SLIIT – Sri Lanka Institute of Information Technology

Group Assignment

IE2042 – Database Management System for Security

Analysis of Database Vulnerabilities

Submitted by :

|  |  |
| --- | --- |
| Student Registration Number | Student Name |
| IT20613372 | P.H.Badullege |
| IT20627928 | H.M.T.D.Herath |
| IT20624958 | I.B.C.M.J.Bandara |
| IT20625320 | U.H.S.N.Sadakelum |

Date of Submission

2021.10.03

Abstract

For every individual or company, data is one of the most valuable assets.

For every individual or company, data is one of the most valuable assets.

keep  data and organize it properly is very important.

Datasets are kept in databases to make it simple and efficient.

cybercriminals always focus on the data. The goal is to protect data  from these attackers as well as stop them to get access to information.

Cybercrimes are affecting wide range of industries.

These are the malicious attackers that want to compromise the integrity of the data.

This presentation attempts to categorize two database vulnerabilities,how they work,what are impacts of themand difficulties that the database faces,and by mitigating them keep database management system secure and safe.

SQL injection

What is sql injection

SQL injection is a one of critical database vulnerability in the cyberworld.

SQL stands for Structured Query Language, and it is a computer language used to store, manipulate, and retrieve data from relational database by using commands like INSERT,UPDATE and DELETE.

A attacker manipulates the logic of a SQL command to gain access to a database and other sensitive information using code injection.

Sql injection attack is a one of the most common vulnerability available on the today network.

Any website or web application that have a SQL database, such as MySQL, Oracle, SQL Server, or others, can be vulnerable to SQL Injection.

Cyber attackers get unlimited access to all the data contained in a database as a result of SQL injection. SQL injections, which target conventional databases, and NoSQL injections, which target big data databases, are two kinds of such computer attacks.

Using SQL injection attacker can delete,modify or even steal private data.

It compromises the safety,security and trust of user data.

Also it compromises company’s name and ability to stay in the business.

The primary goal of a SQL injection attack is to gather information while accessing a database table that may include sensitive data such as credit card numbers, social security numbers, or passwords, among other things.

Types of sql injection

Can divided in to 3 main types

In-band SQLI

Inferential/blind SQLI

Out-of-band SQLI

1.In-band SQLI

In-band sql injection affected when an attacker is able to use the same communication channel to both launch the attack and obtain results.

In-band SQLI is 2 types

Error based SQLI – relies on error messages thrown by the database server to get details about the structure of the database

Union based SQLI – leverages the union sql operator to combine the results of two or more select statements into a single result which is then returned as a part of the http response.

2.inferential SQLI/BLIND SQLI

No data is actually transferred via the web application and the attacker would not be able to see the result of an attack web application.

An attacker is able to reconstruct the database structure by sending payloads,observing the web application’s response and the resulting behavior of the database server

Can be divided into two types

Boolean-based blind SQLI –

Attacker sends an SQL query to the database which forces application to return a different result depending on whether the query returns a TRUE or FALSE result.

Depending on the result,the content of the HTTP response will change,or remain the same.

This allow an attacker to infer if the payload used returned true or false,even though no data from the database is returned.

Time-based blind SQLI –

The attacker sends a SQL query to the database which foerces the database to wait for a specific amount of time before responding.the response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

Depending on the result a HTTP response will be returned with a delay or return immediately.

This allow an attacker to infer if the payload use returned true or false,even though no data from the database is returned.

3.Out-of-band SQLI

It occurs when an attacker is unable to use the same channel to launch the attack and gather results.

SQL injection tools

To identify potential vulnerabilities

BSQL Hacker SQLmap SQLninja Safe3 SQLSus Mole Havij

How SQL injection works

The attacker looks for web pages that enable data submission, such as login pages, search pages, and feedback forms.

App sends logging form to user

Cybercriminal submit the form with sql exploit data

* Common vulnerable login query

SELECT \* FROM users

WHERE login = ‘abc’

AND password = ‘123’

Then if it returns something then login

* MS SQL server login syntax

Var sql = “SELECT \* FROM users

WHERE login = +formusr+

AND password = +formpwd+”;

formusr = ‘ or 1=1

formpwd = anything

Injecting through strings

* Final query look like below:

SELECT \* FROM users

WHERE username = ‘ ‘ or 1=1

AND password = ‘anything’

* It closes the string parameter
* Everything after is considered part of the SQL command
* In addition to string fields there are other types of fields like numeric & dates

Injecting numeric fields

SELECT \* FROM student

WHERE studentid = 432567

AND age = 15

* PHP/MySQL login syntax

$sql = “SELECT \* FROM student WHERE “studentid = $formstudentid AND age = $formage”;

$formstudentid = 1 or 1=1#

$formage = 15

* Final query look like below:

SELECT \* FROM student

WHERE studentid = 1 or 1=1

# AND age = 15

Application builds string with exploit data.this string is called SQL query

Application sends sql query to database

Database executes query including exploit,sends data back to application

Application returns data to user

Impact of SQL injection

Leakage of sensitive information.

