

**Procedure for Conducting Third Party Security Audit
by CERT-in Empanelled Security Auditor
for the Websites/Web-enabled Applications of User Department/Organization**

[To be Conducted/Handled by User Department/Organization]

User Departments/Organizations undertake the development of websites/web-enabled applications by third party developers and get the same audited for Security Vulnerabilities from CERT-In empanelled Security Auditors, for further deployment of the same on NIC Server/NICNET. The following guidelines may be followed for the Security Audit of the websites/web-enabled applications conducted with the CERT-In empanelled Security Auditors.

1. **Scope:** - For Websites/Web-enabled Applications proposed to be hosted on NIC Production Server/NICNET, under going Third Party Audits.

2. **Guidelines**

2.1 Web-enabled Application is to be audited as per OWASP (www.owasp.org) Top 10 2007 criteria (Open Web Application Security Project).

2.1.1 Certificate is to state that whether the applications (under audit) has been tested as per the OWASP top 10 criteria and found to be safe? Actual tests should have considered issues of OWASP Top 10 2004 as well as Top 10 2007.

2.1.2 The security certificate from the auditor is to state that the site is free from vulnerabilities as per OWASP Top 10 2007 and is safe for hosting.

2.1.3 A black box approach of application security audit based on OWASP is to be adopted for the purpose of audit. This may be combined with source code review.

2.1.4 Security audits are to be conducted in iterative cycles (may be called a level) of testing and code correction till identified safe for hosting

2.1.5 Optionally, final audit report may be given. In case of dynamic sites the report must include Summary/Checklist of vulnerabilities identified with subsequent correction status.

2.2 In certain cases, audit is carried out on a local server of Security Auditor. In certain other cases audit is conducted on a third party URL or on user system. And the auditor, stating that CD contents have been audited, makes the audited contents available on CD in sealed cover to the NIC coordinator for the following.

2.2.1 In such case, a statement or official communication from the NIC coordinator is to be made available stating that the audited contents have been mounted on the staging URL designated/allotted by IDC for the site.

2.2.2 The staging URL as well as the Production URL, where the site will be hosted is to be mentioned clearly in the certificate.

2.3 It is advisable not to audit on live Servers or on the Production URLs, as results of such tests may not be correct due to attack prevention devices along the way. Client may be asked to provide the application on some separate Server (Staging or Temporary Servers) for test purposes.

2.4 Users often desires to deploy/host applications, which have authentication/authorization based (ex: Admin or CMS) modules. These modules may go un-audited, as they are directly not linked to the site/application and are not easily discovered. In such cases, it is recommended that all details of such applications may be shared with the Security Auditor during discussions with the site/application

owners, before auditing. The test URLs as well as Production/Public URL should be clearly mentioned in the Audit Certificate, by the Security Auditor.

2.5 The Audit certificate should be complete as to state the permissions on file system/site level required for hosting the site and application.

2.5.1 Permission include Read , Execute, Write, etc.

2.5.2 If any other permission is to be given then this also must be clearly stated.

2.5.3 The certificate to state what permission is to be given at the folder or site level and not to individual files.

2.5.4 Care to be taken that combined write+execute permission is not given on any folder/site.

2.5.5 If there is a requirement in the application for file uploads or writing to folders/files, then the absolute URL of the hosting folder needs to be specified along with the permission required.

2.5.6 Also, the permission requirement for the rest of the site also needs to be stated. Care should be taken to see that no folder gets a combination of Write + Execute permissions.

2.5.7 Preferably, segregation of dynamic pages or applications into separate folders under a site comprising of static information is to be considered

(Note: - Refer Execute Permission in Item No.4, below)

2.6 The report to mention about the nature of the site: viz: Static or Dynamic i.e. site with applications.

2.6.1 If the site contains Applications with closed user group access, then this is to be stated.

2.6.2 If the site/application is open for generic visitors, then this is to be stated.

2.6.3 Kind of authentication used such as Basic or Form Based or certificate based is to be stated

2.6.4 If the site is host to web based Content Management module as part of the site then this is to be stated.

2.6.5 If application (above) to be recommended for SSL deployment for the folder hosting the Closed User group (CUG) application. This is to be done after segregating the CUG application to a separate folder.

2.6.6 If the site is host to an administration module for administering tender, announcement, auction, etc. then this also is to be stated.

2.7 A scanned copy of the final Security Audit Report & Certificate to be forwarded to NIC, State Centre for subsequent forwarding to Cyber Security Division, NIC(HQ) along with a official file-note (Green Sheet). State Web coordinators to submit the Audit Report and certificate (scanned soft copy) through the Audit Status Monitoring Application on the <http://security.nic.in>

2.8 Non-functional links are to be tested after restoring functionality instead of just being reported as observations on non-functional URLs.

