# Case study of Database security in Campus ERP System

Varang Acharya, Ph.D
Parul Institute of Engineering and Technology (MCA), Limda, Vadodara

Sweta Jethava
Parul Institute of Engineering and Technology (MCA), Limda, Vadodara

Adarsh Patel
Parul Institute of Engineering and Technology (MCA), Limda, Vadodara

## ABSTRACT
Database Security essentially refers to protection of the information content in database. In general, the decision regarding who should be allowed access to the databases or alternatively who should be denied access to the database is dictated by the security policies of the organization concerned. The implementation of ERP systems has been problematic for much organization because of one of the reason is lack of database security. The aim of this study is to identify the risks and controls used in ERP database access, with the objective to understand the ways in which organizations can minimize the business risks involved. In this paper are describe different types of vulnerability of database and Suggestions are offered in resolving the issues for database security in ERP system

## Keywords
ERP, Database Security, ERP Security Issues,

## 1. INTRODUCTION
Database security is the system, processes and procedure that protect a database from unintended activity. Unintended activity can be categorized as authenticated misuse, malicious attack or inadvertent mistakes made by authorized individuals or process. The main goal of database security mechanism is to protect the data stored in the database from unauthorized accesses or malicious action in general.

In this paper we are study on various departments in any technical educational institution (TEI), they are conducting the various operations from a central database and also maintaining accuracy and convenience of their database. But, every ERP system has two main parts: first one is hardware which can be called as infrastructure system which includes network, databases and computer peripherals including servers. Second one is software part is the data and information which flows through hardware. In both parts has so many failures possibility. Because of that, the both part resources might be fail and information can be corrupted and it can lead to ERP failure. In general, there are various types of failure conditions are handled by the systems and they make sure security of database. [1]

## 2. CASE STUDY OF EXISTING SYSTEM
Enterprise resource planning (ERP) systems integrate internal and external management of information across an entire organization—embracing admission management, student and staff information and attendance, leave and attendance management etc. ERP facilitates information flow between all student, faculties, management and academic functions inside the organization, and manages connections to outside stakeholders. [2]


Figure:-1 ERP System

Enterprise system software for campus that provides variety of academic functions for campus. Campus ERP software packages that offer the potential of integrating data and processes across functions in an enterprise. [3] Organizations who is utilizing the ERP System becomes vital organization because ERP consist of number of interrelated modules which helps the organization to built strong relations among all departments [4]. ERP is nothing but a simple software which provides web or desktop software like interface so the installation is quite easy for any organization as they have to install server software and need to configure the server to start utilization of the ERP software. [5]

## 3. SECURITY ISSUES IN ERP SYSTEM
ERP applications are very large and complex systems that consist of different components such as Database Server, Front-end, Web Server, Application server and other parts. This application relies on different hardware and software that can have vulnerabilities.

During the life cycle of a system, there are many threats of the system security. The system has possible no of security threats in that life cycle state situation. In the bellow describing all situations:

- Development:
  - Architecture
  - Program errors
- Implementation:
  - Architecture
  - Configuration

- Patch management
- Policies
- Awareness

- Control:
  - Policies
  - Security assessment
  - Awareness

This ERP application store data and any vulnerability in these applications will cause a significant monetary loss. Even though, people still do not pay much attention to ERP application. In this paper we are research and assessment all vulnerability of campus ERP Database security.

During the life cycle of a system, there occur certain situations which cause many threats to system security. The system is required to have certain security attributes in that situation. This relationship between conditions and attributes is depicted in figure 1. [1]

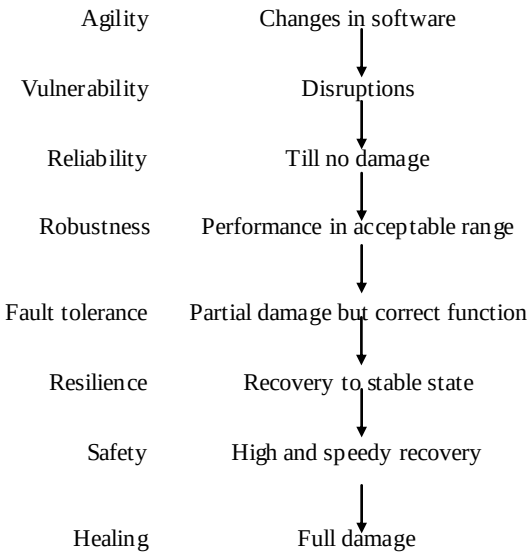


Figure 2: Relation between failure conditions and attributes.

