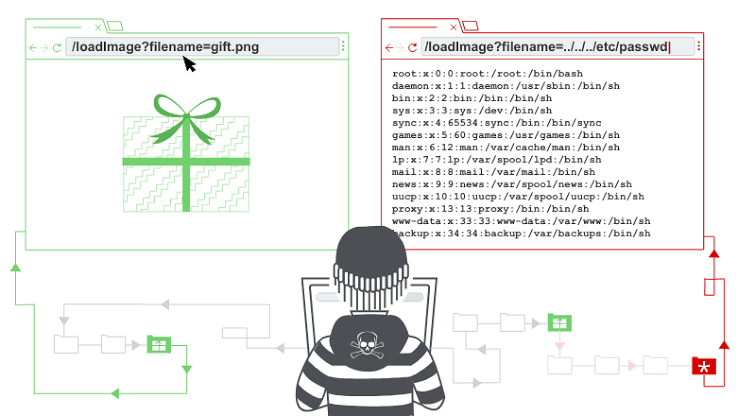
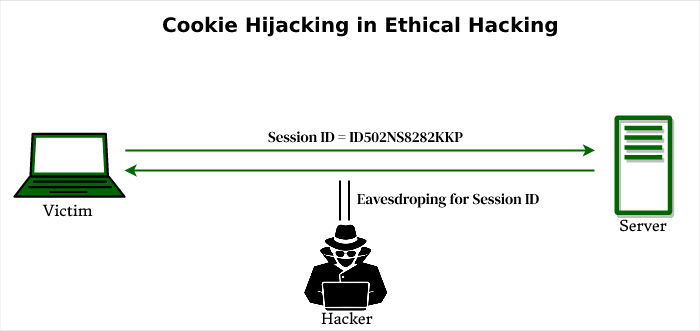
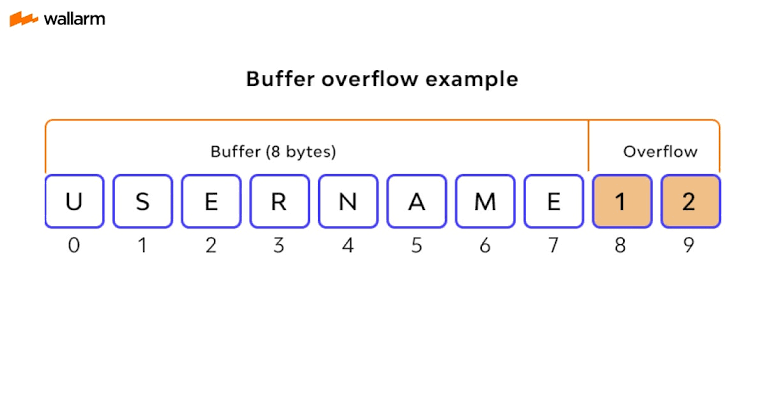
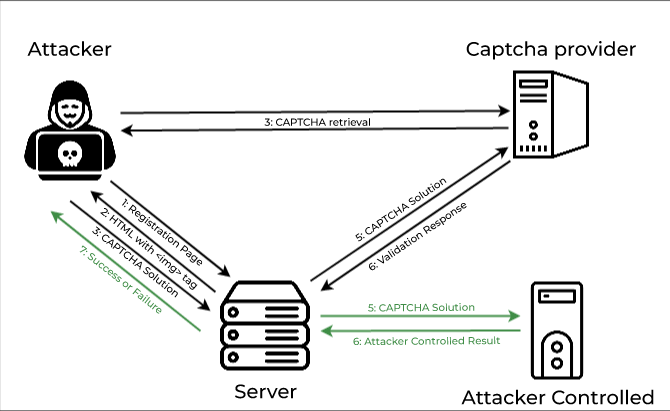
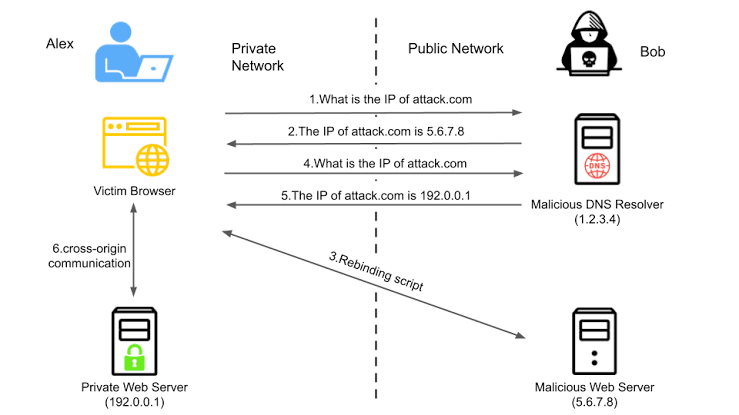
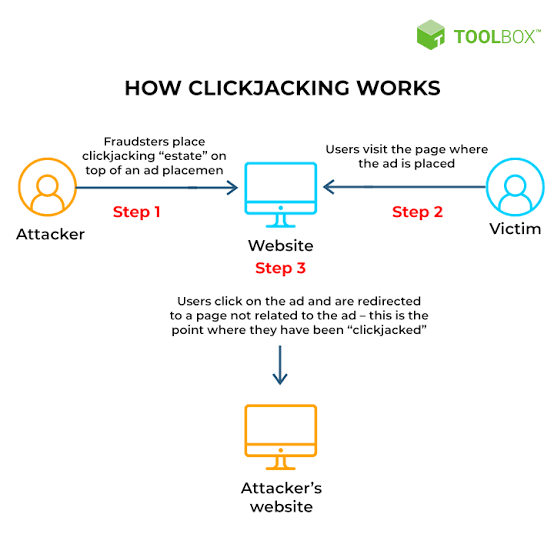
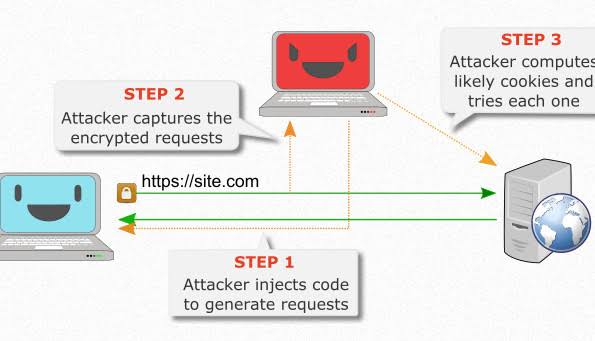
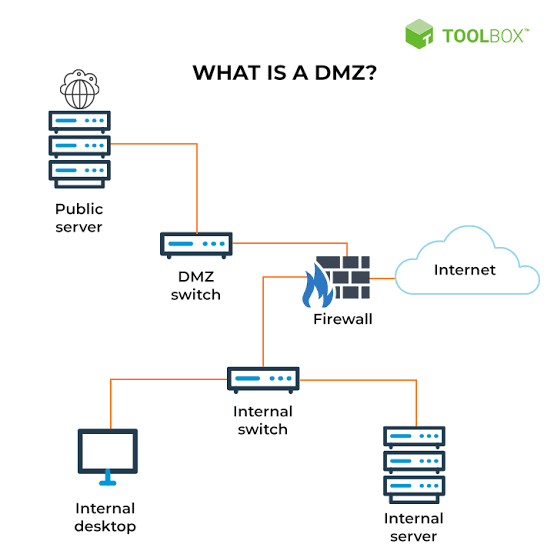
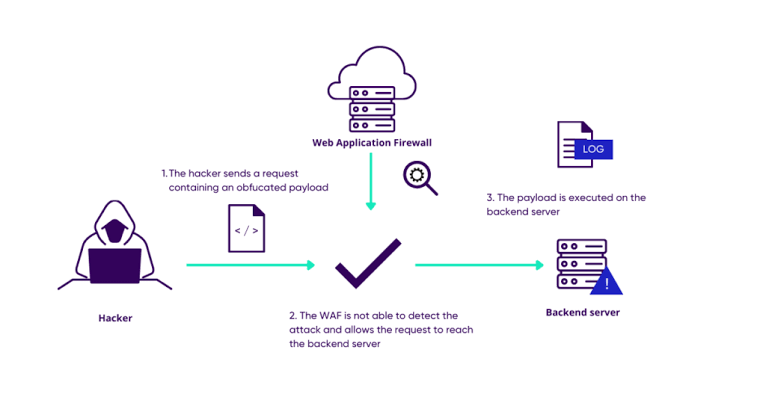
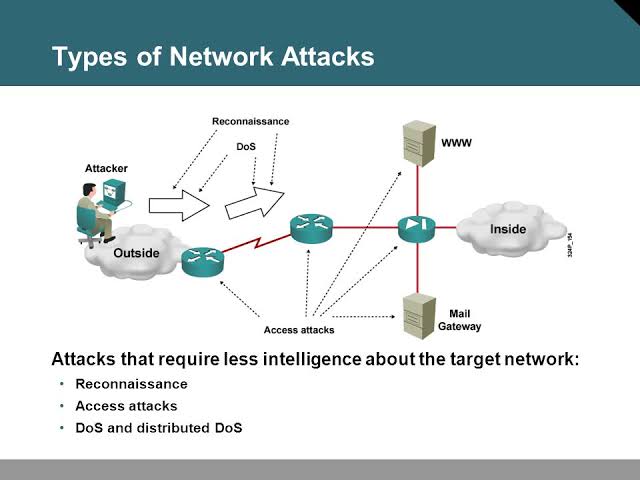
-> Understanding of web-application attacks :-

* 1.) Directory traversal :-
* Description : Directory traversal, also known as path traversal or directory climbing, is a vulnerability in a web application server caused by a HTTP exploit. The exploit allows an attacker to access restricted directories, execute commands, and view data outside of the web root folder where application content is stored.
* 
* Business Impact :- When using this attack, the directory traversal can lead to unauthorized access of sensitive information stored in files outside of the web root directory. This could include: system files, configuration files, or even user data. The unauthorized access of confidential data is a direct breach of privacy and can lead to information theft.
