Chapter VIII
Timestamp Management and Application Security

Chapter VIII

Timestamp Management and Application Security

8.1 Gap in sequential numbers in database tables

System security

During analysis of database design of e-Procurement system, Audit observed that each table of the database contained a data field named "ID", which is a system generated sequential number[10] to each record in the tables to maintain uniqueness. As it is a system generated sequential number, there should not be any gaps between any two consecutive ID numbers except in the event of deletion of records, sequence failures due to server shutdowns/ restarts or transaction rollbacks.

Audit analysed the sequence of ID columns in ten important tables out of the total 742 tables in the database and found that there were 6.06 lakh records (IDs) missing in these tables. The numbers of missing records from these tables were as follows:

Table No. 10: List showing gaps in IDs in various tables

Sl No	Table description	Last ID in table	Total number of records	Number of times the gaps occurred	Number of missing serial numbers
1	User Master	87,621	87,105	186	516
2	User Certificate Master	1,75,307	1,73,718	805	1,589
3	User Login Logs	44,54,352	44,29,771	21,037	24,581
4	Tender Basic	84,384	79,588	3,287	4,796
5	Tender Master (Work items)	3,96,156	3,81,968	9,954	14,188
6	Bids details	18,24,643	18,22,882	1,508	1,761
7	Bank Transaction Details	6,66,989	6,66,766	70	223
8	History of Bank Transactions	27,01,771	21,91,022	21,238	5,10,749
9	Tender Fee Details	18,43,314	18,24,425	15,298	18,889
10	Decryption of bids	19,95,857	19,67,589	19,056	28,268
	Total	**1,42,30,394**	**1,36,24,834**	**92,439**	**6,05,560**

(***Source: extracted from e-Procurement database)***

The gaps between the sequential IDs of these ten tables ranged between 1 to 827. Gap of one in sequential ids can be explained due to server shutdowns / restarts; however, larger gaps indicated manual intervention at the back end of the system to delete records. The Department had not conducted a review of such deletion, and identified the root causes for the missing IDs. The existence of these sequential gaps raised doubts on the integrity of the database.

[10] Starting from one and incremented by one *i.e.,* if ID of first record is one, then ID of second record is two and so on.

In reply, Department stated (December 2023) that gaps had occurred during transaction failures in the events of network issues, users cancelling transactions, logical errors *etc.*

The response was not tenable, as the gaps were larger in size than would be expected with transaction failures. Audit examined these larger gaps and found that application logs were also missing for those periods (**details in *Appendix-II***), which indicated the material risk of manual intervention to modify data at the back end of the system.

8.2 Unreliable and incomplete user logs

As per SRS, every user is required to login to the e-Procurement portal using their username, password and Digital Signature for carrying out different activities. Therefore, the activities of users like tender creation, tender publishing, bid creation and submission by bidder, tender opening, and decryption and downloading of bids by department users *etc.,* should have corresponding user log record in the session login table. As both the login and logout time of the user were captured for all the user login session from 01 May 2017, Audit analysed the login records in the user login session tables for the period from May 2017 to March 2022 and observed that the above activities were carried out by the users where the log record about their logins were not available in the user login session table.

The major user actions which did not have associated user logs included the following:

1. Creation of tenders without log
2. Creation of bids without log
3. Submission of bids without log
4. Opening of bids without log
5. Decryption of bids without log
6. Absence of/ incorrect recording of IP addresses of users

These missing logs indicated the material risk of modification/ deletion of records through manual intervention at the back end of the system, and hence raised doubts on the integrity of the database and the procurement process as a whole.

8.3 Use of SHA1 instead of minimum SHA2

System Security

As per 'IT (Intermediary guidelines and digital media ethics code)– Rule 2021, Digital signature End Entity Rules 2015 – Rule 7, SHA2 was prescribed as the hashing algorithm for use in Digital Signature. Further, in view of the detected collisions in SHA1 algorithm, SHA2 should be used in the e-Procurement application.

During scrutiny of the application, Audit noticed that different hashes like password hashes, file name hash, file date hash, document hashes *etc.,* are calculated using SHA1 or MD5 algorithm. Even the digital signature process

in e-Procurement (GePNIC) is still using the SHA1 with RSA instead of SHA2.

