CHAPTER 10

SQL Injection Attacks in Web-Based and Mobile Applications: Challenges, Detection Techniques and Effect on Sustainable Development Goal 4 (Quality Education)

Gauri Thite Patil and Mahesh Potadar***

ABSTRACT

The United Nations agenda 2030 for Sustainable Development Goal - Quality Education (SDG 4) which aims to "Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all". In the era of digitization almost all education platforms are digitized so as to provide Online Education Platforms. To provide the user-centric and customized experience to the users, the Web / Mobile applications stores the user information (Personal, Educational, financial etc.) in the databases. These Applications are vulnerable to the Cyber Attacks. The most common and dangerous attack on the databases is SQL Injection Attack (SQLi). In SQLi, attacker inserts malicious code into input fields and manipulates SQL Queries to get database access. Once attackers gain unauthorized access, the data may be compromised. The serious threat of SQLi could lead to data/financial loss, access denial, data alteration and may hamper reputation of the organization. Misuse of data creates trust issues in online learning platforms and may results into distrustfulness amongst the users. Further this could lead to reduction in the engagement of digital learning platforms. This paper focuses on SDG 4: Quality Education and impact of SQLi on online education systems /providers, various Detection mechanisms to detect SQLi Attacks and challenges in detecting SQLi Attacks.

Keywords: Sustainable development goals; SDG 4; SQLi; SQL injection; Unauthorized access; Modification/deletion of records; Cyber-attacks; Digital learning.

1.0 Introduction

Sustainable Development Goals (SDGs) are adopted by United Nations and it ensures that by the end of Year 2030 all people will enjoy peace and prosperity.

**Corresponding author; Assistant Professor and Research Scholor, IT Department, BPHE Society's Institute of Management Studies Career Development and Research, Ahilyanagar, Maharashtra, India (E-mail: gauri.patil28@gmail.com)*

***Associate Professor, IT Department, BPHE Society's Institute of Management Studies Career Development and Research, Ahilyanagar, Maharashtra, India*
(E-mail: maheshpotdar12345@gmail.com)

There are 17 integrated SDGs goals designed for the sustainable future for all by 2030. One among the 17 SDGs is "Quality Education (SDG No.4)". The agenda of Quality Education is to "Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all". While achieving this goal, the key focus is:

- To provide free primary and secondary education to all.
- To increase literacy
- To promote digital literacy and technical skills
- To give equal access to all for affordable Higher Education, Technical Skills and Vocational Skills.

We all know that COVID- 19 affects every industry including Education Industry. A new door of "Online /e – education" is introduced to the world. Almost all the educational things are digitized using various platforms like e-learning tools, Online Exams, Online Lecture series, admissions, exam evaluation, results, fees payment, regular classes were conducted online.

Various e-platforms like Google meet, Zoom, google-classroom are introduced with the help of which education of lacks of candidates continued in a smooth way, while sitting at home. Online, video based platforms, which gives the students the feel of actual classroom teaching. Educational Institutes/colleges/schools/organizations created their online existence using websites, Web/Mobile applications, Portals, using which the users can access the study materials, give tests, submit assignments, check the result, search resources etc.

To give personalized experience to the users, the online platforms gather the personal and other information of the users and store it in the database on servers or clouds, for further use. Huge no. of records are stored in the databases of the Institutes/ universities/organizations and digital learning platforms. And here comes the threat of Cyber Security.

One of the most common but dangerous cyber-attack on the Web and Mobile Applications is SQL Injection Attack (SQLi). In this type of attack, an attacker injects malicious SQL code through the input fields such as Text Boxes, Search Boxes, login forms where the user enters their credentials. Once the attackers gets unauthorized access to the data/ records from the database, they can either by modifying or deleting it which may results in a huge financial loss and /or loss of reputation to a firm or company providing online Education.

Trust issues may be developed among the current and prospective users of the system due to the leak of personal and financial data due to cyber-attack. The companies may have to bear huge financial loss due to loss of reputation and sometimes due to paying compensations for the customer loss or because of paying the ransom amount to the attackers for getting back the data access.

