Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 12, December-2020

Web Application Safety by Vulnerability Assessment and Penetration Testing using SQL Injection Techniques

Puja Rai, Pema Dorjee Lepcha, Zening Biswakarma, Shadew Rai, Sukman Subba, Arvind Lal
Centre for Computers and Communication Technology

***Abstract*- Today's world is largely dependent on the internet; global internet users are growing more rapidly. People are more developing their skills and getting advanced in every field using internet. In the same time SECURITY has become the major issue of the internet. Sharing data from the wireless technology can be easily breach the security by hackers and access their confidential data. Vulnerability Assessment and penetration testing is a solution for problem to overcome. A Vulnerability Assessment is the process of defining, identifying the vulnerabilities. A Penetration Testing, is a process to attack in a computer system or network with an authority to evaluate and analyze the computer and network security. The purpose of this testing method is to fix the loopholes and secure the data from the skilled hackers. In our project we are going to show one of the web hacking technique i.e. SQL injection.**

1. INTRODUCTION

We know that everyone is interacts with the internet. Our world is transforming into a digital world where the security problem is increasing rapidly. Managing security is the big task where we have to stay alert in every step against our opponents well known as attackers or hackers who are highly technically skilled using different methods and techniques to exploit their targets confidential data and information without breaking a glass. To run a successful business computer is playing the most vital role in today's date. Having a computer system is not enough, they need to be connected with a network to facilitate with external business. Without internet hacking cannot take place, every year cybercrime is increasing at a high rate and cost many organizations millions of dollars every year. To solve this hacking problem ethical hackers are introduced who knows about assessing the security of a computer system and ultimate security professional. They are employed by companies to penetrate the network and computer system by aiming to fix the vulnerabilities. In our project we are going to do SQL injection vulnerability assessment which is one of the common web hacking techniques that might destroy our database.

2. PROBLEM STATEMENT

To study the different types of vulnerability scanners and pen testing techniques. To find and solve the vulnerability of web application by using one of the hacking techniques.

3. PROPOSE METHODOLOGY

Vulnerability Assessment and Penetration **Testing** (VAPT) helps an organization to increase the security of web applications, website or network, in our methodology to protect the data of web application from the third party we are using a SQL injection technique.

3.1 VULNERABIULITY ASSESSMENT

Vulnerabilities are an open door which leads to threat and exploit the data occurring unexpected events. Vulnerability is a security bug, flaws, errors, fault, holes, or weakness in software that is a big opportunity for attackers to exploit the system. A vulnerability assessment is the process of finding the open doorways or vulnerabilities in the systems. In order to perceive the vulnerabilities, vulnerability assessment demand to operate automated testing tools. These tools help to expose the weakness of the systems and suggest the remedies of the problem.

3.2 PENETRATION TESTING

A penetration testing is also known as pen testing, and testers are known as pen testers, penetration testers, or ethical hackers. Pen testing is the cyber-attack against the computer system accessible vulnerabilities with permission and to increase security solution. This testing is about to know how far the attackers can breach the security system. This testing is done after the vulnerability assessment to expose the weakness of your system which gains unauthorized access.

3.3 CYBER SECURITY

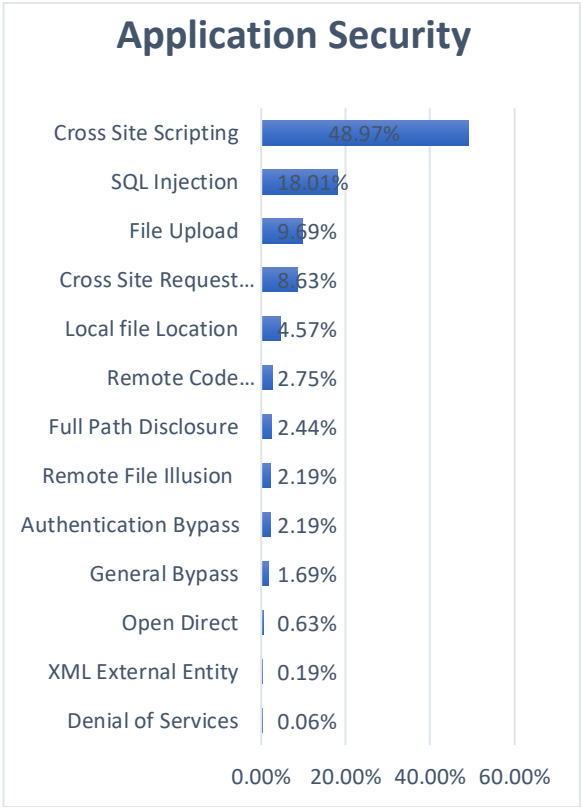
Cybercrime is a global problem that is being dominating the new cycle. It possesses a thread to individual security and even bigger thread to large international companies, banks, or government. Cyber security is a technique that is designed to protect the digital data, the digital data that which deal with daily basis. There are many categories under cybersecurity, but in this paper, we are just concerned about application security.

