice Shop

3. **Make a screen capture** showing the unknown table error.



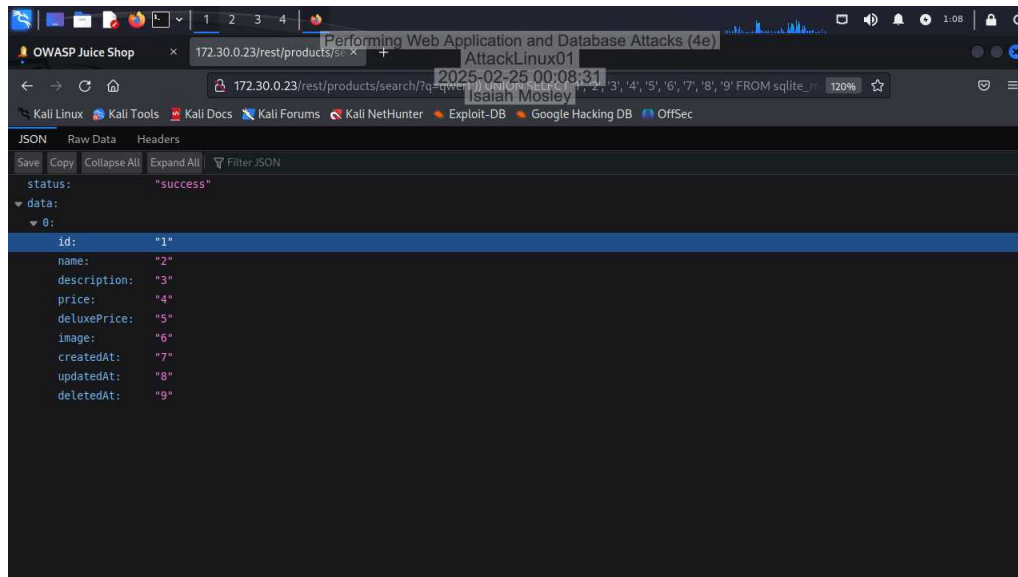
6. **Make a screen capture** showing the wrong column count error.



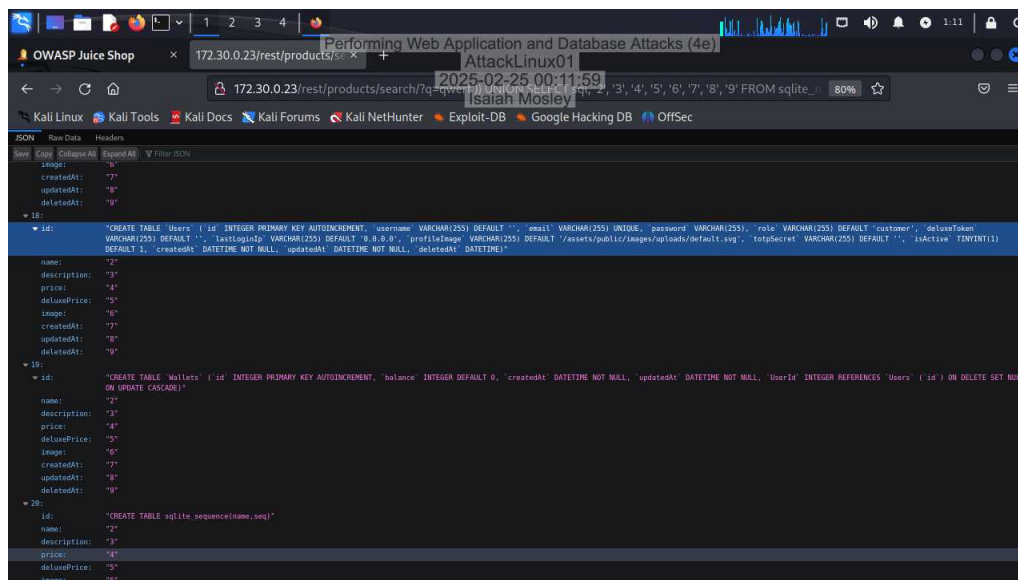
Performing Web Application and Database Attacks (4e)