2.0 How SQLi Attack Works

A SQLi Attack generally has following workflow:

- Identification of sensitive or vulnerable inputs
- Designing of SQL Query for injection
- Bypassing the application securities
- Execution of the injected malicious SQL Query
- Retrieving / manipulating data or information
- Make most of the use of database server weaknesses

3.0 Online Education Platforms/System and Impact of SQLi Attack on it

In the digital era, almost all the information regarding the users, their evaluations, question paper, study material, fees payment details, personal information is stored in the database. The attacker's main aim behind SQLi Attack is to gain unauthorized access to the database of an application. After gaining unauthorized access the attackers may delete records / modify records or some portions of records, delete whole database(s) or they can even deny the database access to the owners. Attackers may charge huge amount of money /ransom to regain access to the database.

- *Data Manipulation:* The attackers may delete or modify the records or even destroy the database after gaining unauthorized access to the database.
- *Denial of Service Attacks (DoS):* The attackers may lock the database and deny access of the database/records to its owners the database or records, after a successful SQLi attack.
- *Data Breach:* The attackers can retrieve sensitive information like personal information, financial reports, login or other important credentials of the users once they got unauthorized access to the database through SQL Query (SQLi). Such type of privacy violation may cause a huge financial and reputation loss to the company.
- *Damage to the reputation:* Educational Portals / Web Applications/ Mobile Applications stores the user information which may include financial, personal and/or other data. When the Attacker's gain unauthorized access to the database / records of the Company /organization/institute, the access of the same may denied to the owners / company. In such cases the company may face huge damage to its reputation and may have to face legal issues due to violation of privacy policy, if the user information is leaked to the outside world. Such Cyber Attack incidences may create trust issues among the students/users of the Application which may affect the reputation of the educational organization/ company/institute.

- *Compromising Systems and servers:* By getting unauthorized entry into the database, attackers silently keep trying to gain unauthorized access to the other parts of the database like server, operating system, and other applications like payment gateways, bio matric authentication files etc. and may delete the database(s), corrupt the OS or forcefully shut down the Servers.
- *Financial Loss:* Attackers may steal the personal and other stored details of users/employees and other stakeholders of the system from the database with the help of SQLi Attack and leak or lock the access to the records. Attackers may demand huge ransom amount to give the database access back to the company and/or company may have to pay the compensation for "Leak of Private Information / Violation of Privacy Act" of the users. In such cases the company will be in huge financial loss if the legal actions are initiated against them.
- *Bypassing Authentication:* Once the malicious SQL Query is injected through the application's input fields, security measures are compromised and attackers may gain access to admin privileges, database servers and operating system etc.
- *Entry for future attacks:* After gaining access to the database, attackers can further gain unauthorized access to the database server, Third Party Applications, operating system etc. and can damage the entire system which may cause severe security issues.

4.0 Detection Techniques for SQLi

One of the main reasons for cyber-attack /Cyber Security Threat is the poorly written code. Poor coding practices make the applications more vulnerable for cyber-attacks. Buffer overflow, no or partial Data Encryption, cross -site scripting etc. make the applications vulnerable for cyber-attacks. Some preventive measures, if applied properly can help in minimizing /preventing the cyber – attacks. Following are some SQLi Attack Detection methods:

- Database Activity Monitoring (DAM): Continuous monitoring of the Application Log for suspicious queries can help in early detection of SQLi Attack. Generally, the queries which needs access of admin rights, deleting of the entire database/table (drop table) might contain malicious code.
- Static Analysis of Source Code method: In this type of detection method Source of the Application is analyzed statically i.e. without executing the source code for the untrusted query inputs. Here the URLs, form inputs are analyzed.
- Dynamic Analysis: In this type of detection, the applications are analyzed at runtime i.e during the execution of the application. Here the queries sent to the database for accessing data are monitored and analyzed.

This helps in real time attack detection.

