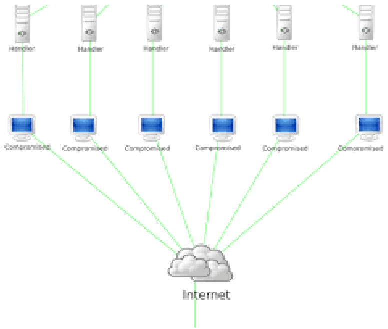
Rohit Patiballa

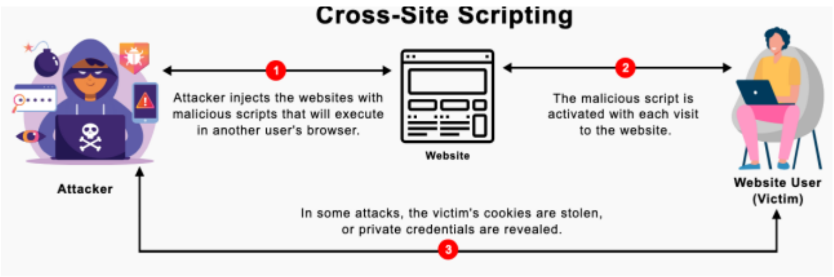
Task - 5

10 most common web server attacks

1. Denial of Service (DoS) attack: This is an attempt to make a web server accessible to legitimate users. This can be done by flooding the server with so much traffic that it cannot handle it, or by exploiting a vulnerability in the server software.

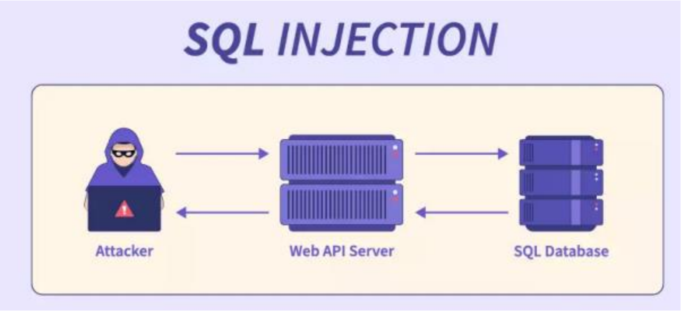


2. Cross-site scripting (XSS) attack: This is an attack that injects malicious code into a web page. When a user visits a page, code is executed in their browser that can steal their cookies or other sensitive information.

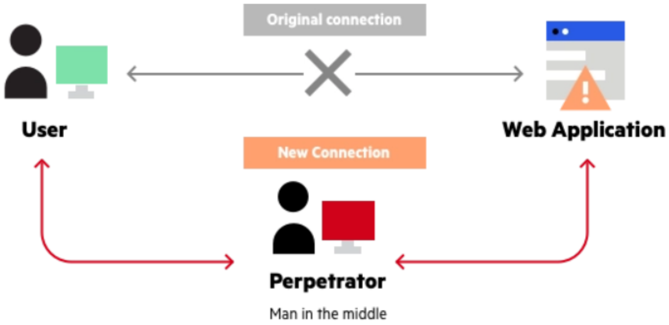

Cross-Site Scripting
1
Attacker injects the websites with malicious scripts that will execute in another user's browser.
Website
2
The malicious script is activated with each visit to the website.
Attacker
Website User (Victim)
In some attacks, the victim's cookies are stolen, or private credentials are revealed.
3

3. SQL Injection Attack: This is an attack that exploits a vulnerability in the database of a web application. An attacker can

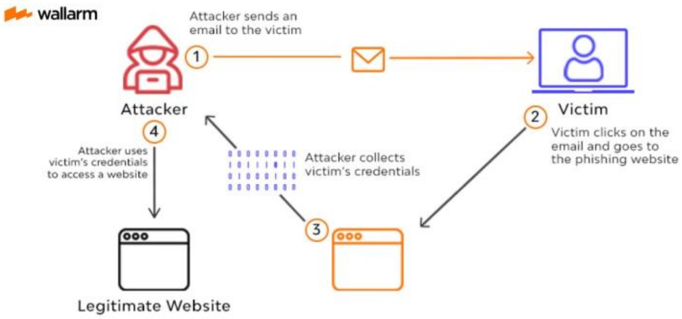
insert malicious code into the request, which can be used to steal data from the database or change its content.



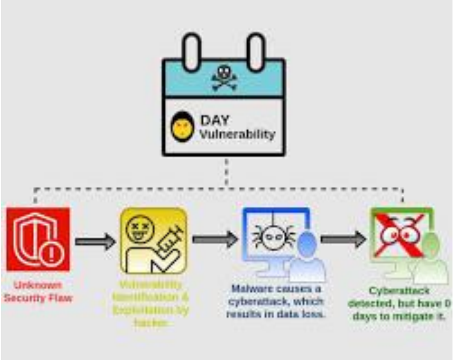
4. Man-in-the-middle (MitM) attack: This is an attack where the attacker breaks the communication between the client and the server. The attacker can then read or modify the communication or impersonate the client or server.