3.4 Web Application Vulnerabilities

As the advancement in web application and other technology have changed the way we do business or the way we do access and share information, but with all of this advancement and web application have also attracted malicious hackers and scammers because just like in any industry there is money to be gained illegally in this industry as well. This led to birth of web application security. Web application security is simply nothing but practice of protecting websites and other online services against different security fetch that exploits loopholes that are

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 12, December-2020

present in applications code. So, organizations who are failing to secure web application run the risk of being attacked and this is mostly due to vulnerabilities which are present in web application, and with help of these loopholes or vulnerabilities attackers can easily manipulate web application and do whatever they want with them. For example, let's consider word press, if we consider word press vulnerabilities, SQL injection vulnerabilities are the second most common loopholes vulnerabilities found in word press after cross site scripting, while cross site scripting or XSS is also another popular kind of web application vulnerability, and SQL injection is the second most popular one. So, SQL injection is one of the common and dangerous type of attack that they're on internet. A successful internet attack can result in confidential data being deleted, lost, or stolen, websites being defaced, unauthorized access to systems and ultimately compromising individual machine and sometimes entire network as well.



Application Security is a process for protecting software, hardware, and procedural methods applications from external threats.

3.5 SQL INJECTION

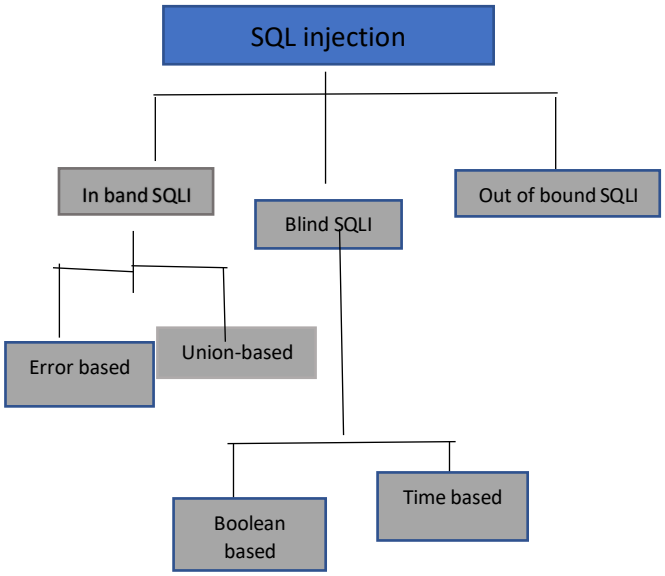
SQL query language or SQL is a language which is designed to manage and manipulate data in a database. SQL Injection attack is a type of cyber security attack that targets these databases using specifically crafted SQL statements to trick the systems into doing unexpected and undesired things. So by leveraging and SQL injection vulnerability present in web application or website gibing the right circumstances an attacker can use it to bypass web application authentication details as in , if you have login and password an user can or attacker can enter just the user id, skip the password entry and get into the system, or it can sometimes retrieve the content of entire database. They can also use SQL injection vulnerability to add modify and, sometimes delete record in the database affecting data integrity. Well using the vulnerability an attacker can do unimaginable things. This exactly shows how dangerous SQL Injection can be.

3.5.1 IMPACT OF SQL INJECTION ATTACK

There are number of things that an attacker can do when an exploiting SQL injection on a vulnerable website.
Firstly, he can access data without authorization. **Example:** by tricking the database into providing too many results for a simple query, then he can extract sensitive information, social security numbers, or credit card details.
Next thing he might somehow get in touch with authentication of users registered on website and then he can use the information to login during other attacks. He can also alter data in database without authorization**. Example:** he can create fraud Ent records or extra users or he might actually delete the entire table.
And attackers can actually control application behaviors that based data in the database. **Example:** by tricking an application into allowing a login without a valid password which we solve or assured how using SQL injection attack you can bypass an authentication mechanism or you can avoid password verification.

