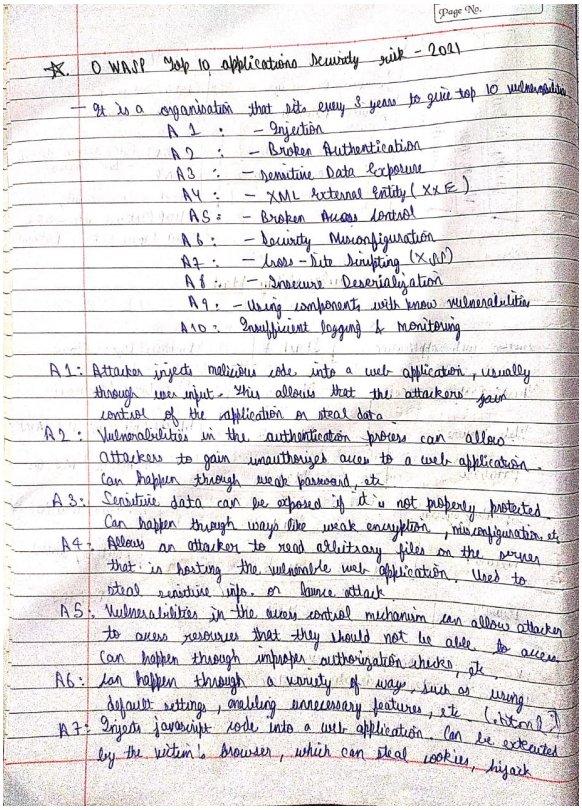
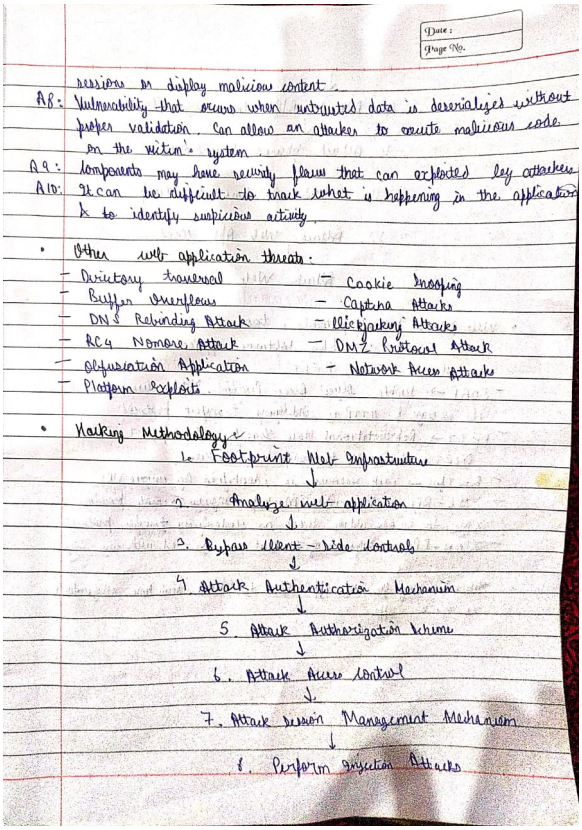
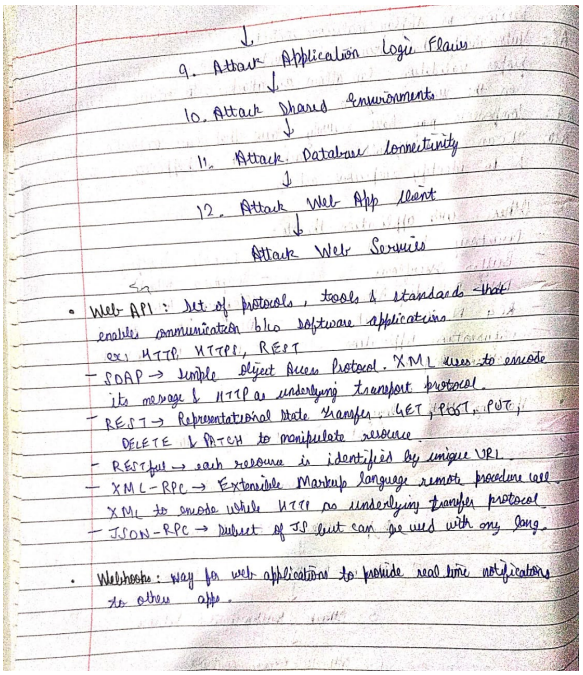
Class 5 - 28/08/2023

Today we studied about the 5-10 top 10 OWASP vulnerabilities, and some other web application threats like cookie snooping, etc. Then we studied the hacking methodology, then we studied about the web APIs like SOAP, REST, etc. At the end we studied about web hooks.

