**Practical: 10**



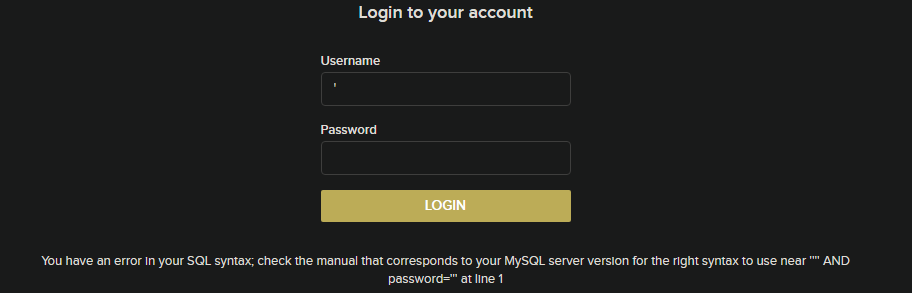
**Implementation Of SQL Injection:**

SQL injection is a technique used to exploit user data through web page inputs by injecting SQL commands as statements. Basically, these statements can be used to manipulate the application’s web server by malicious users.

* SQL injection is a code injection technique that might destroy your database.
* SQL injection is one of the most common web hacking techniques.
* SQL injection is the placement of malicious code in SQL statements, via web page input.

**Checking the form for SQL Injection:**

The Simplest way is to put “ ” (without quotes) at the username or password field. If the server returns any kind of SQL error in the Response then the website is most probably vulnerable to SQL Injection attack.



**Bypassing Authentication:**

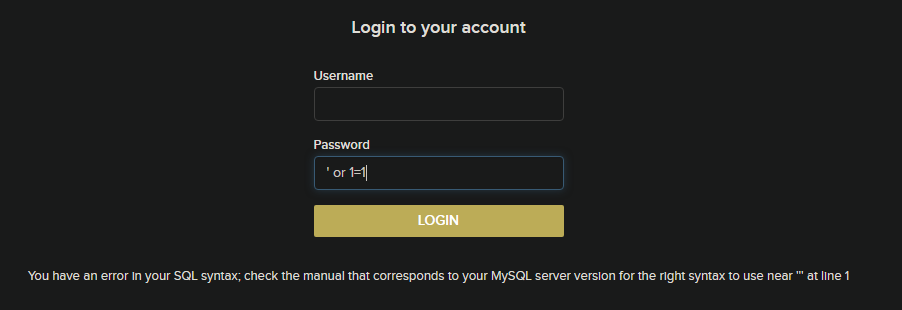
**1.**After we confirm that the site is vulnerable to SQL injection, the next step is to type the appropriate payload(input) in the password field to gain access to the account.

**2.**Enter the below-mentioned command in the vulnerable field and this will result in a successful Authentication Bypass.

Select id from users where username=’username’ and password=’password’ or 1=1--+

**In the above command:**

* Since 1=1 is always true, and we combined 1=1 with an OR operator, now we don’t have to know username or password as whatever be the username, password, our 1=1 will always be true thus giving us access to our account.
* ‘ or 1=1–+(in the password field) ‘ before OR operator is used to terminating the single quotes of password(ie- Select id from users where username=’username’ and password=’password’)
* So that after we insert ‘ before OR operator, our SQL command becomes: Select id from users where username=’username’ and password=’’ or 1=1–+
* –+ is used to ignore the rest of the command. Its main use is to ignore the ‘ after the password and if we won’t use that ,we will get the following error.

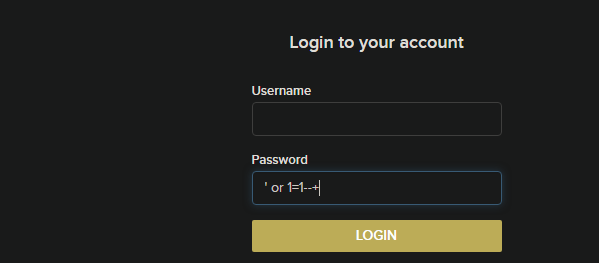


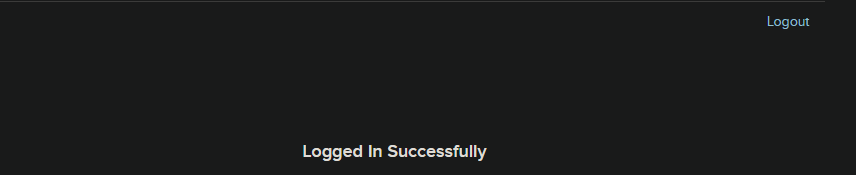
**Why that ‘ at end of 1?**

It’s the passwords closing single quote. Remember we already gave a closing single quote of our password. But the websites SQL command just puts ‘ at the end of our password. (ie- whatever we write in the password field, it gets stored inside the ‘’ of password Suppose, our password is hello The SQL command corresponding to this will be: Select id from users where username=’username’ and password=’hello’. Here, we didn’t add the quotes, but the SQL command added quotes in our input field). Since the SQL command puts ‘ at end of our 1=1, our mission fails. So, in order to ignore that closing single quote of password, we use –+.

**Executing the Injection:**

Just insert the command in the password or vulnerable field and then click login then the authentication would be bypassed.





As we can see, we finally cracked the login portal and logged in successfully.

**Conclusion**

* In this practical, I have learnt 12 different techniques to crack password

And we have seen Phishing + Social Engineering attack implementation with theory.