Name: Sheikha Farook Batha

Regno:21bce8436

Task 1 week 2

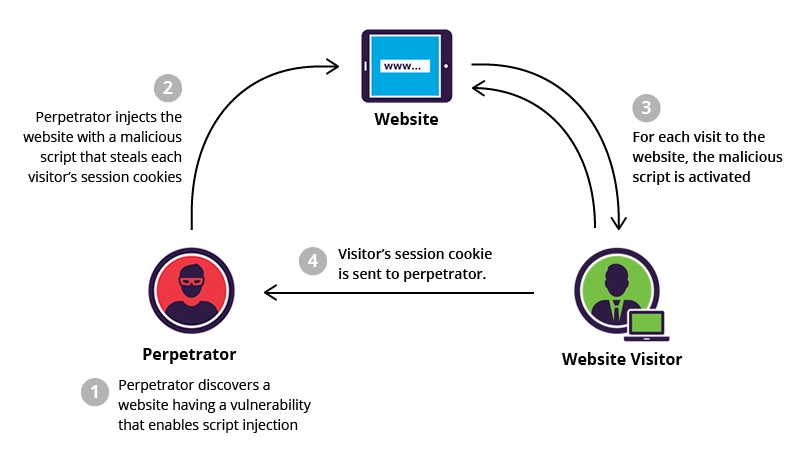
**10 web applications attacks**

https://smartinternz.com/externship-curriculum/1238

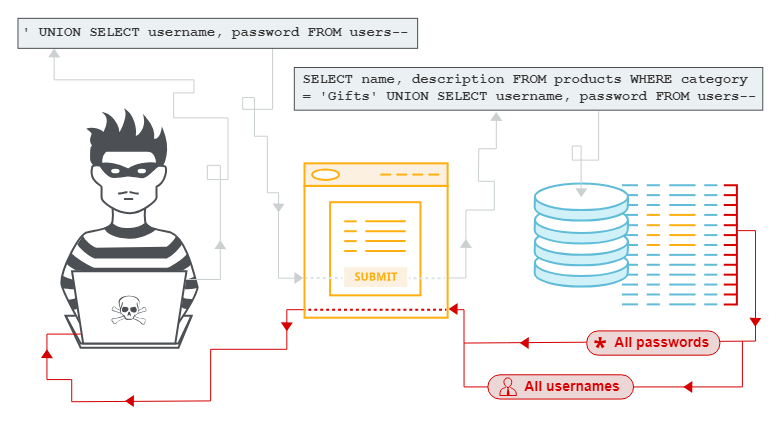
TASK 2 WEEK 2

**10 Web server attacks**

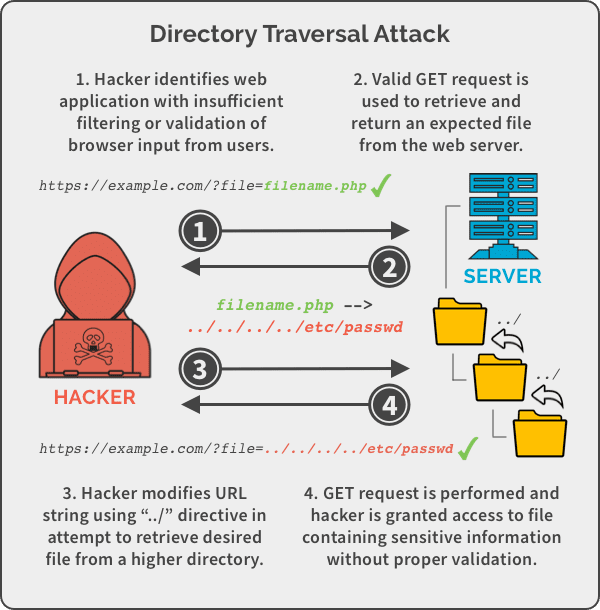
1. Cross-site scripting (XSS). This attack injects malicious code into a web page that is then executed by the victim's browser. XSS can be used to steal cookies, session tokens, or other sensitive information.



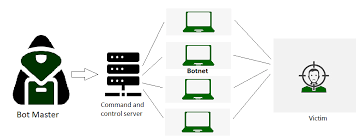
1. SQL injection. This attack injects malicious code into a SQL query that is then executed by the web server. SQL injection can be used to steal data from the database, modify data, or even take control of the web server.



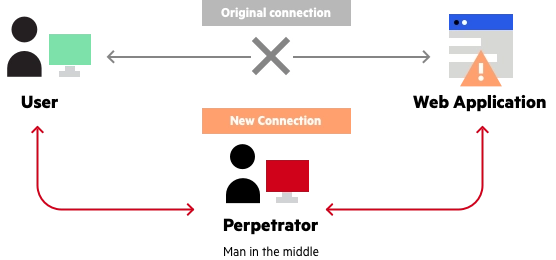
1. Directory traversal. This attack exploits vulnerabilities in the web server's file system to access files that are not supposed to be accessible. Directory traversal can be used to steal sensitive files, such as source code or configuration files.



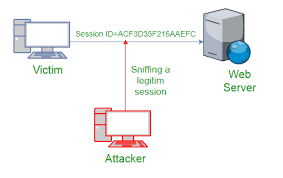
1. Denial-of-service (DoS) attack. This attack overwhelms the web server with traffic, making it unavailable to legitimate users. DoS attacks can be carried out using a variety of methods, such as flooding the server with requests or sending large amounts of data.



1. Man-in-the-middle (MitM) attack. This attack intercepts communication between the client and server, allowing the attacker to read or modify the data. MitM attacks can be carried out using a variety of methods, such as spoofing the victim's IP address or setting up a rogue Wi-Fi hotspot.



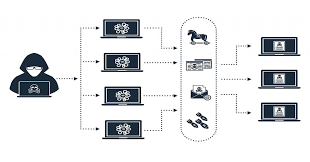
1. Session hijacking. This attack steals the victim's session token, allowing the attacker to impersonate the victim. Session hijacking can be carried out using a variety of methods, such as exploiting a vulnerability in the web server or using a malicious cookie.



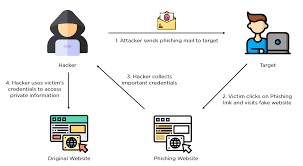
1. Zero-day attack. This attack exploits a vulnerability in the web server that is not yet known to the vendor. Zero-day attacks are the most dangerous type of attack because there is no patch available to protect against them.



1. Botnet attack. This attack uses a network of infected computers, called a botnet, to attack the web server. Botnet attacks can be used to carry out a variety of attacks, such as DoS attacks, spam attacks, or click fraud.



1. Phishing attack. This attack sends fraudulent emails that appear to be from a legitimate source, such as a bank or credit card company. The emails often contain a link that, when clicked, takes the victim to a fake website that looks like the real website. The fake website then asks the victim to enter their personal information, which the attacker can then use to steal the victim's identity.



1. Watering hole attack. This attack targets a specific website that is known to be frequented by the victim. The attacker then infects the website with malware that is triggered when the victim visits the website.

