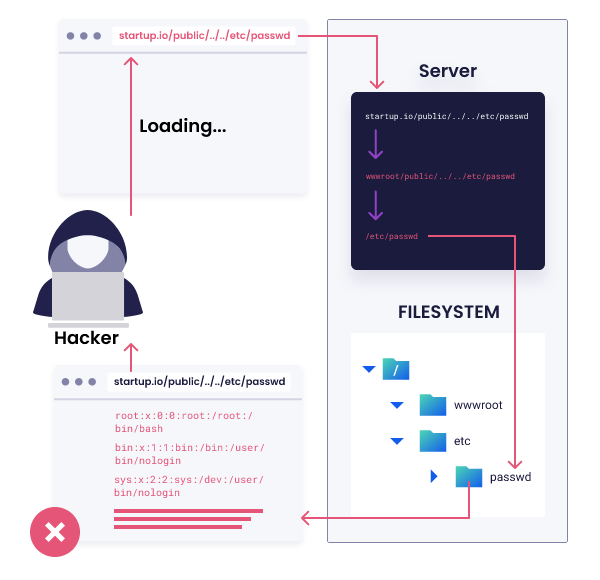
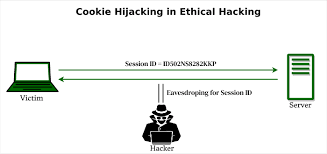
**TASK -4(28-08-23 MONDAY) by Sameer chauhan**

**UNDERSTANDING WEB APPLICATION ATTACK OR THREATS-**

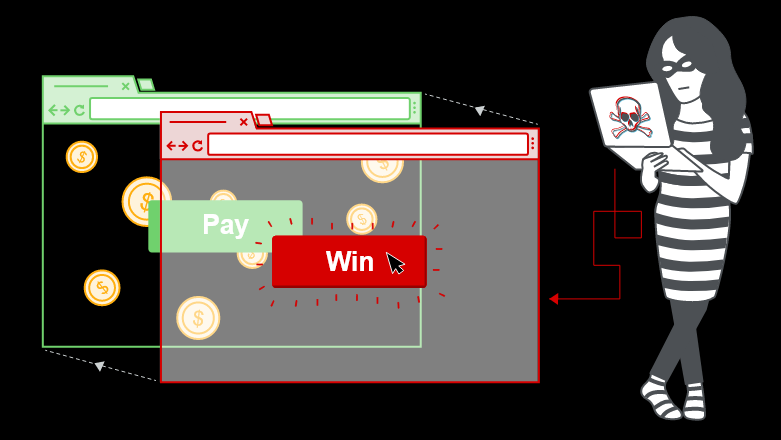
**1-Directory traversal-Directory traversal also known as file path traversal is a web security vulnerability that allows an attacker to read arbitrary files on the server that is running an application. This might include application code and data, credentials for back-end systems, and sensitive operating system files.**



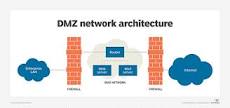
**2-cookie snooping-Cookie snooping, also known as cookie stealing or session hijacking, is a type of cyber attack where an attacker gains unauthorized access to a user's cookies in order to impersonate that user and gain access to their authenticated sessions on a website or application.**

****

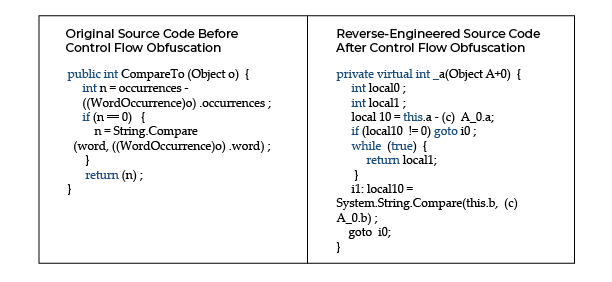
**3-Click jacking attacks-Clickjacking is an interface-based attack in which a user is tricked into clicking on actionable content on a hidden website by clicking on some other content in a decoy website. A web user accesses a decoy website (perhaps this is a link provided by an email) and clicks on a button to win a prize. Unknowingly, they have been deceived by an attacker into pressing an alternative hidden button and this results in the payment of an account on another site**.



