CS6035 Summer 2016

Project 4 Report

Yan Cai ID: ycai87

Target 1: XSRF

The idea is to submit the corrent hidden respnse value to circumvent XSRF check from index.php, here the value is fixed.

Target 2: XSS-password theft

The attacker is able to inject malicious javascript in the login input value from index.php since there is really no input validation.

Target 3: SQL Injection

The vulneralbility is that the input is not verified and "'" is allowed so that extra SQL statement can be injected