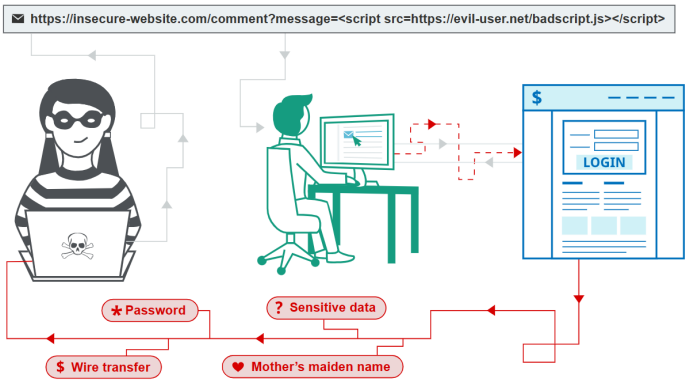
TASK 2 (28-08-23)

Overview of the assignment :

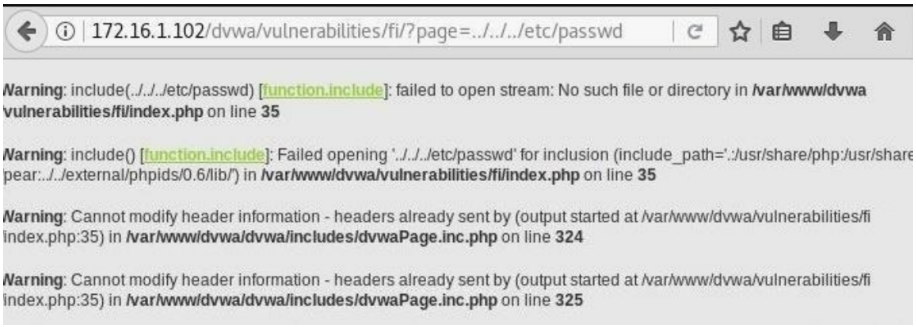
Explain about any 10 web application attacks

WEB APPLICATION ATTACKS

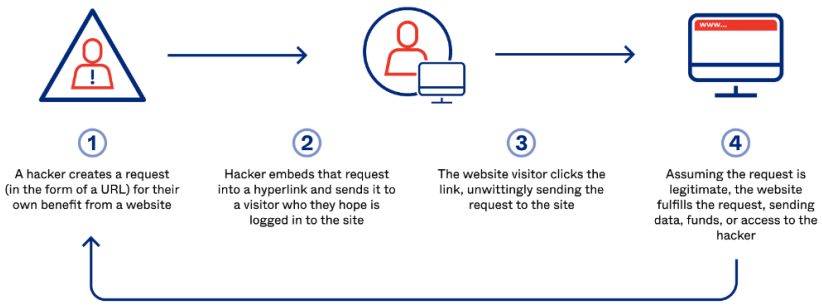
1.Cross site scripting attack (XSS) : Cross-Site Scripting (XSS) is a type of security vulnerability that occurs when an attacker injects malicious scripts into web applications that are then executed by unsuspecting users.Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data.



2.Directory traversal attack : A Directory Traversal attack (also known as a Path Traversal attack or Directory Climbing attack) is a type of security vulnerability in which an attacker can access files or directories that are outside the intended scope of a web application's file system. This type of attack occurs when the application does not properly validate or sanitize user input that specifies file or directory paths. Directory Traversal attacks can have serious consequences, including unauthorized access to sensitive files, data leakage, and remote code execution in some cases.