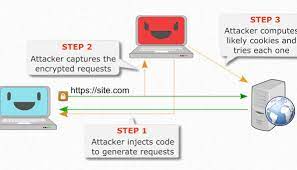
**4-DMZ Protocol attack-A DMZ Demilitarized Zone protocol attack typically refers to a type of cybersecurity attack that targets vulnerabilities within the protocols and services used in the DMZ network architecture.** **However, if the protocols and services used within the DMZ are not properly secured and configured, they can become entry points for attackers to compromise systems and gain unauthorized access**

****

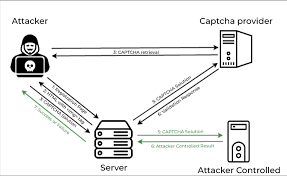
**5-Obfuscation application-*an attacker might use obfuscated code as part of their attack strategy. They might inject malicious code into a system while obfuscating it to make it harder for security tools or analysts to detect and understand the malicious intent.***



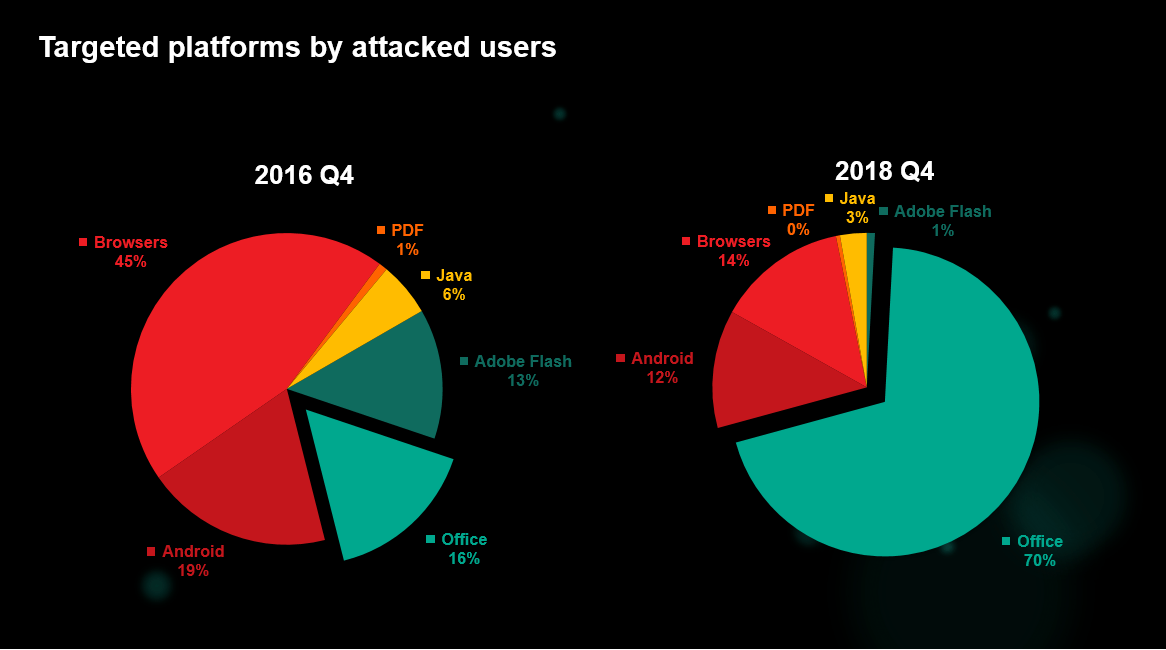
**6-RC4 Nomore attack-The RC4 NoMore attack, specifically, highlighted new biases in the RC4 keystream generation process, which could be exploited to recover portions of the plaintext in certain scenarios.**

****

**7-Captcha attack- Attackers use human workers or automated services to solve CAPTCHAs. These services employ individuals who manually solve CAPTCHAs in real-time or use advanced image recognition algorithms to automate the process.**

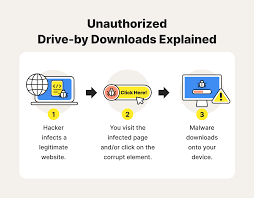
****

**8-Platform exploits- refer to vulnerabilities and techniques that malicious actors use to exploit weaknesses in software platforms, operating systems, applications, or hardware.**



**9-Fuzz testing-** **also known as fuzzing, is a software testing technique used to discover vulnerabilities, bugs, and security flaws in applications by providing them with unexpected or invalid input.**



**10-Drive by Download attack-A drive-by download attack is a type of cyber attack where a user's device is infected with malicious software (malware) without the user's knowledge or consent, simply by visiting a compromised or malicious website.**