Screenshots from my short notes of today's class:





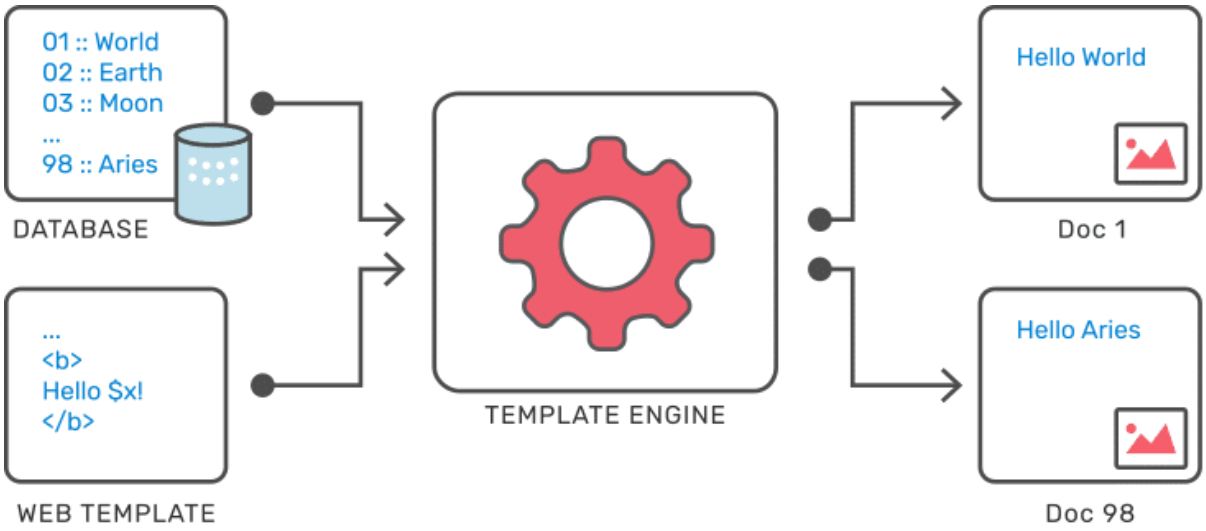


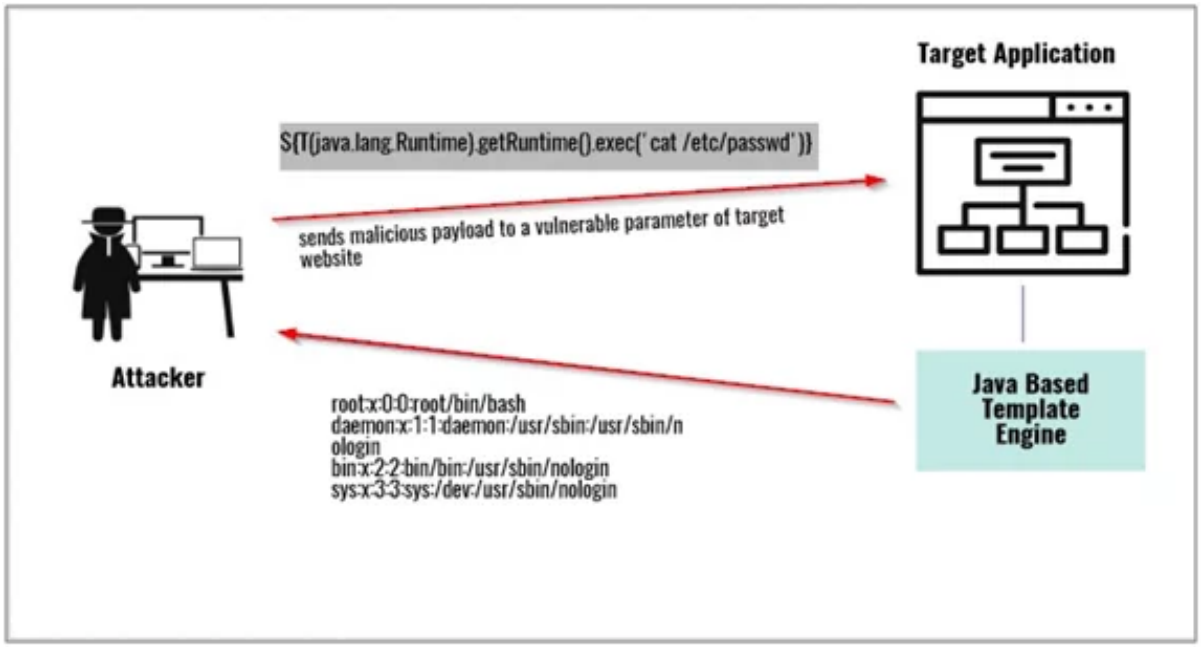
Task - Understanding Web Application attacks

