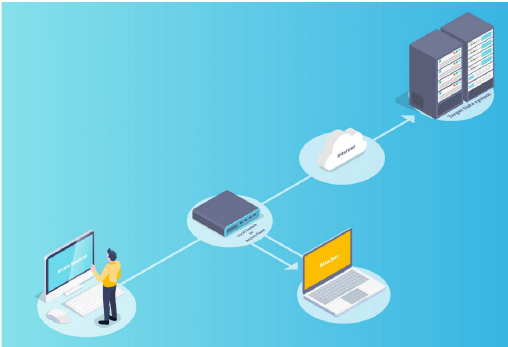
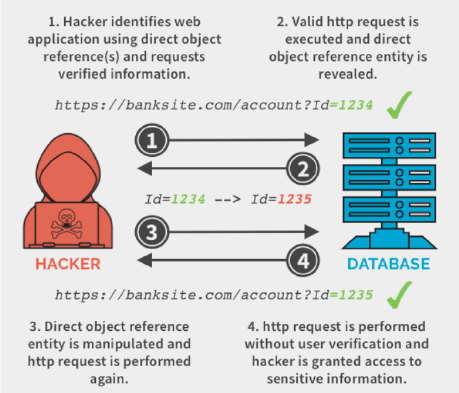
TASK 2

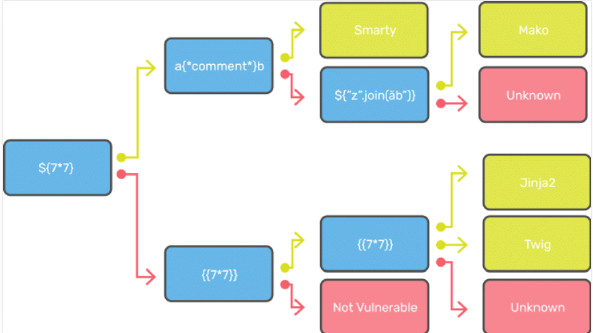
1. Remote Code Execution (RCE): Remote code execution is a cyber-attack where an attacker can remotely execute commands on someone else’s computing device. This can occur due to the installation of malicious software on the host and is not limited by the device’s geographical location. RCE can lead to complete control over a targeted application or system, potentially compromising sensitive data or even taking over the entire system.



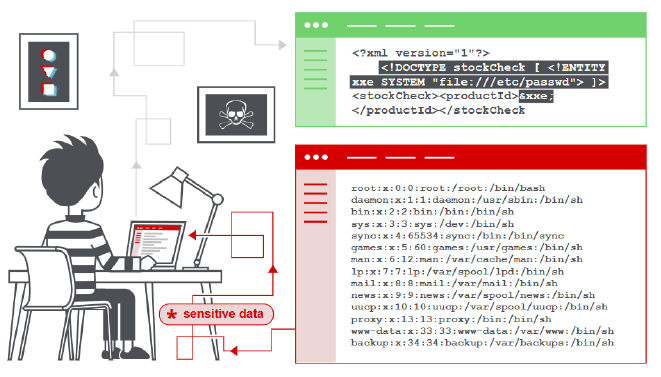
1. Insecure Direct Object Reference (IDOR): Insecure Direct Object Reference (IDOR) is a security vulnerability that occurs when an application lacks proper access controls for objects like files or database records based on user input. Malicious users can exploit this vulnerability to gain unauthorized access to or modify objects. This vulnerability often stems from inadequate or incorrectly implemented authorization checks, and can lead to unauthorized access or manipulation of sensitive information.



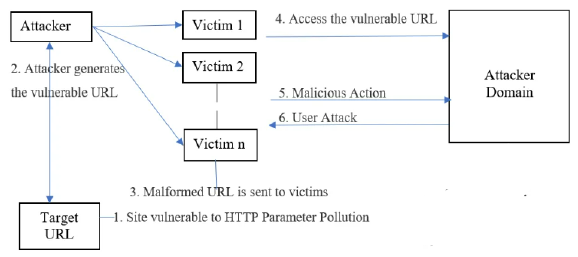
1. Server-Side Template Injection (SSTI): Server-Side Template Injection (SSTI) is a web application vulnerability that allows an attacker to inject malicious code into server-side templates used for generating dynamic content. This can enable the execution of arbitrary code on the server. SSTI can have severe consequences, potentially leading to data breaches, server compromise, and other serious security breaches.



