**Code Review Report**

**Introduction**

This report provides details about the specific weaknesses that were found during the review. These details are designed to provide the developers with proof that the stated weaknesses exist as well as to provide examples that the developers can use to find and fix similar areas of the code. As mentioned before, the Code Review does not claim to find every issue; as such the development team should use the information in these findings as an opportunity to improve the entire code base. Just fixing the specific examples identified below will most likely not remove the higher level risks from the application.

Each finding is given a qualitative risk rating assigned by the reviewers at the time of the review. The general guidelines used when assigning risk levels are as follows:

* **High** - Serious impact to the application security, generally unmitigated, large-scale issues, such as an attack that is currently exploitable from the Internet.
* **Medium** - Notable impact to the application security, or somewhat mitigated high risks (e.g., being available only to the user's Intranet).
* **Low** - Potential impact to the application security, or heavily mitigated high risk (e.g., being in dead code or after an abort call).
* **Informational** – Does not directly make the code less secure, but bad coding practice.

The risk ratings should be considered risks to the application itself. In other words, the risk that the application behavior could be subverted in an unintended way could lead to a possible compromise. This information should then be used by the appropriate teams (developers/management/Information Security) in conjunction with the additional 'big picture' information that they have, to make the appropriate risk mitigation decisions.

1. **Section of code written after HTML closing tag**

**Category**: Code written outside scope

**Weakness**: HTML code or JavaScript file loaded will not work if it is not inside scope (Inside HTML tags - <html></html>).

|  |  |  |  |
| --- | --- | --- | --- |
| Source File | Line Number | Description | Risk |
| add-mom.php | 917 | In line number 917, “footer-script.php” loaded and some html codes and javascript files loaded after that line. | Low |

|  |  |
| --- | --- |
| Current Code | Suggestion |
| <!-- footer-script -->  <?php include\_once("include/footer-script.php"); ?>  <!-- /footer-script -->  <!--------------------------------------  /\*ADD NEW PAGE MODELS ONLY\*/  ------------------------------------->  <!-- create-next-popup modal -->  <div id="create-next-popup" class="modal fade ">  <div class="modal-dialog">  <div class="modal-content">  …………………..  …………………..  </div>  <!-- create-next-popup end modal --> | <!--------------------------------------  /\*ADD NEW PAGE MODELS ONLY\*/  ------------------------------------->  <!-- create-next-popup modal -->  <div id="create-next-popup" class="modal fade ">  <div class="modal-dialog">  <div class="modal-content">    …………………..  …………………..  </div>  <!-- create-next-popup end modal -->  <!-- footer-script -->  <?php include\_once("include/footer-script.php"); ?>  <!-- /footer-script --> |

This issue is also in these pages: mom.php, edit-mom.php, report-mom.php, response-mom.php

1. **Comments contain unwanted code**

**Category**: Code written inside comments

**Weakness**: The codes inside comments will confuse the developer. Comments should clearly describe what the code does.

|  |  |  |  |
| --- | --- | --- | --- |
| Source File | Line Number | Description | Risk |
| response-mom.php | 711 | In line number 711, some unwanted codes were commented. Remove the code from the page if it is not required. This issue not only in 711, there are several lines contain this problem. | Informational |

|  |  |
| --- | --- |
| Current Code | Suggestion |
| //if (($creator\_initial\_response\_flag == 1 || $creator\_response == 1 || $creator\_draft == 1) && $mom\_status != "Drafted" && $action\_by\_status == 1) { | Remove unwanted code from comments. |

This issue is also in these pages: mom.php, add-mom.php, edit-mom.php, report-mom.php

1. **Unused code**

**Category**: Unused code written

**Weakness**: Page contains unused code, which will increase the file size of the code file and the loading time of the page.

|  |  |  |  |
| --- | --- | --- | --- |
| Source File | Line Number | Description | Risk |
| add-mom.php | 935 | In line number 935, unused “Create Next Popup” modal is found. If it is not required remove them. | Informational |

|  |  |
| --- | --- |
| Current Code | Suggestion |
| <tbody>  <tr>  <td><div class="ckbox">  <input type="checkbox" id="checkbox1">  <label for="checkbox1"> </label>  </div></td>  <td> 01 </td>  <td> Please do something... </td>  <td> John Doe </td>  <td> 02 Jun 2016 </td>  <td> Open </td>  <td align="center"><a href="" class="btn btn-view" data-placement="left" data-toggle="tooltip" data-original-title="View"><em class="fa fa-eye"></em></a></td>  </tr>  </tbody> | Remove unused code from the page. |

This issue is also in these pages: edit-mom.php, response-mom.php

1. **Hardcode found**

**Category**: Hardcoded contents inside page.

**Weakness**: Page contains hardcoded contents, which is not dynamic and not useful. It contains dummy text also.

|  |  |  |  |
| --- | --- | --- | --- |
| Source File | Line Number | Description | Risk |
| report-mom.php | 725 | In line number 725, the “View Report Action Popup” modal contains full of hardcoded values and dummy content. Make it dynamic. | Low |

|  |  |
| --- | --- |
| Current Code | Suggestion |
| <!-- create-next-popup end modal -->  <div id="view-report-action-popup" class="modal fade ">  <div class="modal-dialog">  <div class="modal-content">  <div class="modal-header"> <a class="pull-right" data-dismiss="modal"><i class="fa fa-close"></i></a>  <h4 class="modal-title"> View / Minutes Action Item No. <span class="view\_minutes\_ai\_item\_no"></span> Details </h4>  </div>  …………………….  …………………….  <!-- /.modal-dalog -->  </div> | Make hardcoded contents dynamic. |