## 4. VULNERABILITY FOUND FOR DATABASE SECURITY DURING CASE STUDY

In this paper we have studied one campus ERP system and to find database security problems of campus EPR system. We have also given the solution of the database security problems of ERP system.

Bellow describes all vulnerabilities found during the case study:

### 4.1 DEFAULT PASSWORDS AND ROLE FOR DB ACCESS

**Problem:** Each ERP module must have identify and implement appropriate logging and monitoring controls for its information assets. When default passwords for database access to all user that means to anyone can access to any data from the database. That was one security issue for ERP system.

**Solution:** In ERP Modules are accessible through network. But each user has own role and access right on each pages of ERP module. That was Non-public access systems are those which are available only after authentication or other special access process.

All remote access (wired or wireless) to non-public ERP information assets must:

- Be authorized and authenticated by use of a unique user identifier.
- Pass through a campus-approved access control device (e.g., a firewall or access server).
- Be made using an approved method (e.g. campus-authorized remote desktop service).
- Use a secure encrypted protocol

### 4.2 EXTENSIVE USER AND GROUP PRIVILEGES

**Problem:** ERP system is used by so many users. All user has own purpose to access ERP system. Here, important thing to whom one to access database for which purpose. How to tracked and logged following campus defined processes and must include information such as:

- Date of authorization
- Identification of individual approving access
- Description of access privileges granted
- Description of why access privileges granted

**Solution:** ERP system must identify the role of each user when they are logged into the system. EPR system must maintain the detailed log for the login process. Authentication controls must be implemented for campus information assets. Campus-defined controls must take into consideration:

- Validating user identity prior to granting access to system resources or data.
- Uniquely identifying users and their corresponding access privileges.
- Denying all access rights until rights is formally assigned.
- Detecting and warning about repeated failed access attempts.
- Allowing access rights to be promptly modified or revoked.
- Allowing authentication credentials to be regularly changed.

### 4.3 UNENCRYPTED SENSITIVE DATA

**Problem:** ERP system is collection of sensitive data. That is important to secure sensitive data from hacker or third person or public person. ERP system was not protect their information when data transforming in actual form. That was easy way to capture important data from ERP system. That was meaningless to maintained role and right module for protecting EPR system data. Current ERP System uses unencrypted data while login into system.

**Solution:** When encryption is used to protect ERP information systems, data, or network resources, the following minimum requirements must be met:

- Strong cryptography (e.g., Triple-DES, AES, etc.,) must be used.

There are two situations to hacked data:

1. Data in Transmit: One of the situation when data transfer from network must be using encryption measures strong to minimize the risk of the of the information's exposure if intercepted or misrouted.

2. Data in Storage: Second situation when data finally storage in database is again risks to the availability of that information, due to the possibility of encryption key loss. Because anyone can hack the database from the server and can easy to misused it. The solution is to storage encrypted data in database. That, means anybody want to get the data before they want to require decrypted it.

## 4.4 STORAGE OF UNENCRYPTED PASSWORD

**Problem:** Password in the ERP system are stored without any kind of encryption, if any user gets access to the database he/she can able to know the password of any user.

**Solution:** Encryption of password stored in the ERP database is one solution of hacking password from the database. In short only one time encryption used for password storage. So that there is no one possibility for password hacking.

## 4.5 LACK OF MISS CONFIGURATION NETWORK ACCESS

**Problem:** (1) In current system there is lack of system configurations. The main feature is directory listing is enable for the all directory, so there is major threat that users can able to know the file name of all files stored inside the directory and subdirectory. (2)Another point is website is hosted using http protocol only so the transmission of data is without any kind of encryption.

**Solution:** (1) Directory listing is major threat for any website application. Because this website storing listing directory is always set as an enable for all users. So, this problem solution is to set a website storing directory as a disable to listing for all users. (2) This problem solution is security connection by SSL. If you're entering sensitive personal information on a page, look for a pad lock icon on the status bar of the browser

## 4.6 LACK OF PASSWORD LOCKOUT

**Problem:** If someone not working on system after login their account. There is troubleshooting situation because, the person is may be present or not. In case person has just logged into the system and got an urgent call and moved out of office at that time someone from their staff can misuse their account.

