COMP 116
Fall 2015
Zachary Sogard

Assignment 4 – Technical Risk Analysis

| ID | Technical Risk | Indicators | CVE/CWE/OSVDB | Impact Rating | Impact | Mitigation | Validation Steps |
|---|---|---|---|---|---|---|---|
| 1 | SQL Injection | Code allows unintended SQL queries to be run via user input. | CWE-89 | H | Users can gain access to database containing confidential information and passwords. | Sanitize user input to remove special characters. | Run a tool like sqlmap. Attempt to insert queries into input. |
| 2 | XSS | Code allows user to insert <script> tags into web page. | CWE-80 | H | Arbitrary code can be executed on the site to cause unintended behavior. | Sanitize user input to remove unnecessary HTML tags. | Attempt to insert <script> tags into user-submitted fields on the web page. |
| 3 | Directory Traversal | Users are able to access directories by modifying URL or supplying pathname. | CWE-22 | H | Users can gain access to files they shouldn't have access to. | Sanitize user input to prevent inputs such as “../../etc/passwd”. Configure web server to deny access to certain files. | Attempt to access directories that should be denied. |
| 4 | Improper Restriction of Excessive Authentication Attempts | Users can brute force login information limitlessly. | CWE-307 | M | Attackers can gain access to other users' accounts via a brute force attack. | Lock account access after a certain number of failed login attempts. Set a timer before next login attempt is allowed. | Ensure logging in with incorrect credentials over and over eventually results in a timeout or lock on the account. |
| 5 | Plaintext Storage of a Password | Attackers can see all users' passwords if | CWE-256 | M | Attackers can use password information to gain access and steal | Store hash of password + a salt. | Ensure database does not contain any plaintext sensitive information. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | access is gained to database. | | | information from other people's accounts. | | |
| 6 | Weak Password Requirements | Users can choose very simple, easily guessed passwords. Bobo had a password of “supermodel”. | CWE-521 | L | Attackers can more easily break into victim's accounts and steal information. | Require a certain mix of special characters and alphanumerics for a password. Set expiration on password. | Ensure users cannot enter in simple passwords. |
| 7 | Cookie Tampering | Users can modify cookies before sending them to server. One could change “lg” from false to true. | CWE-565 | H | Attackers can pretend they are someone else or change parameters of request to cause unintended behavior. | Add integrity checks to cookies. Avoid reliance on them when possible. Validate input. | Ensure users cannot change cookies to successfully change parameters or identity. |
| 8 | Information Exposure Through Comments | Users can view source code of page to expose sensitive information about application. | CWE-615 | L | Attackers can gain information about the application that can be used to exploit it. | Remove sensitive information about implementation from HTML comments. | Ensure sensitive comments are removed from source code. |