International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 11 | Nov - 2021 ISSN: 2582-3930

SQL INJECTION ATTACKS

AUTHOR NAME: SAKSHI SAKPAL

INSTITUTE NAME: KERALEEYA SAMAJAM MODEL COLLEGE , DOMBIVLI

1]ABSTRACT

SQL injection attack is widely used by attackers to gain unauthorized access to systems. This software system is developed to prevent unauthorized access to system using SQL injection attacks. This is done by adding unique value and a signature based authentication technique to verify authenticity. SQL injection is a major security issue these days that allows an attacker to gain access of a web system or application exploiting certain vulnerabilities. This method exploits various web application parameters such as transmitting the traveling form data parameters with an efficient integration of amino acid codes aligned in it

KEYWORDS: SQL INJECTION , DATABASE , SQL, DATA LEAKS.

1] INTRODUCTION

In this era, websites have become the most essential part in our lives. Among the top most security threats SQL Injection Attack ranks top based on OWASP[1] Top 10 security vulnerability report. Through these websites we insert number of Personal data which gets stored in the database. We can access it from anywhere using network. This opened the gate for The attackers to grab those data from vulnerable web pages. To find those vulnerable web pages the attackers can find. Many efficient tools like botnet [2] which generate the list of vulnerable web pages.

2] OVERVIEW OF SQL INJECTION

2.1 Terms :SQL stands for structured query language which must be pronounced as se-qual. This language is mainly developed for interacting with the relational database. For data

manipulation, Query is used to insert data, modify the database, to access the required data alone. Here comes the injection which is done through SQL query under data manipulation

2.2 Purpose of attack :This attack is done based on two tasks. One is to gain benefit out of grabbing others sensitive data and another one is to test the knowledge i.e. curiosity in learning new tasks and try to prove them.

2.3 Processing steps :Attacker finds out the vulnerable web pages with the help of some predefined tools. Through those webpage manipulation HTTP request is send to the database where injected query try to get privileges for data manipulation

2.4 Consequences :The consequences are very high since the database consists of sensitive information. We can categorize the cost based on Authorization, Authentication, Data Confidentiality and Data Integrity.

2.5 Classification :The attack is classified based on the attackers intention, vulnerabilities and asserts. Based on intention of the attacker we can have a classification in their goals.

2.5.1 Goals

i) To extract data – Sensitive data will be grabbed by the attacker. Suppose if admin database is hacked the entire database becomes vulnerable.

ii) To access data – They try to break the privileges and get access to the entire database and try to manipulate the data.

iii) Finger print the database- In this attack, database version and its type will be derived out by the attacker. This attack Help them to try different type of queries in different application.

iv) Injectable parameters are found – using some of the automatic tools the vulnerable parameters will be found for attack.

v) Authentication Bypass –application authentication mechanisms will be bypassed to enter inside the database.

vi) Database schema identification – From the database table name, data type of each field, column name, etc. will be retrieved to gather information .

vii) To perform denial of service – Dropping table and system shutdown falls under this category. Attacker tries to intrude inside the system to

perform some specific instruction within the database

2.5.2 Vulnerabilities

i) Improper validation done in a webpage leads to exploitation
ii) Privileged access for particular account

2.5.3 Asserts

i) Database fingerprint
ii) Schema
iii) Data
iv) Network

3] TYPES OF SQL INJECTION ATTACKS

There are numerous SQL Injection attacks and it is performed sequentially or in combinatorial. Table-1 shows examples

For each types of attack and its illustration is given below.

Tautological attack:

Result – authentication page is bypassed for data extracting

Tricks applied – 'where' clause in SQL tokens is injected to make the conditional query remains true

Union Query:

Result – Different dataset is returned from the Database

Tricks applied – SQL Injected query remains safe by joining the keyword 'union'

Illegal/Logically Incorrect Queries:

Result – Error message with useful debugging information

Tricks applied – By cause injects query with type mismatch, syntax error, logical errors

Piggybacked Queries:

Result – multiple queries are executed without the knowledge of the user which may lead to Database exploitation

Tricks applied – injected queries are added to the normal executable query

Inference:

Result – different responses from database is cross checked by changing its behavior.

Tricks applied – True/False questions using SQL statements is asked in serious (Blind attack). Based on time delay

injected SQL queries are executed using if/then statement (Timing attack)

Stored procedure:

Result – remote commands, denial of service is performed

Tricks applied – Injection is done to the stored procedure present in the Database

4] DATA & RESULT

Mostly intermediate layer is used to accept input from the user through web application. To build this layer scripting Languages are used. So to exploit the database attacker uses SQL Queries. To confuse this layer SQL Queries are reshaped by the attackers. In this paper we have focused on those reshaped SQL Queries. We have discussed about SQL

Injection attack and its various prevention and detection mechanisms used before and after 2011. We can conclude that even there are more number of security measures developed there are

S.No	SQL Injection Attack Types	Purpose	Example Code
1	Tautologies	Bypassing authentication	Select * from userdet where uid='abcd' and pwd ='a' or **'3'='3'**
2	Union	Extracting Data	Select * from userdet where uid='' **union** select * from details -- and pwd='a';
3	Illegal/ logical incorrect queries	Identify injectable parameters	SELECT * FROM students WHERE username = **'ddd"'** AND password =
4	Piggybacked Queries	Extract different dataset	SELECT Rno FROM St WHERE login = 'abc' AND pass = ''**; DROP table St --'**
5	Inference	Determining Database Schema	SELECT name, email FROM members WHERE id=1; **IF SYSTEM_USER='sa' SELECT 1/0 ELSE SELECT 5**
6	Stored Procedure	Executing remote commands	SELECT Eid, Ename FROM Employee WHERE Ename LIKE '8' or '8' = '8'; **EXEC master.dbo. xp_cmdshell 'dir'--'**

Table 1: Types of SQL Injection

5] CONCLUSION

also equal number of exploitation done.

ACKNOWLEDGEMENT

I would like to express my sincere thanks to all the teachers who helped us throughout.Iam also grateful to, Head of Department. This acknowledgment will remain incomplete if I do not mention the sense of gratitude towards our esteemed Principal who provided me with the necessary guidance, encouragement, and all the facility available to work on this project.

REFRENCES

1. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project/
2. https://www.google.in