Security Risk Assessment

|  |  |  |  |
| --- | --- | --- | --- |
| Security Risk | Probability (3=high, 1=low) | Impact | Risk Mitigation, Monitoring, and Management (RMMM) Plan |
| SQL injection | 3 | 3 | Risk Mitigation & Management: Disallow angle bracket, other suspicious script in text boxes  Monitoring: |
| Weak Authentication | 2 |  | Risk Mitigation & Management: Require two-factor authentication or use Google authentication  Monitoring: |
| Member access to officer view/information | 1 | 3 | Risk Mitigation & Management: Inform the admin of the risks that users might be impersonating officers. Authenticate officer account applications.  Monitoring: |
| XSS Scripting | 3 | 3 | Risk Mitigation & Management: Disallow angle bracket, other suspicious script in text boxes; use input filtering client/server side.  Monitoring: |
| Member financial information leaked from scholarship app | 2 | 3 | Risk Mitigation & Management: Protect database  Monitoring: Brakeman (?) |

Project Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk | Prob in % | Impact | Risk Mitigation, Monitoring, and Management (RMMM) Plan | Status |
| Web application link not accessible | 30% | High | Mitigation & Management: Code reviews; identify the bug(s); Review deployment environment, check Procfile, etc. (e.g. Heroku). | Integrate and ensure CI/CD to fully test changes before it hits production |
| Disengagement | 10% | Medium | Mitigation & Management: Have daily standups and access engagement. Talk to the team member privately, then to the instructor if problem is not resolved. | Encourage high involvement |
| Delay in deployment | 60% | Medium | Mitigation & Management: Emergency meeting to assign immediate work for finishing deployment  Monitoring: keep a close eye on deadlines and project completion | Schedule mob coding session |
| Customer discovers many defects | 50% | High | Mitigation & Management: Find all bugs through code test coverage reports and fix them before next release.  Monitoring: # of defects discovered per release | Schedule mob coding sessions |
| Test coverage isn’t sufficient | 50% | Medium | Mitigation: Research and identify good tests to implement. Management: If bugs occur and aren’t caught by tests, go back to test case development. Monitoring: Make sure test coverage is complete/nearly complete | Write tests using SimpleCov and RSpec |