- Machine Learning Based Approach: This is a modern approach for detecting the SQLi Attacks. Machine learning model helps in identifying whether the queries are normal or malicious.
  Supervised Learning Methods: In this, common algorithms like decision trees, logistic regression, random forest, Support Vector Machine (SVM) are used.
  Deep learning methods: In this, the methods like LSTM (Long Short-Term Memory), CNN (Convolutional Neural Network), RNN (Recurrent Neural Network) are used
- Signature-based Detection: This method identifies malicious activity by comparing network traffic or file data against a database of known threat signatures. e.g. attack patterns, unique byte sequences, hashes. This method allows rapid detection of known vulnerabilities or malware. It is like a Digital Fingerprint Scanner. But the limitation of this method is that it checks against a known attack patterns (e.g., UNION SELECT,' OR 1=1).
- Use of Web Application Firewalls (WAF) for detection: Web Application Firewalls plays an important role in protecting Web Applications from potential cyber threats and attacks such as SQLi, Cross-site Scripting (XSS) etc. Web Application Firewalls continuously monitors and filters the HTTP traffic between the Internet and a Web Application. Thus, helps in detection of the SQLi attack. OWASP ZAP, Tulpar, SQLMate, TheDoc, SQLMap, Whitewidow, Pybelt, etc. are some of the popular SQLi Scanners available in the market.
- Continuous monitoring of database logs: To monitor any SQLi Command intrusion for attacks on Web/Mobile Applications, Intrusion Detection Systems (IDS) should be used. IDS helps in monitoring the log activities related to database for any suspicious or malicious entry using SQL.

5.0 Challenges in Detection of SQLi Attack

It is very critical to detect SQLi Attacks. Following are some of the key reasons/ challenges while detecting SQLi Attacks:

- The attack techniques are continuously changing,
- The positive-false ratio is very high
- Dynamic & Complex Web Applications
- Dataset Imbalance (For ML-Based Detection)
- Zero-Day SQLi Attacks
- Bypass of Web Application Firewalls (WAF)

6.0 Conclusion

Post COVID, every industry including Education System become highly dependent digital or Online resources. Various Online Platforms are used by various stakeholders for performing day-to-day tasks. Education Sector is also witnessing the same revolution by adopting digitization. The Sustainable Development Goal (No. 4) i.e. "Quality Education" which aims "Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all".

To achieve this goal, in the era of digitization, education institutions/organizations /companies are dependent on Web / Mobile Applications, digital libraries, LMS (Learning Management System), various e-Learning platforms. The first step to achieve "Quality Education" is to avail universal Primary and Secondary education to all. E-Learning/digitization helps in providing Quality Education to the various stakeholders i.e. "anyone can learn from anywhere". But this online existence comes up with a common but equally dangerous Cyber Security Threat i.e. SQL Injection Attack. SQLi can cause data breach, misuse of personal /financial information, financial loss, reputation issues. The Web / Mobile Applications, having poor or less security measures are more vulnerable to the SQLi. Early detection of SQLi Attack can help in reducing potential SQLi attack threat.

References

1. Global Goals – Industry, Innovation and Infrastructure. (n.d.). *Goal 9: Industry, innovation and infrastructure*. Global Goals.
2. United Nations – Infrastructure and Industrialization. (n.d.). *Industry, innovation and infrastructure*. United Nations.
3. SEI Journal Article. (n.d.). *Journal article*. SEI Journal.
4. IEEE Xplore Document 9491117. (2021). *Conference paper/document*. IEEE Xplore.
5. SQL Injection PDF – Montana State University. (n.d.). *SQL injection*. Montana State University.
6. SQL Injection Attack PDF. (n.d.). *SQL injection attack*. Research Publish Journals.
7. Geeks for Geeks – Types of SQL Injection. (n.d.). *Types of SQL injection (SQLi)*. Geeks for Geeks.
8. Splunk – SQL Injection. (n.d.). *What is SQL injection?* Splunk.
9. Contrast Security – SQL Injection Glossary. (n.d.). *SQL injection*. Contrast Security.
10. Bright Security – SQL Injection Attack. (n.d.). *SQL injection attack*. Bright Security.
11. eSecurity Planet – Prevent SQL Injection Attacks. (n.d.). *How to prevent SQL injection attacks*. eSecurity Planet.
12. AltexSoft – ORM Tools. (n.d.). *Object-relational mapping tools*. AltexSoft.

13. Cloudflare – Web Application Firewall. (n.d.). *What is a web application firewall (WAF)?* Cloudflare.
14. Pentest-Tools SQL Injection Scanner. (n.d.). *SQL injection scanner online*. Pentest-Tools.
15. Acunetix SQL Injection Scanner. (n.d.). *SQL injection scanner*. Acunetix.
16. Linux Security Expert – SQL Vulnerability Scanners. (n.d.). *SQL vulnerability scanners*. Linux Security Expert.