

Performing Web Application and Database Attacks (4e)

Ethical Hacking, Fourth Edition - Lab 05

Student:

Leandro Junior

Email:

juninhoromagnoli11@gmail.com

Time on Task:

2 hours, 23 minutes

Progress:

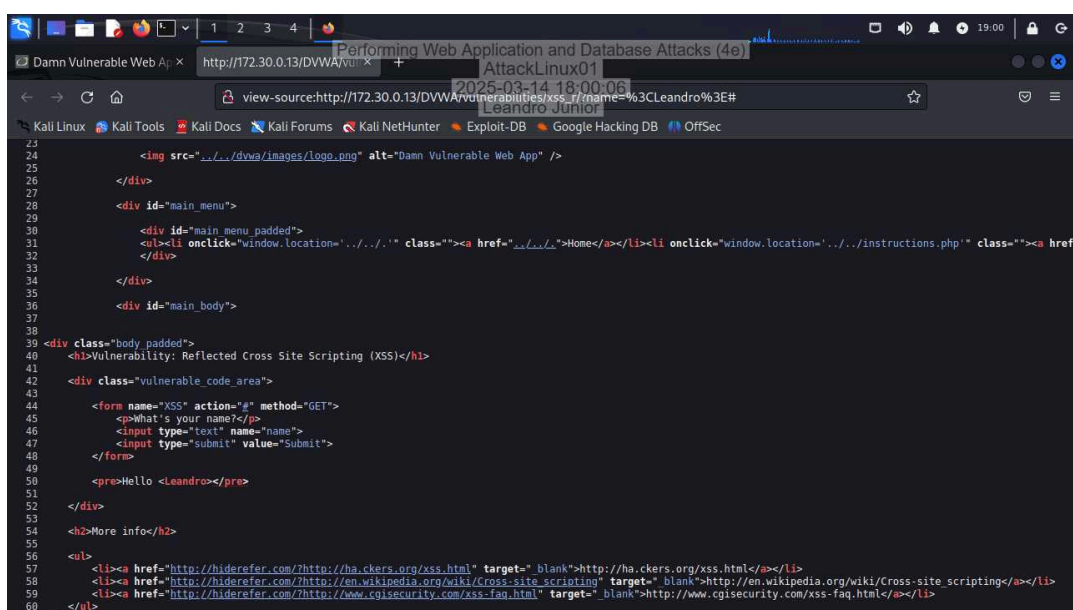
100%

Report Generated: Saturday, March 15, 2025 at 5:32 PM

Hands-On Demonstration

Part 1: Demonstrate XSS Attacks Using DVWA

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

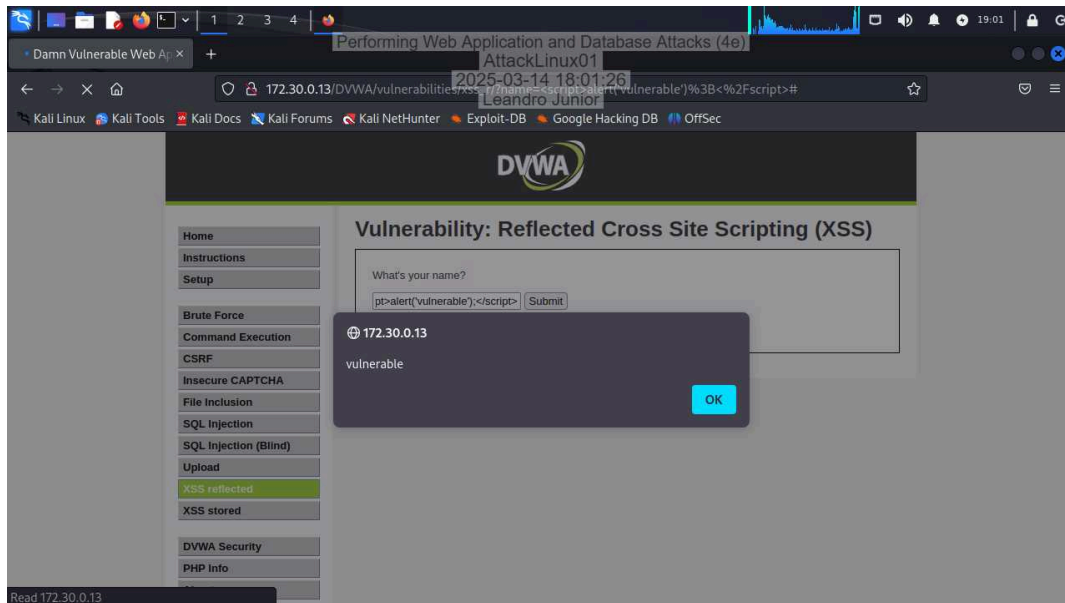


```
23
24 
25
26 </div>
27
28 <div id="main_menu">
29
30 <div id="main_menu_padded">
31 <ul><li onclick="window.location='../..' class=""><a href="/">Home</a></li><li onclick="window.location='../..instructions.php'" class=""><a href=
32 </div>
33
34 </div>
35
36 <div id="main_body">
37
38
39 <div class="body_padded">
40 <h1>Vulnerability: Reflected Cross Site Scripting (XSS)</h1>
41
42 <div class="vulnerable_code_area">
43
44 <form name="XSS" action="#" method="GET">
45 <p>What's your name?</p>
46 <input type="text" name="name">
47 <input type="submit" value="Submit">
48 </form>
49
50 <pre>Hello <Leandro></pre>
51
52 </div>
53
54 <h2>More info</h2>
55
56 <ul>
57 <li><a href="http://hiderefer.com/http://ha.ckers.org/xss.html" target="_blank">http://ha.ckers.org/xss.html</a></li>
58 <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>
59 <li><a href="http://hiderefer.com/http://www.cgisecurity.com/xss-faq.html" target="_blank">http://www.cgisecurity.com/xss-faq.html</a></li>
60 </ul>
```

