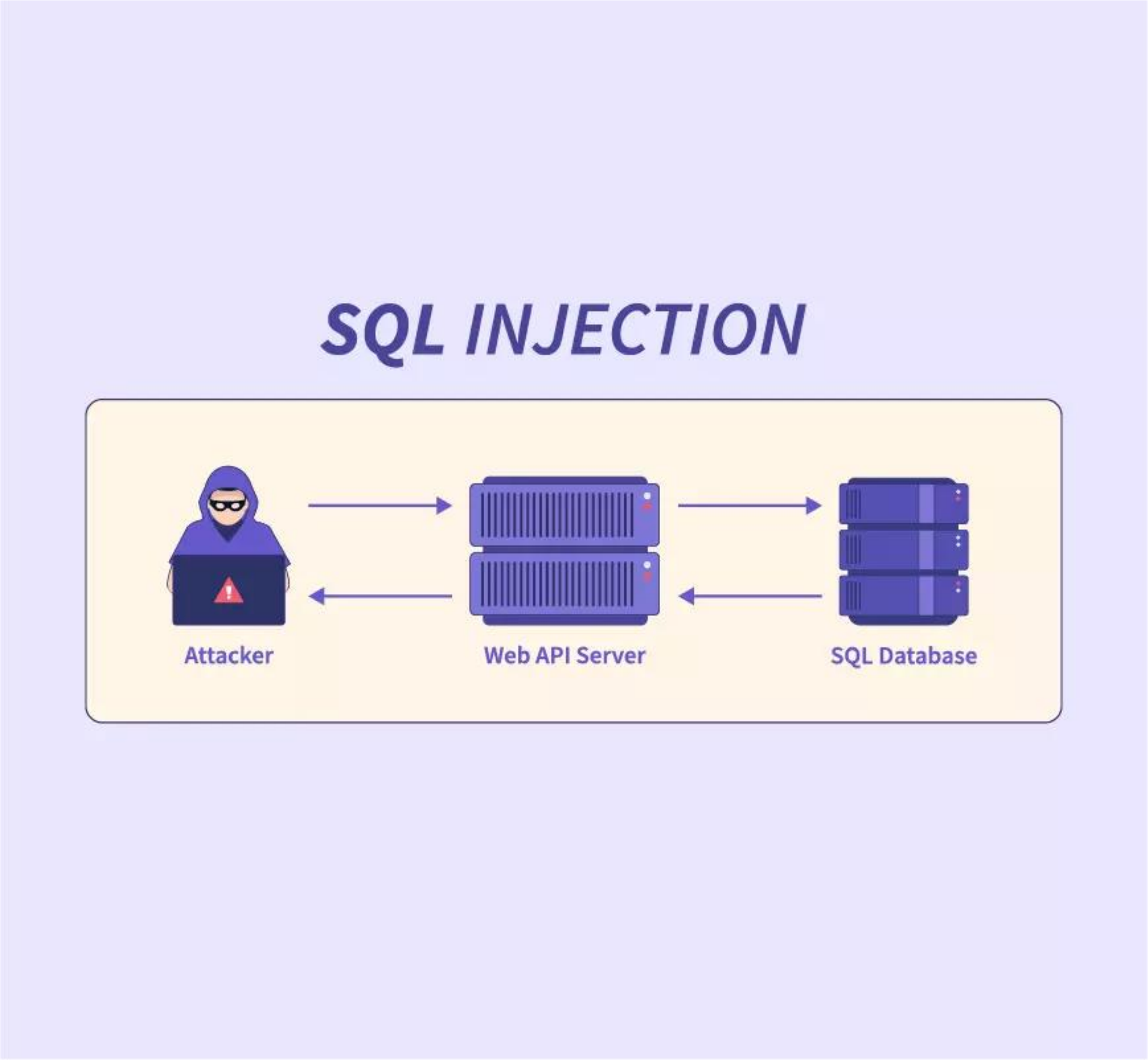
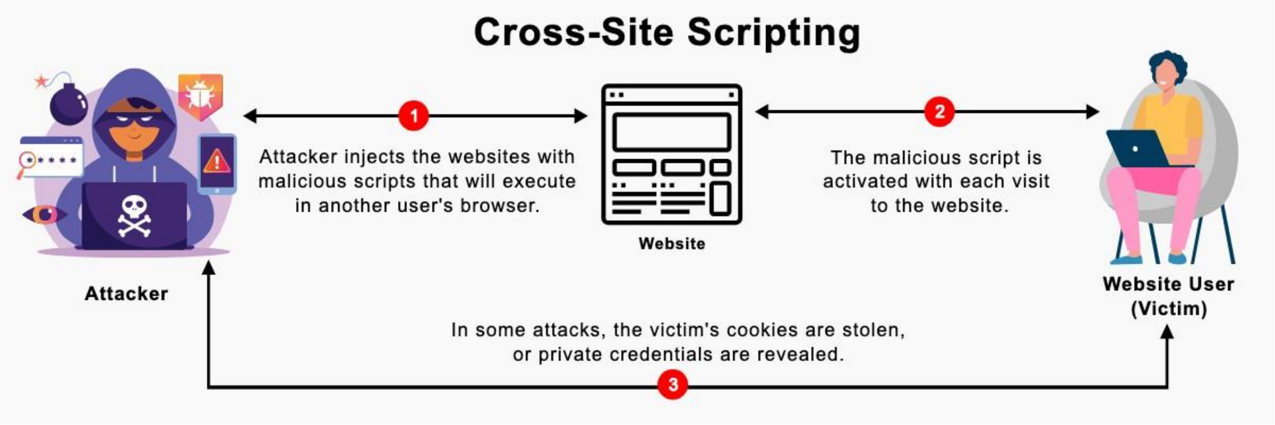
Assignment 1

