|  |
| --- |
| University of Sunderland |
| Secure Coding Safety Checklist |
| An overview and checklist of the possible checks to perform. |

|  |
| --- |
| Heslop, Alan John  10-17-2020 |

**Security Code Review - Checklist**

Focus of a Secure Code Review

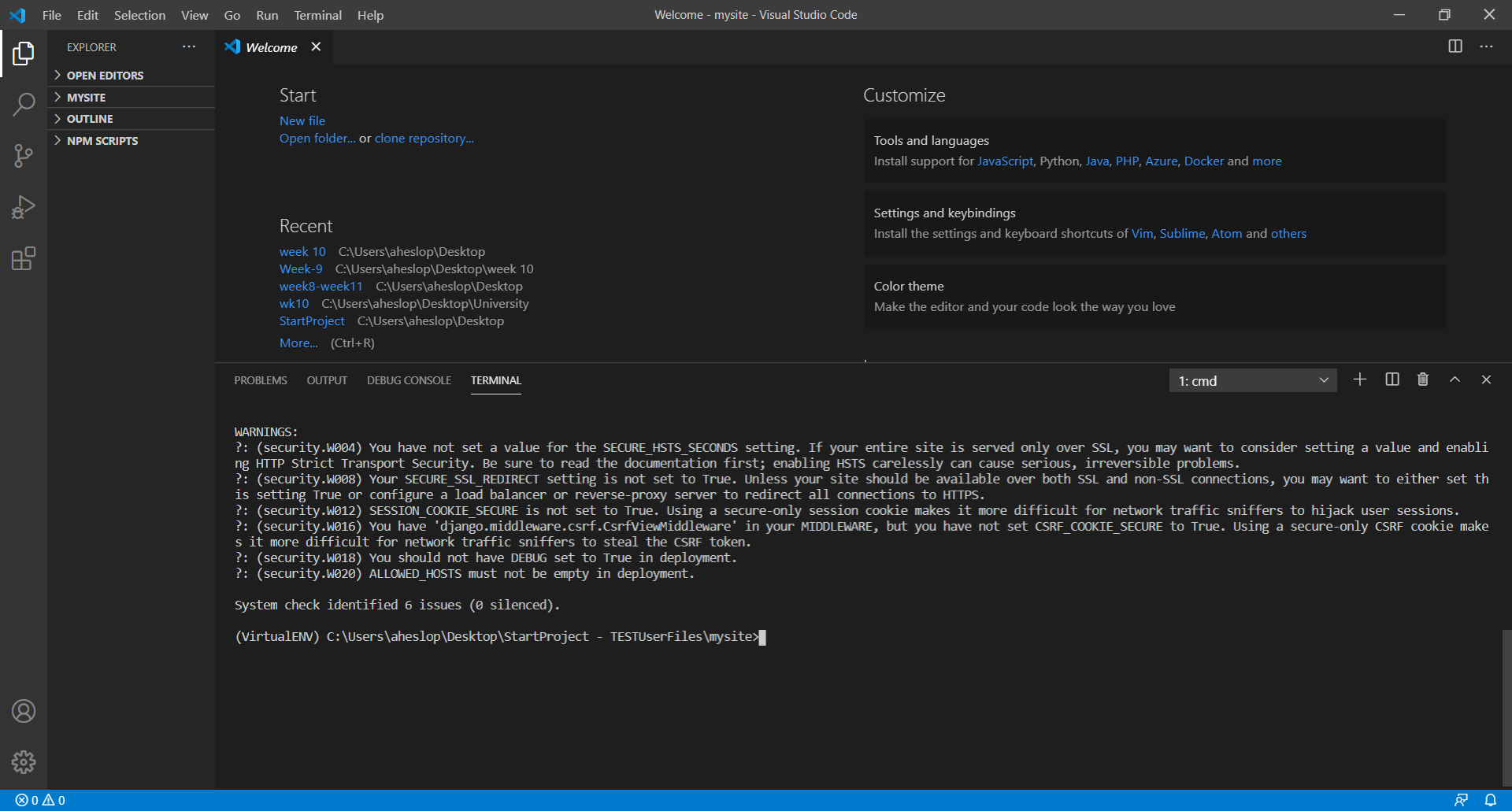
A secure code review focuses on seven security mechanisms, or areas.  An application that is weak in any area makes itself a target for a malicious user and increases the likelihood that the application will be used in an attack. A secure code review should inform the developers of the soundness of the source code in each of these areas:

* Authentication
* Authorization
* Session management
* Data validation
* Error handling
* Logging
* Encryption

When checking your code/application, please use the command:

python manage.py check --deploy

This command will perform a check to see if your application is ready to be “deployed”. Example output below:



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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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** | Debug Mode | Debug Mode set to FALSE when you’re going into production and TRUE when you’re in development. |  |  |
| **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** | Duplication of code | Try to avoid using duplication of code, having duplication of code can enhance the chances of an attack. |  |  |
| **8** | Have all user permissions been applied using principle of minimum usage? | All users only provided the access/rights that they require. |  |  |
| **9** | Session cookies within the application  SESSION\_COOKIE\_SECURE | Using a secure-only session cookie makes it more difficult for network traffic sniffers to hijack user sessions. |  |  |
| **10** | HTTPS/SSL | Unless your site should be available over both SSL and non-SSL connections, you may want to either set this setting True or configure a load balancer or reverse-proxy server to redirect all connections to HTTPS. |  |  |

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