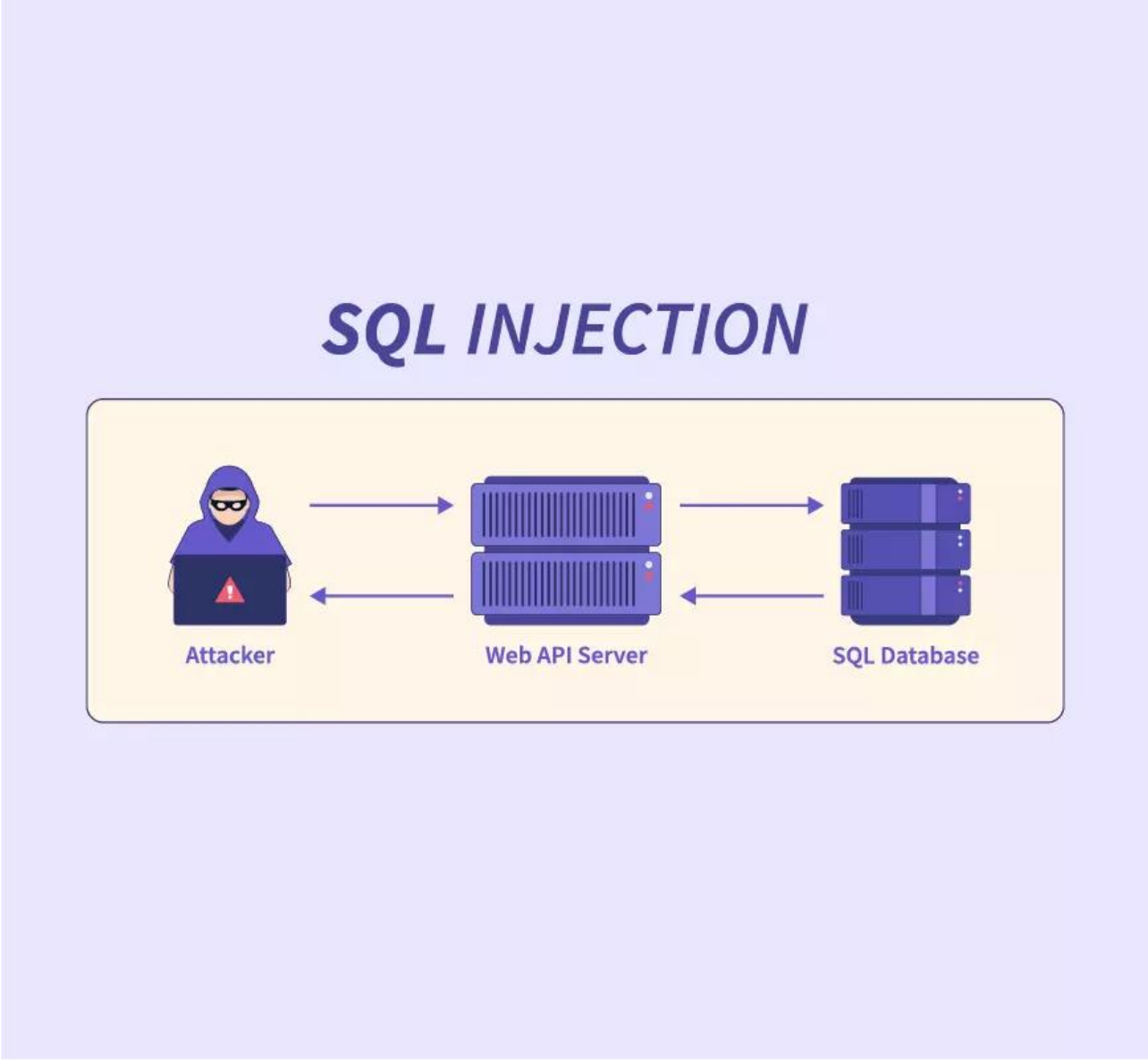
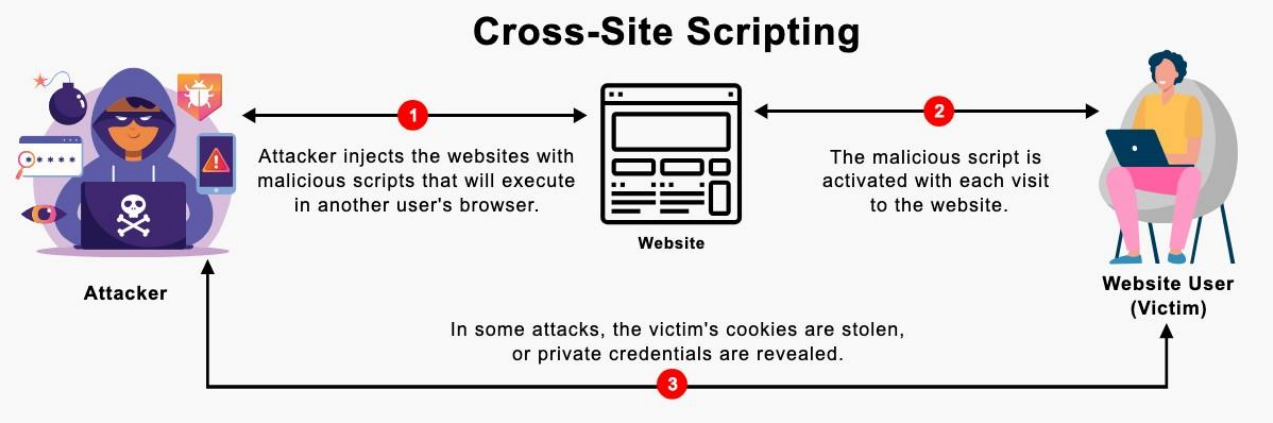
NAME – ARAVIND
REG.NO – 21BCE8127
ASSIGNMENT – 1

