**Security Code Review - Checklist**

A Security code review checklist is a manual process of checks that a project team should perform on any coding project that is being prepared to go from a testing or development environment to a production or live environment. These can take many forms. The example given below is a checklist that would be required to be filled in manually and signed off by a project lead. (Example result and remedial action provided for illustration.)

Project Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Date of Review: \_\_\_\_\_\_\_\_\_\_\_\_

Reviewers: \_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_.

**Checklist**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Check #** | **Check** | **Expected Result** | **Actual Result** | **Remedial Action** |
| **1** | Code has been linted and all dependencies/packages checked via relevant software. | Linted code and dependencies are safe. | *One package(example.py) deemed unsafe.* | *Example.py to be replaced with secure package.* |
| **2** | Any web forms have the CSRF Token added in. | All web forms have CRSF Token added | *All web forms have CSRF token added.* | *None needed.* |
| **3** | In the settings files has the Debug Mode been disabled. | Debug Mode set to FALSE |  |  |
| **4** | Hard coded variables (e.g. Secret Keys) have been removed from settings files and contained securely via vaults or environment variables. | All hard coded variables stored securely and separately to main program code. |  |  |
| **5** | Are all environment variables being used correctly, and *not* being pushed to the repository. | Environment variables set correctly. Information is not being pushed to the repository. |  |  |
| **6** | Any raw SQL queries are not being used and have been replaced with models et. Al. | All raw SQL has been removed from the code. |  |  |
| **7** | Have allowed/disallowed hosts lists been configured correctly? | All initially required allowed/disallowed hosts have been configured correctly using correct environment variables. |  |  |
| **8** | Have all user permissions been applied using principle of minimum usage? | All users only provided the access/rights that they require. |  |  |

Code Review Accepted by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.