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.

Version 1 Issue: 22 Feb 2022

Prior to Development

- Identify the criticality of the contents 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 website 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 website is developed and hosted in accordance with the Technical Guidelines for Web Application and Website Security.
- If the website offers a service through a web application, refer to the Web Application and Website Security Guidelines for Government Organizations for more information.

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).
- Website Security Risks mentioned in “OWASP” shall be taken into consideration when designing and developing the website.
- 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).
- Malware detection through scanning is essential when attachments in the form of pdf, word, excel, text files are uploaded to the website. Encrypted / compressed files shall not be allowed to be uploaded on the website. 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 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 website. 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.
- Establish multifactor factor authentication for users who have access to CMS or backend. Enforcing strong passwords policies is also essential for government organizations as mentioned in the Section 4.4. of the Minimum Information Security Standards for Government Organizations.
- Developer shall limit the usage of third-party components in the form of plugins and codes. In the event if such components are to be used, a comprehensive risk assessment is to be performed before deployment.
- Default and/or vendor supplied passwords shall be changed or disabled prior to deployment.
- Government organizations shall take into consideration the security requirements mentioned under Section 2.1.1. of the Technical Guideline for Web Application and Website Security.
- Whenever possible, an effective CAPTCHA shall be implemented to minimize potential attacks.
- Prior to deployment of the website, an assurance shall be obtained from the vendor that website is developed in accordance with the Technical Guideline for Web Application and Website Security.
- A security assessment must be carried out through Sri Lanka CERT prior to the production release.

Deployment and Maintenance

- If the website is developed by a vendor, the government organization shall 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 shall be given to authorized users only. Sharing crediential with unathorized users shall be strickly prohibitted.
- If the website administrator uses their own devices to access the CMS or the website administration panel, it is essential the stated devices are adequately secured and updated with security patches.

- A security assessment is to be performed by Sri Lanka CERT at least on an annual basis. Other circumstance in which that organization shall perform security assessment include, after an incident has occurred or after a change is made to the website, platform or hosting environment, standards, policies and guidelines, after the spread of virus/malware, or as determined by the organization.
- Maintain a formal and up to date copy of the Website on a host that is not connected to the Internet. Maintaining regualar backups of website, content and data are essential.

Retirement and Disposal

- At the decommissioning stage, the website 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.