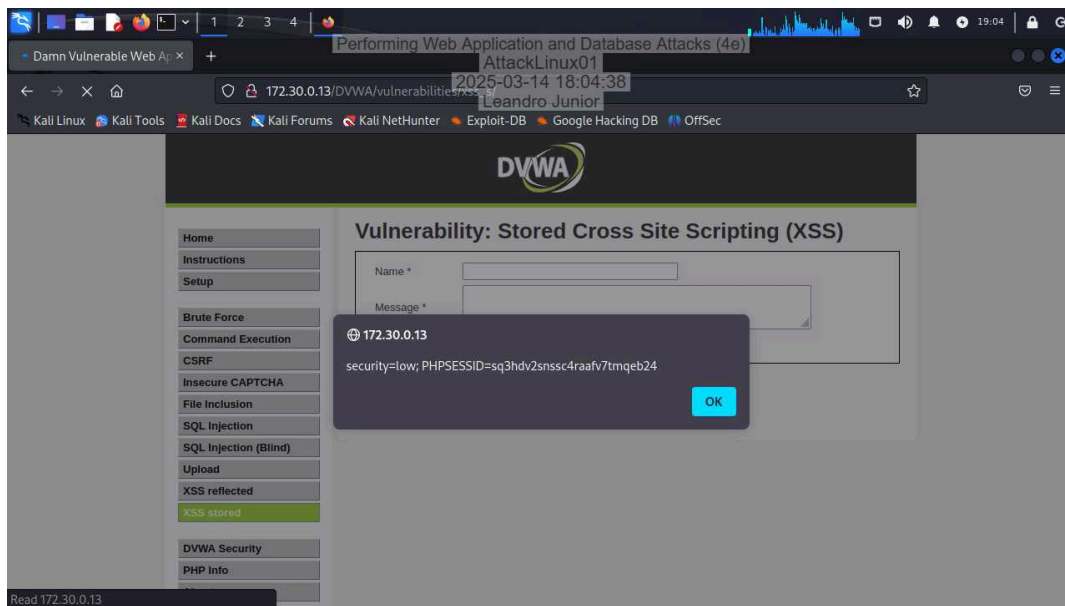
Performing Web Application and Database Attacks (4e)