Common Web Server Attacks

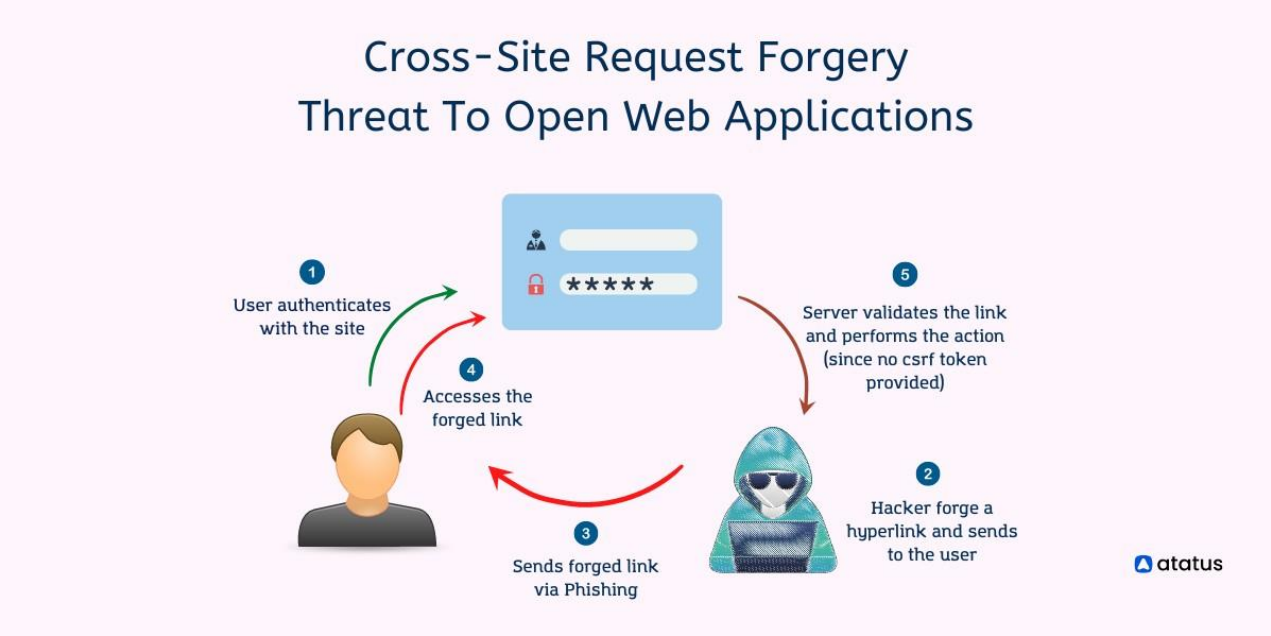
. SQL Injection: Attackers insert malicious SQL queries into input fields, exploiting vulnerabilities in web applications to manipulate databases, potentially gaining unauthorized access to sensitive data.