* 2.) Cookie Snooping :-
* Description: Cookie poisoning is a type of cyber attack in which a bad actor hijacks, forges, alters or manipulates a cookie to gain unauthorized access to a user's account, open a new account in the user's name or steal the user's information for purposes such as identity theft. Cookie poisoning is also known as session hijacking.
* 
* Business Impact :-By using this attack, the attacker thus by stealing a user's cookies, a cybercriminal can gain access to the user's online accounts without permission. This unauthorized access can be used for nefarious activities, such as stealing personal information, financial data, or intellectual property.
* 3.) Buffer Overflows :-
* Description : A buffer overflow occurs when a program or process attempts to write more data to a fixed-length block of memory, or buffer, than the buffer is allocated to hold. Buffers contain a defined amount of data; any extra data will overwrite data values in memory addresses adjacent to the destination buffer.



* Business Impact :-The buffer overflow attacks have been responsible for some of the biggest data breaches in history. A buffer overflow attack will typically lead to the system crashing. It may also result in a lack of availability and programs being put into an infinite loop.Buffer overflows can be exploited by attackers to corrupt software. Despite being well-understood, buffer overflow attacks are still a major security problem that torment cyber-security teams.
* 4.) Captcha attacks :-
* Description :This type of attack is dangerous as users unknowingly solve the Captcha and provide information to hackers which breaches their privacy or the nature of confidential info. The Captcha attacks have a hundred percent of success as these are designed as deep learning or machine learning models.
* 
* Business Impact :- When using captcha tools and multi-factor authentication (MFA) to protect against fraud can also have the unintended consequence of increasing user friction and customer support calls, as these processes can be challenging to complete correctly and can lead to account lockout for legitimate customers.
* 5.) DNS Rebinding attack :-
* Description : DNS rebinding is a method of manipulating resolution of domain names that is commonly used as a form of computer attack. In this attack, a malicious web page causes visitors to run a client-side script that attacks machines elsewhere on the network.
* 
* Business Impact :- The DNS rebinding attack can compromise victims' browsers as traffic tunnels to exploit private services. With this technique, attackers can steal confidential information and send forged requests to victims' servers.DNS tunneling techniques enable threat actors to compromise network connectivity and gain remote access to a targeted server. Other forms of DNS attacks can enable threat actors to take down servers, steal data, lead users to fraudulent sites, and perform Distributed Denial of Service (DDoS) attacks.
* 6.) Clickjacking attacks :-
* Description : It is also known as a “UI redress attack”, is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page.
* 
* Business Impact :- It is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.This spells trouble for any organizations that rely on protecting sensitive data and intellectual property.
* 7.) RC4 NOMORE attack :-
* Description : The RC4 NOMORE attack exposes weaknesses in this RC4 encryption algorithm. More precisely, in most situations where RC4 is used, these weaknesses can be used to reveal information which was previously thought to be safely encrypted.
* 
* Business Impact :- Because RC4 is a stream cipher, it is more malleable than common block ciphers. If not used together with a strong message authentication code (MAC), then encryption is vulnerable to a bit-flipping attack. The cipher is also vulnerable to a stream cipher attack if not implemented correctly.The vulnerabilities found in RC4 means RC4 is extremely insecure, so very few applications use it now. RC4 cannot be used on smaller streams of data, so its usage is more niche than other stream ciphers.
* 8.) DMZ Protocol attack :-
* Description : A DMZ or demilitarized zone is a perimeter network that protects and adds an extra layer of security to an organization's internal local-area network from untrusted traffic.
* 
* Business Impact :- The DMZ can have a major impact on security if not protected properly. In the event that a hacker gains entry to a file server in the DMZ, they may be able to access and download sensitive data and trading partner files that were placed there.No internal protections, so your employees and authorized users will still tap into the very sensitive data you store for your company.
* 9.) OBFUSCATION attack :-
* Description : Obfuscation refers to the process of concealing something important, valuable, or critical. Obfuscation means to make something difficult to understand. Programming code is often obfuscated to protect intellectual property or trade secrets, and to prevent an attacker from reverse engineering a proprietary software program. Encrypting some or all of a program's code is one obfuscation method.
* 
* Business Impact :- It adds time and complexity to the build process for the developers. It can make debugging issues after the software has been obfuscated extremely difficult.The main weakness cited against obfuscation is that adding extra layers of security bogs down code performance. Some estimate that obfuscation can impact program performance between 10% and 80%.
* 10.) Network access attacks :-
* Description : It is a malicious software that attacks a set of computers connected through a private network. The attacker gains access and controls all the systems on that network without the knowledge of the owner.
* 
* Business Impact :- A cyber attack can damage a company's reputation, which can lead to a loss of trust from customers, partners, and investors. Cyber attacks can result in the theft of a company's intellectual property, which can damage its competitive advantage.Nowaday's today's consequences of cyber attacks can include stolen data, destroyed networks, and thousands or even millions of dollars in recovery efforts.