Reputation decline.

Modification of sensitive information.

Loss of control of database server.

Data loss.

Countermeasures & how Mitigate SQL injection

Input Validation

Input Checking Functions

Validate Input Sources

Access Rights

Configure database error reporting

SQL server firewalling.

Don’t store password in plain text in the database

Keep a database backup

Update database drivers

Enable database logging and connection filtering procedures.

Input Validation

– Simple input check can prevent many attacks.

– Always validate user input by checking type, size, length, format, and range.

– Test the content of string variables and accept only expected values.

– Reject entries that contain binary data, escape sequences etc. This can help prevent script injection and can protect against some buffer overrun exploits.

– When working with XML documents, validate all data against its schema as it is entered.

Input Checking Functions

– Certain characters and character sequences such as ; select, insert can be used to perform an SQL injection attack.

– Remove these characters and character sequences from user input which reduces the chance of an injection attack.

– Scan query string for undesirable word like "insert", "update", "delete", "drop" etc. check whether it represent a statement or valid user input.

– Write a function which can handle all of this.

Validate Input Sources

– There are so many ways to attack a database, therefore the developer should check and authenticate all input sources and disallow unidentified or untrusted users/websites.

Access Rights/User Permissions

– Create "low privileged" accounts for use by applications.

– Never grant instancelevel privileges to database accounts.

– Never grant databaseowner or schemaowner privileges to database accounts.

– Be aware of the permission scheme of your database.

Configure database error reporting

– Some application server's default error reporting often gives away information that is valuable for attackers (table name, field name, etc.).

– The developer should configure the system correctly, therefore this information will never expose to an unauthorized user. Apart from the above, these are several methods which can prevent from SQL injection

Network based IDSes can monitor all connections of database server and can flag suspicious activity.

Hosted based IDS can monitor web server logs and alert when something bad happens.

END

DOS attack

Dos – denial of service attack is a another serious vulnerability on database management systems.

The phrase DOS-Denial of Service refers to a network-based attack on a computer system.

DOS is an attack used to deny legitimate users access to a resource such as accessing a website,database,network,email,etc. or making it slow.

It's  a malicious effort to make a networked system inoperable sometime without  permanently damage it.

The attacker sends a flood of data packets to the target machine using customized software in order to overload its resources.

Goals of dos attacks is harm to the reputation of company, customer and financial loses, and in the vital service cases even has an impact on human lives.

Denial of Service is currently the most expensive computer crime for victim organizations

Types of DOS attacks

1. Bandwidth attacks

* Attacks will consume all available network bandwidth.
* Every site is given with a particular amount of bandwidth for its hosting,Now if more visitors consume all bandwidth then the hosting of the site can band the site.
* The attacker does the same. Attacker will open many pages of a site and keeps on refreshing and consuming all the bandwidth, thus the site become out of service.
* Eg: UDP floods, ICMP floods, spoofed packet floods

1. Application layer attacks

* Failures of applications or OS components to handle exceptional conditions
* The goal of this attack is to crash the web server.

1. Protocol attacks

* Attacks will consume system resources such as CPU, memory, storage
* Protocols here are rules that are to be followed to send data over network.
* These kind of attacks exploit a specific feature or implementation bug of some protocol installed at the victim’s system to consume excess amount of its resources.
* Eg: TCP SYN floods, fragmented packet attacks, Ping of death, Smurf attack etc.

DOS attack types & how they work

ICMP Flood Attack

* Ping flood, also known as ICMP flood, is a common Denial of Service (DoS) attack in which an attacker takes down a victim’s computer by overloading it with ICMP echo requests.
* The attacker hopes that the victim will respond with ICMP "echo reply" packets for each ICMP request, thus consuming both outgoing bandwidth as well as incoming bandwidth of target device.
* It is most successful if the attacker has more bandwidth than the victim. If the target system is slow enough, it is possible to consume enough of its CPU cycles for a user to notice a significant slowdown.

UDP flood

* A UDP flood is a type of denial-of-service attack in which a large number of User Datagram Protocol (UDP) packets are sent to a targeted server with the aim of overwhelming that device’s ability to process and respond.
* The firewall protecting the targeted server can also become exhausted as a result of UDP flooding, resulting in a denial-of-service to legitimate traffic.

Ping of Death Attack.

* An attacker sends an ICMP ECHO request packet that is much larger than the maximum IP packet size to victim.
* Since the received ICMP echo request packet is bigger than the normal IP packet size, the victim cannot reassemble the packets. The OS may be crashed or rebooted as a result.

Teardrop Attack.

* A teardrop attack is a DOS attack that involves sending fragmented packets to a target machine.
* Here the size of one fragmented packet differs from that of the next fragmented packet.
* Since the machine receiving such packets cannot reassemble them and hence the packets overlap one another, crashing the network device or server
* The size is different for each fragmented packet the server will not be able to reassemble the packet properly and leads to server failure. Server failure will lead to Denial of Service.