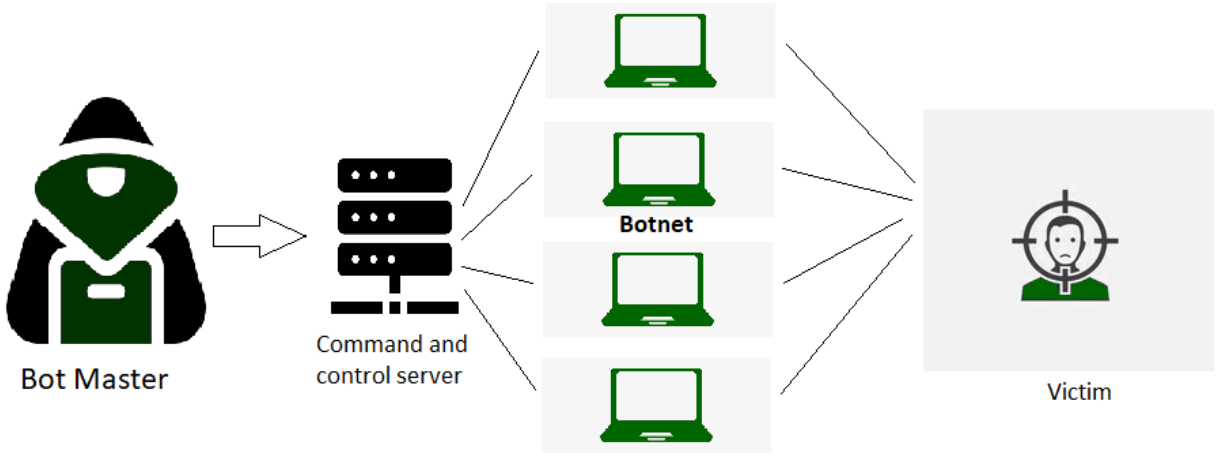
. Cross-Site Scripting (XSS): By injecting malicious scripts into web pages, attackers exploit vulnerabilities to execute scripts in users' browsers, allowing them to steal user data, session information, or redirect users to harmful sites.


Cross-Site Scripting
Attacker
1
Attacker injects the websites with malicious scripts that will execute in another user's browser.
Website
2
The malicious script is activated with each visit to the website.
Website User (Victim)
In some attacks, the victim's cookies are stolen, or private credentials are revealed.
3

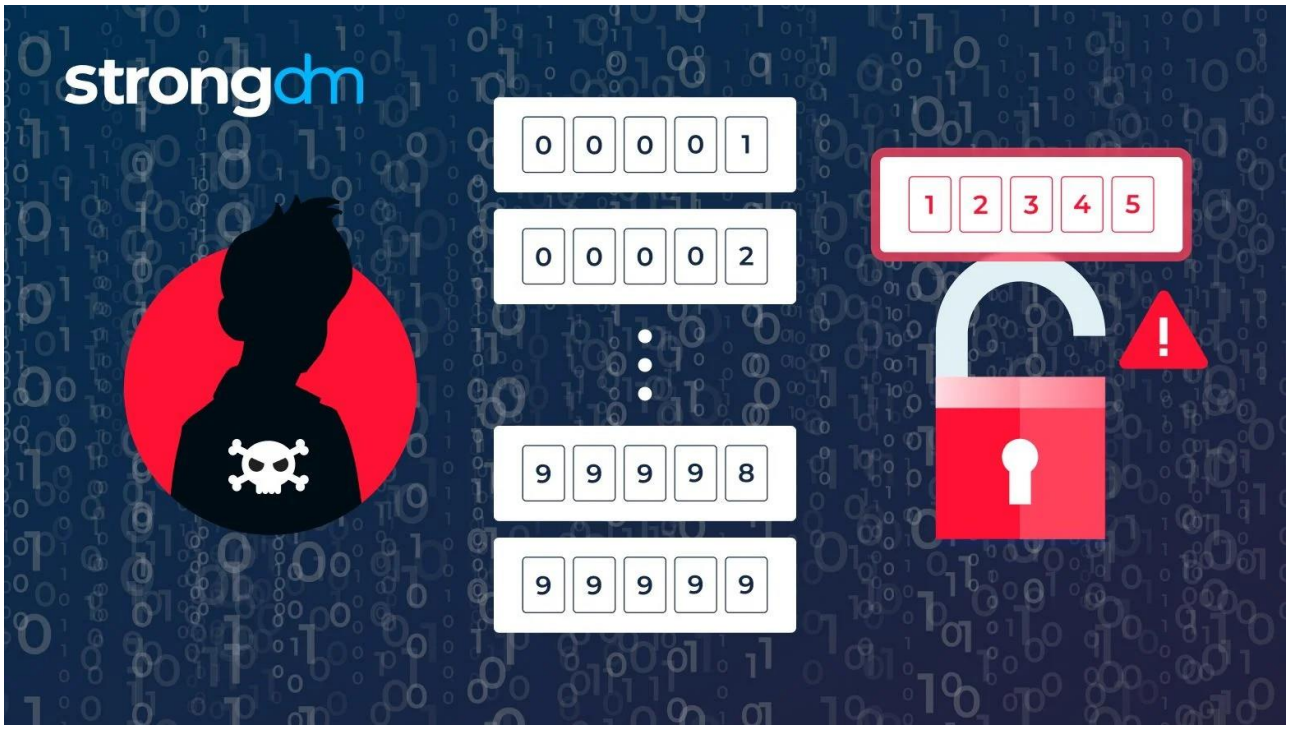
. Cross-Site Request Forgery (CSRF): Attackers trick users into unknowingly executing unauthorized actions on web applications, exploiting their authenticated sessions to perform unintended actions, potentially leading to unauthorized data changes or transactions.