Server-Side Template Injection (SSTI):

Description: SSTI occurs when user input is injected into server-side templates, allowing attackers to execute arbitrary code on the server.

Business Impact: SSTI can lead to complete server compromise, unauthorized data access, and sensitive information leakage. This can result in business downtime, data breaches, and severe reputational damage.

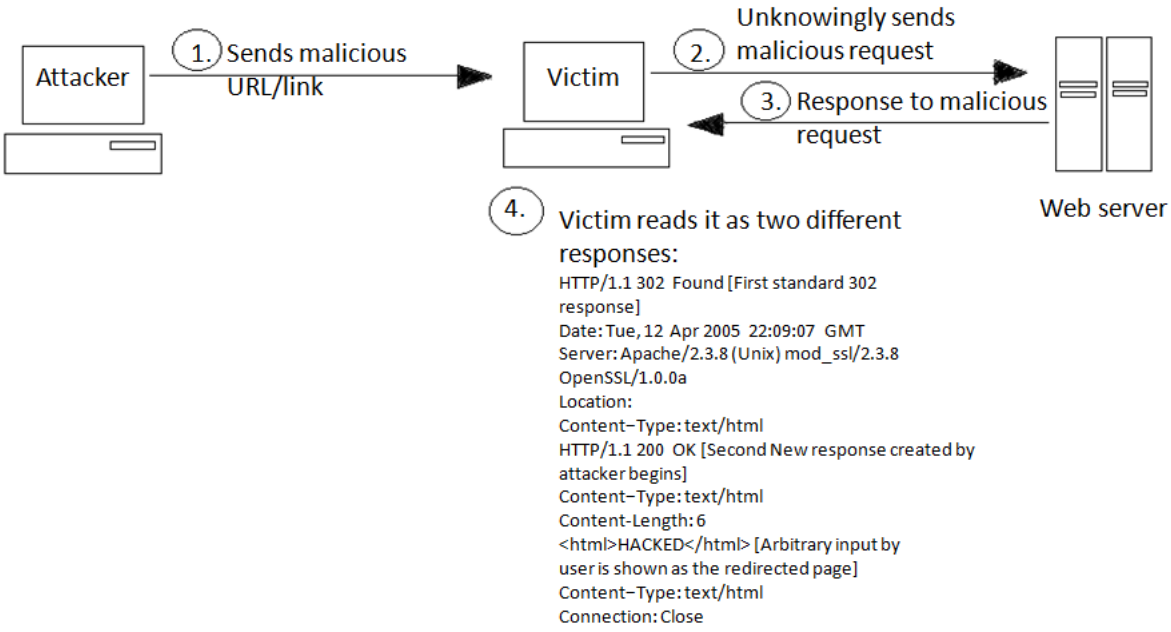




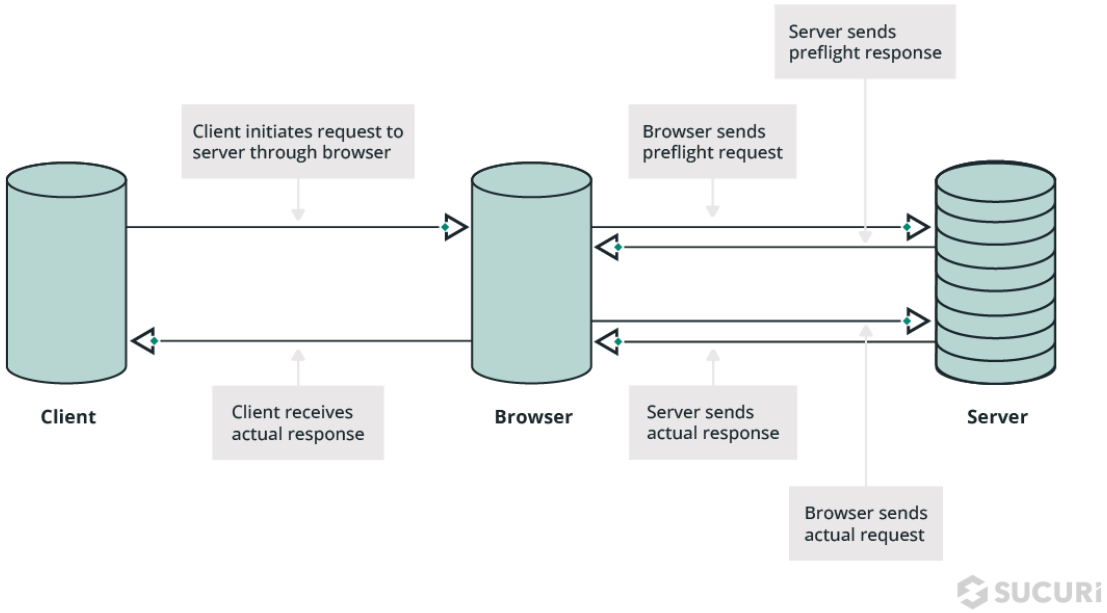
