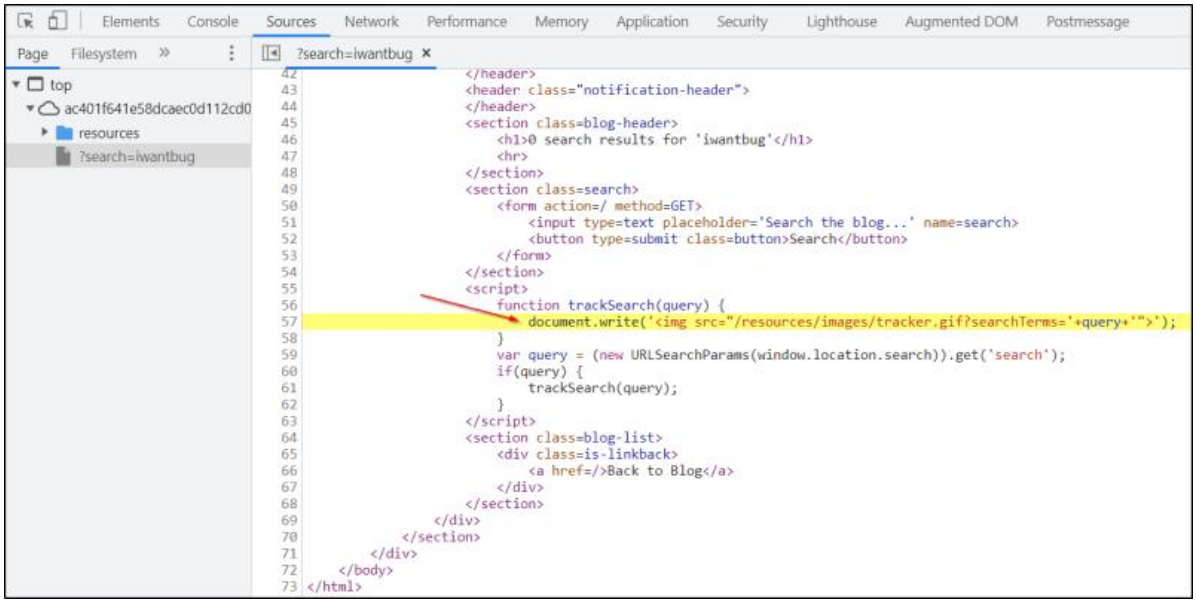
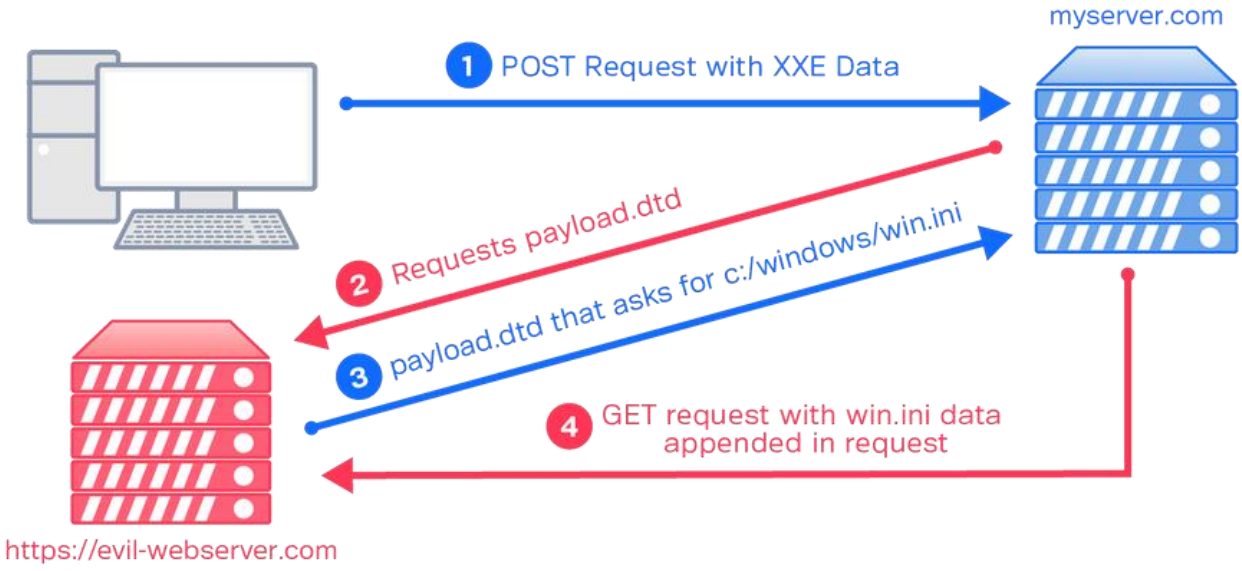
Name : Veekshitha
Reg no: 21BCE8943

Task - 3

DOM-Based Cross-Site Scripting (DOM XSS):
DOM-based XSS attacks occur when the manipulation of the Document Object Model (DOM) in a web page leads to the execution of malicious scripts. These attacks can bypass traditional XSS defenses that focus on server-side input validation.

