Web Application Security Guidelines for Government Organizations

With the advancement of technology, there has been a significant increase in information security threats that web applications are being subjected to. This guideline outlines the basic principles that are to be followed by government organizations to prevent or mitigate web application compromise.

SRI LANKA CERT|CC

An Agency under the Ministry of Technology

Version 1 Issue: 22 Feb 2022

Prior to Development

- Identify the criticality of the contents of the web application based on the types of information which will be published, processed and stored, and determine security requirements for the protection of web application in accordance with the Technical Guidelines for Web Application and Website Security issued by Sri Lanka CERT.
- Include mandatory security requirements to the tender document as depicted in Table 10-1 Section 10 of the Information and Cyber Security Implementation Guide, an extract is attached as Annexure A.
- A clause shall be included in tender document to ensure that the web application is developed and hosted in accordance with the Technical Guidelines for Web Application and Website Security.

Design and Development

- Web application shall be developed by following the Technical Guidelines for Web Application and Website Security.
- Web applications of government organizations shall be in the “gov.lk” domain name.
- Input validation shall be in place for allowing input of the data fields at the client and server sides for data types (integer, text, etc.) and data specification (For example, the number of digits in telephone number).
- If files are to be uploaded then these are to be restricted to the file types specified by the application to prevent uploading of malicious files.
- Government organizations shall ensure that the web application is developed taking into consideration the Web Application Security Risks published by OWASP.
- Malware detection through scanning is essential when attachments in the form of pdf, word, excel, text files are uploaded to the web application. Encrypted or compressed files shall not be allowed to be uploaded on the web application. Exceptions shall only be accommodated with

the recommendation of Sri Lanka CERT.

Ensure “HTTPS” has been enabled on the web server. Login details shall only be transmitted over HTTPS, login form is delivered over HTTPS, and tokens only delivered over HTTPS.

- Use two-way SSL authentication for accessing the backend (CMS) of the web application.
- Sensitive information must be encrypted in transit and at rest. E.g. Storing in databases, file servers, backups and when managing unstructured data for compliance, privacy and security as mentioned in the Data Protection Regulation.
- Ensure that the developer implement integrity checks such as digital signatures on any serialized objects to prevent hostile object creation or data tampering.
- Developer shall limit the usage of third-party components in the form of plugins and codes. In the event of such components is to be used, a comprehensive risk assessment is to be performed before deployment.
- Host server platform shall be hardened and configured to ensure the removal or disabling of unnecessary services and applications as mentioned in Section 2.2.3. of the Technical Guidelines for Web Application and Website Security.
- Government organizations shall take into consideration the security requirements mentioned under Section 2.1.1. of the Technical Guideline for web application security when selecting a hosting platform for the web applications.
- Whenever possible, an effective CAPTCHA or any other two factor authentication mechanism shall be implemented to minimize potential attacks (Eg. Login, Contact Us, etc.).
- Administration access to the Web Applications shall be restricted through multi factor authentication. At a minimum strong password and one-time password (OTP) shall be enabled as mentioned in the Section 4.4. of the Minimum Information Security Standards for Government Organizations.
- A security assessment must be carried out through Sri Lanka CERT prior to the production release.
- Prior to the deployment of web application, organization shall obtain a legally binding assurance from the developer that web application is developed and hosted in accordance with the Technical Guidelines for Web Application and Website Security.
- Default and/or vendor supplied passwords shall be changed or disabled prior to deployment in the production environment.
- If there is a database in use, is shall not be exposed to the Web Application users directly. Any manipulation to data in the database shall be carried out only through the application.

Deployment and Maintenance

- Web application is hosted according to the secure web hosting guideliness as specified in the Technical Guideline for Web Application and Website Security.
- Ensure that authenticated users are granted access to the web application on a “need to know”, least privilege basis. Sharing crediential with unathorized users shall be strickly prohibitted.
- If administrators use their own devices to access the CMS or the web application administration panel, it is essential the stated devices are adequately secured and updated with security patches.
- The web application, content management systems, database, operating system and web server platform need to be patched and updated with latest security patches.
- Route the web traffic through a managed device/service which safeguards web applications and their data from malicious attacks. Traffic is to be routed through firewalls before it reaches the web application. It can be through a physical firewall and a web application firewall. The firewall definitions and (or) Antivirus signatures must be updated periodically.
- A security assessment is to be performed through Sri Lanka CERT at least on an annual basis. The other circumstance in which the organization shall perform security assessments include, after an incident has occurred or after a change is made to the application, or after changes have been made to the platform or hosting environment, or after changes to standards, policies and guidelines, after the spread of virus/malware, or as determined by the organization.
- Changes to the application or its environment shall be performed only after conducting a comprehensive risk assessment.
- Audit trails for all activities shall be maintained, backed up and archived regularly.
- Maintain an formal and up to date copy of the Web Applications on a host that is not connected to the Internet. Maintaining regular backups of application, content and data are essential.

Retirement and Disposal

- At the decommissioning stage, the web application shall be securely disposed of to ensure that its data and other information assets cannot be accessed and recovered by unauthorized individuals as mentioned in the Section 4.14. of the Minimum Information Security Standards for Government Organizations.