HTTP Response Splitting:

Description: HTTP response splitting involves injecting CRLF (Carriage Return Line Feed) characters into HTTP responses, allowing attackers to manipulate headers and potentially conduct attacks like session fixation.

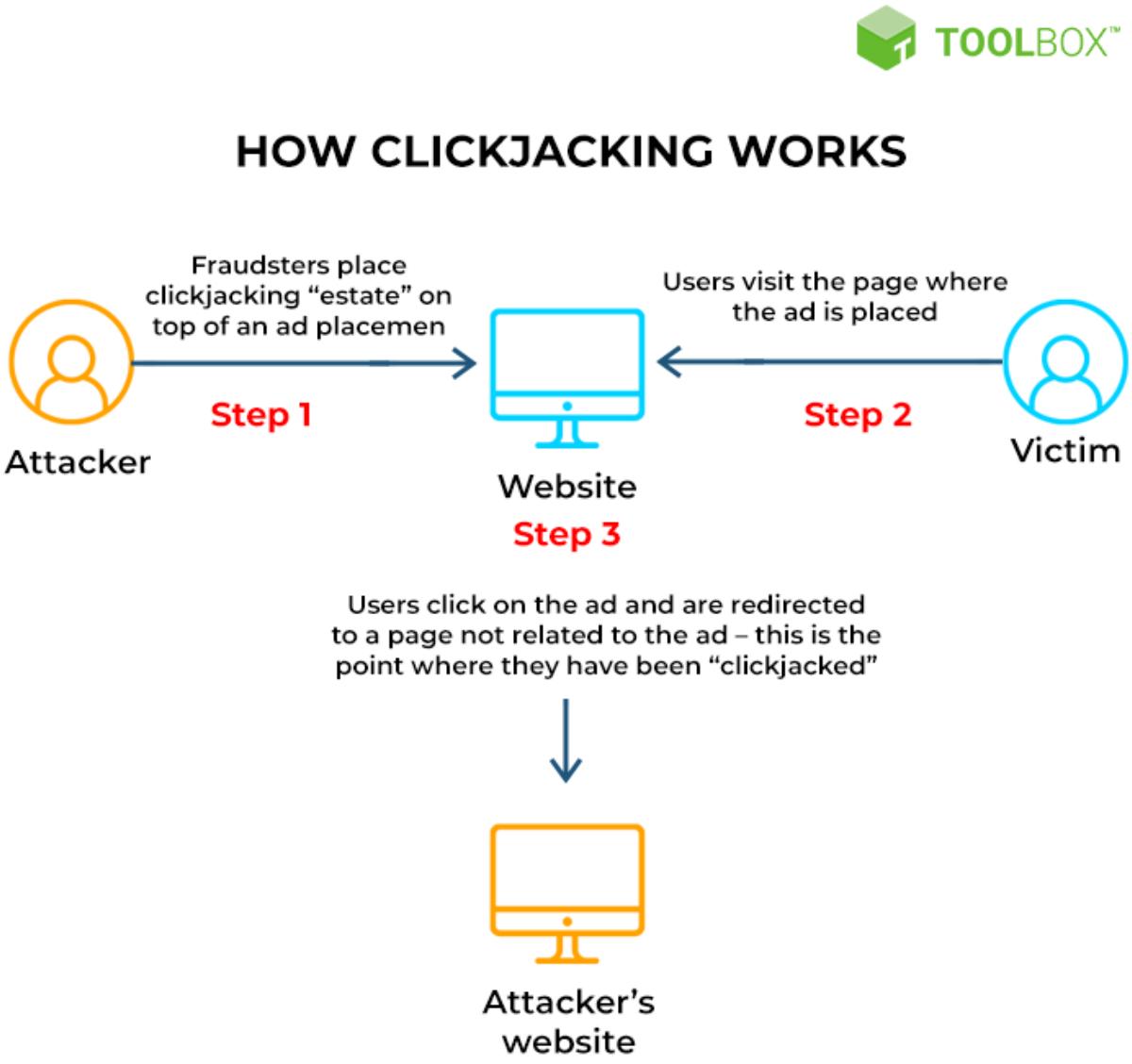
Business Impact: HTTP response splitting can lead to session hijacking, data manipulation, and phishing attacks. This can result in unauthorized access, loss of customer trust, and financial repercussions.



