SQL Injections

SQL Injection attack is the injection of SQL commands into the SQL queries of the web application with the purpose of accessing and manipulating the database on which the application relies upon.

Common SQL databases: Mysql, MSSQL, Postgre-SQL, Oracle

SQL Injections

Almost all of the online store and CMS web applications uses database to store information.

SQL stands for Structured Query Language

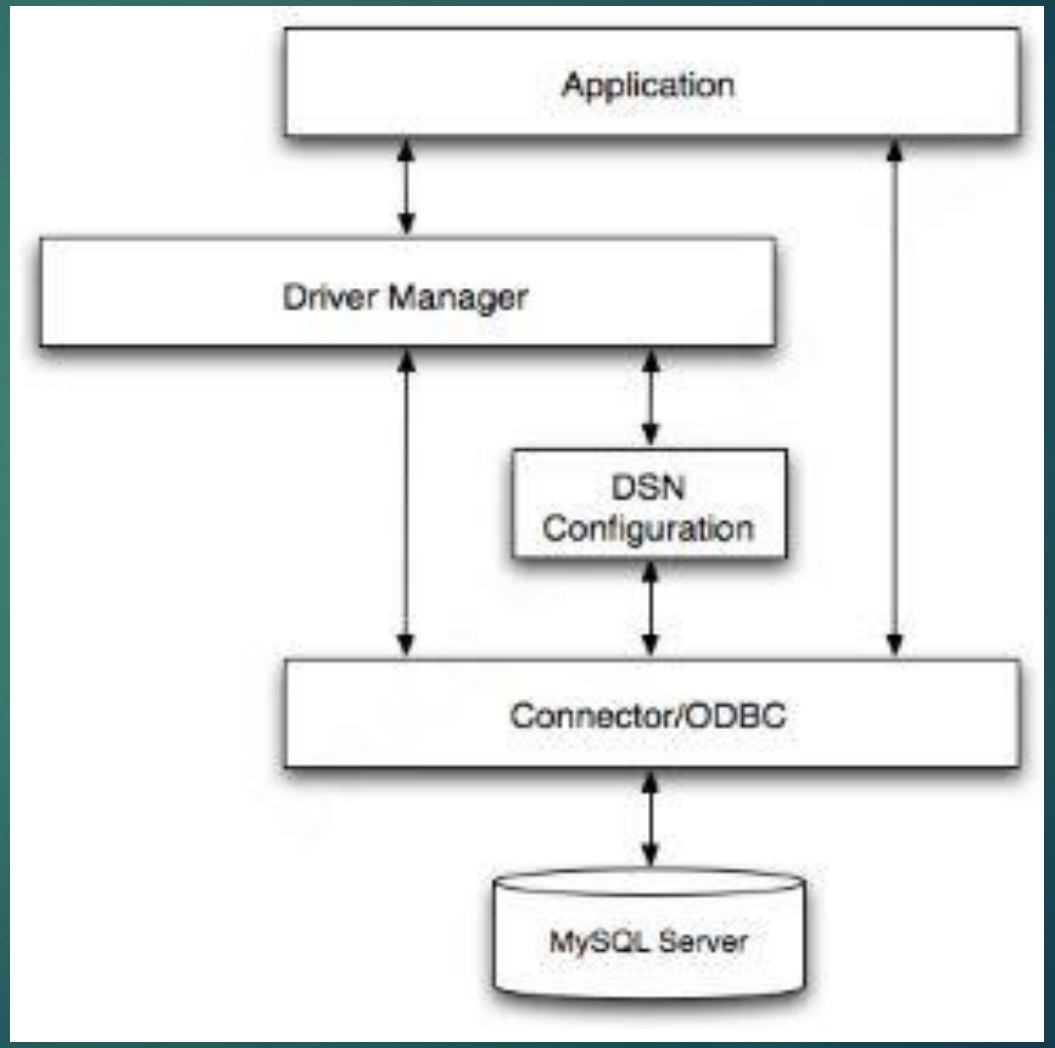
Even simple website uses database to connect and retrieve the details related to web pages.

SQL Injections

SQL is a powerful interpreted language used to extract and manipulate data from a database. SQL commands, are usually embedded in the server side scripting code (ASP,PHP,JSP etc) that establish and keep the connection to the database open through the use of connectors that sits between the web application and the database.

