**Jasons Baking Services**

***Web***

**Challenge:**

Hey intern! We were able to swipe Jasons application from Github, see if you can find anything useful in the code that will allow you to exploit the real application.

(Be ready to be flash-banged, the web-app is all white!)

<https://spooky-jason-bakeshop-web.chals.io/>

Attached - jasons-bakeshop-src.zip

**Approach:**

Inspecting the file contents and the website, we see there’s a route to /flag but it prints the flag only if the user is an admin else it redirects to the dashboard.

We see that the program is using JWT to verify the data, but wait, the process.env file is given? and it contains the secret key LOL??

This is what made the challenge easy.

We first register a fake user and try to open the /flag but obviously, we ended up on the dashboard page.

We open the network tab in developer tools and see the request made, as expected we see a cookie token=<JWTtoken>

We use the online tool <https://jwt.io/> to check the JWT token and enter the secret key given in the process.env file. We see that the admin parameter is set to false. We change it to true and copy the new generated jwt encoded data.

Now this is new token we’re going to use to get ourselves admin privileges and finally accessing the flag page. You can confirm this by using cyberchef as well, by using JWT verify to see if the new encoded data you created will really give you the permission or not.

We create a new request and set the Cookie: token=<our crafted token> and send a request to the /flag page, finally getting our flag as response :)))

**Flag: NICC{jWoT\_tOkeNs\_nEed\_saf3\_secr3ts}**

Congrats!!

Happy Hacking!