Ethical Hacking, Fourth Edition - Lab 05

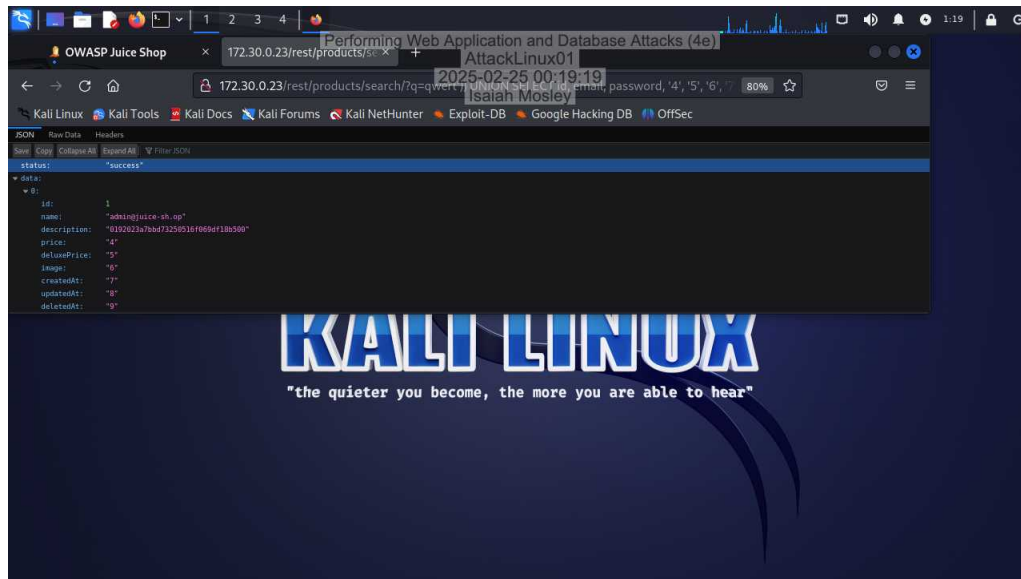
9. Make a screen capture showing the query result with the values 1 through 9.



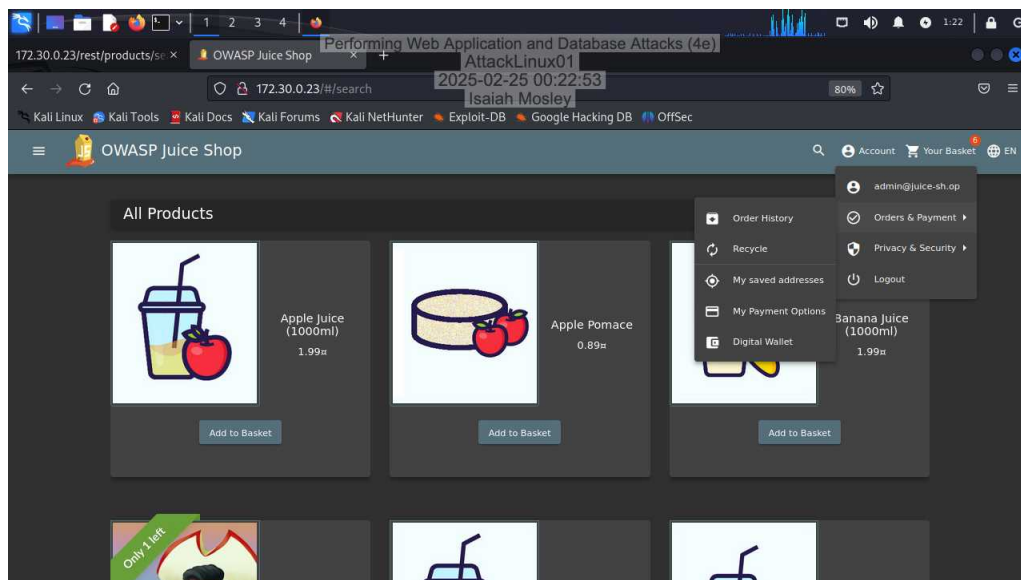
12. Make a screen capture showing the schema for the Users table.



14. Make a screen capture showing the information for the first user.



19. Make a screen capture showing the login name.



Challenge and Analysis

Part 1: Perform a Reflected XSS Attack Manually

Document the attack string that can be used to execute the alert function from the /search endpoint in Mousepad on the virtual machine and take a screenshot.

Incomplete