**Id: 1**

**Title:** Search page: unhandled SQL error when entering single quote

**Steps to reproduce:**

1. Open the home page http://localhost/bWAPP/login.php.

2. Enter your credentials (bee/bug) and click “Login”.

3. Select “SQL Injection (GET/Search)” in the list on the page “Portal” and click “Hack”.

4. Enter single quote (‘) in the search field and click “Search”.

5. Pay attention to the message.

**Actual result:** Get message unhandled SQL error: “Error: You have an error in your SQL syntax: check the manual that corresponds to your MySQL server version for the right syntax to use near ‘%’ at line 1”.

**Expected result:** Get message: “No movies were found!”

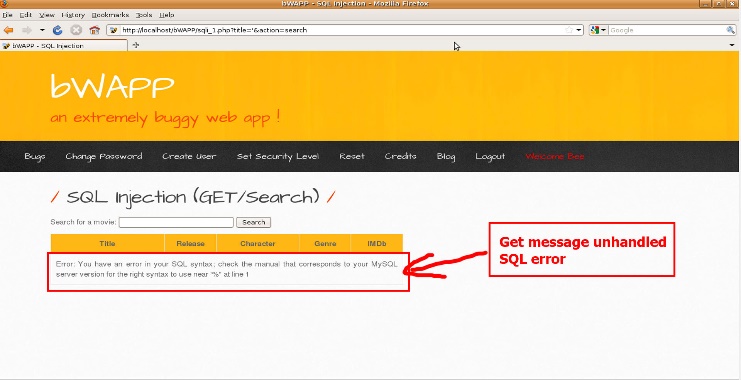
**Environment:**

1. Os: Linux Ubuntu 8.04;
2. Browser: Mozilla Firefox 3.6.17

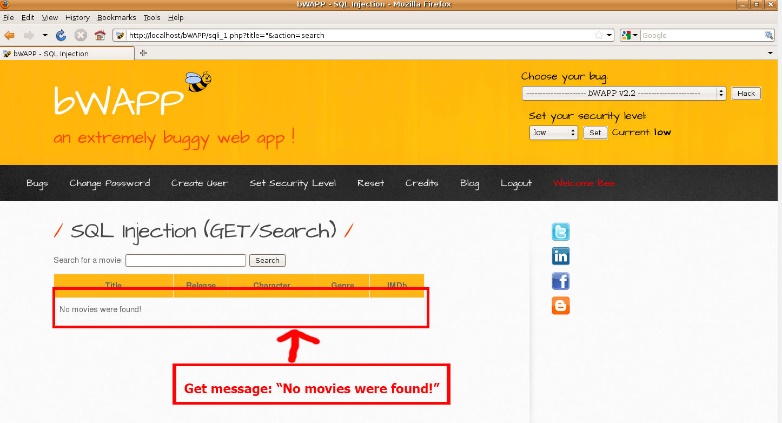
**Severity:** Major.

**Priority:** Critical.

**Attachment:**



Screenshot 1.1



Screenshot 1.2

**Id: 2**

**Title:** Cross-Site Scripting - Reflected (GET): Сompilation of the script when entering js-text in the field

**Steps to reproduce:**

1. Open the home page http://localhost/bWAPP/login.php.

2. Enter your credentials (bee/bug) and click “Login”.

3. Select “Cross-Site Scripting - Reflected (GET)” in the list on the page “Portal” and click “Hack”.

4. Enter “<script>for(;;){alert(‘bee’);}</script>” in the field “First name” and anything in the field “Last name”.

5. Click “Go” and pay attention to the popup window.

**Actual result:** The entered script is executed and a pop-up window appears.

**Expected result:** Get message: “Welcome ‘First name’ ‘Last name’”.

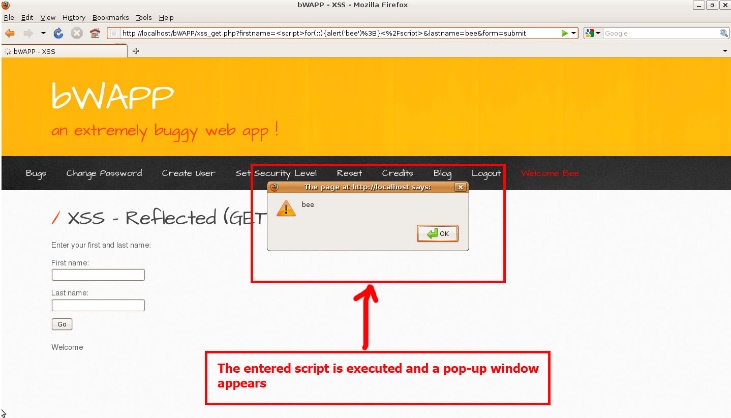
**Environment:**

1. Os: Linux Ubuntu 8.04;
2. Browser: Mozilla Firefox 3.6.17

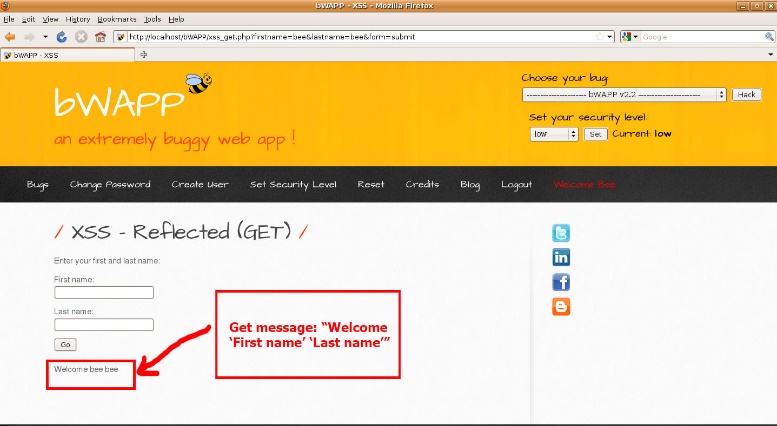
**Severity:** Major.

**Priority:** Critical.

**Attachment:**



Screenshot 2.1



Screenshot 2.2