2.9 Care to be taken in recommending Execute permission for sites. If the applications have not been tested due to non-function and execute permission, the application will not be made functional on Production Server. So as to avoid shifting of such applications with vulnerabilities into production server.

2.10 Clarifications regarding audit report or security certificate or info in the certificate found insufficient to host the site will be sought from the Auditor conducting the security audit for the site with the help of the NIC coordinator for the site. If required, a revised document would be sought.

3. A sample Recommendation of the Security Auditor may be send from the following.

- 3.1 Auditor Organization Name/Logo: -
- 3.2 Application Description/Name: -
- 3.3 Production URL of proposed Application: -
- 3.4 Temporary/Staging URL: -
- 3.5 Audit Performed by (Name & Contact Details): -
- 3.6 Testing Date: -
- 3.7 Observation (in Details): -
- 3.8 Conclusion: - Application/Site is free from OWASP (and any other known) vulnerabilities and is safe for hosting.
- 3.9 Recommendation:
 - 3.9.1 Site may be hosted with the privileges of read & Script execution permission for the general public.
 - 3.9.2 WRITE & Read Permission: to the "writereaddata" Folder as this folder is concerned with the uploading of files.
 - 3.9.3 WRITE: - The folder 'writedata' containing the database file should be given 'WRITE' permission. (Note: Execute permission not to be given to the above folder)
 - 3.9.4 To be deployed over SSL with proposed URL.
 - 3.9.5 Web server and OS level hardening need to be in place for the production server.

Note: - All of the above recommendations may not be included. However, these are to be determined as per the requirements of the application. This is to be stated clearly along with the production URL and Staging URL address. The certificate should state clearly as to that the site is free from application vulnerabilities as per OWASP and is safe for hosting.

4. Execute Permission: - The term Execute permission means that a script or application to be allowed to execute within the resource context of the host environment.

- 4.1 Ex: An .asp script file hosted in an IIS environment may be given read and Script or Execute access at the site/virtual directory level in addition to Read permission at the file system level.
- 4.2 Where as a .php script file may be given read access in an Apache web server host environment.
- 4.3 These permissions may be determined with the help of the developer of the site.
- 4.4 Special care to be taken in case of modules facilitating File upload option. Check should be done that a file once uploaded does not execute with in the resource context of the site/folder. Combination of Write + Execute not to be given.

Note: -

- This Document is also available on the website of NIC, Madhya Pradesh (www.mp.nic.in)
- List of Empanelled Security Auditor is available on the website of CERT-in (Presently available at URL <http://cert-in.org.in/PDF/emprog.pdf>.)

5. Details of Web-enabled application, which can be forwarded to Security Auditor(s) to assess the Audit Requirements precisely & completely.

SN	Item	Description
1.	Title & Relevant Description of the Application, proposed for Audit	
2.	Name, Address & Contact Details of User Organization	
3.	Whether the target Application is accessible remotely from Internet? (Y/N)	
4.	Whether the Security Audit is to be conducted remotely (over Internet)? [Y/N] If Yes, please provide URL of the target application for conducting Security Audit. (If No, you will have to send target application on a CD to Security Auditor for conducting Security Audit after finalization of Auditor.)	
5.	Operating System Details (i.e., Windows-2003, Linux, AIX, Solaris, etc.)	
6.	Web/Application Server with version (i.e., IIS 5.0, Apache, Tomcat, etc.)	
7.	Front-end Tool [Server side Scripts] (i.e., ASP, Asp.NET, JSP, PHP, etc.)	
8.	Back-end Database (MS-SQL Server, PostgreSQL, Oracle, etc.)	
9.	Database access type (Read Only or Read/Write)	
10.	Type of Cryptography used for Storage & Transmission of Data & Credentials	
11.	Type of Authentication Used (Basic/Form Based/Certificate Based)	
12.	Authorization No. of roles & types of privileges for the different roles.	
13.	Provision of e-Commerce and/or Payment Gateway	
14.	Brief description about security functions or mechanisms used in the application. (i.e., Authentication, Authorization, Input Data Validation, Exception handling, audit & logging, session management, sensitive data handling, etc.)	
15.	Site users (Closed user group and/or open to public)	
16.	Whether the site contains any content management module? (Y/N) If Yes, please indicate which module.	
17.	Total Size (estimated) of the Website in MB and also mention No. of estimated Pages	
18.	Total No. (Approximate) of Form Fields are there in the Data Entry Pages for input.	
19.	Please enclose SRS document or Manual, if availability & feasible.	