Department stated (December 2023) that they are planning to use SHA512 hashing mechanism. The fact remained that there was lack of security in hashes.

8.4 Absence of provision for verification of digital signatures of bidders

System Security

IT Act 2000 Chapter-II Para 3 provides that in case of a person who authenticates an electronic record by affixing digital signature, any person by user of a public key of the person can verify the electronic record. This implies that important electronic records of an e-Procurement application, like – Tender Notice, Corrigenda, Tender Documents, Addenda, Clarifications to Tender Documents, Bids, *etc.,* should not only be electronically signed, there should also be provision in the e-Procurement application to verify the electronic signatures.

Audit noticed that in compliance to a query raised (November 2019) by STQC during their audit of the e-Procurement system, it was commented that electronic record can be verified using public key.
However, Audit noticed that NIC had not provided for verification of digital signatures by stakeholders anywhere in the application. Further, Audit observed during testing of e-Procurement system that during uploading of bid documents by the bidders, the system mandated digital signature by bidders. Audit downloaded bid documents submitted against 48 tenders from the e-Procurement system and observed that there was no digital signature affixed on any of the bid documents.

It was explained by NIC that the digital signatures were detached and stored separately in the system and there was no provision for Departmental users to verify these digital signatures of the bidders.

The absence of this provision resulted in non-compliance with the IT Act 2000.

The Department stated (December 2023) that the provision to verify the digital signatures would be implemented in future versions of the system.

8.5 Maintenance of logs

System Security

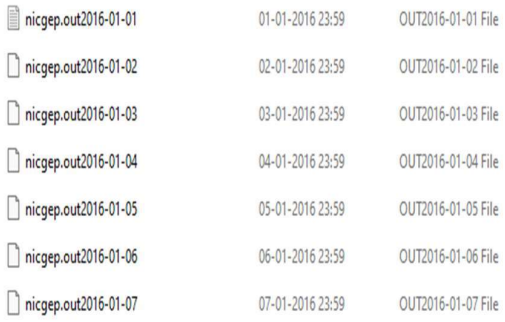
As per System Requirement Specification, a secure central logging server should be deployed for recording all the events in system and access to such central logging server shall be completely restricted for the system administrators. The server was to be synced with the International Time zone server and a log of these time synchronization details was to be maintained in the server. Logs shall be enabled for access methods of the servers (especially for production servers) and audit and log of activities referring to the operating system, access to the

system shall be maintained. Therefore, among other security logs, web logs[11], application logs[12], and DBA logs[13] are important.

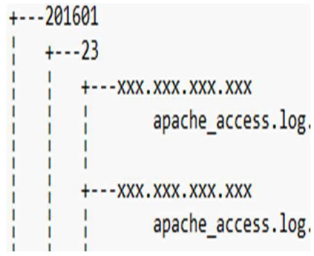
Department had furnished two types log data *i.e.,* web log (January 2016 to December 2022) and application log from (Jan 2016 to April 2022). Application logs collected during the whole day were taken to a file named after the same date with prefix 'xxxxx.out'. As an example, the log of 01 January 2016 is collected in the file "xxxxx.out2016-01-01 which is collected normally at the day end at 23.59 hours each day. Similarly, the web logs (apache web logs) collected were stored in log store in a folder named after the server address like 'xxx.xxx.xxx.xxx' which was in a date wise folder and the date wise folders were kept within a month wise folder named with year and month like '201601' for January 2016.

Figure 8: Extracted data from log files furnished by NIC

Application Log storage in file system



Web log storage in log store



Analysis of these logs revealed the following:

8.5.1 Missing logs

Application logging ensures that each application's logging verbosity is set to an appropriate level in order to provide appropriate information when needed for security review. Web logs captures visitors browser agent, date time of access, method, IP address *etc.,* for analysis in case of forensic investigation.

Analysis of web logs revealed that out of 2,556 days period *i.e.,* (from 01 Jan 2016 to 31 Dec 2022), log for 1,087 days were not provided to Audit as follows:

[11] Web logs contain traces regarding the activity of users while accessing the web pages like date and time, IP address, method, name of page (URL endpoint), browser agent, *etc.*

[12] Application logs contain traces of activity of user in the system like IP address, User ID, Module Name executed, timestamp of activity, other details like bid id, tender id *etc.*

[13] DBA logs record details of all back-end activities of the DBA user like modification, deletion, insertion of transaction or master records in the backend or changing the definition of table structures, functions, procedures, other configurations *etc.,* by using SQL statements or scripts.