Ethical Hacking, Fourth Edition - Lab 05

15. Make a screen capture showing the popup.

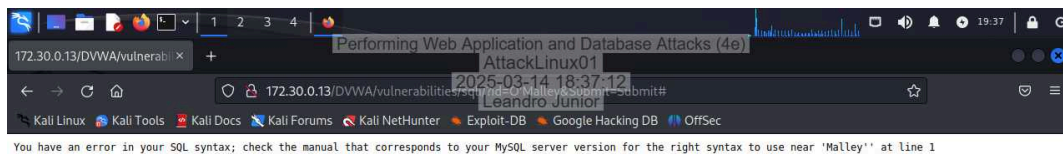


22. Make a screen capture showing the popup.

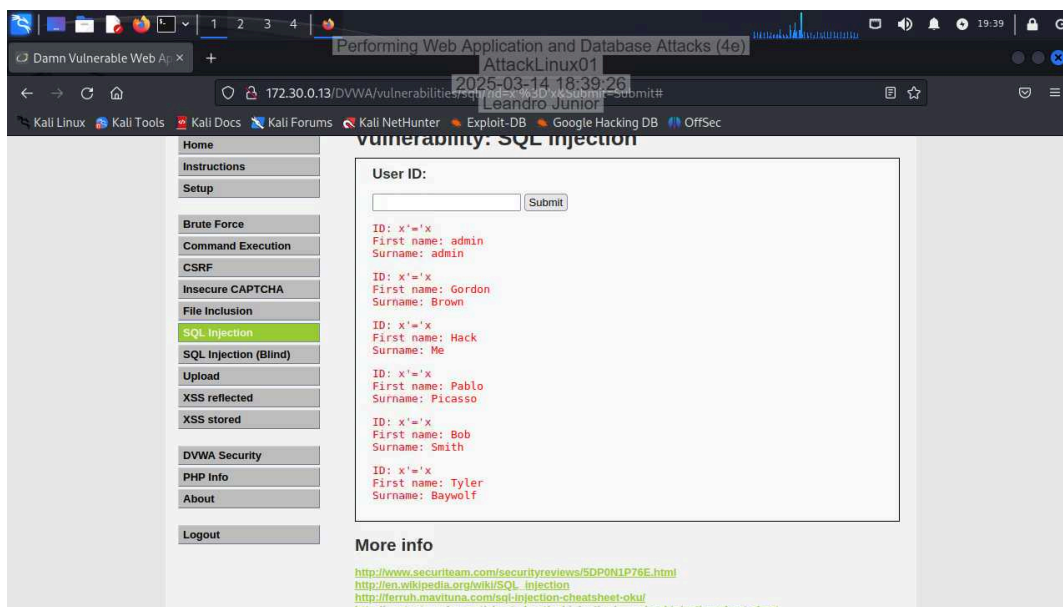


Part 2: Demonstrate SQL Injection Attacks Using DVWA

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

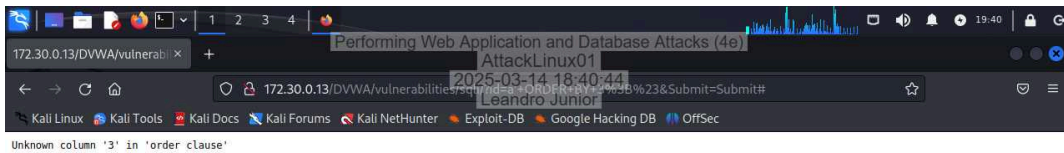


9. Make a screen capture showing the results of the query.

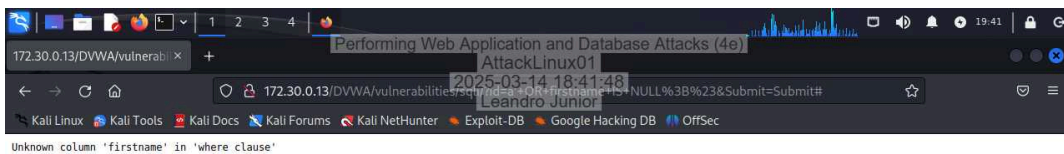


Ethical Hacking, Fourth Edition - Lab 05

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

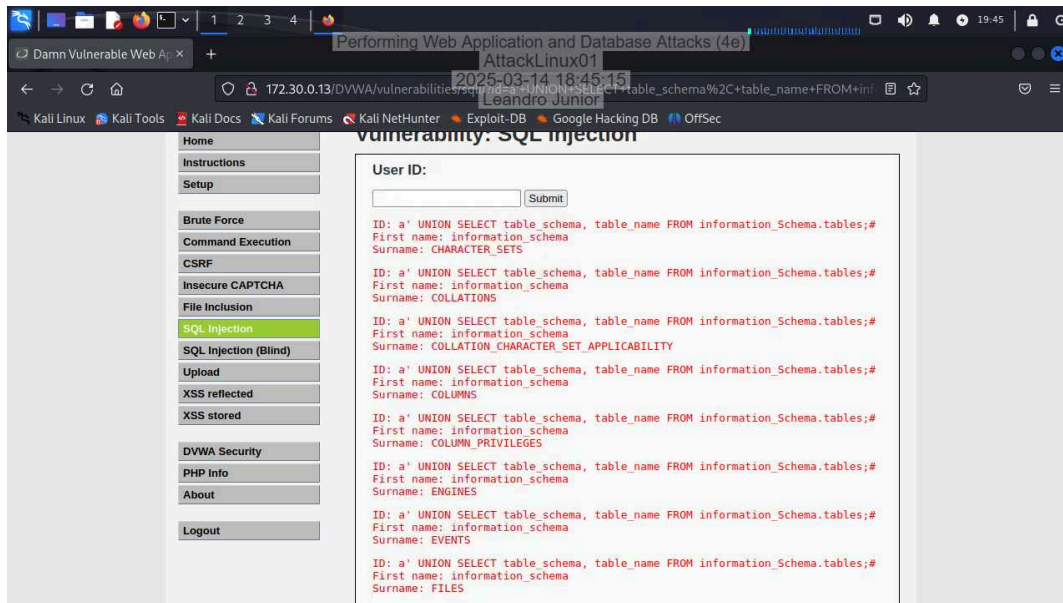


16. **Make a screen capture** showing the error page for the firstname field.

