Project Writeup Act 3

CSEC-380 Project Group 13

Connor Leavesley, Joshua Niemann

**Provide a link to the test cases you generated for this activity.**

<https://github.com/clev98/CSEC380-Project/tree/master/Tests>

**How do you ensure that users that navigate to the protected pages cannot bypass authentication requirements?**

To access the protected pages, the user needs to have a session ID from the server. Without the session ID, protected pages cannot be accessed, and the user will be returned to the login page.

**How do you protect against session fixation?**

When ever a user reauthenticates, a new session ID is assigned. This eliminates the risk of session fixation.

**How do you ensure that if your database gets stolen passwords aren’t exposed?**

A salt is added to the password and is then hashed using SHA256. If the database is stolen attackers will only have a list of hashes.

**How do you prevent password brute force?**

Only ten passwords can be entered per minute, per IP, to prevent brute forcing.

**How do you prevent username enumeration?**

The application gives a generic “Invalid Credentials” and nothing on whether the username exists.

**What happens if your sessionID is predictable, how do you prevent that?**

If the session ID is predictable then an attacker can guess the ID and gain access to the site. Session IDs are cryptographically random to make them as hard to guess as possible.