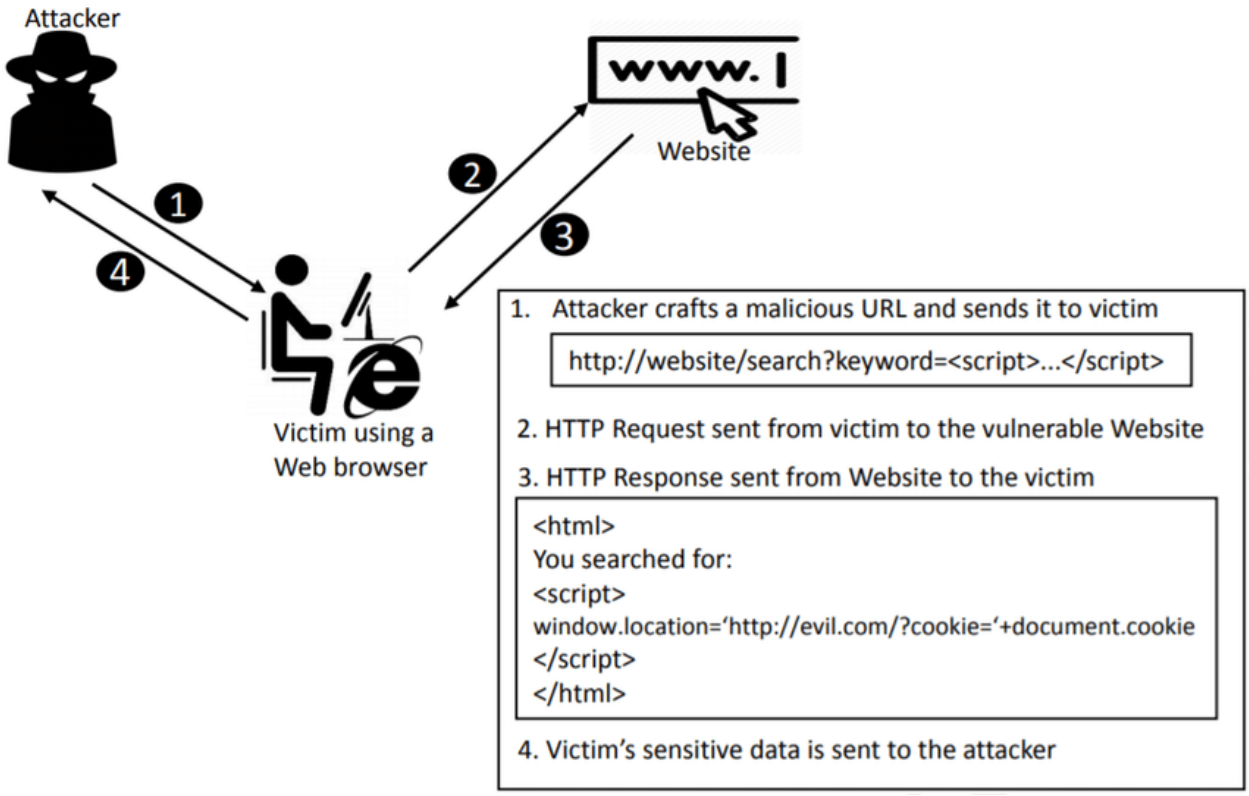
CORS Misconfiguration (Cross-Origin Resource Sharing):
Description: CORS misconfiguration occurs when inadequate security measures are in place, enabling unauthorized domains to access sensitive resources.
Business Impact: CORS misconfiguration can lead to data exposure, data theft, and unauthorized data modifications. This can result in legal consequences, regulatory non-compliance, and reputational harm.