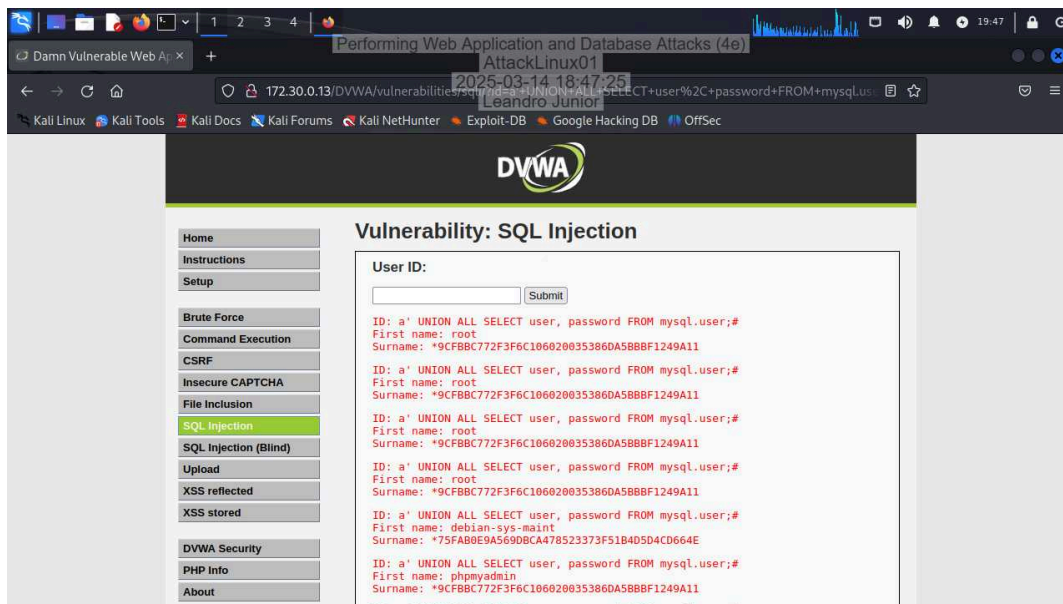


Ethical Hacking, Fourth Edition - Lab 05

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

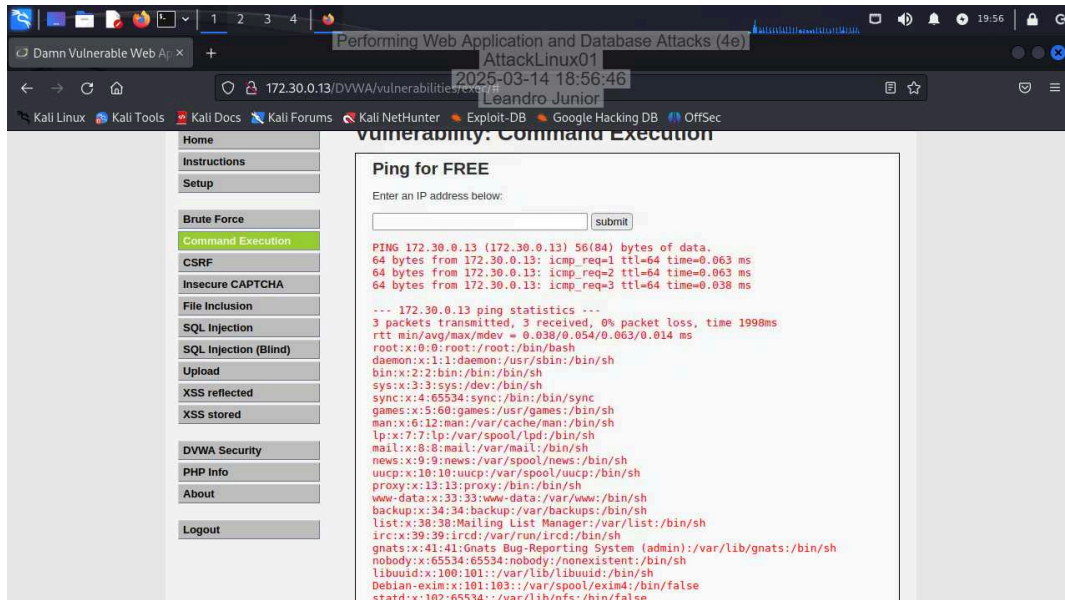


23. **Make a screen capture** showing the **first few results** of the query.

