Project 4.5: Web Security Optional

mmendiola3

Task 1: XSRF Prevention

1 Patched code

The vulnerability exists because the server-side CSRF check is using the challenge value supplied by the form submission to create the hash that is then compared to the supplied response value. This allows an attacker to bypass the CSRF prevention mechanism by supplying the expected response for an attacker provided account, challenge, and routing input.

```
    $teststr = $_POST['account'].$_POST['challenge'].$_POST['routing'];
```

This vulnerability was patched with the following changes:

```
    $teststr = $_POST['account'].$_SESSION['csrf_token'].$_POST['routing'];
```

Furthermore, the expected response value is displayed on a failed CSRF attempt. This should be removed.

2 Improved Security

The security of the site has improved since requests to the server issued after initial login will be validated to ensure they are part of the same session.

3 Same Origin Policy

Same Origin Policy would not prevent this attack because TODO

Task 2: XSS Prevention

In this case index.php sends unvalidated user input back to the client browser. This can be used to inject malicious code that is then run in the victim's browser.

Task 3: SQL Injection Prevention

Task 4: Further Security Fortification