Table No.11: Table showing Period of missing web logs

From Date	To date	Missing days
10-Nov-2018	16-Jun-2019	219
18-Jun-2019	25-Jun-2019	8
05-Aug-2019	26-Aug-2021	753
27-Mar-2022	10-Jul-2022	106
12-Jul-2022	12-Jul-2022	1
Total Missing days		**1,087**

(Source: Apache Logs provided by NIC)

Similarly, in the application log, it was found that out of 2,311 days period, there were missing logs for 27 days as follows:

Table No.12: Table showing Period of missing application logs

From date	To Date	Missing records
24-Feb-2016	24-Feb-2016	1 day
28-Sep-2016	28-Sep-2016	1 day
29-Jan-2017	29-Jan-2017	1 day
31-May-2017	31-May-2017	1 day
07-Jun-2017	07-Jun-2017	1 day
12-Jun-2017	12-Jun-2017	1 day
16-Jun-2017	16-Jun-2017	1 day
19-Jun-2017	19-Jun-2017	1 day
24-Jun-2017	24-Jun-2017	1 day
27-Jun-2017	27-Jun-2017	1 day
01-Jul-2017	01-Jul-2017	1 day
04-Jul-2017	04-Jul-2017	1 day
09-Jul-2017	09-Jul-2017	1 day
14-Jul-2017	14-Jul-2017	1 day
04-Feb-2018	04-Feb-2018	1 day
23-Apr-2020	24-Apr-2020	2 days
26-Apr-2020	26-Apr-2020	1 day
03-May-2020	03-May-2020	1 day
31-May-2020	31-May-2020	1 day
03-Aug-2020	03-Aug-2020	1 day
02-Mar-2021	02-Mar-2021	1 day
21-Mar-2021	21-Mar-2021	1 day
08-Jun-2021	08-Jun-2021	1 day
05-Sep-2021	07-Sep-2021	3 days
Total		**27 Days**

(Source: e-Procurement database)

This indicates that these logs were deleted. Due to missing logs, the objective to provide appropriate information when needed for security review could not be achieved and reliability of system was compromised.

In reply, Department stated (December 2023) that Apache web logs only contains the URL ends points with the client IP and browser agent. Application logs are critical. Due to technical glitch, few times application logs may not be generated and subsequently by the end of day (EOD) the problems were resolved and logs were generated. However, the fact remained that there are losses of critical logs to both application and web logs. It is pertinent to mention here that further audit process is hindered due to absence of logs as pointed out in ***Appendix-II***.

Further, Department stated (December 2023) that CERT-ln recommendation is 180 days for ICT logs retention period. In addition to that, few times back Odisha e-Procurement was running under the Odisha NIC Data centre. The reply is not acceptable as CERT-In recommended the minimum period 180 days for log retention and the logs generated during the period when application was hosted in Odisha server could have been maintained separately.

8.5.2 Non Maintenance of DBA Logs

As per infrastructure administration policy, all internal servers deployed at National Informatics Centre must be owned by an operational group (e.g. data centre) and/or administrators who shall be responsible for System Administration of these servers. Operational group or administrators should monitor implementation and compliance of policy tailored to their environment. All servers not under the direct ownership of the respective data centre, must be identifiable to a particular group and/or administrator. A secure central logging server should be deployed for recording all the events in system and access to such central logging server shall be completely restricted for the system administrators.

Audit requisitioned (August 2022) the DBA logs to the Department. As the system did not preserve DBA logs, the same could not be provided to Audit for analysis. In the absence of DBA logs, unauthorised access and modification of the data at the back end of the system could not be ruled out.

In reply, Government stated (December 2023) that the server log has been maintained for last 3 years but the transaction log is not maintained beyond a week due to shortage of space.

Recommendation

Government may consider to

- Enquire into the reasons for the gaps in the sequence of IDs in the major tables of the database;
- Implement appropriate application controls to enforce chronological and logical sequencing for user actions in the system;
- Ensure maintenance of web, application and DBA logs for the system.
- Adopt relevant standards specified by Ministry of Electronics and Information Technology, Government of India from time to time.