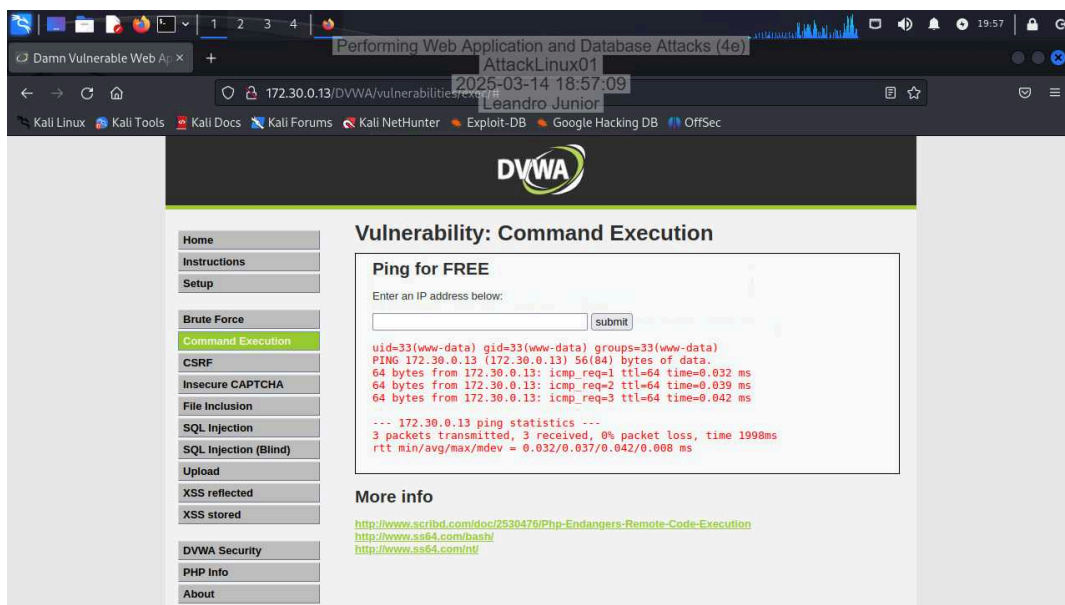


Part 3: Command Execution

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



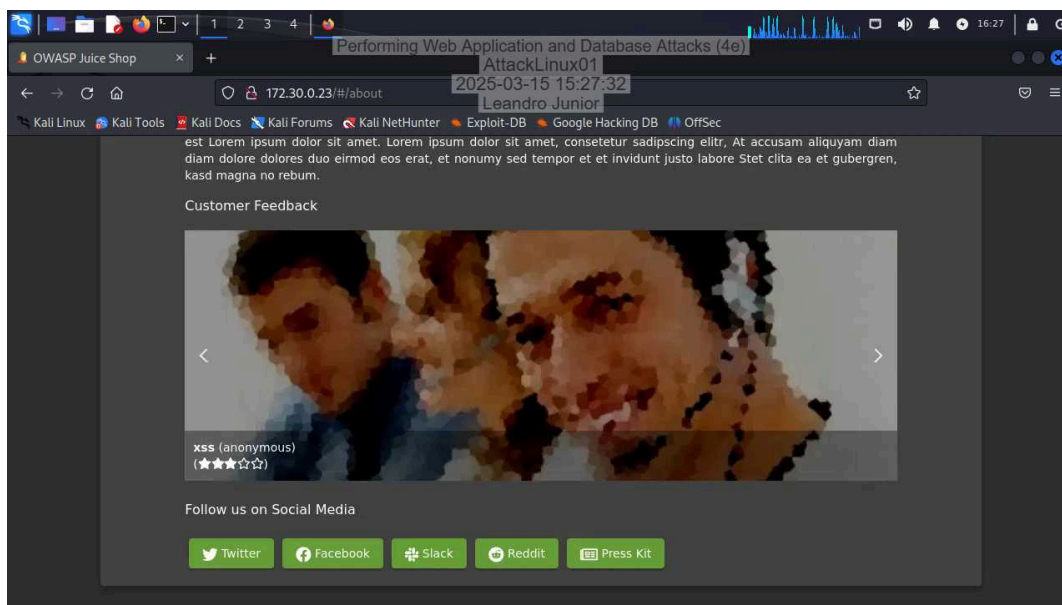
6. Make a screen capture showing the results of the command injection.



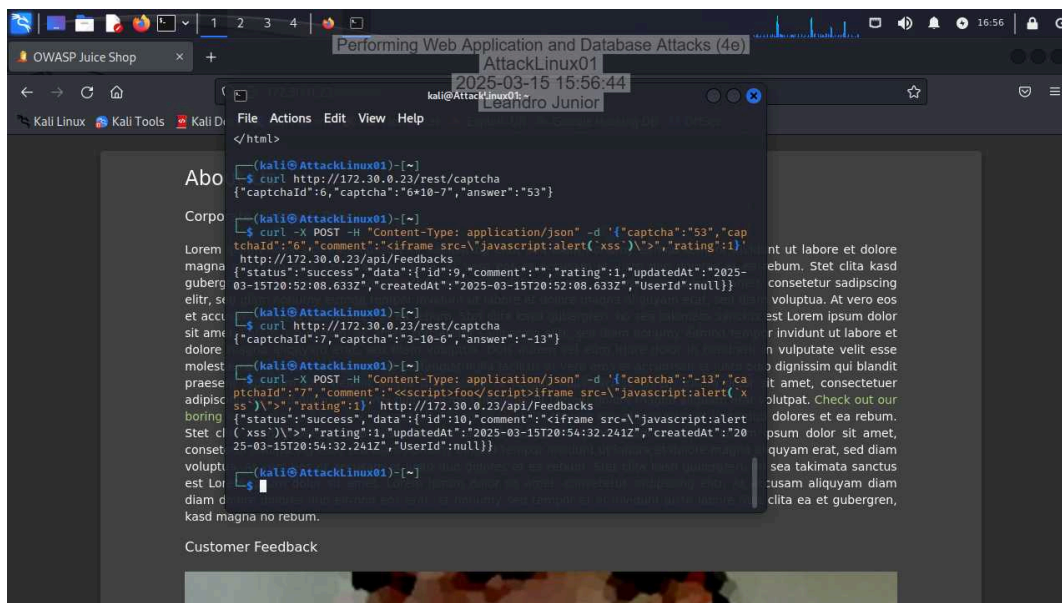
Applied Learning

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

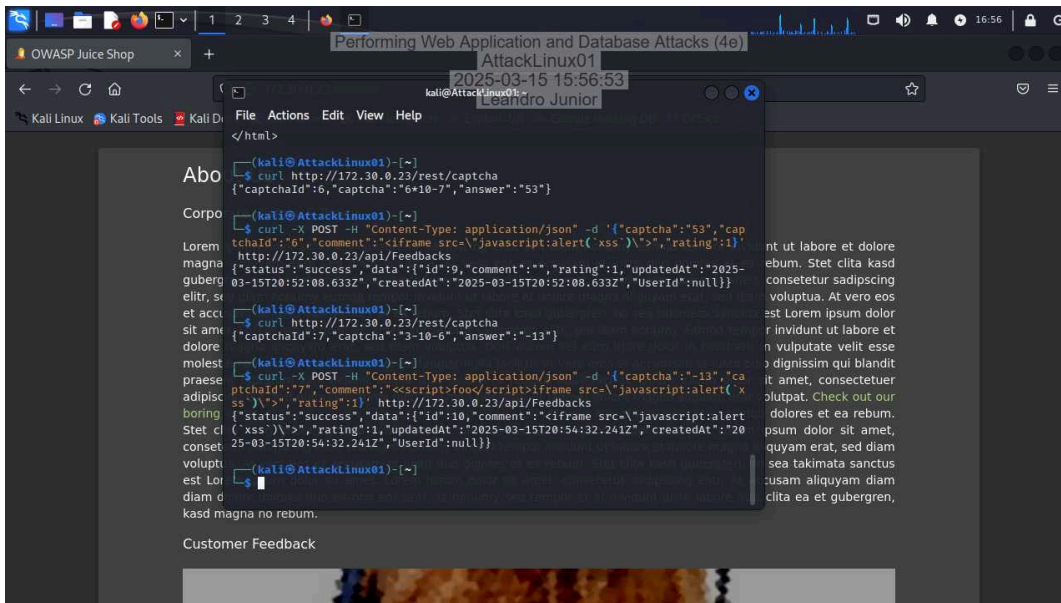
7. Make a screen capture of the page showing your comment.