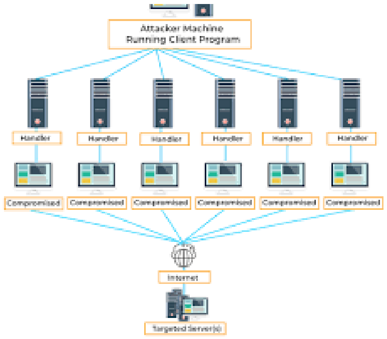
5. Phishing attack: This is an attack where an attacker sends fraudulent emails or text messages that appear to be from a legitimate source. Emails or text messages often contain a link that, when clicked, takes the victim to a fake website that looks like a real website. If the victim enters their credentials on the fake website, the attacker can steal them.


wallarm
Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
3
Legitimate Website

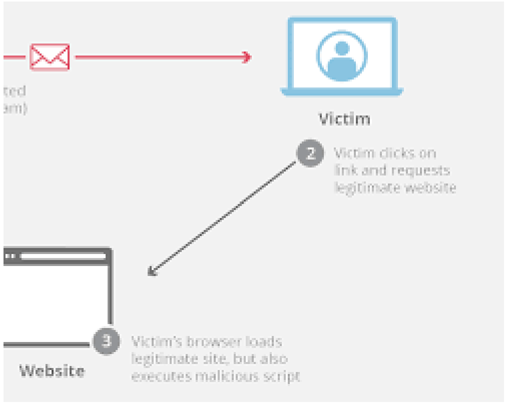
6. Zero-day attack: This is an attack that exploits a software vulnerability unknown to the software vendor. Zero-day attacks are often very difficult to defend against because there is no patch available to fix the vulnerability.


DAY
Vulnerability
Unknown Security Flaw
Vulnerability Identification & Exploitation by hacker.
Malware causes a cyberattack, which results in data loss.
Cyberattack detected, but have 0 days to mitigate it.

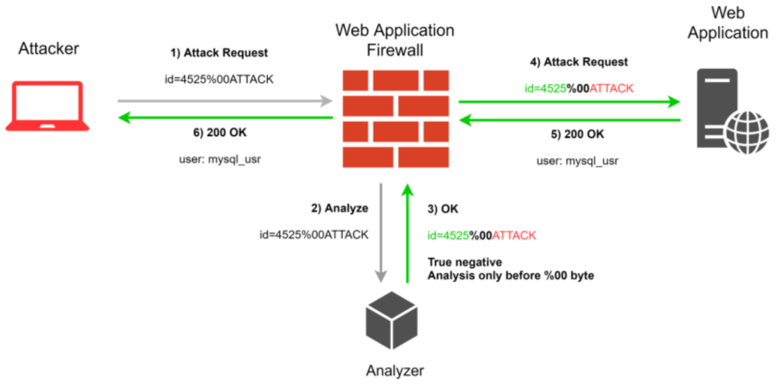
7. Botnet attack: This is an attack in which an attacker takes over a large number of computers (called bots) and uses them to attack other computers or websites.



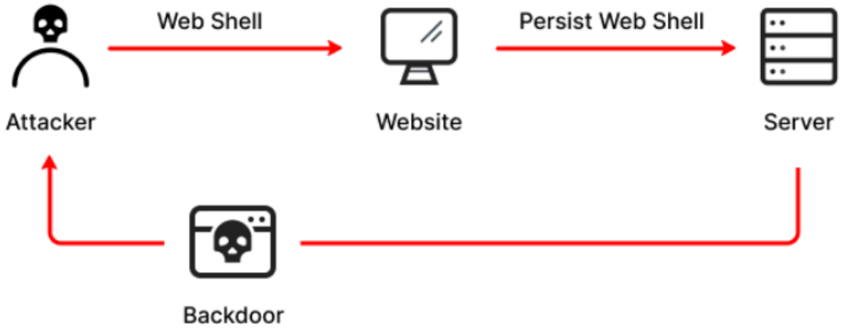
8. Distributed Denial of Service (DDoS): This is a DoS attack that uses a large number of bots to flood the target server with traffic. DDoS attacks can be very difficult to defend against because they can generate a lot of traffic.


ted
am)
Victim
2
Victim clicks on link and requests legitimate website
3
Victim's browser loads legitimate site, but also executes malicious script
Website

9. Web Application Firewall (WAF) Bypass Attack: This is an attack that bypasses WAF security features. WAFs are designed to protect web applications from attacks, but attackers who know how to exploit their weaknesses can bypass them.



10. Web Shell Attack: This is an attack where an attacker gains access to a web server and installs a web-based shell. A web shell is a program that allows an attacker to execute commands on a server. Web shell attacks can be used to steal data, install malware, or take control of a server.


Web Shell
Persist Web Shell
Attacker
Website
Server
Backdoor