Database Management System for Security

Group ID : [redacted]

Y2.S1 (2021) Weekday

Subgroup : [redacted]

Database Vulnerability

- SQL Injection vulnerability
- Buffer Overflow Vulnerability

Group Members

- Abeywickrama O.D – [redacted]
- Dilshan K.N – [redacted]
- Samarasinghe H.P.M.S – [redacted]
- De Silva N.T.S – [redacted]

Introduction

SQL injection…..

- SQL injection is a type of cyber attack which work against the web applications which use SQL database
- In here the attacker inject malicious SQL statement to interfere with the queries Because of that malicious query injection the attacker can view data that they are not normally able to retrieve .
- The simplest form of SQL injection is through user inputs. Web application accept user inputs through a form .The form passes the user inputs to the back end to process. If web application fails to sanitize user inputs an attacker can inject malicious SQL statement into the back end and delete ,copy or modify the content of database
- SQL injection can be categorized into three sectors
- Among them the Inferential SQL can be classified into two major categories such as

  Boolean based SQL

  Time based SQL
- From all of those vulnerabilities we discuss about tome base SQL injection vulnerability which is a type of inferential SQL injection. In here the attacker inject a SQL segment which contain a query that generate a time delay.
- By injecting time delay in the query attacker can ask a yes /no question to the database. The time delay will be executed depending on the point that the condition is verified or not .After he execution of the time delay the server response will be abnormally long .

Buffer overflow…

What is buffer overflow?

- Buffers are memory storage regions that temporarily hold data while it is being transfemed from one location to another. A buffer overflow occurs when the volume of data exceeds the storage capacity of the memory buffer As a result the program attemting to write the data to the buffer overwrites adjacent memory locations.
- Buffer overflow can affect all types of software.
- There are several types of buffer overflow attacks. Stack overflow attack and heap overflow attack are the major attacks of them.
- Stack overflow attack is the most common type of buffer overflow attack.

Latest incidents of SQL & Buffer overflow Vulnerabilities…….

SQL injection Vulnerability	Buffer Overflow Vulnerability
• In early 2021, 70 gigabytes of data was exfiltrated from the far-right website Gab through a SQL injection attack. • A second attack against Gab was launched the next week using OAuth2 tokens stolen during the first attack.	• In May 2019, Facebook announced a vulnerability associated with all its WhatsApp products. • The vulnerability exploited a buffer overflow weakness in WhatsApp's VOIP stack on smartphones.

Functionality

SQL Injection…..

- Time-based SQL injection could be a sort of inferential-blind injection attack. This type of injection could be a time critical, but no information transferred between the attacker and the database. Therefore, an attacker won’t get any data as a result but instead of that attacker able to examine the database structure and the resulting behavior of the database Sever.

- In a time-based attack, An attacker input SQL command to the server which consist of malicious payload. When that SQL command being executed that may force the server to wait some specified number of seconds before responding.

- Most commonly attackers use ‘’SLEEP’ , ‘WAIT FOR DELAY’, ‘WAIT FOR TIME’ functions to delay the execution of the queries.

- Latency period of response indicates whether the results of the queries were true or false. By looking on the response, attacker will try to execute other queries because attacker must enumerate each characters. Finally, as a result attacker will reconstruct and make a new database structure inside the database.

Buffer overflow…..

- A stack buffer is a predefine fixed length memory space. When any program being executed, then the temporary data may store in the stack buffer.

- Intruders try to exploit the buffer by injecting executable codes from client or other software process to write more data to a fix length block of memory or buffer , than the buffer is allocated to hold.

- When that buffer got overflowed remaining data has to flow into another buffer. That may corrupt the data which already in that buffer and result in erratic program behavior, including memory access errors, a crash, incorrect results, or a breach of system security.

- Sometimes intruders try to hijack the control of the process by injecting additional codes. Usually this may accomplish by overwriting return address on the process stack or by overwriting function pointer in the memory. If either one succeed, injected code points to transfer the control flow execution into wrong address.

Mitigation

SQL Injection….

❖ There are various ways in which patch SQL injection attacks from happening likewise as defensive against them. Information that comes from a third-party reference, mustn’t be trustworthy and it ought to assume to be malicious in nature.

•Used of stored procedure - The easiest way to prevent SQL injection from happening, is to use parameters and sp_ execute sql to execute the dynamically generated statement.

•Use of prepared statements with parameterized queries - parameterized query, is used to execute the same statement repeatedly in an extremely efficient manner.

•Whitelist input validation - Whitelist, defines a set of valid characters while blacklist, or exclusive validation defines a set of invalid characters to try to remove.

•Escaping all user-supplied inputs - This is done to make sure the DBMS never confuses it with the SQL statement provided by the developer

•Web application firewall - One of the best practices to identify SQL injection attacks is having a web application firewall (WAF)

Buffer overflow…..

❖ When considering the Stack based buffer overflow, there are various tools and techniques available to mitigate and prevent against the that vulnerability.

- Use of Canary - based Technique - Compilers create random values known as canaries when the program being executing and then place it on the stack after each buffer. While checking the original buffer value against the canary can determine whether a buffer overflow has occurred. If any overflow occurred process will terminate.
- Non-Executable stack or Data Execution Prevention - Some operating systems provide patches for marking the stack address as areas where code cannot be executed.
- Address space layout randomization - Randomizing the address space, make difficulties for the attackers to determine the target addresses in the memory.
- Pointer protection - Encrypting the pointers when stored in memory and decrypt when only loaded to the CPU registers.
- Use of secure functions - Unlikely the other string handling library functions [strcpy(), strcat(), print(), gets()] , secure functions can only write inside the maximum size of the buffer

Countermeasures

SQL Injection….

- ❑ Though SQL injection attacks are still the most dangerous there are plenty of ways to prevent database from attackers

•Data sanitization- In data sanitization data must be submitting through a function to ensure that there is no dangerous characters.

•Update and patches – It is essential to search for vulnerabilities and apply patches and update as soon as practical because if attackers find vulnerabilities in system, they try to exploit it.

•Use firewall protection- It filter the malicious data.

•Establish appropriate privileges and strict access- least privilege access polices with strict rules and don't use data base with admin level privileges when it not necessary.

•Data validation- It is a common step to ensure that there is no invalid and malicious data

•Encryption- Most of the time we assume that the internet connected applications are not secure there for encryption ,hashing passwords are important.

Buffer Overflow….

❑ Following Countermeasures are generally use to detect and prevent from Buffer Overflow vulnerability.

- Use of Buffer overflow immune programming languages - Some programming languages like Java, Python, .NET are providing strong object typing and prohibited the direct access to the memory.
- Deploying an Intrusion Detection System(IDS) - which may monitor and analyze the traffic from all devices going in and out of the network. Then identify the abnormal behaviors and then warning will be sent if any malicious activity fund.
- Implementing a system patches in timely manner - Vulnerable version of the code need to replace with the new patched version.
- Deploying a fully licensed applications - Pirate applications always carrying a hidden backdoors
- Use of proper Compiler tools - Try to use Various compiler tools which offer warnings on the use of unsafe constructs such as libraries, malicious codes.
- Security best practice for handling the buffers - Existing system can be tested by Performing the vulnerability assessment or penetration testing

Thank you