Lab: JWT authentication bypass via weak signing key

This lab uses a JWT-based mechanism for handling sessions. It uses an extremely weak secret key to both sign and verify tokens. This can be easily brute-forced using a wordlist of common secrets.

To solve the lab, first brute-force the website's secret key. Once you've obtained this, use it to sign a modified session token that gives you access to the admin panel at `/admin`, then delete the user `carlos`.

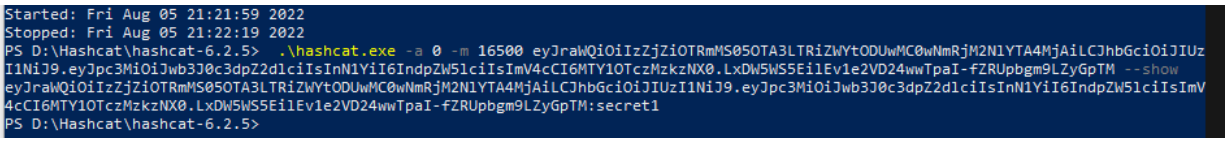
You can log in to your own account using the following credentials: `wiener:peter`

Part 1 - Brute-force the secret key

1. In Burp, load the JWT Editor extension from the BApp store.
2. In the lab, log in to your own account and send the post-login `GET /my-account` request to Burp Repeater.
3. 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.

4. Copy the JWT and brute-force the secret. You can do this using hashcat as follows:

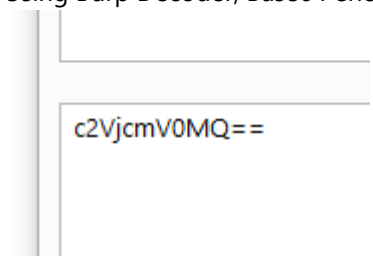
```
`hashcat -a 0 -m 16500 <YOUR-JWT> /path/to/jwt.secrets.list`
![[Pasted image 20220805212301.png]]
```



If you're using hashcat, this outputs the JWT, followed by the secret. If everything worked correctly, this should reveal that the weak secret is `secret1`.

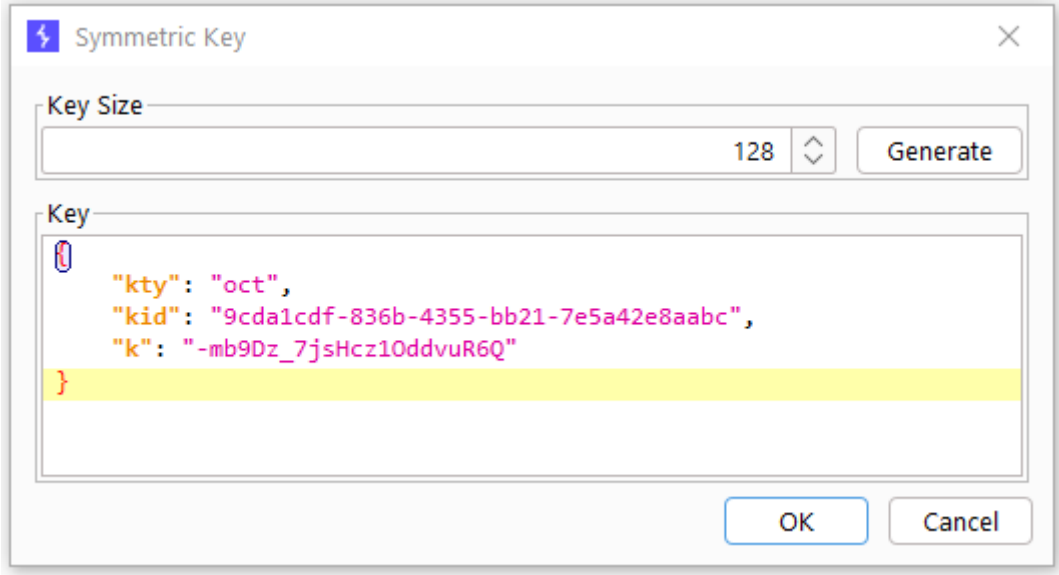
Part 2 - Generate a forged signing key

1. Using Burp Decoder, Base64 encode the secret that you brute-forced in the previous section.



c2VjcmV0MQ==

2. In Burp, go to the **JWT Editor Keys** tab and click **New Symmetric Key**. In the dialog, click **Generate** to generate a new key in JWK format. Note that you don't need to select a key size as this will automatically be updated later.



3. Replace the generated value for the `k` property with the Base64-encoded secret.

Keys

ID	
23378c37-d9c9-4e7b-9c49-06abb950be4d	OCT 56

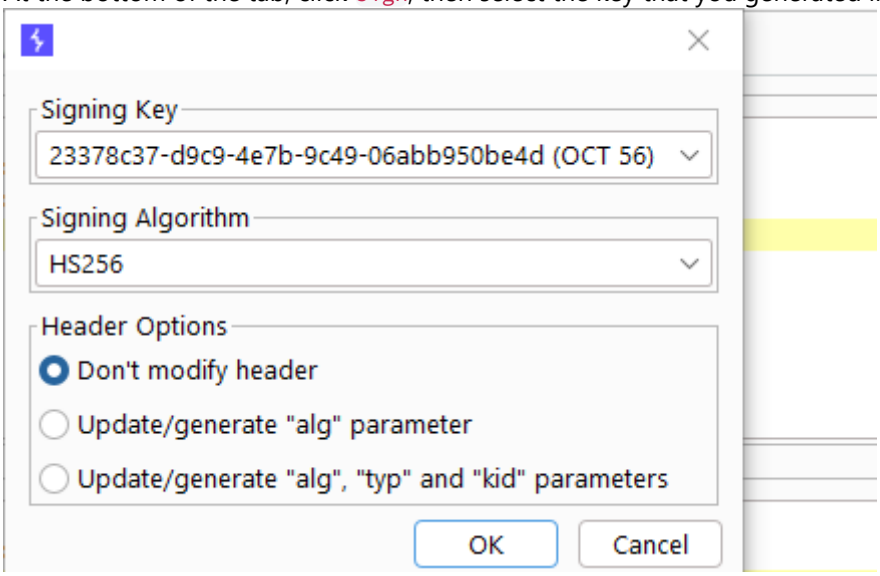
4. Click **OK** to save the key.

Part 3 - Modify and sign the JWT

1. Go back to the `GET /admin` request in Burp Repeater and switch to the extension-generated **JSON Web Token** message editor tab.
2. In the payload, change the value of the `sub` claim to `administrator`

```
{
    "iss": "portswigger",
    "sub": "administrator",
    "exp": 1659733935
}
```

3. At the bottom of the tab, click `Sign`, then select the key that you generated in the previous section.



4. Make sure that the `Don't modify header` option is selected, then click `OK`. The modified token is now signed with the correct signature.
5. Send the request and observe that you have successfully accessed the admin panel.

Response

Pretty Raw Hex Render

Web Security Academy

JWT authentication bypass via key

Back to lab description »

Users

carlos - Delete
wiener - Delete

6. 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>
  </div>
  <div>
    <span>
```

Request

Pretty Raw Hex JSON Web Token

```
1 GET /admin/delete?username=carlos HTTP/1.1
2 Host: 0a4300dd03ceec0fc093950800980022.web-sec
3 Cookie: session=
  eyJraWQiOiJhZTI2ZDUwOS0zNWI1LTQ4NTctYThkNiO2Nj
  1YiI6ImFkbWluaXNOcmFOb3IiLCJleHAiOjE2NTk3MzUyM
```

Congratulations, you solved the lab!