Common Web Server Attacks

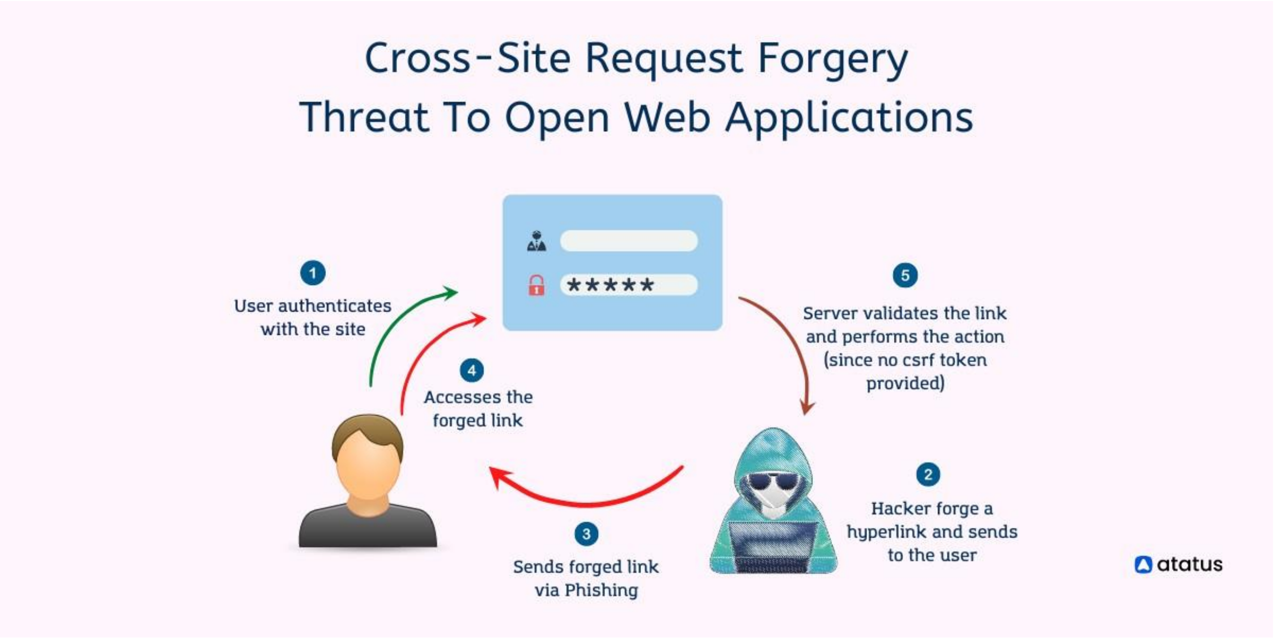
1) SQL Injection: Attackers insert malicious SQL queries into input fields, exploiting vulnerabilities in web applications to manipulate databases, potentially gaining unauthorized access to sensitive data.