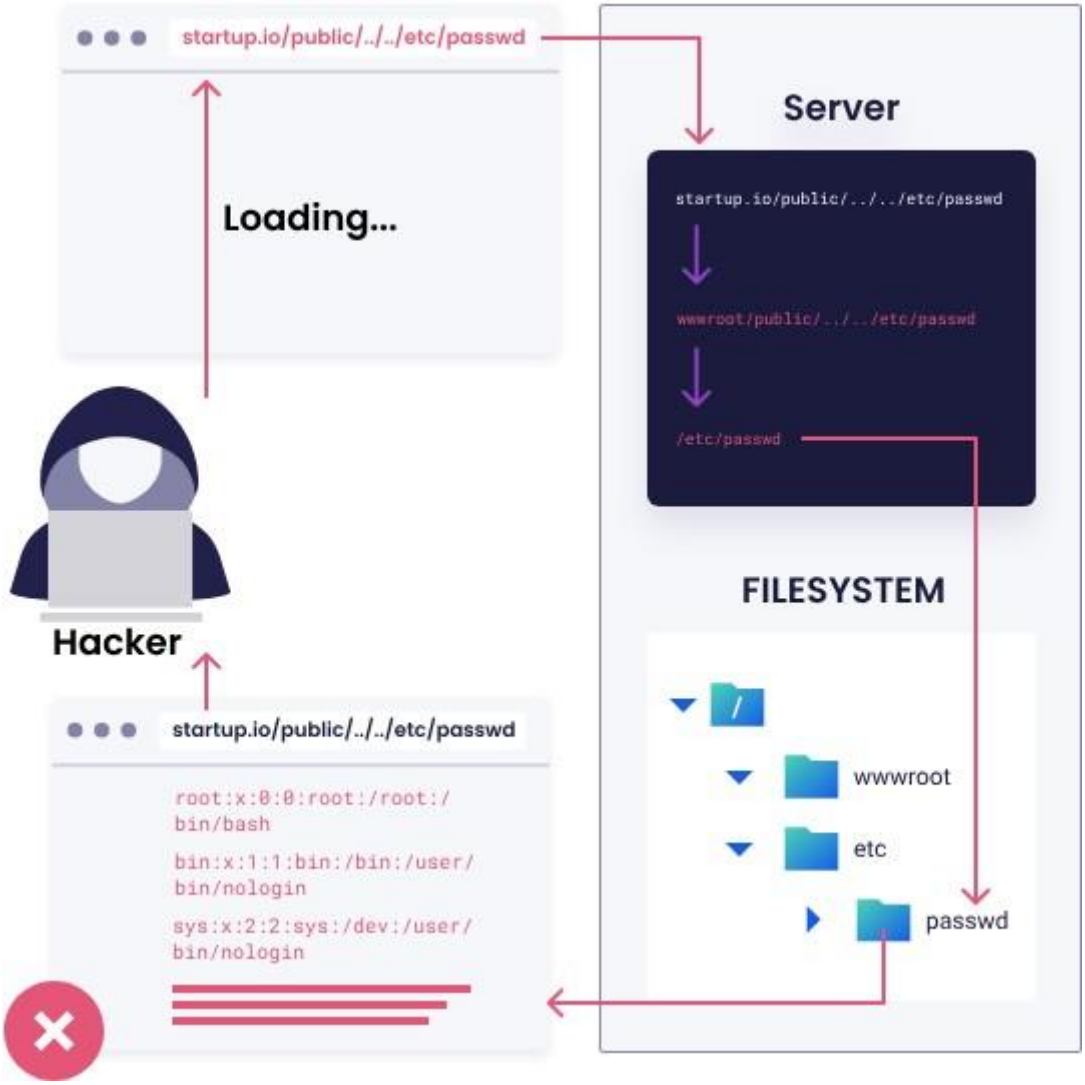
. DDoS (Distributed Denial of Service): Attackers overwhelm web servers with a flood of traffic from multiple sources, causing them to become inaccessible to legitimate users, disrupting services.



