Website Security Guidelines for Government Organizations

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

Classification: Public *Draft Version 1* *Issue: 27 May 2021*

Prior to Development

- Identify the criticality of the website based on the types of information which will be published, processed and stored, and determine security requirements for the protection of the site.
- 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

- Websites of government organizations shall be in the “gov.lk” domain name.
- Websites shall use latest and stable version of content management tool (CMS).
- Web Application Security Risks mentioned in “OWASP” should be taken into consideration when designing and developing the website.
- Input/output validation shall be in place to allowing only input and output of only those data types that are known to be correct.
- 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 (or CMS) of the web site. Sensitive information must be encrypted before storing in a database for compliance, privacy and security.
- Establish two factor authentication for users who has access to CMS or backend. Enforce strong passwords policies is also essential.
- Developer should limit the usage of Third-Party Components in the form of plugins and codes.
- Default and/or vendor supplied passwords should be changed or disabled prior to deployment.
- Websites shall be hosted on the Lanka Government Cloud.
- Whenever possible, an effective CAPTCHA shall be implemented to minimize potential attacks.
- Prior to deployment of the website, an assurance should be obtained from the vendor that

website is developed in accordance with the Technical Guide for Web Application Security.

- A Vulnerability Assessment and Penetration Tests (VAPTs) must be carried out by Sri Lanka CERT prior to the production release.

Deployment and Maintenance

- If the website is developed by a vendor, the government organization should always have an active maintanance agreement with the vendor.
- The website CMS, database, operating system and webserver platform need to be patched and updated with latest security patches.
- Access credentials to the website CMS or backend should be given to authorized users only. Sharing crediential with unathorized users should be strickly prohibitted.
- A VAPT is to be performed by Sri Lanka CERT at least on an annual basis. Other circumstance in which that organization should perform VAPTs include, after an incident has occurred or after a change is made to the application, platform or hosting environment, standards, policies and guidelines, after the spread of virus/malware, or as determined by the organization.
- Maintain an authoritative copy of the Website 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 website should be securely disposed of to ensure that its data and other information assets cannot be accessed and recovered by unauthorized individuals.