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.

An Agency under the Ministry of Technology

Classification: Public Draft Version 1 Issue: 27 May 2021

Prior to Development

- Identify the criticality of the application based on the types of information which will be published, processed and stored, and determine security requirements for the protection of application.
- Include mandatory security requirements to the tender document.
- A clause should be included in tender document to ensure that applications are developed and hosted in accordance with the “Technical Guide for Web Application Security” issued by Sri Lanka CERT.

Design and Development

- Web application shall be developed by following the “Technical Guide for Web Application Security”.
- Websites of government organizations shall be in the “gov.lk” domain name.
- Application logic analysis, input/output validation shall be in place to allowing only input and output of only those data types that are known to be correct. E.g. Telephone number can only contain numeric values.
- Government Officers should 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.
- Ensure “HTTPS” has been enabled on the web server. Login details should only be delivered 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 site.
- Sensitive information must be encrypted before storing in a database for compliance, privacy and security.
- Ensure that the developer implement integrity checks such as digital signatures on any

serialized objects to prevent hostile object creation or data tampering.

- Developer should 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 should be hardened and configured to ensure the removal or disabling of unnecessary services and applications.
- Web applications (web sites) shall be hosted on the Lanka Government Cloud.
- Whenever possible, an effective CAPTCHA shall be implemented to minimize potential attacks.
- Administration access to the Web Applications should be restricted through two factor authentication. At a minimum strong password and one-time password (OTP) should be enabled.
- A Vulnerability Assessment and Penetration Tests (VAPTs) must be carried out by Sri Lanka CERT prior to the production release.
- Prior to the deployment of web application, organization should obtain an assurance from the developer that web application is developed and hosted in accordance with the guidelines.
- Default and/or vendor supplied passwords should be changed or disabled prior to deployment in the production environment.

Deployment and Maintenance

- Web application is hosted according to the secure web hosting guideliness as specified in the “Technical Guide for Web Application 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 should be strickly prohibitted.
- The web application, content management systems, database, operating system and webserver 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) AV signatures must be updated periodically.
- A VAPT is to be performed by Sri Lanka CERT at least on an annual basis. The other circumstance in which that organization should perform VAPTs 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 should be done only after conducting a comprehensive risk assessment.
- Transaction logs for all activities should be maintained, backed up and archived regularly.
- Maintain an authoritative copy of the public Web Applications on a host that is inaccessible to the Internet. Maintaining regualar backups of application, content and data are essential.

Retirement and Disposal

- At the decommissioning stage, the web application should be securely disposed of to ensure that its data and other information assets cannot be accessed and recovered by unauthorized individuals.