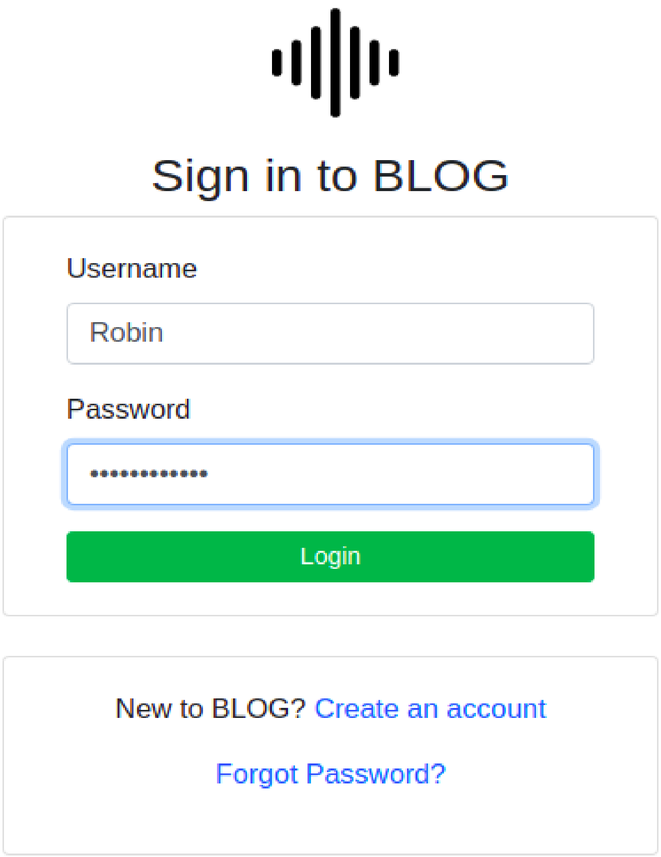
122022010 Shrayank Mistry

Demonstrating SQL Injection Attack:

Simulate an environment for the demonstration of SQL Injection attack. Make use of a simple web based application for authentication of users which is accessing databases in the background. Show that clearly with the help of message the SQL injection attack with its detection and prevention.

Simple Web Login Page with No Protection

Verified user login in to access database

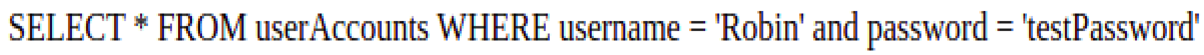


Sign in to BLOG

Username: Robin

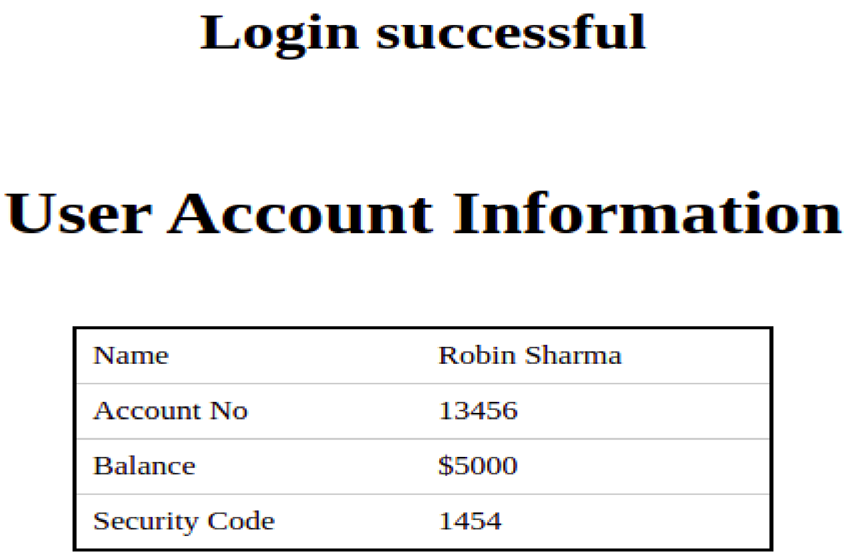
Password: •••••••••••••

Query Executed internally



```
SELECT * FROM userAccounts WHERE username = 'Robin' and password = 'testPassword'
```