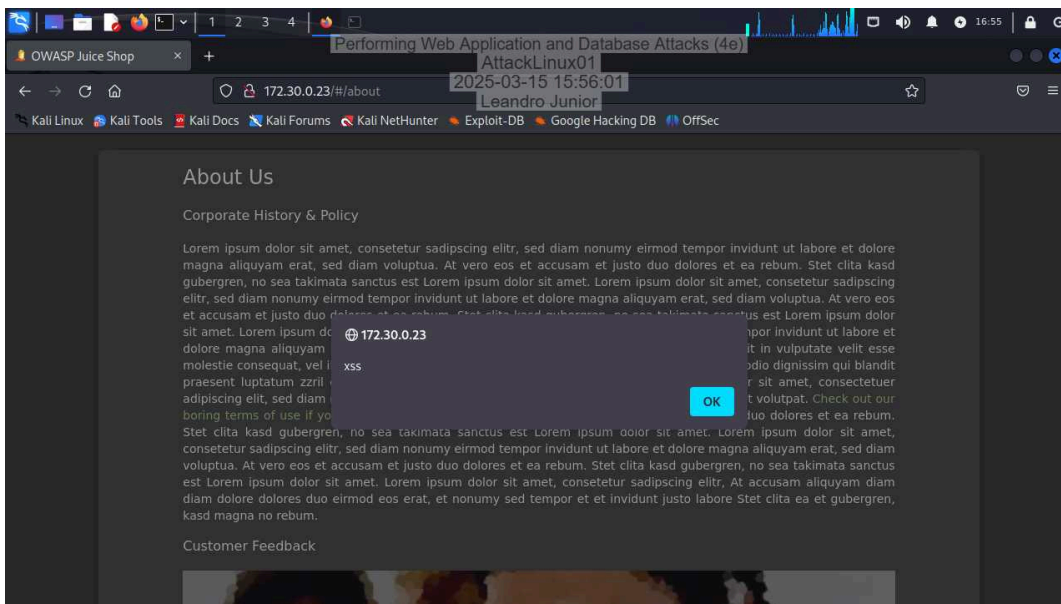
12. Make a screen capture showing the successful addition of Feedback but with an empty result.



