

Title : - SQL Injection in website login page

Description : - SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.
For more information on SQL Injection attacks visit this [link](#)

Summary : - By using the SQL Injection we can execute malicious SQL statements or queries on the website's database and interact with it to fetch the sensitive data of the users.

Steps to Reproduce : -

Step 1 - Open the link <https://jupiter.challenges.picoctf.org/problem/33850/>

Step 2 - Go to the Admin Login Page.

Step 3 - In the Username type the malicious SQL query, 'OR 1=1 -- and in password type anything and press enter.

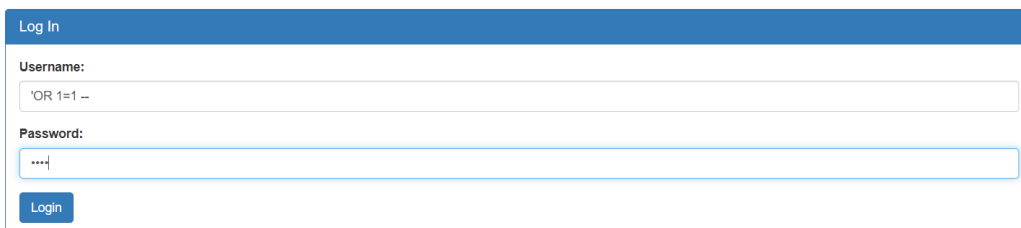
Step 4 - and now we got the flag, paste the flag in the picoCTF Submit box.

Payload : - 'OR 1=1 --

Impact : - By using this SQL query the website give us the services and control of the admin.

Mitigation :- Don't except every input from the client or the user and we can also apply the python regex methodology in the website.

Proof of concept : -



The screenshot shows a web form titled "Log In". It contains two input fields: "Username:" and "Password:". The "Username:" field has the text "'OR 1=1 --" entered. The "Password:" field has masked characters "....". Below the fields is a blue "Login" button.

Logged in!

Your flag is: picoCTF{s0m3_SQL_f8adf3fb}