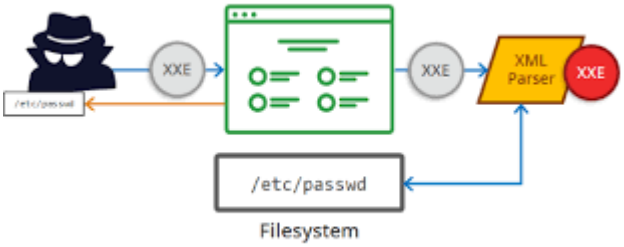
Saumyaa Prajapat
21BCI0265

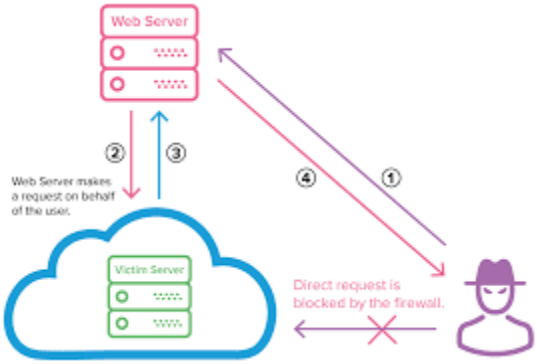
Task4:

The top 10 plot attacks other than OWASP Top 10

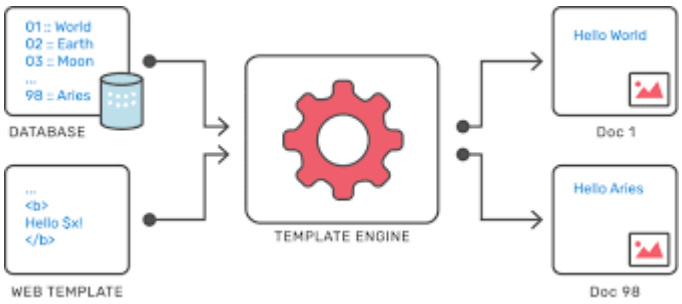
1. **XML External Entity (XXE) Attack:**
   Description: Attackers exploit XML processors that can parse user-provided XML input with external references, allowing them to retrieve sensitive data or execute remote code.



2. **Server-Side Request Forgery (SSRF):**
   Description: Attackers trick the server into making unintended requests to internal resources or external endpoints, often leading to data leakage or unauthorized access.

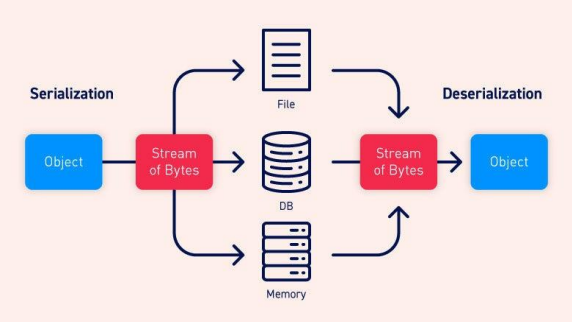


3. **Server-Side Template Injection (SSTI):**
   Description: Attackers manipulate server-side templates to execute arbitrary code, potentially leading to remote code execution and data compromise.

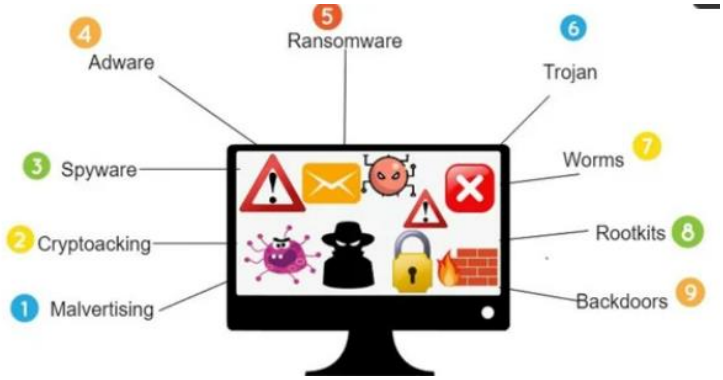


4. **Content Spoofing:**
   Description: Attackers manipulate content to present misleading information to users, often for phishing or social engineering purposes.

5. **Insecure Deserialization:**
   Description: Attackers exploit vulnerabilities in the deserialization process to execute arbitrary code, potentially leading to remote code execution.

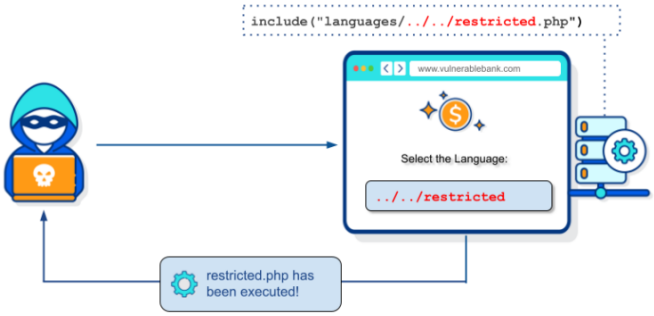


6. **Malware:**
   This is software that is designed to harm a computer system. Malware can be installed on a system through a variety of ways, such as clicking on a malicious link, opening an infected attachment, or downloading a file from an untrusted source

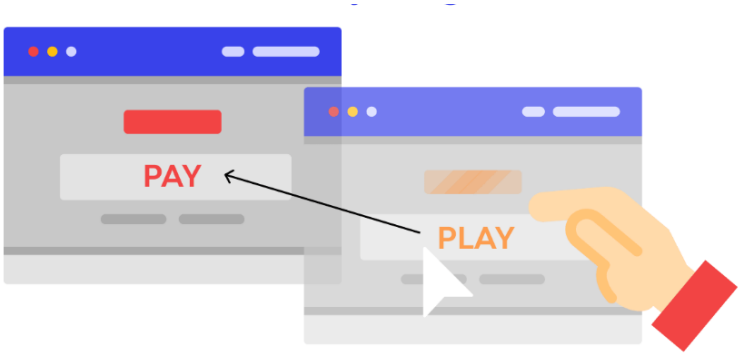


7. **Ransomware:**
   This is a type of malware that encrypts the victim's files and demands a ransom payment in order to decrypt them. Ransomware attacks are often very successful because victims are often willing to pay the ransom to get their files back.

8. **File Inclusion Attacks:**
   Description: Attackers manipulate file inclusion mechanisms to execute malicious files or gain unauthorized access to server files.



9. **Clickjacking:**
   Description: Attackers overlay legitimate UI elements with hidden malicious elements to deceive users into clicking on something they didn't intend to, potentially leading to unauthorized actions.



10. **DOM (Document Object Model)-Based Attacks:**
    Description: Attackers manipulate the DOM to execute malicious code in the client's browser, often leading to data theft or unauthorized actions.