**STIGS Checklist:**  
Web Server STIG

Web server sample code applications may be an exploitable threat to a web server. A web server may only contain components that are operationally necessary (e.g. validator scripts, web-content, etc. Sample applications or scripts have not been evaluated and approved for use and may introduce vulnerabilities to the system.  
Mentioned Below are few of the STIGS checklist materials which we have incorporated into our project.

|  |  |  |  |
| --- | --- | --- | --- |
| Sr.No | STIGS Checklist | Severity | Description |
| 1 | Anonymous access accounts are restricted. | High | Both DB and server accounts are password protected. |
| 2 | The service account ID used to run the web site will have its password changed at least annually. | Medium | Our Project has the feature to change password, also we can recover a forgotten password. |
| 3 | Log file data must contain required data elements | Medium | We have a log file tracing transaction and special logs for invalid attempts |
| 4 | All interactive programs will be placed in a designated directory with appropriate permissions | Medium | All the templates are placed in a root folder with access by owner. |
| 5 | The web client account access to the content and scripts directories will be limited to read and execute. | High | Handled by Flask; Certain files are eligible to be accessed by the client. |
| 6 | Web server software will always be vendor-supported versions. | High | All the versions of module we have used are vendor-supported |
| 7 | A web server will be segregated from other services. | High | No other services than this application |
| 8 | PERL scripts will use the TAINT option. | Medium | No PERL script used |
| 9 | Web server and/or operating system information will be protected. | Low | Implemented in the server side code, refer Project report for detailed explanation |
| 10 | All utility programs, not necessary for operations, will be removed or disabled. | Medium | Not Applicable |

## Application Security and Development STIG Checklist

## The goal is to ensure no loss of Confidentiality, Availability or Integrity of the system associated data, is addressed as the application is being developed.

Mentioned Below are few of the STIGS checklist materials which we have incorporated into our project.

|  |  |  |  |
| --- | --- | --- | --- |
| Sr.No | STIGS Checklist | Severity | Description |
| 1 | The designer will ensure the application executes with no more privileges than necessary for proper operation. | High | Case Condition: - If bank balance of an user is 500$, He cannot send 501$. |
| 2 | The Release Manager will establish a Configuration Control Board (CCB), that meets at least every release cycle, for managing the CM process. | Medium | Team lead is sending out minutes of meeting for every version |
| 3 | The designer will ensure the application is not subject to error handling vulnerabilities. | Medium | We have handled errors for wide set of errors. |
| 4 | The designer will create and update the Design Document for each release of the application. | Medium | For every release of this portal we guarantee to create and update design document |
| 5 | The designer will ensure uncategorized or emerging mobile code is not used in applications. | Medium | No mobile codes are generated , for any kind of authentication. |
| 6 | The designer will ensure the application does not contain invalid URL or path references. | Medium | No Invalid URL present |
| 7 | The designer will ensure the application does not allow command injection. | High | We don’t run any commands from the server |
| 8 | The designer will ensure the application does not have cross site scripting (XSS) vulnerabilities. | High | Input is validated |
| 9 | The designer will ensure the application transmits account passwords in an approved encrypted format. | High | All the data is encrypted |
| 10 | The designer shall use both the <NotBefore> and <NotOnOrAfter> elements or <OneTimeUse> element when using the <Conditions> element in a SAML assertion. | High | Not applicable |

We didn’t use OpenVas or Nessus to do a vulnerability scan.