Vulnerabilities

Matthew Wisden, Jake Watkins-Brown, Owain Mahoney & Pawel Kaczmarczyk

Contents

SQL Injection

SQL Injection is used to allow an attacker to mess with queries within a database. It allows them to see data within the database which they should not be able to access. The attacker can also delete or modify data other users on the network which may cause changes to the application which may be undesirable.

In extreme cases, it can cause the attacker to gain access to the back end of the application which can cause mayhem to the application. They can also perform DoS (Denial of Service) attacks which will hit the application offline.

impact of a successful attack can have horrendous implications. The attacker will have gained access to sensitive information such as passwords, credit card information and personal information such as home address, which can lead to severe identity theft.

Incorrect Authentication

Incorrect authentication is when the developer doesn't develop the session management and user authentication correctly. This issue leads to attacks being able to exploit flaws in password, keys and/or session tokens. They can also exploit these flaws to use other user's identities.

An example of this is when a user is sharing the link of a bank, but the link includes their session id and other details in the url. That other user can then use that link as if it was being accessed by user 1. a way to prevent this is to encrypt the important information and to make it server side.

Data leaks

Data leaks is a part of human error that could happen due to employees intentionally leaking the data or it can be done accidentally. Data leaks is when data is shared from within an organisation to an external recipient. This can be crippling to a company or organisation as it can cause a decline in revenue, tarnish their reputation or the company can face lawsuits. There are many causes of data leaks. They are "The accidental breach", "the ill-intentioned employee", "Electronic communications with malicious intent". Firstly, the accidental breach could just be the employee sharing information with the wrong person on accident. Secondly, the ill-intentioned employee could carry out this act if they are bribed to do so or if they are unhappy with their employers. Finally, the malicious intent is simply data leak using malicious software or viruses that could be inserted through various means.

Viruses

Viruses are a very dangerous threat to organisations that use computer systems, a virus is a long string of code which can be discretely installed onto a computer with the user not even knowing, the virus can gain access from email attachments or visiting websites. One of the scariest things about a virus is that it can duplicate itself and if it infects a computer connected to a network it can infect many of the computers connected to that network too. The impact can cause a large amount damage to systems such as corrupting files and a large loss of data, it may also cause the computer systems that are infected with the virus stop working all together.

Phishing

Phishing is where a user is sent an email from an anonymous source pretending to be a well-trusted organisation such as their bank. The phishing email will try to persuade the user to input their login details for the organisation they are pretending to be.

Denial of Service Attacks

Denial of Service (DoS) attacks are attacks against websites such as ecommerce websites, these attacks cause websites to go offline for a duration of time. After the DoS attacks the users of the website will not able to purchase or access the website until the website is back online again and this will impact the business because they won’t be getting sales during the site downtime. A person can cause DoS attacks by sending high traffic to the website.

Human Error

Human error such as accidental deletion of files can lead to the loss of customer records. If the customer records are lost, then the customer must recreate their account if they would like to continue using the service the organisation provides but the customers may not want to recreate their account because the organisation lost their records before and may lose them again. Human error can also cause the leak of person information due to incompetence such as a high permission level user of the system writing down their password then leaving it in a public place which anyone can see