**WEB**

**EASY WEB CHALLENGE -** First, open the Burpsuite tool and navigate to the "Target" tab. Then, open your browser and enter the provided link. Once the link is loaded, return to Burpsuite and locate the file named "script.js" under the target tab. Within this file, you'll find both the username and password needed to access the flag!.

**MINI VULNERBLE COMPILER** - To get the flag, first write the code provided below into your compiler:

import os

print(os.system('cat flag.txt'))

Next, compile and run the code. The contents of flag.txt, which include the flag, will be displayed as output!.

**IDOOR** - To find the flag using SHA256 encryption, follow these steps: First, open the given link and copy the hashed value you see there. Then, paste this value into CrackStation to identify its type. Next, use the command echo -n 0 | sha256sum to create a hash for the root user value "0". Finally, use this information to get the flag!.

**XSS VULNERABILITY** - “<img src=x onerror=alert('test')>” Type this in text box and het the flag!.