Successful access to data records



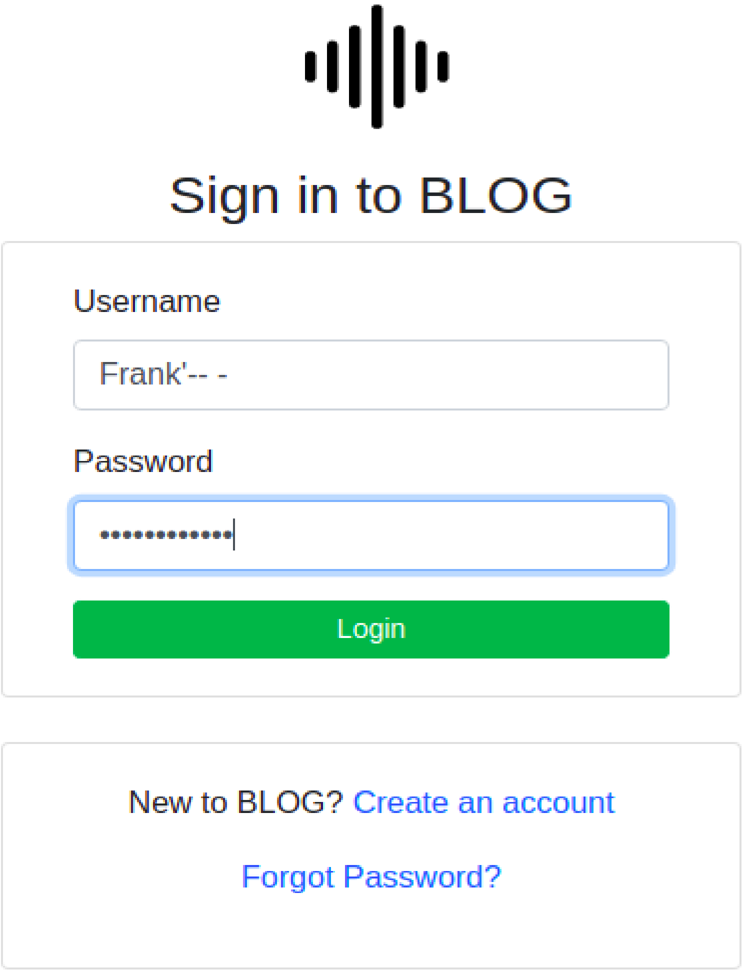
Login successful

User Account Information

Name	Robin Sharma
Account No	13456
Balance	$5000
Security Code	1454

SQL Injection Attack on-site with No Protection

Wrong username and password = ‘anythinghere’

