|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk | Risk Statement | Response strategy | Objectives | Likelihood | Impact | Risk Level |
| Hacking  passwords can be guessed or cracked | Not Defined | Change password to something more secure (not root) | Make database un-hackable  Validation of all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification of what should be allowed | High | High | High |
| Use of new technology | Not Defined | To learn step by step technology and |  | Med | Med | Med |
| Data could be inappropriately extracted/modified from eclipses database by entering SQL commands into input fields  Hackers + Criminals / SQL Injection | Not Defined | Ensure that all parameters are validated before they are used. A centralized component or library is likely to be the most effective, as the code performing the checking should all be in one place. Each parameter should be checked against a strict format that specifies exactly what input will be allowed | Limited validation checks on inputs | High | High | High |
| **Testing Risks** | Not Defined | Test step by step | Need to do acquainted with the platform you are working on, along with the [software testing tools](https://www.edureka.co/blog/software-testing-tools/) being used. | High | High | High |
| Web server and application server running unnecessary services | Not Defined | All / Unnecessary Services | Reconfigure systems to remove unnecessary services | High | High | High |
| Disaster recovery plan has not been established | Not Defined | Environment / Disaster Recovery | Develop and test a disaster recovery plan | Med | Med | med |