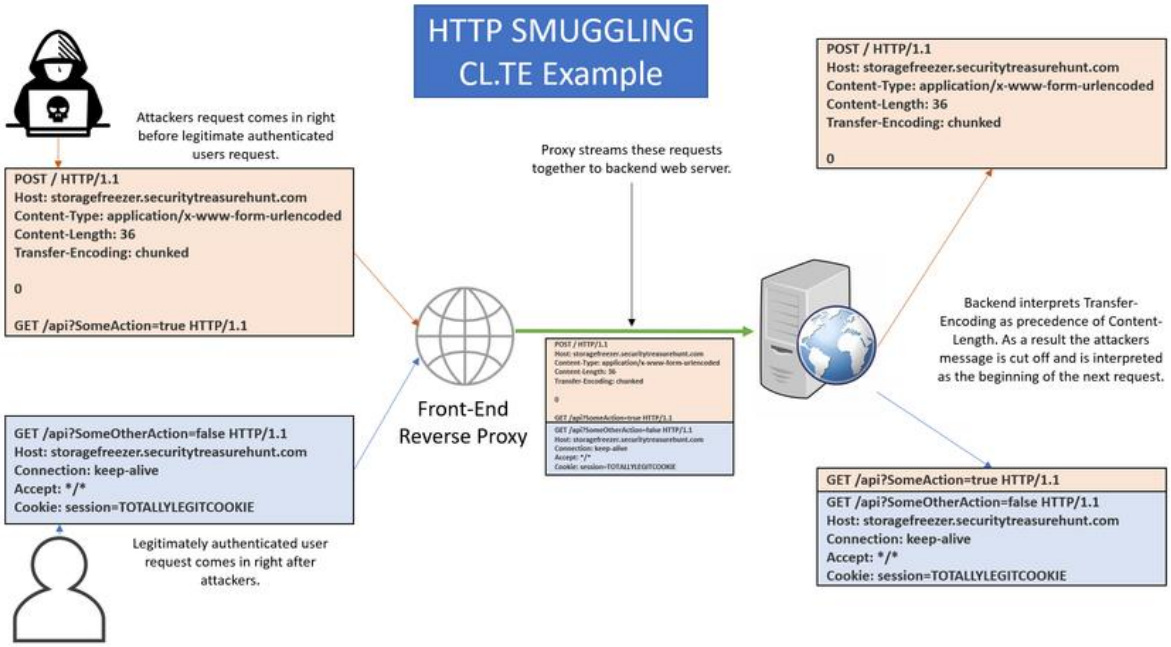


XML External Entity (XXE) Attacks:
XXE attacks target vulnerabilities in XML parsers by exploiting the ability to include external entities. Attackers can use XXE to read files, perform port scans, or launch denial-of-service attacks.



Content Security Policy (CSP) Bypass:
CSP is a security feature that helps prevent XSS attacks by defining which sources of content are considered legitimate. Attackers in 2021 developed techniques to bypass or circumvent CSP rules to execute malicious scripts.

