Login

Category: SQL Injection, Web
Created: Nov 18, 2020 1:44 AM
Points: 175
Solved: Yes
Subjective Difficulty: 🔥🔥

WriteUp:

Author: @Tibotix

🔎 Research:

We are given an address that hosts something like a login form. We can submit a username and a password. The credentials are sent to `/auth.php` in a POST requests.

📝 Vulnerability Description:

The Login From seems to be vulnerable to a basic SQL Injection.

🧠 Exploit Development:

The credentials are checked on the server side with a SQL Statement that probably looks something like this:

```
"SELECT * FROM users_db WHERE user='" + $_POST['username'] + "' and password='"
+ $_POST['password'] + "'
```

So when feeding username=`' or '1'='1` and password=`' or '1'='1`, the SQL Statement will look like this:

```
SELECT * FROM users_db WHERE user='' or '1'='1' and password='' or '1'='1'
```

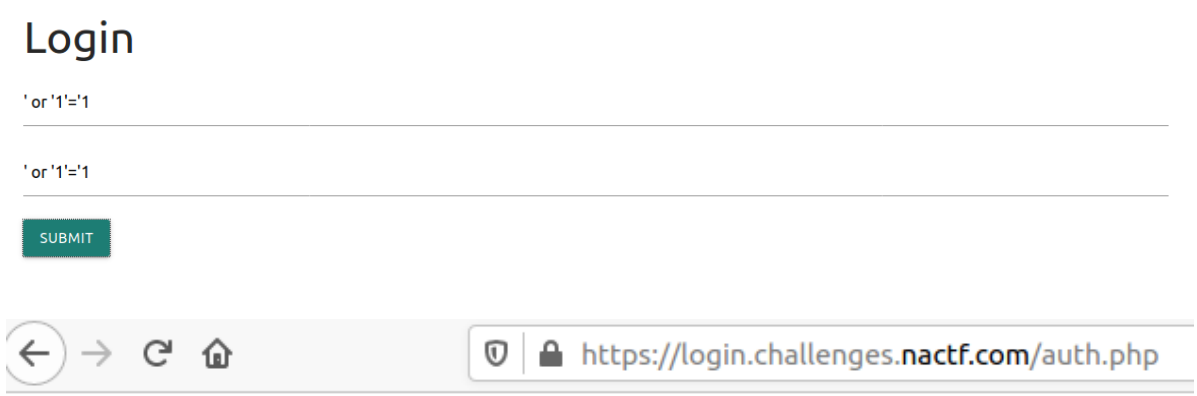
This is a valid SQL Statement and will always return true.

🔐 Exploit Programm:

```

```

💥 Run Exploit:



FLAG: nactf{sQllllllll_1m5qpr8x}

Summary / Difficulties:

This was a basic SQL Injection.

Further References:

- SQL Injection

Used Tools:

-

Notes:

-