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

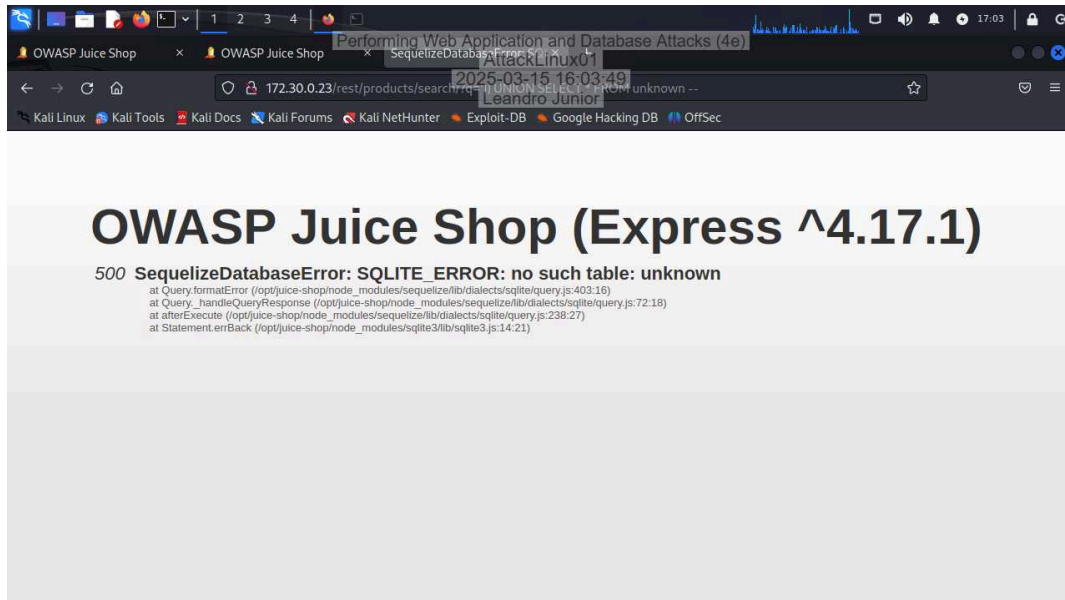


17. Make a screen capture showing the XSS alert.

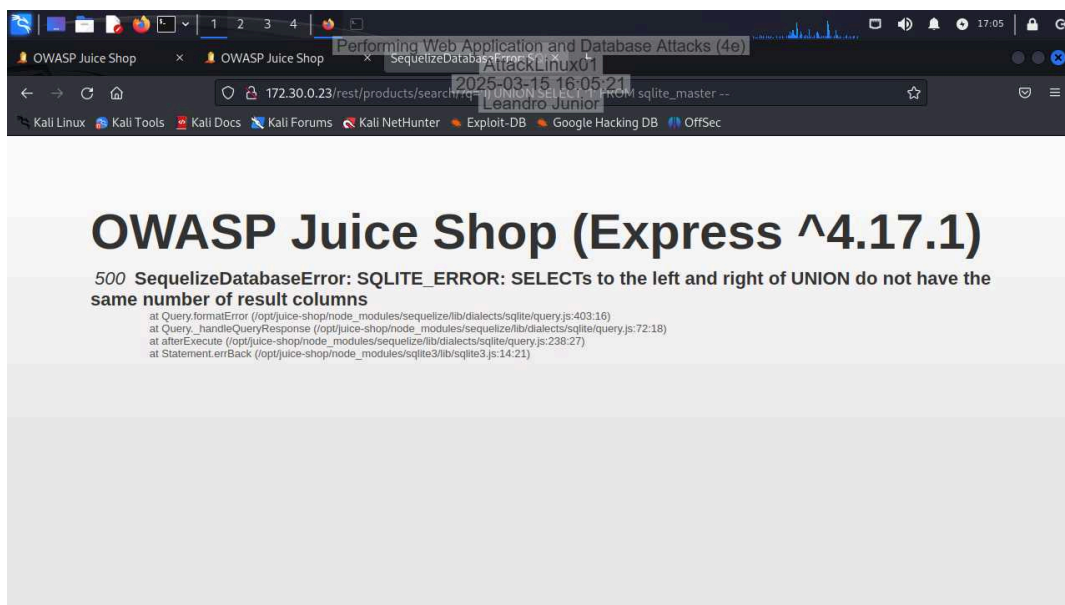


Part 2: Perform an SQL Injections Attack on the Juice Shop

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



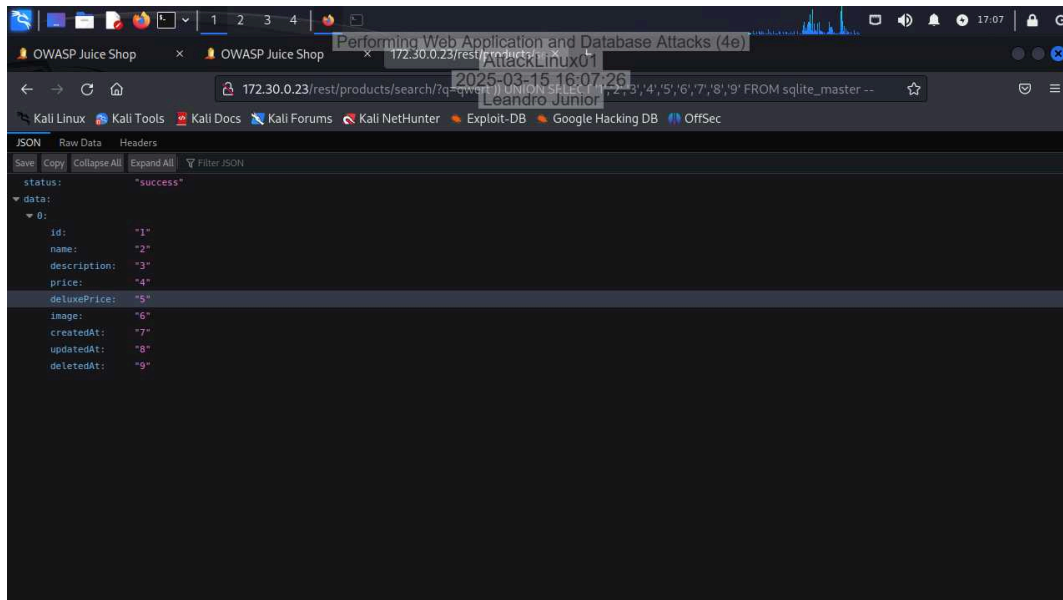
6. Make a screen capture showing the wrong column count error.



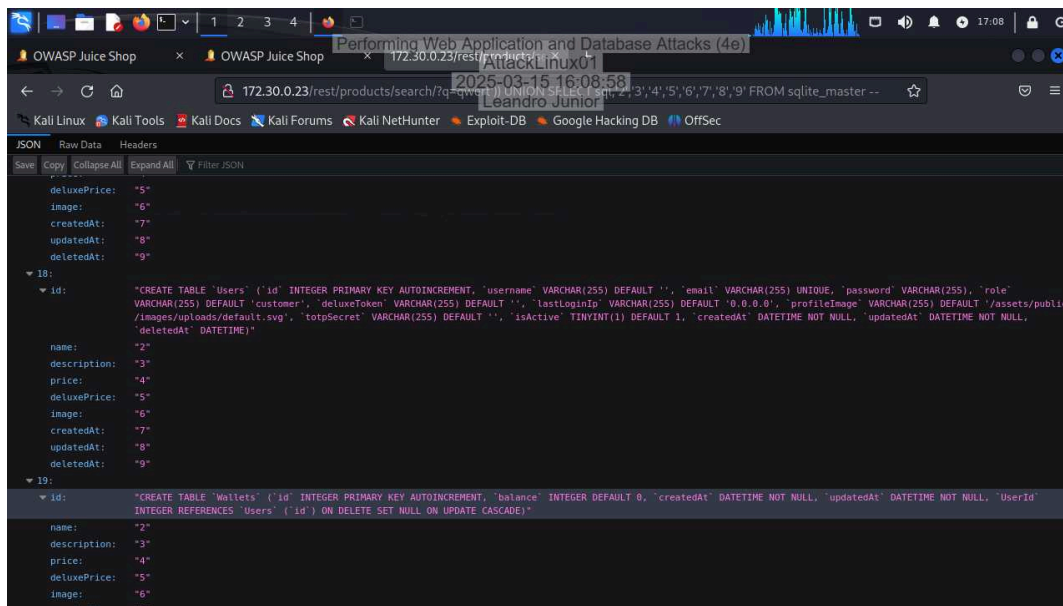
Performing Web Application and Database Attacks (4e)

