XSS

1. Cross-site scripting (XSS) attacks: XSS attacks are another type of web application vulnerability. Attackers inject malicious code into a website to steal user data, gain control of user sessions, or redirect users to malicious websites.
   1. Reflected XSS: This type of attack involves injecting malicious code into a web page that is reflected back to the user, often through a search box or a URL parameter.
   2. Stored XSS: This attack involves injecting malicious code into a web page that is permanently stored on the server and served to all users who access the page.
   3. DOM-based XSS: This attack involves injecting malicious code into the Document Object Model (DOM) of a web page, often through client-side scripting, such as JavaScript.
   4. Blind XSS: This attack involves injecting malicious code into a web page that is stored on the server but not directly displayed to the user, such as in a database or log file.
   5. Multipart/form-data XSS: This attack involves injecting malicious code into a form that accepts file uploads, allowing an attacker to upload a file with malicious code and execute it on the server.
2. XSS affecting casual internet users:
   1. Cross-site scripting (XSS) attacks: These attacks are hard to detect and be prevented by a careful user, they can contain any type of malware.