Clickjacking:
Description: Clickjacking involves overlaying malicious content on top of legitimate web content, tricking users into performing actions they didn't intend to. This vulnerability occurs when an attacker tricks a user into clicking on a malicious link or button. This can be used to steal the user's credentials or to perform other unauthorized actions.
Business Impact: Clickjacking can lead to unauthorized actions, data manipulation, and fraud. This can result in financial losses, damage to user confidence, and legal liabilities.



DOM-Based Vulnerabilities:
Description: DOM-based vulnerabilities arise when client-side scripts manipulate the Document Object Model (DOM) in an insecure manner, potentially leading to unauthorized actions or data exposure.
Business Impact: DOM-based vulnerabilities can result in account compromise, data theft, and defacement. This can lead to loss of customer trust, reputational damage, and financial repercussions.

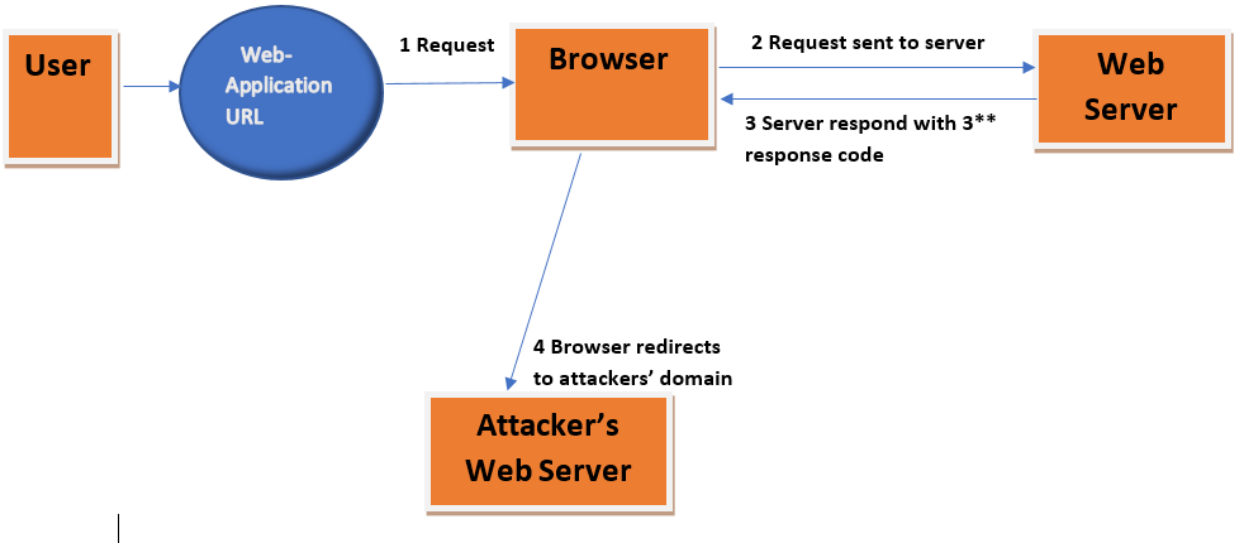


Insufficient Session Expiration:

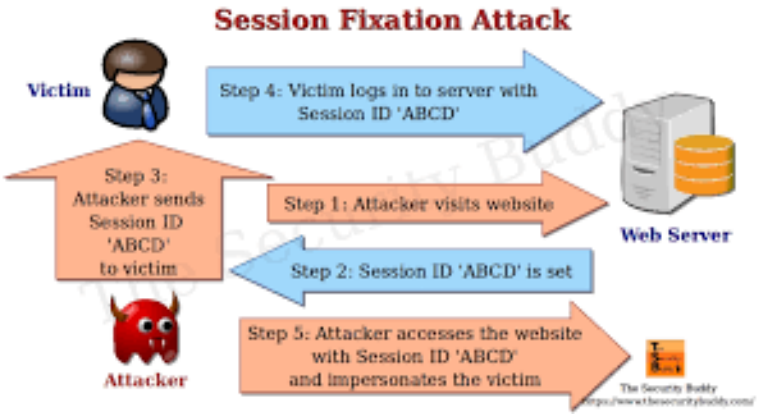
Description: Insufficient session expiration occurs when sessions remain active for too long after a user logs out, potentially allowing attackers to gain unauthorized access. This vulnerability occurs when an application does not properly manage sessions. This can allow attackers to hijack sessions or to steal session cookies.

Business Impact: Insufficient session expiration can lead to unauthorized access, data exposure, and compromised accounts. This can result in data breaches, legal issues, and reputational harm.

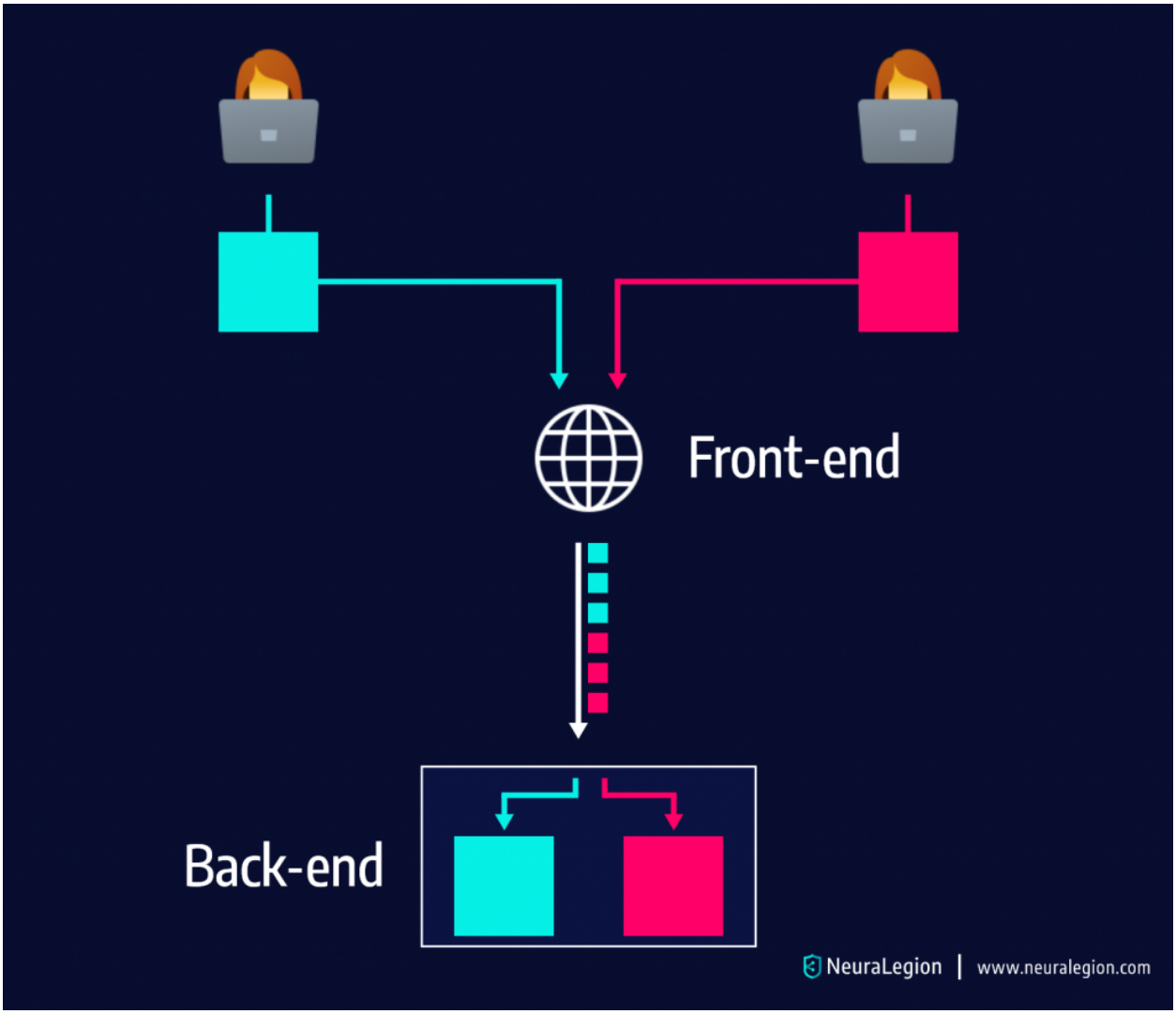
Unvalidated Redirects and Forwards:
Description: Unvalidated redirects and forwards involve improper validation of user-generated URLs, enabling attackers to redirect users to malicious websites. This vulnerability occurs when an application redirects or forwards users to a URL without properly validating the URL. This can allow attackers to redirect users to malicious websites.
Business Impact: Unvalidated redirects can lead to phishing attacks, malware distribution, and data theft. This can result in compromised user accounts, legal consequences, and reputational damage.