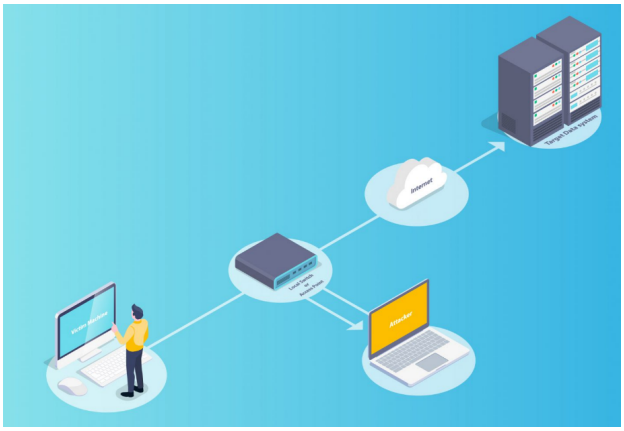


3.Cross site request forgery (CSRF) : Cross-Site Request Forgery (CSRF) is a type of security vulnerability in web applications where an attacker tricks a user into performing an unwanted action without their knowledge or consent while the user is authenticated on a website. CSRF attacks exploit the trust that a website has in a user's browser by making unauthorized requests on behalf of the victim.

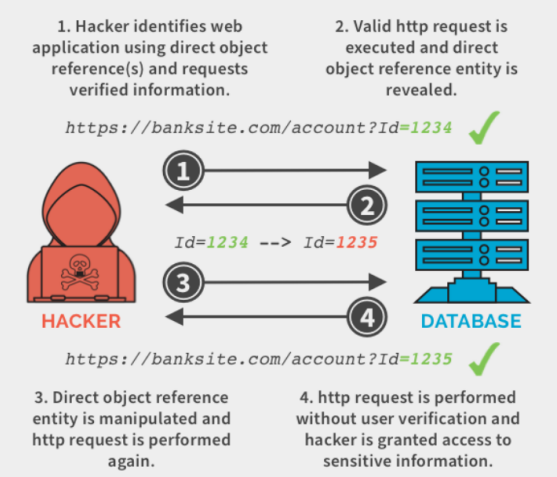


4.Remote code execution (RCE) : Remote code execution is a cyber-attack whereby an attacker can remotely execute commands on someone else's computing device. Remote code executions (RCEs) usually occur due to malicious malware downloaded by the host and can happen regardless of the device's geographic location. Remote Code Execution (RCE) is also referred to as Remote Code Evaluation.

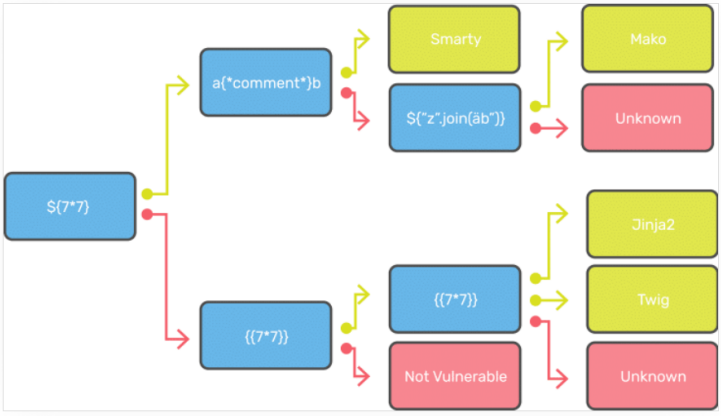
For example, a threat actor in Ukraine could silently place malicious code on a targeted device in the United States. Additionally, RCE enables a threat actor to control a computer or server by executing malicious software. RCE can, of course, lead to the complete takeover of a targeted vulnerable application.



5.Insecure direct object reference (IDOR) : Insecure Direct Object Reference (IDOR) is a security vulnerability that occurs when an application provides improper access controls for objects (such as files, database records, or resources) based on user-supplied input. In an IDOR attack, a malicious user can manipulate input parameters to access, modify, or delete objects that they should not have permission to access. This vulnerability typically arises from insufficient or improperly implemented authorization checks in the application.For instance, changing a URL from "/profile?id=123" to "/profile?id=456" to access another user's profile.

