Task - 4

The top 10 plot attacks other than OWASP Top 10

1. **Phishing:** This is a social engineering attack that involves sending fraudulent emails or text messages that appear to be from a legitimate source. The goal is to trick the victim into clicking on a malicious link or providing personal information.

Pic - www.imperva.com

Phishing attack illustration

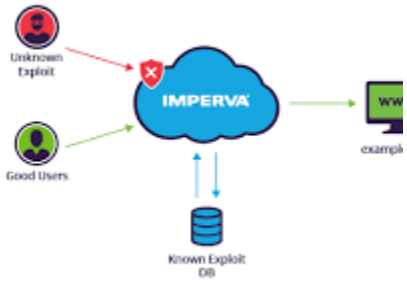
2. **Malware:** This is software that is designed to harm a computer system. Malware can be installed on a system through a variety of ways, such as clicking on a malicious link, opening an infected attachment, or downloading a file from an untrusted source.

Pic - www.freepik.com

Malware attack illustration

3. **Zero-day attacks:** These are attacks that exploit vulnerabilities in software that the software vendor is not aware of. Zero-day attacks are often very difficult to defend against because there is no patch available to fix the

vulnerability.



Pic - www.imperva.com

Zero-day attack illustration

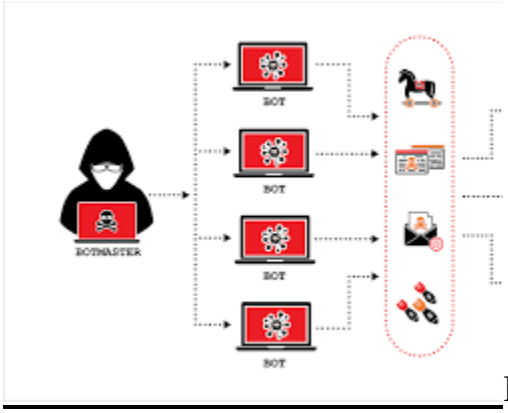
4. **Ransomware:** This is a type of malware that encrypts the victim's files and demands a ransom payment in order to decrypt them. Ransomware attacks are often very successful because victims are often willing to pay the ransom to get their files back.

Pic - www.finance-monthly.com

Ransomware attack illustration

5. **DDoS attacks:** These are attacks that overwhelm a website or server with traffic, making it unavailable to legitimate users. DDoS attacks can be

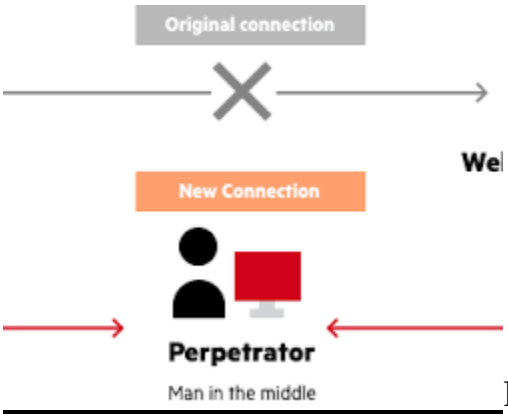
carried out using a variety of methods, such as botnets or rented servers.



Pic - www.thesslstore.com

DDoS attack illustration

6. **Man-in-the-middle attacks:** These are attacks that intercept communications between two parties. The attacker can then read, modify, or even drop the communications. Man-in-the-middle attacks can be carried out using a variety of methods, such as WiFi spoofing or DNS poisoning.

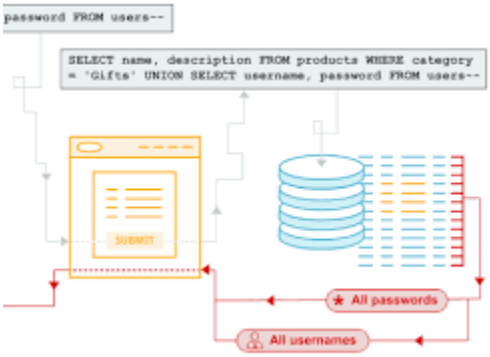


Pic - www.imperva.com

Man-in-the-middle attack illustration

7. **SQL injection:** This is an attack that exploits vulnerabilities in SQL databases. The attacker can use SQL injection to steal data from the database, modify data in the database, or even take control of the database

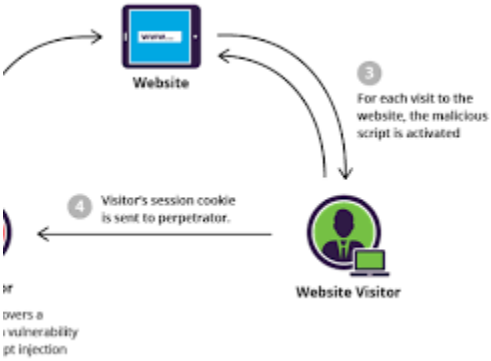
server.



Pic - portswigger.net

SQL injection attack illustration

8. **Cross-site scripting (XSS):** This is an attack that injects malicious code into a legitimate website. The malicious code can then be executed by the victim when they visit the website. XSS attacks can be used to steal cookies, session tokens, or other sensitive information.

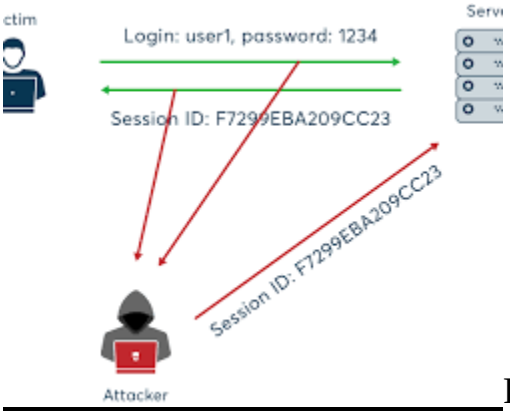


Pic - www.imperva.com

Cross-site scripting (XSS) attack illustration

9. **Session hijacking:** This is an attack that steals a victim's session token. The session token is used to authenticate the victim to a website. Once the attacker has the session token, they can impersonate the victim and access

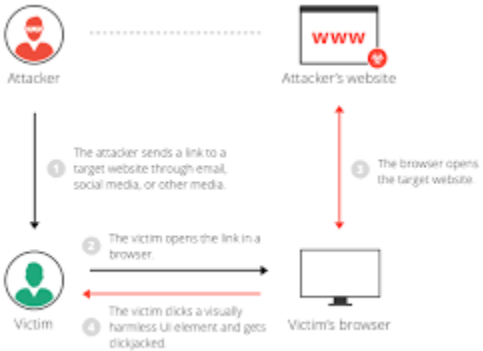
the victim's account.



Pic - cyberhoot.com

Session hijacking attack illustration

10. **Clickjacking:** This is an attack that tricks the victim into clicking on a malicious link or button. The malicious link or button may be hidden in a egitimate-looking image or web page.



Pic - www.imperva.com

Clickjacking attack illustration

These are just a few of the many types of plot attacks that exist other than Top 10 OWASP attacks , it’s advisable to educate ourselves about these attacks and take possible precautions for them.