Date : 13/2/2024

SQL INJECTION

Vulnerability that consists of an attacker interfering with the SQL queries that an application makes to a database.

Impact of SQL Injection attacks:

* Unauthorized access to sensitive data

Confidentiality- Sqli can be used to view sensitive data, such as application usernames and passwords.

Integrity- Sqli can be used to alter data in the database

(can change the email address of a user….and can reset the password by sending code to the changed email address)

Availability- Sqli can be used to delete data in the database

(after getting the access he then can delete the data and make information unavailable to the user)

* Remote code execute on the operating system

TYPES of SQL Injection:

3 major :

* In band(classic) (error, union)

Attackers uses same communication channel for launching the attack and gathering the result of the attack)

Error(force the db to generate an error giving you more info like the version of db, query used)

Union

* Inferential(boolean, time)

(no actual transfer of data)

* Out of band

In band(classic) :

Attackers uses same communication channel for launching the attack and gathering the result of the attack

Retrived data is presented directly in the application web page

Easier to exploit than other categories of sqli

Error based SQLI:

force the db to generate an error giving you more info like the version of db, query used

Union based SQLI:

is an in- band sqpli technique that leverages the union sql operator to combine the results of two queires in to a single result set

not only outputs the results of the original query, but also the results of chosen query

Inferential(blind):

* Where there is no actual transfer of data via web application
* Data is extracted by asking the db some true or false ques
* Just as dangerous as in-band sqli
* Attacker able to reconstruct the info by sending particular requests and observing the resulting behavior of db server
* Takes too longer to exploit than in-band

Boolean based SQLI:

Sends queries of true false and monitor the web responses and collect the payload information

Time based SQLI:

Relies on db pausing for a specific amount of tym, then returning the results, indicating a successful sql query execution

If 1st character of administrators hashed password id ‘a’, wait for 10sec…if response takes 10sec then 1st letter is ‘a’……if response does not take 10sec then 1st letter is not ‘a’.

Out of band SQLI:

Vulnerability that consists of triggering an out of band network connection to a system that you control

Used when you cont apply the above techniques

Not common

A variety of protocols can be used(dns,http)

How to find SQLI vulnerabilities

* Black box testing ( when tester id given little information about system (access url,scope of engagement)
* White box testing ( …complete access inlcuding source sode)
* Grey box testing ( Mix)

Black box testing :

* Map the application
* Fuzz the application

1.submit sql- specific characters such as ‘ or ’’ and look for errors or other anomolies

2.submit boolean conditions such as OR i=1 and OR i=2, and look for differences in the applications reponses

3.submit payloads designed to trigger time delays when executed within a sql query and look for differences in time taken to respond

4.submit OAST payloads designe dto trigger an out of band network interaction when executed within an sql query and monitor for any resulting interactions

White box testing:

* Enable web server logging
* Enable datbase logging
* Map the application

(visible functionalities in aplication)

* (Regex search on all instances in the code that talk to database)
* Code review

(follow the code oath for all input vectors)

* Test any potential sqli vulnerabilities

How to exploit vulnerabilities

Exploiting error based SQLI:

Submit sql-specific character such as ‘ or “ and look for errors or other anomolies

Different characterrs can give you different errors

Exploiting union based SQLI:

2 rules for combining the result sets of two queries by using union:

1.The number and the order of the coulumns must be the same in al queries

2.The data types must be compatible

Exploitation : figure out number of columns that query is making

Figure the data types of columns(mainly interested in string data)

Use the union operator to output information from rhe database