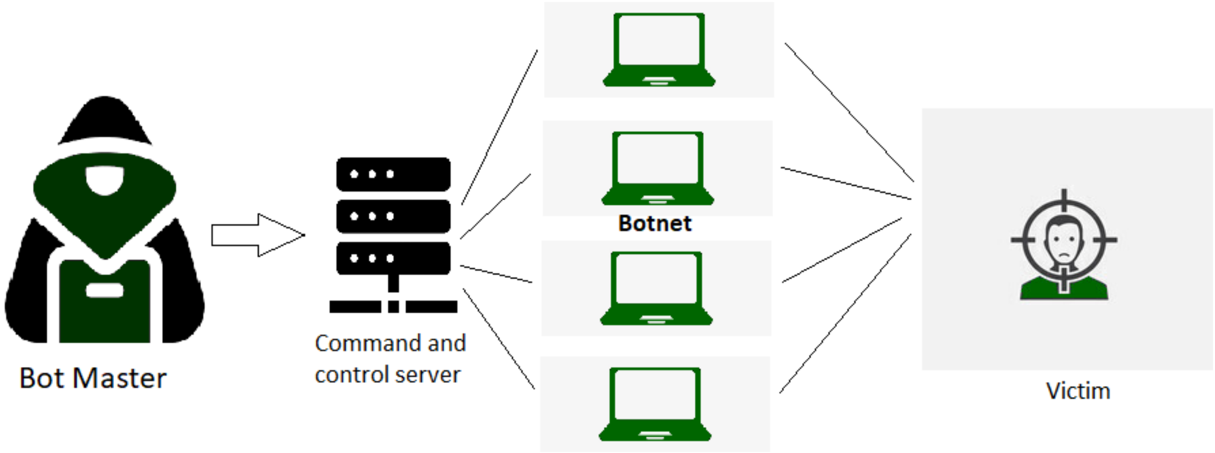
2) Cross-Site Scripting (XSS): By injecting malicious scripts into web pages, attackers exploit vulnerabilities to execute scripts in users' browsers, allowing them to steal user data, session information, or redirect users to harmful sites.


Cross-Site Scripting
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.
Attacker
Website User (Victim)
In some attacks, the victim's cookies are stolen, or private credentials are revealed.
3

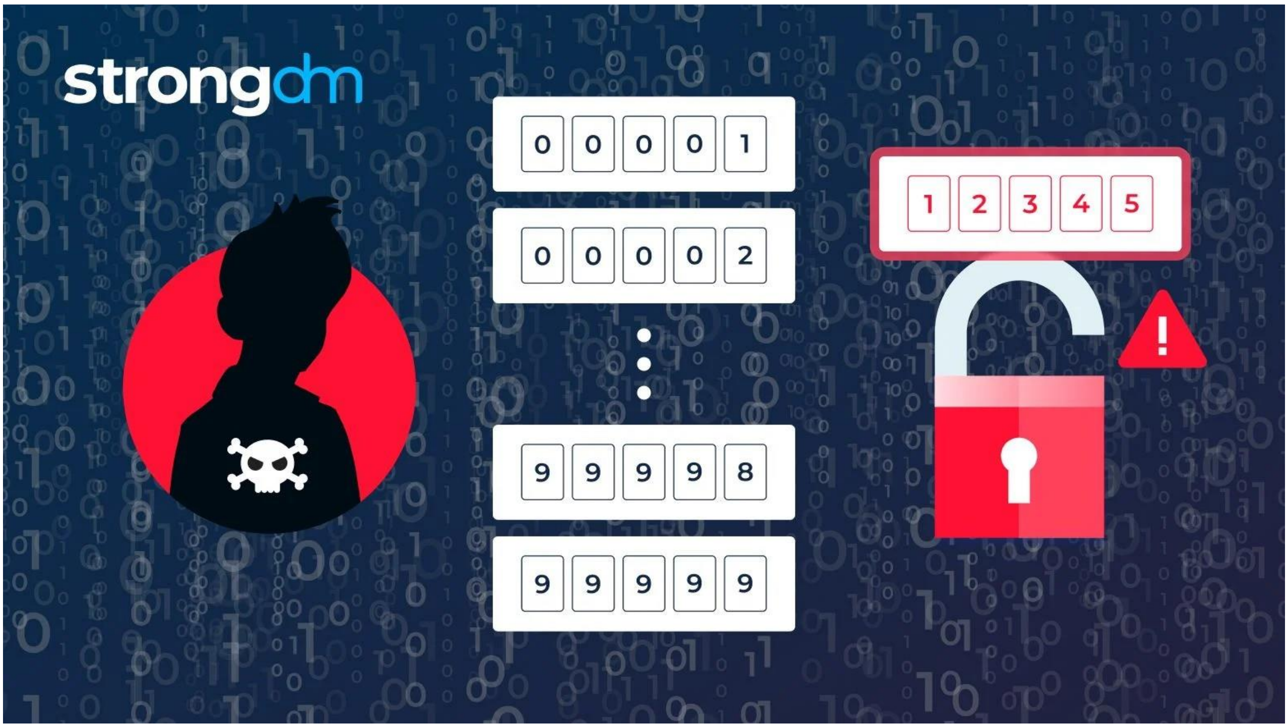
3) Cross-SiteRequestForgery(CSRF):Attackerstrickusersintounknowinglyexecutingunauthorized actions on web applications, exploiting their authenticated sessions to perform unintended actions, potentially leading to unauthorized data changes or transactions.