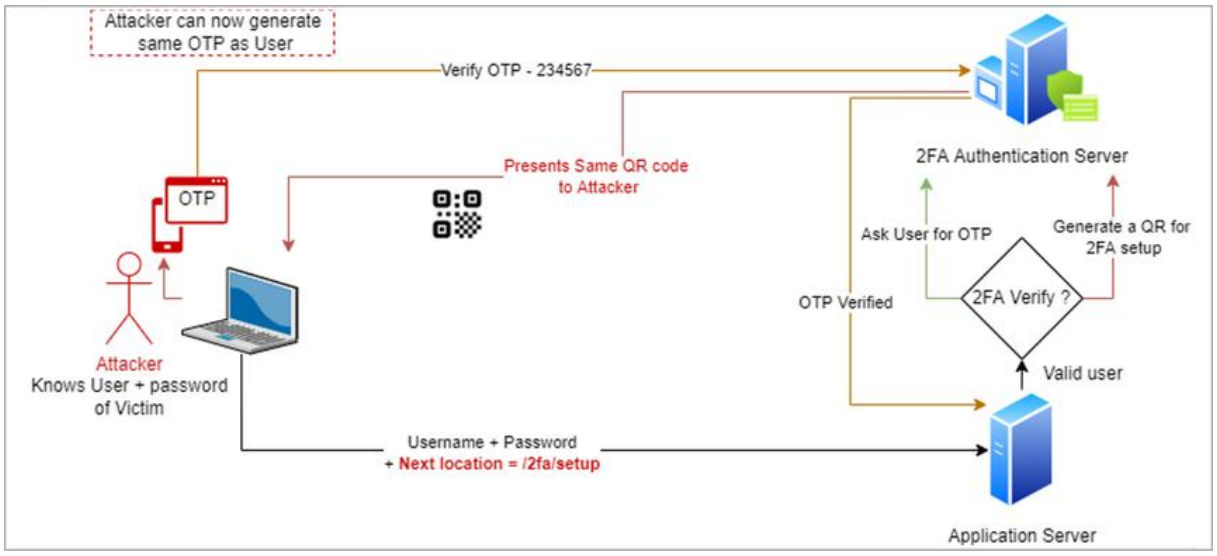
HTTP Request Smuggling:
This attack involves manipulating HTTP requests and taking advantage of differences in the way front-end and back-end servers interpret them. Attackers could use this technique to bypass security measures and potentially access unauthorized resources.



Server-Side Template Injection (SSTI):
SSTI attacks involve injecting malicious code into server-side templates, which are then executed by the application. This could lead to code execution on the server and potentially a full compromise.

Serverless Function Attacks:
As serverless architecture gained popularity, attackers targeted serverless functions with various attacks like code injection, privilege escalation, and resource exhaustion to exploit vulnerabilities.

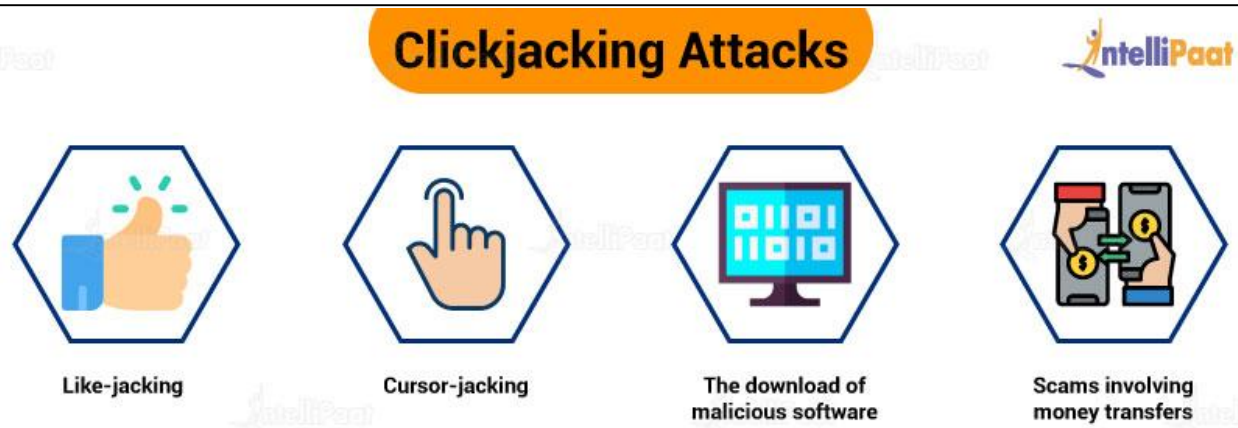
Bypassing Two-Factor Authentication (2FA):
While not exclusively a web application-based attack, attackers devised methods to bypass or circumvent two-factor authentication mechanisms, often by targeting the communication channel or exploiting vulnerabilities in the implementation.



HTML Injection:
Similar to XSS, HTML injection attacks involve injecting malicious HTML code into a web application. This could lead to the manipulation of content displayed to users or the stealing of sensitive information.

Path Traversal:
Path traversal attacks exploit vulnerabilities in the application's file handling to access files and directories that are not intended to be accessible. This can lead to unauthorized access to sensitive files.

Clickjacking:
Clickjacking attacks involve overlaying malicious content on top of legitimate web pages, tricking users into clicking on something different from what they perceive. These attacks can lead to unintended actions or disclosures.



Unvalidated Redirects and Forwards:
Attackers can exploit vulnerabilities that allow them to redirect users to malicious websites or manipulate URLs to trick users into performing actions they didn't intend.

Biometric Data Spoofing:
With the increasing use of biometric authentication, attackers began exploring ways to spoof biometric data to gain unauthorized access to accounts or devices.