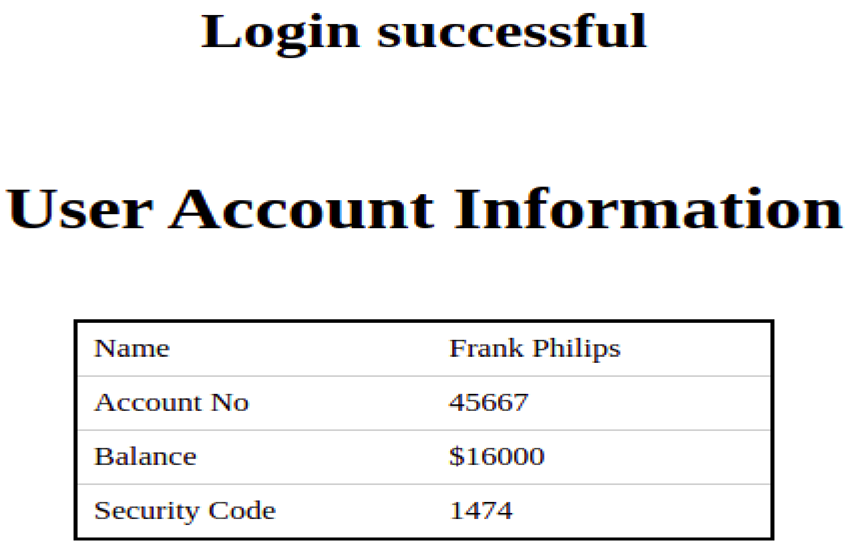


Sign in to BLOG

Username: Frank'-- -

Password: •••••••••••••

Successful login from Attacker without correct username and password



Login successful

User Account Information

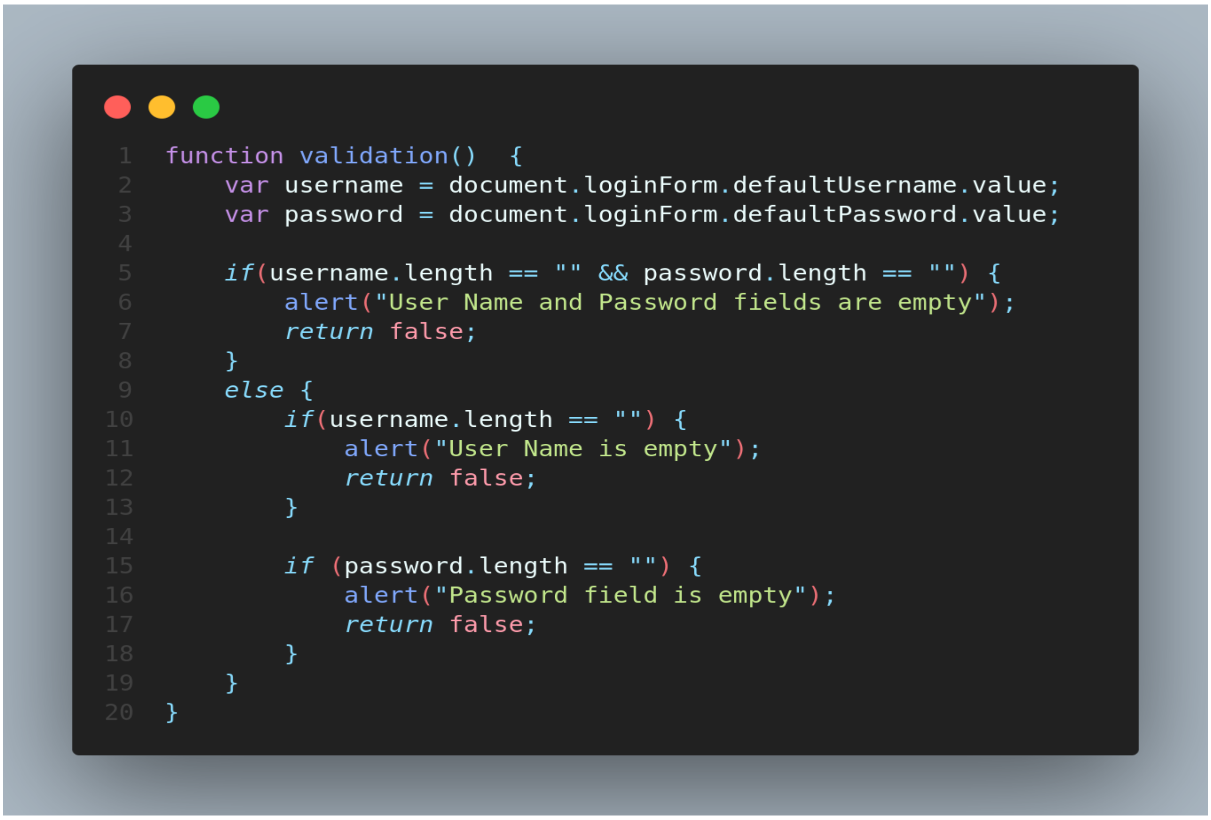
Name	Frank Philips
Account No	45667
Balance	$16000
Security Code	1474