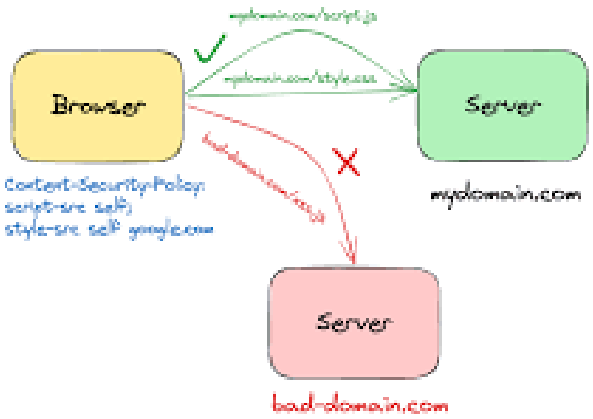
Session Fixation:
Description: Session fixation occurs when attackers set a user's session identifier, allowing them to hijack the user's session after login.
Business Impact: Session fixation can lead to unauthorized access, data exposure, and financial loss. This can result in compromised customer accounts, reputational harm, and potential legal liabilities.



Cross-Site Request Smuggling (CSRS):
Description: CSRS involves manipulating inconsistent interpretation of HTTP requests by different servers or proxies, potentially leading to unauthorized actions or data exposure. This vulnerability occurs when an attacker tricks a user into submitting a request to a website that the user is not authorized to access. This can be used to perform unauthorized actions on the user's behalf.
Business Impact: CSRS can lead to unauthorized actions, data leakage, and privilege escalation. This can result in unauthorized data access, financial losses, and reputational damage.



Content Security Policy (CSP) Bypass:
Description: CSP bypass occurs when attackers find ways to circumvent the security restrictions defined by Content Security Policy headers.
Business Impact: CSP bypass can lead to successful cross-site scripting attacks, data breaches, and unauthorized data modifications. This can result in compromised user data, legal issues, and loss of customer trust.


mydomain.com/script.js
mydomain.com/style.css
Browser
Server
mydomain.com
Content-Security-Policy:
script-src self;
style-src self ymyle.com
bad-domain.com/evil.js
Server
bad-domain.com