Muhammed Raihan P A

17 July 2021

Reported to picoctf.org

Cookies are vulnerable

SUMMARY :-

‘**logon**’ challenge in picoCTF challenges was vulnerable to SQLinjection attacks. I could bypass the login page by using some SQLi payloads and by commenting the password field out.

STEPS :-

- Every credential we give successfully logs us in but doesn't give us the flag. I assumed that a cookie might be used to store a separate variable that might be preventing us from seeing the flag. I notice an admin cookie set to False. Changing this to True and refreshing the page gives us the flag:

  picoCTF{th3_c0nsp1r4cy_l1v3s_6edb3f5f}

IMPACT :

Vulnerable to cookie stealing and session hijacking. If the connection is not secure, a hacker can easily intercept and steal these cookies.

MITIGATION :

- Install an SSL certificate, SSL (Secure Sockets Layer) will encrypt the data before it’s transferred. So even if a hacker manages to steal it, they can’t read the data.

- Install a security plugin like wordpress security plugin, such as MalCare active on your website. The plugin's firewall will prevent hack attempts on your website and block malicious IP addresses.