|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Project Code** | | **Vulnerability Fixes** | **Reviewer Name** | | **Srikanth** |
| **Project Name** | | **Malaysia Airlines Berhad** | **Date (mm/dd/yyyy)** | | **09/18/2020** |
| **#** | **Check** | | | **Yes/ No/ NA** | **Remarks** |
|  | Copyright notice at the top of file. | | | **NA** |  |
|  | Included only required files. | | | **Yes** |  |
|  | Order of variable declarations | | | **Yes** |  |
|  | Order of method declaration | | | **Yes** |  |
|  | Naming convention of method. | | | **Yes** |  |
|  | Implementation comments. | | | **Yes** |  |
|  | Use General Coding Conventions wherever applicable | | | **Yes** |  |
|  | Indentation should be maintained | | | **Yes** |  |
|  | Avoid assigning several variables to the same value in a single statement. It is hard to read. | | | **Yes** |  |
|  | Any connection obtained should cleared and closed. | | | **Yes** |  |
|  | Miscellaneous checks (including some useful checks like unnecessary echo and print\_r) | | | **Yes** |  |
|  | Unused local variables | | | **Yes** |  |
|  | Empty if statements | | | **Yes** |  |
|  | Unused parameters | | | **Yes** |  |
|  | Maintaining session variables | | | **Yes** |  |
|  | Proper usage of control structures | | | **Yes** |  |
|  | PHP code tags to delimit PHP code | | | **Yes** |  |
|  | One statement per line | | | **Yes** |  |
|  | Following PHP variable declaration rules | | | **Yes** |  |
|  | PHP naming conventions | | | **Yes** |  |

2.0 Programming Mistakes:

* Performing operation on null objects.
* Not closing statement and connection.
* Not assigning variables to null while declaring
* Declaring variables in loops
* Lack of knowledge on Indentation
* Including unnecessary files.
* Unnecessary declaration of some local variables which are not being used
* Breaking of statements is not as per the conventions (Line size should not exceed 120)
* Usage of variables before initialization
* Misplacing of operators
* Use of hard-coded file paths and URL’s
* Usage of hardcode text sizes which effect GUI across the platforms
* Leaving dangling array references after foreach loops
* Performing queries in a loop such that each iteration of the loop would result in a separate query to the database.
* Inefficient memory usage while fetching records by running single query for each row to fetch, such approach leads to ‘out of memory’ condition.
* Assuming $\_POST will always contain your POST data
* Thinking PHP supports a single character data type
* Misusing empty() for Boolean checks
* Not using E\_ALL Reporting for error reporting
* Not sanitizing the data before it enters any sort of storage, like database.
* Usage of PHP code tags shorthand that is ‘<??>’ instead of ‘<?php?>’