Cross-Site Request Forgery
Threat To Open Web Applications
*****
1 User authenticates with the site
4 Accesses the forged link
5 Server validates the link and performs the action (since no csrf token provided)
2 Hacker forge a hyperlink and sends to the user
3 Sends forged link via Phishing
atatus

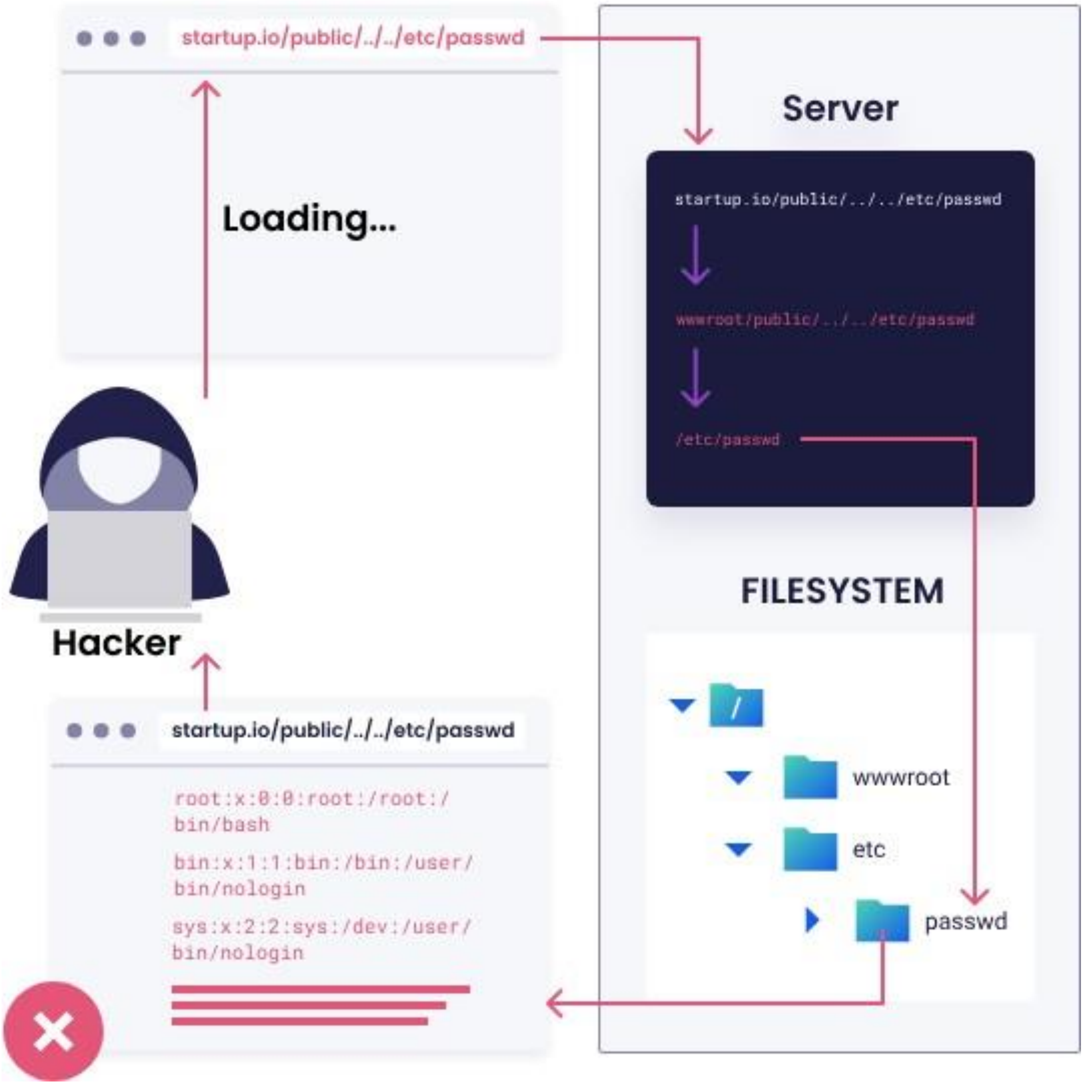
4) DDoS(DistributedDenialofService):Attackersoverwhelmwebserverswithafloodoftrafficfrom multiplesources,causingthemtobecomeinaccessibletolegitimateusers,disruptingservices.