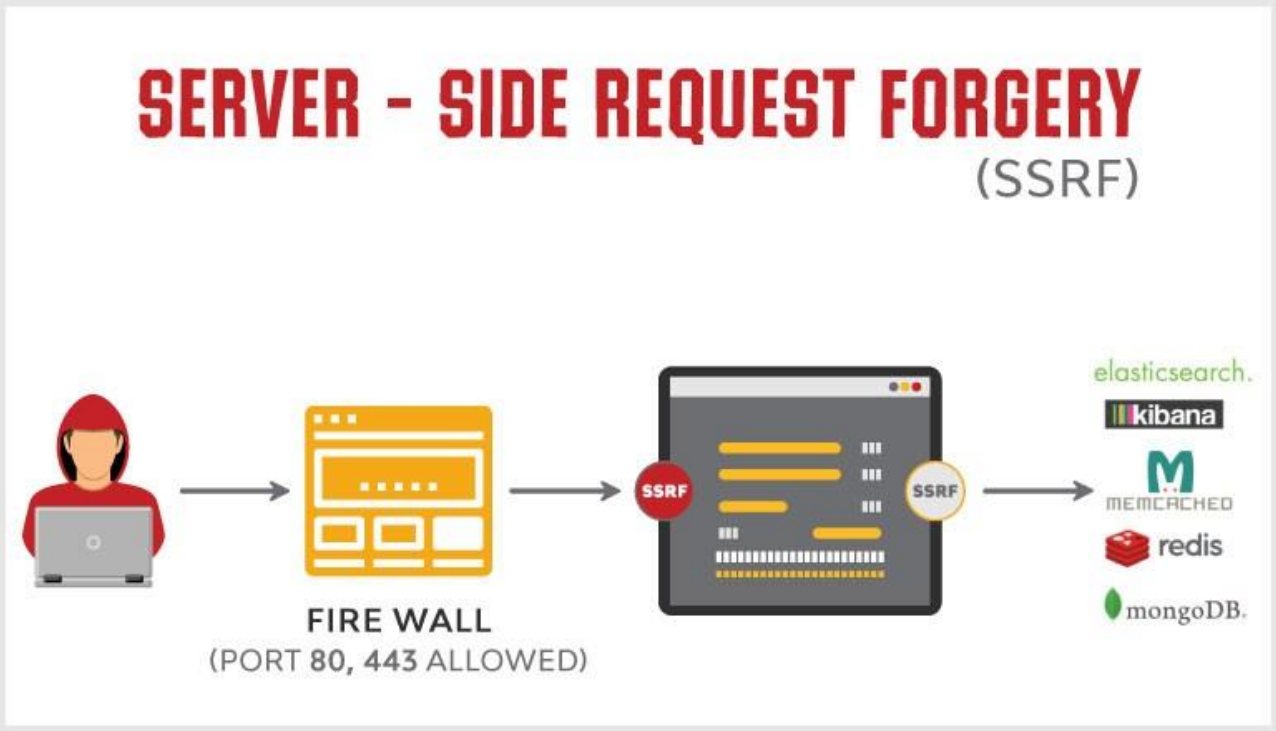
. Brute Force Attacks: Attackers systematically try various username and password combinations to gain unauthorized access to web servers, accounts, or applications.



