20 mins

Online on SQL Injection - A1

Marks:10

You will have to exploit SQL injection vulnerabilities in a web application to retrieve a hidden flag. The application consists of two pages: the public login page and the admin product search page, each with a form susceptible to SQL injection. Your goal is to first log in as an admin and then extract a hidden flag from the product search page.

Website URL: http://98.70.26.135:8080

1. **Login Page**:
   - Contains a login form with *username* and *password* fields.
   - On successful login (legitimate or via SQL injection), you will be redirected to the product search page.
   - **Challenge**: Use SQL injection to bypass authentication and log in as an admin.
2. **Product Search Page**:
   - Contains a search form with a single *query* field to search for products by name.
   - **Challenge**: Use SQL injection to retrieve the secret key from a hidden table. To make the task easier, you can assume there is a table named hidden_data, which has a column named secret_key. You will get the secret key from this table.

Submission: Copy the payloads you designed for both pages in a text file, and rename the text file as your student ID. Submit the text file to the Moodle submission link.

Example submission format:
Payload 1: <your input>
Payload 2: <your input>

Constraints:

1. **Don't use any tools, i.e, sqlmap**