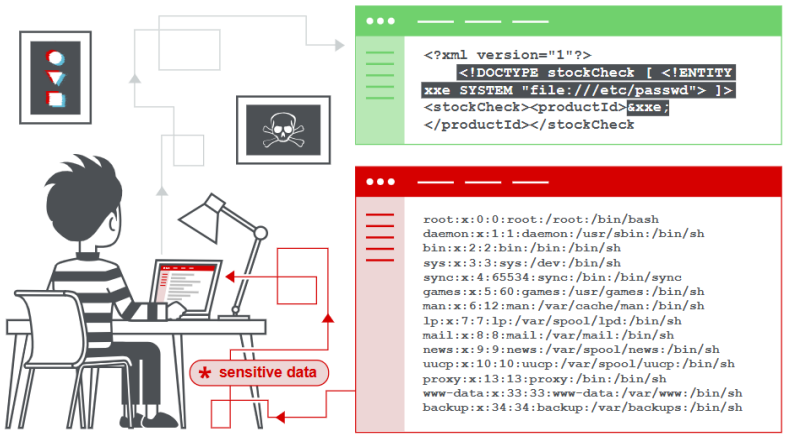


6.Server side template injection : Server-Side Template Injection (SSTI) is a web application vulnerability that occurs when an attacker is able to inject malicious code into server-side templates, which are used to generate dynamic content on web pages. This type of vulnerability can have serious consequences, as it often allows attackers to execute arbitrary code on the server, potentially leading to data breaches, server compromise, and more.

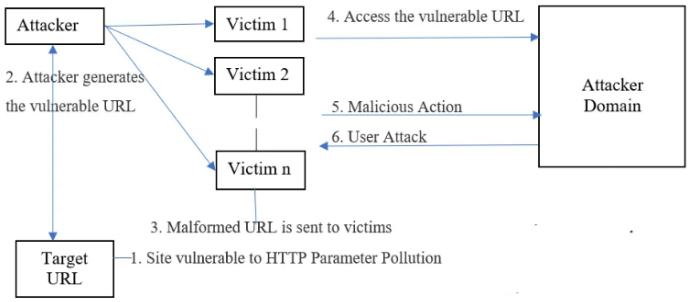


– {{7*'7'}} will result in 49 in Twig and 7777777 in Jinja2

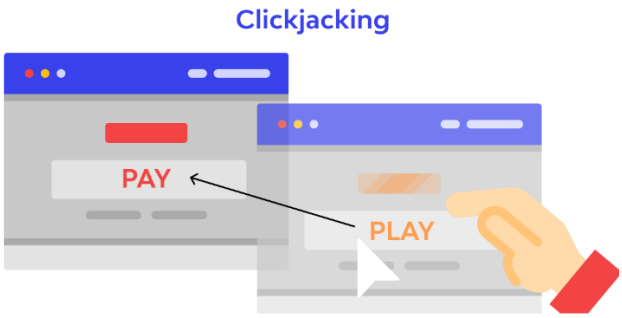
7.XML entity expansion (XXE) : XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the application server file system, and to interact with any back-end or external systems that the application itself can access.In some situations, an attacker can escalate an XXE attack to compromise the underlying server or other back-end infrastructure, by leveraging the XXE vulnerability to perform server-side request forgery (SSRF) attacks.



8.HTTP Parameter Pollution (HPP) : It is a web security vulnerability that occurs when an attacker manipulates or pollutes the parameters of an HTTP request to confuse the server, potentially leading to unexpected or unintended behavior. This attack exploits ambiguities in the way web applications handle multiple instances of the same parameter or how they prioritize input values.



9.Clickjacking attack : Clickjacking, also known as a UI (User Interface) Redressing attack, is a web security vulnerability and attack technique that tricks a user into clicking on something different from what they perceive, effectively "hijacking" their clicks. In a clickjacking attack, the attacker overlays a malicious webpage element (usually an iframe) on top of a legitimate website, making it appear as if the user is interacting with the trusted site while, in reality, they are interacting with the attacker's malicious content.



10. Brute force attack : A brute force attack is an automated method of guessing a username and password combination to gain unauthorized access to a web application. Attackers use software tools to try different combinations of usernames and passwords until they successfully guess the correct one. To prevent brute force attacks, web applications can implement rate-limiting and account lockout policies.