Chapter 15

SQL Injection

Theory

Ethical Hacking

SQL

SQL (Structured Query Language) is a database management language used to manage databases to perform various operations like create, read, update and delete on the database. SQL is used by database administrators, as well as developers to organize user data properly. Web applications interact with the database server in the form of queries. SQL queries include select, add, insert, update, delete, create, alter and truncate.

List of Database software

- MySQL
- Microsoft SQL
- Oracle
- MongoDB
- SQL lite
- Microsoft Access
- DB2 Express-C

Database

A database is a collection of information that is organized into rows, columns, and tables, and it is indexed so that it can be easily accessed, managed and updated. Data in the database gets updated, expanded and deleted as new information is added.

The relation between the Web server and Database server

A server is a software that runs continuously and responds to requests sent by the clients, Communication between a client and a server happens using a specific protocol example HTTP, HTTPS Server running web application include three components like

Web servers which primarily respond to HTTP / HTTPS requests sent by the clients and passes these requests on to handlers.

Application server handles requests to create dynamic web pages. The application server processes the user request to generate the HTML page for the end user, instead of serving a static HTML page stored on the disk. Application server software runs on the same physical server machine as where the web server is running.

The database server is a server which houses a database application like JDBC, ODBC to provide database services to other computer programs. Most database applications respond to a query language. Each database understands its query language and converts each submitted query to server-readable form and executes it to retrieve results.

The relation between the web server and the database server are the web server uses the application server to retrieve the data from the database and host the data with the help of the web server application. So web server works as the front end, and database server works as a backend to provide data to web server.

SQL Injection

The technique used to take advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution on backend database to retrieve information directly from the database. It is used to gain unauthorized access to the database. SQL Injection is not a vulnerability in database or web server; it is a vulnerability in a web application which occurs due to lack of input validation.

Types of SQL Injection attacks

- Authentication bypass attack
- Error-based SQL Injection
- Blind SQL Injection

Authentication bypass attack

The attacker uses this technique to bypass user authentication without providing the valid Username and password and tries to log into a web application with administrative privileges.

Authentication Bypass Cheat Sheet

1’ or ‘1’ = ‘1
or 1=1
or 1=1--
or 1=1#
or 1=1/*
admin' --
admin' #
admin'/*
admin' or '1'='1
admin' or '1'='1'--
admin' or '1'='1'#
admin' or '1'='1'/*
admin' or 1=1 or ''='
admin' or 1=1
admin' or 1=1--
admin' or 1=1#
admin' or 1=1/*
admin') or ('1'='1
admin') or ('1'='1'--
admin') or ('1'='1'#
admin') or ('1'='1'/*
admin') or '1'='1
admin') or '1'='1'--
admin') or '1'='1'#
admin') or '1'='1'/*

Error-based SQL Injection

Error-based SQL injection technique relies on error messages thrown by the database server to obtain information about the structure of the database. In some cases, error-based SQL injection alone is enough for an attacker to enumerate an entire database. While errors are very useful during the development phase of a web application, they should be disabled on a live site or logged to a file with restricted access instead. By analyzing these errors, the attacker can grab system information such as the database, database version, OS, etc.

Blind SQL injection

Blind SQL injection is a type of SQL Injection attack that queries the database true or false questions and determines the answer based on the applications response. This attack is often used when the web application is configured to show generic error messages but has not mitigated the code that is vulnerable to SQL injection. Blind SQL injection is nearly identical to normal SQL Injection, the only difference being the way the data is retrieved from the database.

Countermeasures

- Never trust user input. Sanitize and validate all input fields. Use parameterized statements, separate data from SQL code.
- Reject entries that contain binary data, escape sequences and comment characters.
- Checking the privileges of a user’s connection to the database.
- Use secure hash algorithms to secure user passwords stored in the database.
- Perform source code review before hosting website.

References:

1. Types of SQL Injection? (n.d.). Retrieved from https://www.acunetix.com/websitesecurity/sql-injection2/
2. Blind SQL Injection. (n.d.). Retrieved from https://www.owasp.org/index.php/Blind_SQL_Injection