TCP SYN Flood Attacks

* Taking advantage of the flaw of TCP three –way handshaking behavior, an attacker makes connection requests aimed at the victim server with packets with unreachable source addresses.
* In TCP-SYN Flooding the last message of TCP’s 3 way handshake never arrives from sender.
* This causes server to allocate memory for pending connection and wait. This fills up the buffer space for SYN messages on the target system, preventing other systems on the network from communicating with target system.

Smurf Flood Attacks

* In Smurf attack the attacker will send ICMP request to broadcast IP of a network by using Victim’s IP as source address.
* All the systems on these networks reply to the victim with ICMP echo replies.
* This attack rapidly exhausts the bandwidth available to the target, effectively denying its services to legitimate users.

Land Attack

* Attacker sends a fake TCP SYN packet with the same source and destination IP addresses and ports to a host computer
* IP address used is the host’s IP address
* For this to work, the victim’s network must be unprotected against packets coming from outside with their own IP addresses

DDoS attack

* A denial-of-service attack in which the attacker gains illegal administrative access to as many computers on the Internet as possible and uses the multiple computers to send a flood of data packets to the target computer

Impact of DOS attack

Unusually slow database/server performance

Unavailability of a particular database/server

Inability to access any database/server

increase in spam email received

Disconnection of a wireless or wired internet connection

Countermeasures

There is no single way to stop Database DoS attacks.

Every feature is a potential avenue for attack, so no single response can defend against everything

DoS protection does not happen by itself; it requires and investment in time and tool

put the time in to patch and configure your databases.

Attempt to understand the vulnerability

Disable unnecessary network software

But if your databases are high-profile targets you need preventative and detective controls for reasonable assurance that they won’t be brought down.

How mitigate DOS attack

We can’t stop DOS attack but we can reduce it.

Check for security patches keep updated.

Establish and maintain regular backup schedules.

Buy more bandwidth

To ensure that you have enough bandwidth to handle spikes in traffic that may be caused by malicious activity.

Build redundancy into infrastructure

To make it as hard as possible for an attacker to successfully launch a DDoS attack against servers, make sure you spread them across multiple data centers with a good load balancing system to distribute traffic between them. If possible, these data centers should be in different countries, or at least in different regions of the same country.

Deploy anti-DDoS hardware and software modules

Servers should be protected by network firewalls and more specialized web application firewalls. By configuring firewall or router to drop incoming ICMP packets or block DNS responses from outside, network can help prevent certain DNS and ping-based volumetric attacks.

Software protection can also be used. for example, by monitoring how many incomplete connections exist and flushing them when the number reaches a configurable threshold value.

Practice Basic Network Security

Engaging in strong security practices can keep networks from being compromised. Secure practices include complex passwords that change on a regular basis, anti-phishing methods, and secure firewalls that allow little outside traffic.

Understand the Warning Signs

Some symptoms of a DDoS attack include network slowdown, or broken website shutdowns. No network is perfect, but if a lack of performance seems to be prolonged or more severe than usual, the network likely is experiencing a DDoS and the company should take action.

Maintain spares

Spares means the machines that can be placed into service quickly if a similar machine is disabled.

Removing unneeded user accounts,communication protocols,services and database features.

Several database platforms provide the capability to limit resources on a per-user basis such as number of queries per minute, long running query timeouts, resource throttling for memory and processors etc

Configuring resource limits can help reduce the impact of attacks, attackers may use resource throttles to starve out legitimate users. Consider this a good option for graceful degradation and a good standard operating procedure, but your implementation needs to be very well planned to prevent limits from impinging on normal operation

Many DoS attacks exploit bugs in database code

Buffer overflows, mishandling of malformed network protocols or requests, memory leaks, and poorly designed multitasking have all been exploited

These are not the types of issues you or DBAs can address without vendor support. A small portion of these attacks are preventable with database activity monitoring and firewalls

One of the most popular database protection technologies on the market, Database Activity Monitoring alerts on database misuse.

These platforms inspect incoming queries to see whether they violate policy

DAM has several methods for detecting bad queries, with examination of query metadata such as user, time of day, table, schema, application, etc.

Many monitors offer an option block malicious queries, either through an agent or by signaling a reverse proxy on the network, but most DAM products are deployed in monitor-only mode, alerting when policy is violated. These platforms can be set up to help defend against DoS, but you need to configure them to block traffic and write policies to detect the attacks.

Many database DoS attacks,run through web-facing applications.

You build checks to prevent misuse and cast user-supplied data into properly constrained variables to ensure users don’t pass garbage to database

Conclusion

Security has become a chief concern in today’s world.

It is very necessary that we come across the right solutions to undertake the different security problems. There are various types of threats on a database and numerous kinds of attacks.

Database security can be identified in various forms.In this presentation we have identified two vulnerabilities that a database is prone to.

It also discusses the methods of mitigating the database security threats.

This can help in fixing or atleast reducing the possibility of occurrence of vulnerability that can damage the database security.

With the help of these categories, industries expert and developers can bestow more security to databases of web applications.

END