Ethical Hacking, Fourth Edition - Lab 05

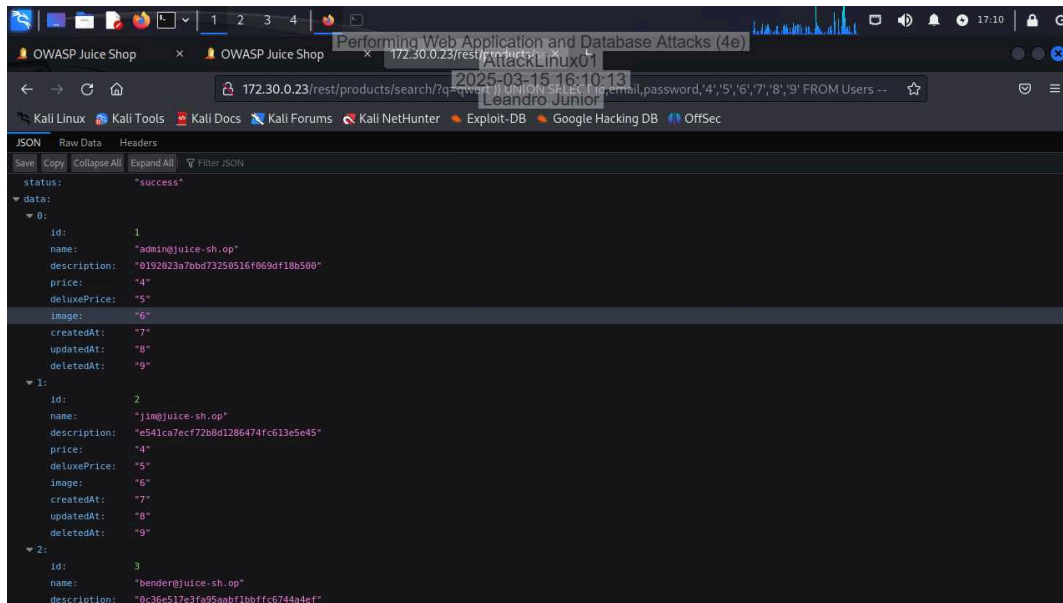
9. Make a screen capture showing the query result with the values 1 through 9.



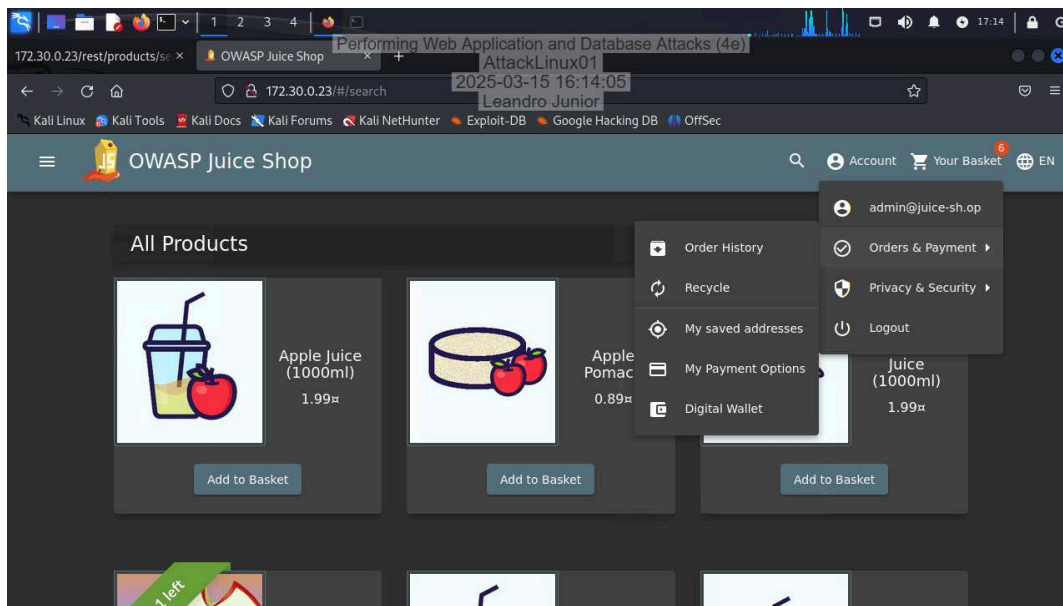
12. Make a screen capture showing the schema for the Users table.



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.

/search?q=alert('xss')