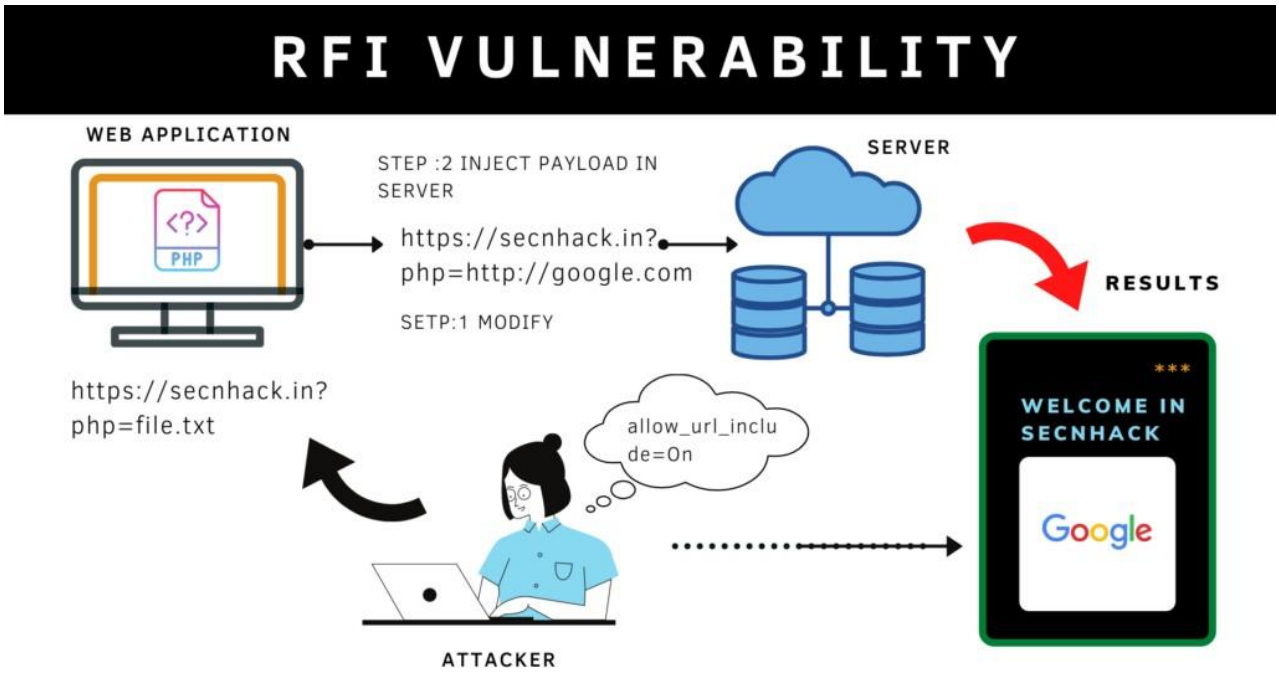
. Directory Traversal: Exploiting input validation weaknesses, attackers navigate beyond intended directories, potentially accessing unauthorized files, directories, or sensitive data.



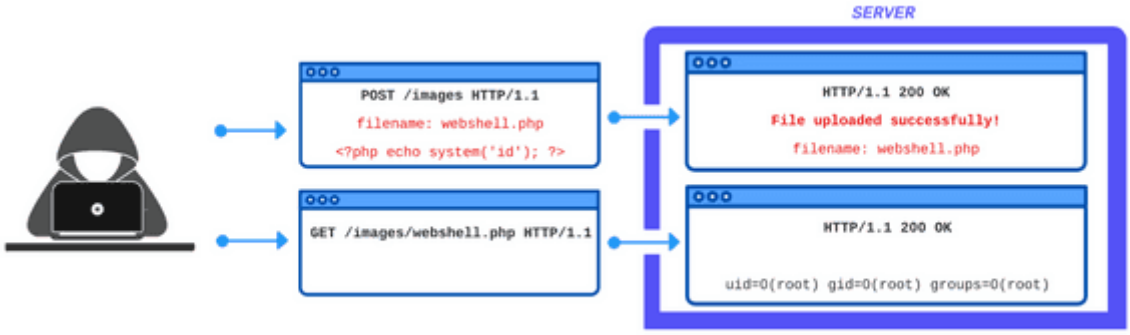
. Server-Side Request Forgery (SSRF): Attackers manipulate a web server into making requests to internal or external resources, potentially leading to data exposure, unauthorized access, or information leakage.



. Remote File Inclusion (RFI): Attackers exploit insecurely designed server-side scripts to include malicious files, executing arbitrary code, gaining unauthorized access, or compromising web servers.



. File Upload Exploits: Attackers upload malicious files via vulnerable input fields, which, when executed, can lead to unauthorized access, data breaches, or even full server compromise.



. XPath Injection: In XML-based applications, attackers manipulate input to exploit vulnerabilities, potentially bypassing authentication, gaining unauthorized access, or extracting sensitive information from web servers.

XPath Injection

Query: //Employee[position()=3]/child::node()[position()=4]/text()

Submit

XPath Query: //Employee[position()=3]/child::node()[position()=4]/text()

Output:

Gates