**Solution:** The solution of this problem is to set login account automatically logout when application is ideal situation. Otherwise to set automatically logout the system when starts screensaver.

## 5. Vulnerability Assessment

During the case study we have discuss major database security vulnerability for ERP database. All of the security procedures and technologies currently available cannot guarantee that any systems are safe from intrusion. Intrusion detection systems warn you of malicious activity. However, the success of each of these technologies is dependent upon a number of variables, including:

- To maintaining ,configuring, monitoring technologies by the expertise of the staff responsible
- To update and patch the services for quickly and efficiently.
- To keep constant awareness over the network.

Security administrators are only as good as the tools they use and the knowledge they retain. Take any of the assessment tools currently available, run them against your system, and it is almost a guarantee that there are some false positives. Whether by program fault or user error, the result is the same. Base on the vulnerability assessment methodology we have define these six vulnerability level.

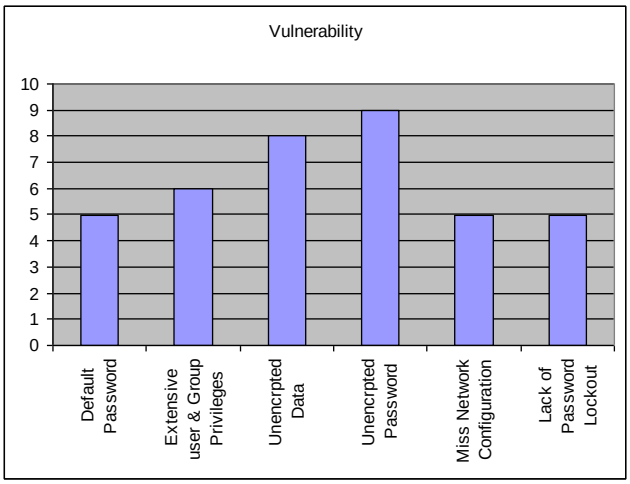


Fig: 3 Vulnerability Level

## 6. CONCLUSION

Although, vulnerability assessments of Campus ERP are necessary as system security functions, they are not sufficient to protect system from all security threats. Both measures should be included in a more comprehensive security strategy that includes security policy and procedure controls, network firewalls, strong identification and authentication mechanisms, access control mechanisms, file and link encryption, file integrity checking, physical security measures and security training.

A simple approach to data protection looks the various layer of security that can be applied. This approach includes activization of protective mechanisms of DB, protection of server, workstations, a local area network, and use of cryptography. The structured approach to protection of a DB is more expanded and includes, except positions of the simple approach, the following:

Researching, studying and advising agencies of IT vulnerabilities and devising techniques of the cost-effective security and privacy of sensitive federal system.

Data is under constant attack from a growing number of sources. It's vital to know what data you have, how sensitive that data is, how critical it is to corporate mission and the risks it faces. Perform a risk analysis and once the role has been determined, assign appropriate role to the each end users of the ERP. Only by being aware of your valuable assets can you properly monitor and protect them.

## 7. ACKNOWLEDGMENTS
We are thankful to the faculty and experts who have helped us to prepare research paper. We are also thankful to administrator of the ERP cell who helped us to know the ERP system in details.

## 8. REFERENCES
[1] Goel, Shivani, Ravi Kiran, and Deepak Garg. "Vulnerability Management for an Enterprise Resource Planning System." arXiv preprint arXiv:1209.6484 (2012).

[2] Molnár, Bálint, and Gyula Szabó. "Information architecture of ERP systems at globalised enterprises in a small EU member state." Information Technology Interfaces (ITI), Proceedings of the ITI 2011 33rd International Conference on. IEEE, 2011.

[3] Adam, Rubina, Paula Kotzé, and Alta Van der Merwe. "Acceptance of enterprise resource planning systems by small manufacturing enterprises." (2011).

[4] Shaul, Levi, and Doron Tauber. "CSFs along ERP life-cycle in SMEs: a field study." Industrial Management & Data Systems 112.3 (2012): 360-384.

[5] Khosrowpour, Mehdi, ed. Emerging Trends and Challenges in Information Technology Management: 2006 Information Resources Management Association International Conference, Washington, DC, USA, May 21-24, 2006. Vol. 1. IGI Global, 2006.