NIC- Computer Emergency Response Team (CERT)

Website Security Guidelines

Document Control

Document Title	Website Security Guidelines
Document Type	Guideline
Document Identifier	WSG
Version	1.0
Date of Release	November 2017
Document Owner	NIC-CERT
Document Author	HARIHARAN M
Document Reviewed By	Nagendra Kumar, HoD, NIC-CERT
Document Approved By	R.S Mani, HoG, NIC-CERT

Document Change History

Version No.	Revision Date	Nature of Change	Date of Approval

Website Security Guidelines

This Guideline is applicable to all NIC Employees, temporary/contractual staffs, Vendors, Third Party Personnel, Central and State Government Employees and other stakeholders who are involved in Website/Application – Development, administration, management.

1. Ensure that the Website is Security Audited and an Audit Clearance certificate is issued by a CERT-IN empaneled vendor before hosting in production environment. The Security Audit should be done every six months or as and when any changes are done to the source code.
2. Use SSL Certificate Site wide on all websites. The SSL Certificate should use at least 2048 bit SHA 256 encryption or higher.
3. Ensure that the SSL Certificate is valid and keep track of the certificate expiry date and take necessary action to renew/replace the certificate before expiry.
4. Disable support for SSL 2.0, SSL3.0, TLS 1.0 at the server level. Use TLS 1.2
5. Disable weak ciphers like DES, 3DES, RC4. Use Strong Ciphers like AES, GCM.
6. Any “non-https” requests received on the website/applications, should be forcefully re-directed to “https”.
7. Ensure that all Websites and Applications and their respective CMS (Content Management System), 3rd party plugins, codes…etc., are updated to the latest versions.
8. All Passwords, connection strings, tokens, keys…etc., should be encrypted with salted hash. There should not be any plain passwords stored in config files or source code or in database.
9. All exceptions should be handled appropriately. Custom error pages should be displayed for any errors/exceptions. At no point of time, a portion of source code should be displayed on the page in case of an error or exception.
10. HTTP Response Headers should be obscured.
11. Directory traversal should be disabled. In case of any specific attempt by a user to access a portion of the code by typing the url path (ex: www.xxx.gov.in/js/custom.js) then the same should be redirected to a custom error page.
12. HttpOnly Cookies should be enabled, to restrict access to cookies.

13. All default user names and IIS/apache pages (like admin, default.aspx, index.aspx...etc) should be renamed. The access url for admin panel/CMS, should also be renamed.
14. The Web Server processes should not be running under Administrator or Root user Account. A dedicated User account with limited privileges should be used for the Web Server Processes.
15. All websites/Applications, should be checked by their respective developers on a daily basis and in case of any security compromise, then the same should be reported to NIC-CERT immediately.
16. Write + Execute Permission - both should not be given to upload directory
17. Ensure Input Validation is done properly, while accepting input from the user through the website.
18. Ensure that the Computer/system, from where CMS/site updates are being done is installed with the latest OS + Antivirus Updates and Patches. No unauthorized software/cracks, should be installed on the machine.
19. Restrict the web application to run Stored Procedures, so that SQL Injection attempts are averted.
20. If your website/application is integrated with any 3rd party Applications or using any APIs for external communication, then ensure that all such communications are done through encrypted channel.