AUDIT STATUS MONITORING SYSTEM V 3.0-

A SYSTEM FOR FACILITATING WEB APPLICATION SECURITY AUDIT SERVICES

Edited by
R. GAYATRI

ABOUT WEB APPLICATION SECURITY AUDIT SERVICES AT NIC

Strengthening and enhancing the security posture of systems and services is one of the objectives of any organization dealing with information assets of different organizations and departments of Government of India. The Cyber Security Division of NIC is dedicated to this task, having adopted a multi-pronged approach to security.

This includes deployment of the requisite technical solutions at the Gateway and Network level and associated monitoring of the traffic and alerts raised.

In the other arm of this security approach, Vulnerability assessment and the consequent remediation are being undertaken as a process for the large number of exposed surfaces of the Web sites and Web applications hosted on many of the servers on NICNET. This includes formulation of Web Application Security Audit policy, procedures and their implementation in addition to conduction of awareness building training and hand holding exercises.

Consequently, today all concerned, including all NIC coordinators as well as users and site owners of various Government Organizations play an active role in complying with Audit policy and in working towards the goal of a secured Information systems hosting environment. All of the above are now a part of the Web Application Security Audit services being undertaken at NIC.

SNIGDHA ACHARYA
Technical Director
NIC, Odisha

The primary requirement in rolling out of this service was (1) maintaining the service delivery in the context of an Audit life cycle of a site/application from development to rollout in production (2) maintaining the context and interaction between different agencies/users amidst rising volumes of constant interactions. This had raised the requirement for the Audit Status Monitoring System.

ABOUT AUDIT STATUS MONITORING SYSTEM (ASMS)

The ASMS is a role based workflow system, available on the https://security.nic.in for facilitating enforcement of the Audit policy and tracking the progression of a Request for audit from submission to Clearance for Hosting by all participating agencies throughout NICNET. This is an Intranet based system for authenticated and authorized users. Over the years it has evolved to include registered users to non-registered/IntraNIC users and emerged from targeting data center at IDC New Delhi to include other data centers on NICNET.

SALIENT FEATURES OF THIS APPLICATION

- Online submission of audit requests by registered/non-registered users.
- Tracking the status of audit of a site with Search facility and reports
- Maintaining the work schedule of Auditors
- Notification for Reports download, audit status etc. to users
- Generation of clearance note and notifying site coordinators and Data Centre Administrator

TECHNICAL FEATURES

- File System and Database based Report Archives
- Integration with LDAP authentication
- Implementation of role based access control logic
- Graphical Dashboards for statistical data
- E-Mail Integration
- Inclusion of a more consistent and uniform user interface giving a better UI navigation experience.

Audit State: Typically a request may be in the following states: Queued, Assigned, Accepted, Paused, Resumed, completed and Cleared.

The following roles are facilitated:

Auditor: is a professional auditor who takes up the tasks as per the scope of work laid down by Cyber Security division and is responsible for undertaking security audit of the web sites/applications. Report of vulnerability findings is uploaded and site coordinators notified for further remedial action through the system.

Site owner(SO) / State Web Coordinator(SWC) : is an NIC official who submits a request for security audit and is able to track the progress. The auditor's reports are used by

