Web Server Attacks

1.Web Cache Poisoning Attack

Web cache poisoning is an advanced technique whereby an attacker exploits the behavior of a web server and cache so that a harmful HTTP response is served to other users.

Fundamentally, web cache poisoning involves two phases. First, the attacker must work out how to elicit a response from the back-end server that inadvertently contains some kind of dangerous payload. Once successful, they need to make sure that their response is cached and subsequently served to the intended victims.

A poisoned web cache can potentially be a devastating means of distributing numerous different attacks, exploiting vulnerabilities such as XSS, JavaScript injection, open redirection, and so on.

2.HTTP Response-Splitting Attack

HTTP Response Splitting occurs when a web server fails to sanitize CR and LF characters before the data is included in outgoing HTTP headers.

To launch a successful exploit, the application must be vulnerable to the injection of Carriage Return (CR, ASCII 13, \r) and Line Feed (LF, ASCII 10, \n) characters, which are used in the HTTP protocol to terminate a line, into the response header. This technique is also referred to as “CRLF Injection in HTTP Headers”, and it gives attackers control of the remaining headers and body of the response that the application will send.

3.Phishing Attacks

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

4.Sniffing Attack

Sniffing attacks refer to data thefts caused by capturing network traffic through packet sniffers that can unlawfully access and read the data which is not encrypted. The data packets are captured when they flow through a computer network. The packet sniffers are the devices or media used to do this sniffing attack and capture the network data packets. They are called network protocol analyzers. Unless the packets are encrypted with strong network security, hackers will be able to steal and access the data.

5.DNS Amplification Attack

This DDoS attack is a reflection-based volumetric distributed denial-of-service (DDoS) attack in which an attacker leverages the functionality of open DNS resolvers in order to overwhelm a target server or network with an amplified amount of traffic, rendering the server and its surrounding infrastructure inaccessible.