

Software Vulnerabilities

30012104, 1703285, 17129001, 18066291, 30008859

LEAVE MANAGEMENT SYSTEM

Table of Contents

[Vulnerability – what is. – Michal 30012104 1](#_Toc63349606)

[Types. 1](#_Toc63349607)

[SQL Injection – Michal 30012104 2](#_Toc63349608)

[Sniffing – Michal 30012104 3](#_Toc63349609)

[Reference 4](#_Toc63349610)

# Vulnerability – what is. – Michal 30012104

According to Wikipedia (Vulnerability (computing), 2021) vulnerability in computing is a weakness which can be exploit by attacker. Intention of attacker is to cross boundaries of privileges and perform unauthorized action within computer system. Vulnerability is also known as attack surface. Reason why is because threat actor must have at least one “tool” to connect him with system weakness point.

In the book “The art of Software Security Assessment” (Dowd, McDonald and Schuh, n.d.) we can find that software vulnerability is weakness in system that attacker can use to do something malicious, as examples author uses disturb and destroy a system, expose or alter sensitive information and take control of program or computer altogether.

## Types.

We will cover 7 different types of vulnerabilities:

1. SQL injection. – Michal 30012104
2. Sniffing – Michal 30012104
3. Xx
4. Xx
5. Xx
6. Xx
7. Xx

# SQL Injection – Michal 30012104

According to portswigger.net SQL injection is a vulnerability that allows threat agent to interference with queries that application makes to its database. (Academy and injection, 2021) This can lead to attacker get data they would be normally would be able to retrieve. In many cases, an attacker can not only retrieve data but also alter or delete that data causing changes to application changes or behaviours. In bad scenarios attacker might even gain access to the underlying server or other back-end infrastructure.

“SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will unknowingly run on your database.” (SQL Injection, 2021).

Data sanitation is an absolute must when it comes to basic protection against SQL injections. We should simply pre-check all data before system entry. Removing all the garbage data allows us to make sure that the query won't break system and or database.

As we can read in (security.berkeley.edu, 2021) its still common misconception that input filtering is still seen as only measure programmers have to think of when designing the application. This is wrong as input filtering does not fix the underlying vulnerability. It is often good enough to stop the most trivial of the attacks.

To protect your application from SQL injection one of the most common practice is to parameterized statements, do not use dynamic SQL. When programming language like python talks to the database it uses database drivers. These simply allowing our application to build and run SQL statements and making requested changes to our database. Parameterized statements simply make sure that inputs passed into SQL are treated in a safe manner.

Configuring proper error reporting shouldn’t be skipped when designing the application. Database error messages should never be sent to a client web browser. This could lead to discovering by attacker technical details of our application and then be used to build successful malicious code to inject.

Needless to say that SQL injection is illegal and can have serious consequences such as massive fines and jail time. But the company who is being hacked merely fixing a problem is often only beginning of trouble. In many cases, companies suffer from bad PR and losing the reliability and trust of customers. For example one of the largest world credit card companies was hacked a couple of years back and some estimated claimed that over 100 million cards and more than 650 financial services companies were compromised. During prosecution, it was three corporate victims reported over 300 million US dollars of losses(Vaas, 2021). Not only large companies suffered due to this incident of SQL injection but also individuals through identity theft. Many of them had to deal with false charges associated with a stolen identity. The scale of this damage was described by the court as “immeasurable”. One of the attackers that pledge guilty was sentenced to 12 years of jail (US prosecutors launch largest-ever hacking fraud case, 2021).

# Sniffing – Michal 30012104

Sniffing in network traffic can be thought of as putting a bug on your telephone line, and listening to what two or more parties have to say. In networking, it will be watching and intercepting data packets that are being exchanged. When data transmitted isn’t encrypted in can be read using application design to intercept data called a sniffer. Using sniffer we can through FTP traffic, Web traffic, email traffic and get hold of sensitive information including passwords and ID’s, bank details etc. According to (Gregorczyk et al., 2020) sniffing is one of the most important techniques that attackers use to collect information. This information later can be used to exploit vulnerabilities within computer systems. Often packet sniffers just listen, display and log the traffic without making any modifications(Wikipedia, 2021). Gregorczyk points out that due passive nature of sniffing it can be very hard to detect.

As we can read in (Greycampus, 2021) There generally two types of sniffing :

* Active - When we sniffing in the switch, point that regulates the flow of data between ports. Active sniffing attacker floods switch with bogus requests. This leads to traffic to in all ports.
* Passive – this type of sniffing occurs in a hub. This type would operate on the data link layer of the network.

There are simple techniques that we should use when connecting the application to the network. These include avoiding all insecure protocols such as HTTP, FTP. Instead, we should always remember to connect application using protocols like HTTPS, SFTP, SSH. We should also consider encrypting our data whenever it is possible.

Other methods of sniffing prevention are using specially design tools to name few: Promqry, Sniffdet, Anti-sniffer.

According to The Register (Data-sniffing attack costs Heartland $12.6m, 2021) In 2009 Heartland Payments System corporation spend over 12milion dollars on encrypting credit card data, this was directly related to the security breach that had a place. Hackers using sniffing techniques got hold of cards holders sensitive data. Luckily these days end-to-end encryption are hugely popular and used in sorts of application (ex. WhatsApp).

# Reference

En.wikipedia.org. 2021. *Vulnerability (Computing)*. [online] Available at: <https://en.wikipedia.org/wiki/Vulnerability\_(computing)> [Accessed 21 January 2021].

Dowd, M., McDonald, J. and Schuh, J., n.d. *The Art Of Software Security Assessment*.

Academy, W. and injection, S., 2021. *What Is SQL Injection? Tutorial & Examples | Web Security Academy*. [online] Portswigger.net. Available at: <https://portswigger.net/web-security/sql-injection> [Accessed 21 January 2021].

W3schools.com. 2021. *SQL Injection*. [online] Available at: <https://www.w3schools.com/sql/sql\_injection.asp> [Accessed 21 January 2021].

Vaas, L., 2021. *Hackers sentenced for SQL injections that cost $300 million*. [online] Naked Security. Available at: <https://nakedsecurity.sophos.com/2018/02/19/hackers-sentenced-for-sql-injections-that-cost-300-million/> [Accessed 4 February 2021].

BBC News. 2021. *US prosecutors launch largest ever hacking fraud case*. [online] Available at: <https://www.bbc.co.uk/news/technology-23448639> [Accessed 4 February 2021].

Security.berkeley.edu. 2021. *How to Protect Against SQL Injection Attacks | Information Security Office*. [online] Available at: <https://security.berkeley.edu/education-awareness/best-practices-how-tos/system-application-security/how-protect-against-sql> [Accessed 4 February 2021].

Gregorczyk, M., Zorawski, P., Nowakowski, P., Cabaj, K. and Mazurczyk, W., 2020. Sniffing Detection Based on Network Traffic Probing and Machine Learning. *IEEE Access*, 8, pp.149255-149269.

En.wikipedia.org. 2021. *Sniffing attack*. [online] Available at: <https://en.wikipedia.org/wiki/Sniffing\_attack> [Accessed 4 February 2021].

Greycampus.com. 2021. *Greycampus*. [online] Available at: <https://www.greycampus.com/opencampus/ethical-hacking/sniffing-and-its-types> [Accessed 4 February 2021].

Theregister.com. 2021. *Data-sniffing attack costs Heartland $12.6m*. [online] Available at: <https://www.theregister.com/2009/05/07/heartland\_breach\_costs/> [Accessed 4 February 2021].