Query executed internally for sql injection attack

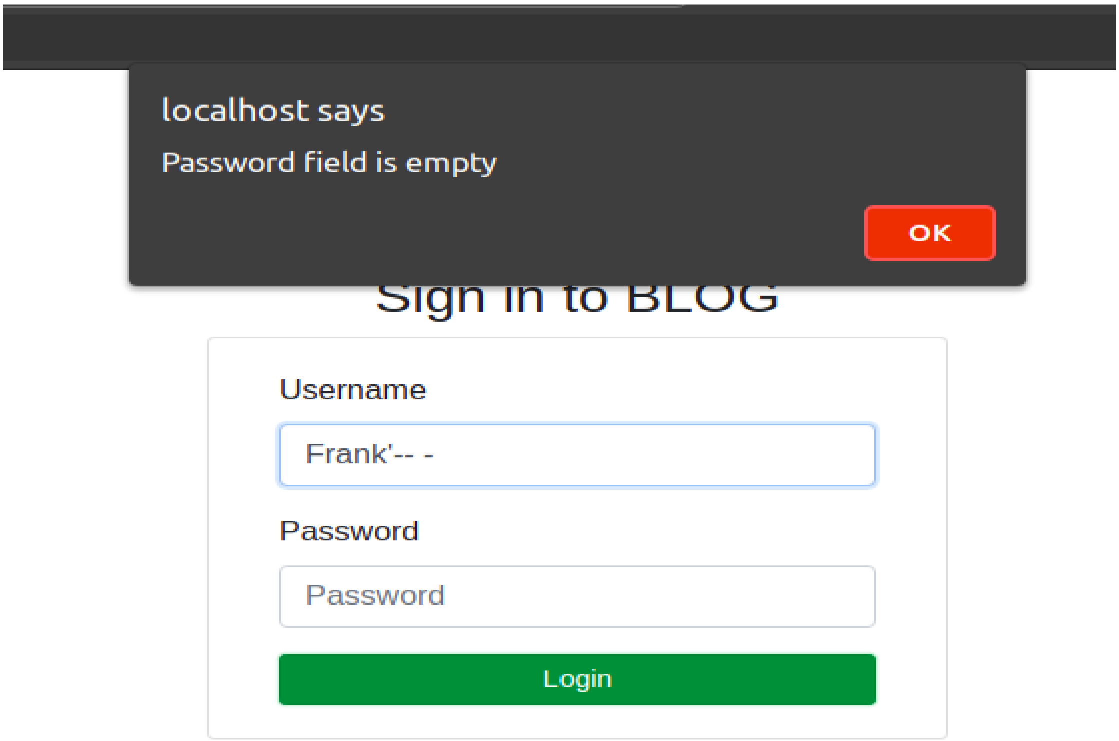
```
SELECT * FROM userAccounts WHERE username = 'Frank'-- -' and password = 'anythinghere'
```