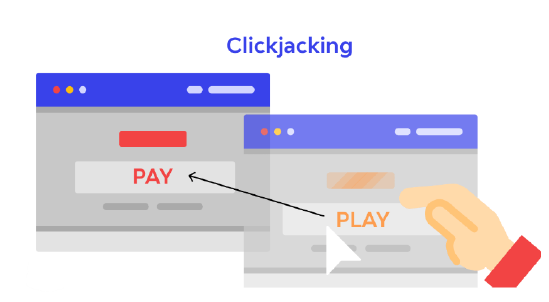
1. XML External Entity Injection (XXE): XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. This can permit the viewing of files on the application server and interaction with back-end or external systems. In certain scenarios, an attacker can escalate an XXE attack to compromise the underlying server or other critical back-end infrastructure by leveraging the XXE vulnerability to perform server-side request forgery (SSRF) attacks.



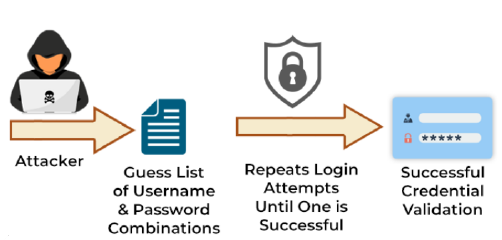
1. HTTP Parameter Pollution (HPP): HTTP Parameter Pollution (HPP) is a web security vulnerability that occurs when an attacker manipulates or confuses the parameters of an HTTP request. This can lead to unexpected or unintended behavior in the targeted web application. HPP exploits ambiguities in how web applications handle multiple instances of the same parameter, potentially causing confusion in input handling.



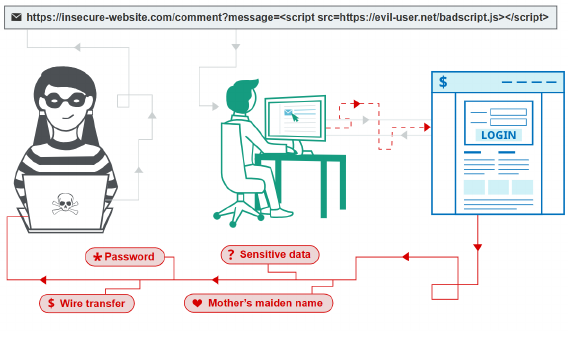
1. Clickjacking Attack: Clickjacking, or UI Redressing, is a web security vulnerability where an attacker deceives a user into clicking on something different from what they perceive. This is achieved by overlaying a malicious webpage element, often an iframe, on top of a legitimate website. The user believes they are interacting with the trusted site, but in reality, they are interacting with the attacker's malicious content. This can lead to unintended actions or disclosure of sensitive information.



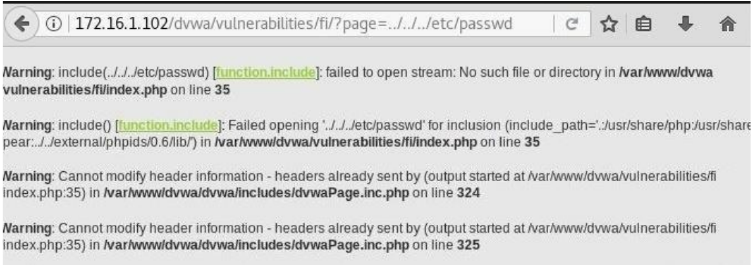
1. Brute Force Attack: A brute force attack is an automated method used by attackers to guess username and password combinations in order to gain unauthorized access to a web application. Attackers utilize software tools to systematically try different combinations until they find the correct one. This type of attack underscores the importance of robust authentication mechanisms and the need for defenses against repeated login attempts.



1. Cross-Site Scripting (XSS): XSS is a security vulnerability that arises when an attacker injects malicious scripts into web applications, which are then executed by unsuspecting users. This allows the attacker to masquerade as a victim user, carry out actions on their behalf, and access their data. This type of attack can lead to serious consequences, as it exploits vulnerabilities in the website's code, potentially compromising sensitive information or allowing for further exploitation.



1. Directory Traversal Attack: Also known as Path Traversal or Directory Climbing, this attack occurs when an attacker gains access to files or directories beyond the intended scope of a web application. It happens when the application fails to properly validate or sanitize user-provided file paths. The consequences of a successful Directory Traversal attack can be severe, ranging from unauthorized access to critical files, to potential data leakage and even remote code execution in certain cases.



1. Cross-Site Request Forgery (CSRF): CSRF is a security vulnerability where an attacker tricks a logged-in user into performing unwanted actions on a website without their knowledge or consent. This is achieved by exploiting the trust that the website has in the user's browser. CSRF attacks can result in actions being taken on a user's behalf, potentially leading to unauthorized changes.