SQL Injections

This is how it establish connections To the DATABASE



SQL Injections

SQL Example in PHP:

```
$dbh=mysql_connect(192.168.64.131,"user","password");
mysql_select_db("test_db");
mysql_query("SELECT * FROM users");
```

SQL Query in these codes are:

```
SELECT * FROM users
```

What we can do with SQL Injection ?

An attacker may read the file system, run OS commands, install shells, access the remote network and compromise a whole network.

This is not always the case but the more powerful the DBMS is, the more advanced supported SQL is, hence the capabilities of an attacker after the exploitation.

What we can do with SQL Injection ?

Moreover, attacking a database that stores confidential data like user credentials, SSN, credit cards, and whatever sensitive information an enterprise, a company or a private may store on the database, is the most dangerous form of attack to a web application.

It can leads to whole network compromise.

What we can do with SQL Injection ?

Among all the vulnerabilities, we always try to find sql injection vulnerability first because it is ready to be exploited once found.

Every hacker attempts sql injection at first, unlike XSS vulnerability it doesn’t takes more time to be exploited.

How SQL injection works

The purpose of a SQL injection attack is to include our own SQL commands within a normal query within the web application. This is possible when a web application pass the user supplied data to database without sanitization.

Example:

```
mysql_query("SELECT * FROM users WHERE username='"
. $_GET["username"] . "'");
```

How SQL injection works

The above line of PHP executes a query that performs a search in the field “username” of the table “users”.

The search keyword is user supplied input in the parameter named “username”. Like below:

http://192.168.64.131/test_web.php?username=atul

How SQL injection works

The SQL query will be as follows:

```
SELECT * FROM users WHERE username='atul'
```

This is the query a web developer meant to be.

Use of single quotes ‘ in SQL are used for strings.

How SQL injection works

Since the user supplied data is not sanitized for bad characters, we will add the more query to attack as follows:

http://192.168.64.131/test_web.php?username=atul' or ''='

This will make query as

```
SELECT * FROM users WHERE username='atul' or ''=''
```

How SQL injection works

Logic will be as follows:

find the word “atul” and if it is not found evaluate ‘’=’’ that is always TRUE thus retrieving all the records in the table “users”.

This is a very basic example of how to alter the logic of the application through a SQL injection.

Let us see a more explanatory example.

How SQL injection works

Suppose a SQL query that checks for the existence for the pair (username, password) in the database in order to authenticate a user.

This is the common query in web applications

```
mysql_query("SELECT * FROM users WHERE username='" .
$_POST['username'] ."' AND password='" .
$_POST['password'] . "'");
```

How SQL injection works

These piece of PHP code does not perform user input sanitization and is only focus to execute when a user tries to authenticate his/her session on a website through the login form.

Bypassing the authentication form using a SQL injection involves using the always TRUE evaluation we have seen in the previous example.

Attacking like ‘ or ‘1’=‘1 also does the same, as 1 is always equal to 1.

How SQL injection works

The very famous technique of using this value pairs for username and password:

```
username= admin
password= ' or ''='
```

Resulting queries will be:

```
SELECT * FROM users WHERE username='admin' AND password='' or ''=''
```

How SQL injection works

That is basically a condition that is always TRUE because the empty string '' is always equal to the empty string ''. So the check is passed and the authentication as the user “admin” is successful (we are making the assumption that no other security check is in place).

This particular authentication flaw was very common until few years ago (you may still find it in custom made application though, so it is always good to check).

How SQL injection works

Now that we have the basics of how SQL injection works, you will see next how to find it in web applications and all the different types of SQL injections with more advanced techniques to carry it out against real world applications

Also with tools like SQLmap, SQLninja etc.

Common Myths

It is a myth that SQL injections does not work in NoSQL database like mongoDB, CouchDB

This is partially true, as the same sql injection works in NoSQL database as well. It depends on the web apps you attacking and your expertise.

NoSQL injection tool: NoSQLmap

Thank you !

It is recommended to learn all the basics before attacking web apps, as sometimes little knowledge can prove to be played great roles in major work.

www.grayhat.in | https://grayhatacademy.wordpress.com