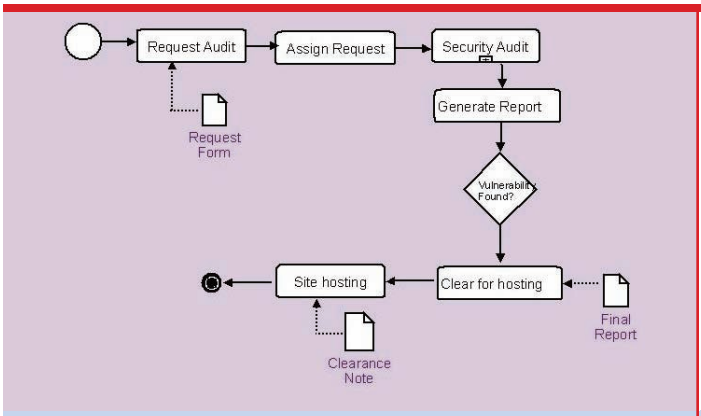

Fig. 1 Audit Process

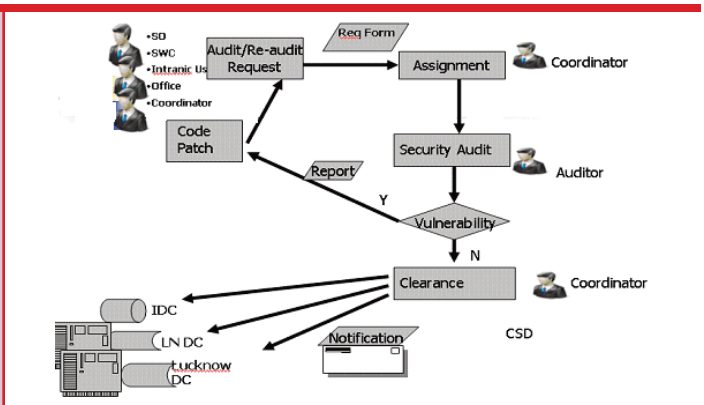

Fig. 2 Audit work flow and the interacting agencies

these roles for remediation if vulnerabilities exist. (Ref. fig. 3 below)

Coordinator: He maintains the flow among the different roles and reflects updates on the system as per action taken and other data keeping activities. Broadly the tasks undertaken include but not limited to Priority determination of audit requests, assignment to auditors, Sending report download notification to users, Generation of Clearance Note and notifying Users and Data Centers, Manage Auditor Work Schedule etc..

Data Center: The data centre administrator responsible for migration of the application from test server into production servers can access the information on sites cleared for hosting and the corresponding clearance notes. Data Centers in this role include Internet Data Center (IDC) Delhi, Laxmi Nagar Data Center (LNDC), National Data Center (NDC) in Pune and Hyderabad and other Data Centers (DC) in NICNET.

Other roles have been provisioned including Management for reporting purposes, SSL for SSL administrators of the common infrastructure providers, appsec monitoring, advanced monitoring, audit report review by users undertaking compliance check related activities, Office for entry of offline requests and moderation of direct online request. (Ref. fig. 4 below)

BENEFITS

- Helps site owner track the progress in audit of their relevant request
- Helps Coordinators keep track of context of the many requests flowing through the system from source to sink.
- Helps auditors to give due attention to the assignments as per priority information.
- The historical purview of Web Application Audit process of any web application hosted within NICNET domain can be ascertained with ease. If any new vulnerability is traced which is not reported in the Audit process, a performance depth analysis of Audit process activity can be carried out.

FUTURE ENHANCEMENTS

Incorporation of digitally signed clearance notes for issuance to the Data centers.

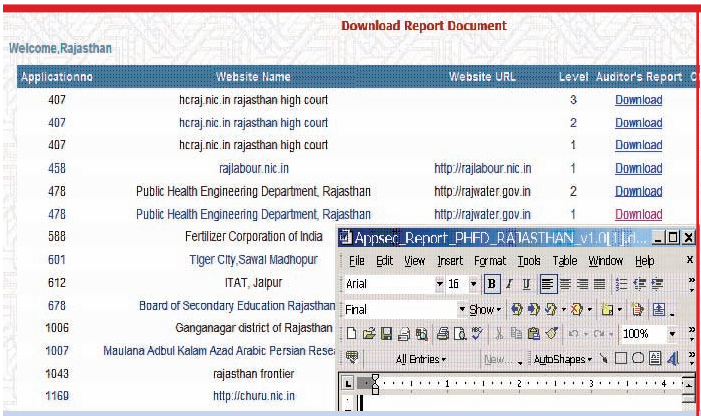

Fig. 3 State Web Coordinator Console

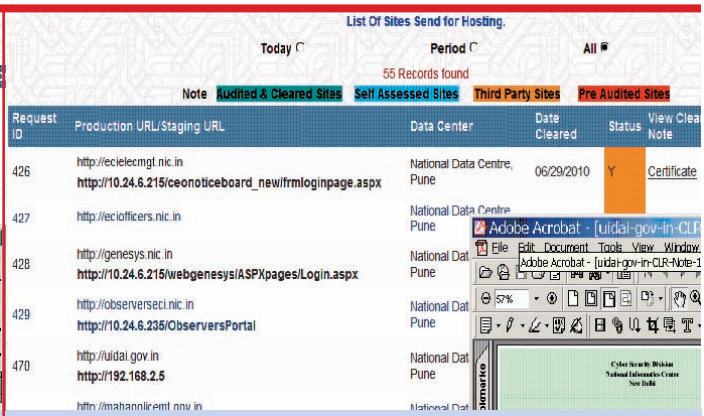

Fig. 4 DC console: View of Green sheet for site clearance