3.5.2 CATEGORIES OF SQL INJECTION ATTACK

SQLI injection can mainly classified into three categories.



TYPES OF SQL INJECTION

(a) Error Based - Its type of In-Band SQL attack. It is a technique that relies on error massage thrown by a database server to obtain information about the structure of the database. Here attacker will relies

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 12, December-2020

on the error message send by the database server to manipulate the database.

(b) Union Based – In this attacker will use union SQL operator to combine the results of two or more statement into a single result and this result is return as a part of http response.

(c) Boolean Based – Here no data is transferred by web application and the attacker will not be able to see the result of an attack. This is the first type which is Boolean based. So, when SQL query fail sometimes some part of page disappear.

These indications allow attackers to determine whether input parameter is vulnerable & whether it allows attraction of data. This attacks are very slow specially on large database.

(d) Time Based – In some cases even though vulnerable SQL query it does not have any visible effect on the output of the page it may still possible to abstract information from an underline database. Hacker determine this by instructing the database do weight or sleep a stated amount of time respond. Basically here if there is no visible output from the database server the attacker will ask the entire database to sleep for a while if the page is non - vulnerable it will load quickly. It is vulnerable it will take longer than usual to response the query.

CONCLUSION

SQL injection is one of the most common and more effective forms of attack on a system. A web developer is still facing the challenge for control the malicious SQL Code/script on the web application and maintaining the end privacy

Data security is one of the most important topics in the jail digital world. Where everyone's privacy matters. These issues must be considered seriously by the web developers involved in developing websites using databases.

REFFERENCE

[1] Irfan Yaqoob1, Syed Adil Hussain2, Saquib Mamoon3, Nouman Naseer4, Jazeb Akram5, Anees Ur Rehman6, "Penetration Testing & Vulnerability Assessment", Volume: 7 issue: 8 | August-2017.

[2] Gurline Kaur1, Gurpreet Kaur2, "Penetration Testing: Attacking oneself to Enhance Security", Volume: 5 issue: 4| April-2016.

[3] Jignesh Doshi1, Bhushan Trivedi2, "Comparison of Vulnerability Assessment and Penetration Testing", volume: 8, No.6 April-2015.

[4] Chanchala Joshi1, Umesh KumarSing2, "Security Testing and Assessment of Vulnerability Scanner in Quest of Current Information Security Lanscape", Volume: 145, No.2, July-2016.

[5] Korra manasa1, L. Venkateswara Reddy2, "Designing a Web Application & Detecting Vulnerabilities using Vega Vulnerabilities Scanner" Volume: 5, Issue: -8, pp-227- 232(2016),

[6] Pawan Kesharwani1, Sudhanshu Shekhar Pandey2, Vishal Dixit3, Lokendra Kr. Tiwari4," A Study on Penetration Testing using Metasploit Framework", Volume: 05 Issue: 12 | Dec-2018.

[7] Leena Jacob1, Virginia Mary Nadar2, Madhumita Chatterjee3, "Web Application Security: A Survey" Volume: 7(1), 2016.

[8] Kyle Coffey1, Richard Smith2, Leandros Maglaras3, Helge janicke4, "Vulnerability Analysis of Network Scanning on SCADA System", Volume: 2018, Article ID 3794603, 21 pages, Published 13 march-2018.

[9] Martin Tomanek 1 Tomas Klima2, "penetration testing in Agile software development project" Volume:5 No,1march-2015.

[10] Gitanjali simran T1, Sasikala D2, "Vulnerability Assessment of Web Application using penetration testing" Volume :8, issue:4Nov-2019.

[11] Grusha Kaur Sahni1, Rabindranath2"VSTAAS-An Integrated Pen-testing tool" Volume:9, Issue2, Dec2019.

[12] Jai Narayan Goel1, BM Mehtra2," Vulnerability Assessment and Penetration Testing as a Cyber Defense Technology," Procedia Computer Defense Technology, Volume 57,2015, Pages 710-715.