SQL Injection Attack Prevention techniques

JavaScript Validation before accessing backend database



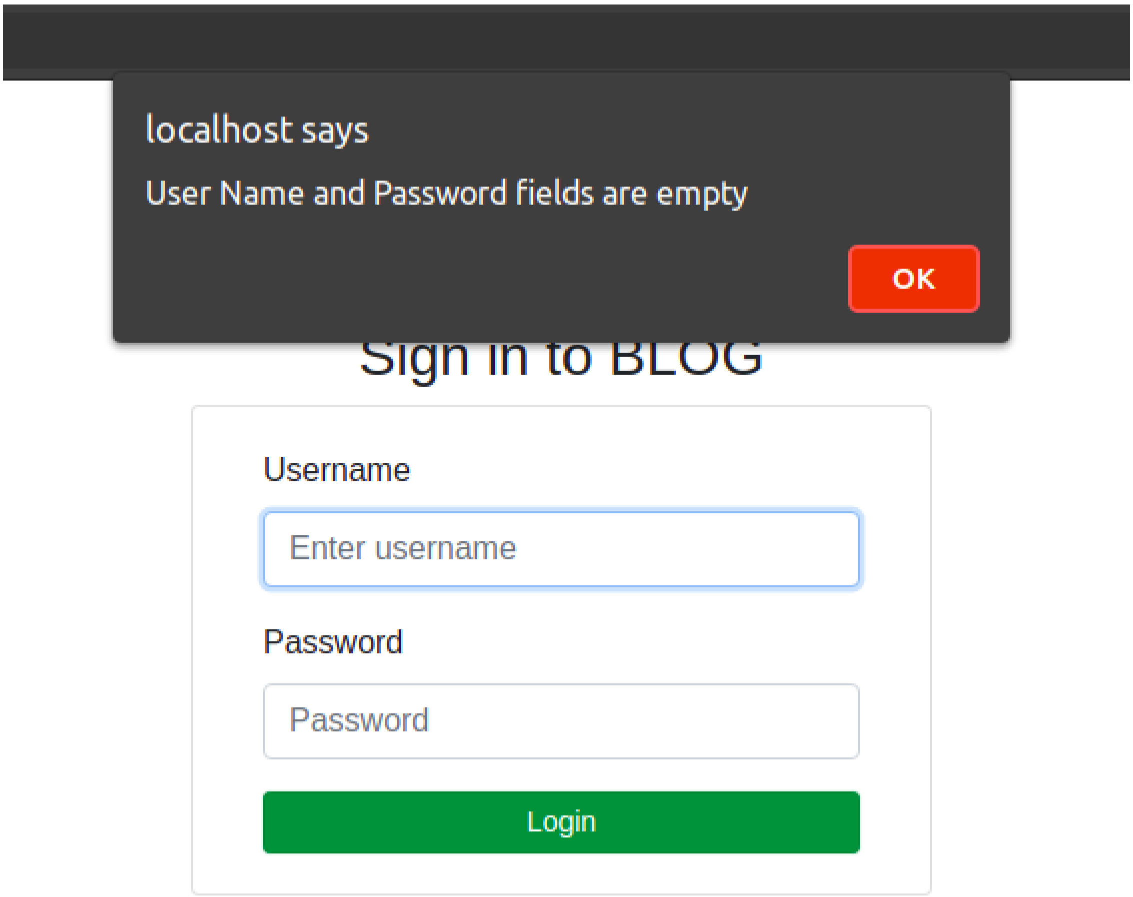
```
function validation()  {
    var username = document.loginForm.defaultUsername.value;
    var password = document.loginForm.defaultPassword.value;

    if(username.length == "" && password.length == "") {
        alert("User Name and Password fields are empty");
        return false;
    }
    else {
        if(username.length == "") {
            alert("User Name is empty");
            return false;
        }

        if (password.length == "") {
            alert("Password field is empty");
            return false;
        }
    }
}
```



localhost says

Password field is empty

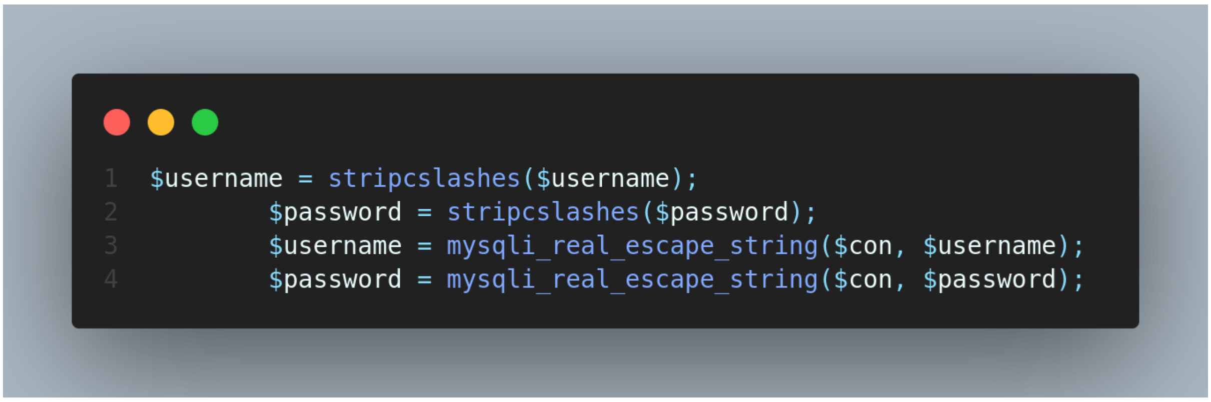
Username: Frank'-- -



localhost says

User Name and Password fields are empty

PHP checking whitespaces and special characters in input from Form



```
$username = stripcslashes($username);
        $password = stripcslashes($password);
        $username = mysqli_real_escape_string($con, $username);
        $password = mysqli_real_escape_string($con, $password);
```