PicoCTF: JAuth

Sam Newman

April 2025

1 Website in Question

The website is a simple login website, with that as it's only functionality. It allows a user to login with a username and password, and uses a JWT to verify their login information

2 Business Impact

This vulnerability potentially enables an attacker to gain administrator account access in the website, achieving anything that an administrator could do. This can include but is not limited to ordering items, stealing password and user info, and accessing the company database.

3 How It Works

The website uses JWT (JSON Web Token) to enable user login. I have used this as a login method when building websites, and it can be quite insecure if used improperly. Specifically, this website is vulnerable to an Auth:None attack, in which the token is encoded with its Auth header set to None, effectively removing the need for the signature at the section of the cookie following the trailing space. When this cookie is then checked using jwt-decode, the decoder sees that no auth signature is required and verifies it. Using this, we can modify the cookie to set the user: payload to 'admin', making our user now a site admin on login.

4 Why It Works + Mitigation

The website does not properly evaluate the given JWT, and assumes it has not been tampered with as it has in this case. To fix it, the site should check the cookie manually and require that the algorithm section of the header is always set to their encryption algorithm of choice, in this case HS256. This would guarantee signatures are always verifies using a serverside secret key and tokens have been generated by the server and only the server.

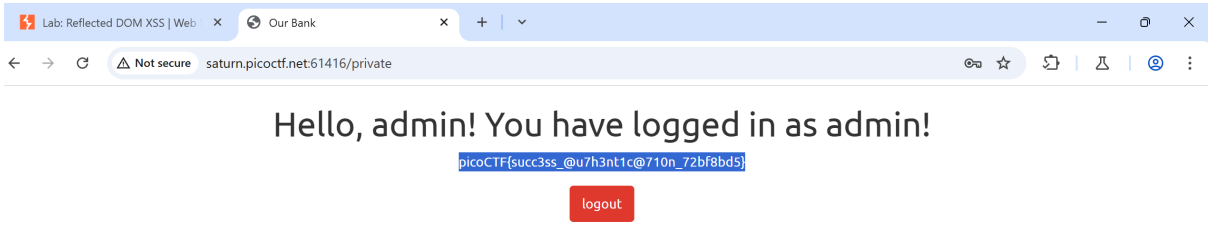

Figure 1: Solved Lab