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



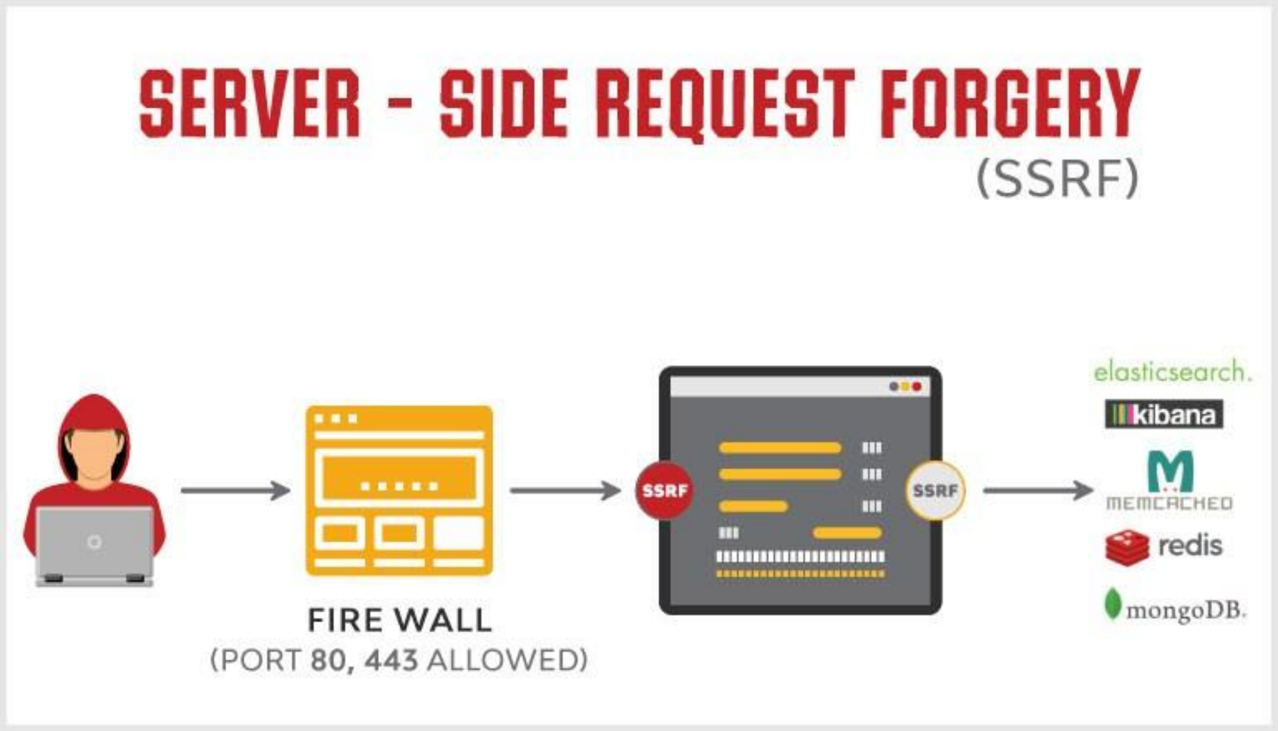
6) Directory Traversal: Exploiting input validation weaknesses, attackers navigate beyond intended directories, potentially accessing unauthorized files, directories, or sensitive data.


startup.io/public/../../etc/passwd
Loading...
Server
Hacker
FILESYSTEM
/
wwwroot
etc
passwd
startup.io/public/../../etc/passwd

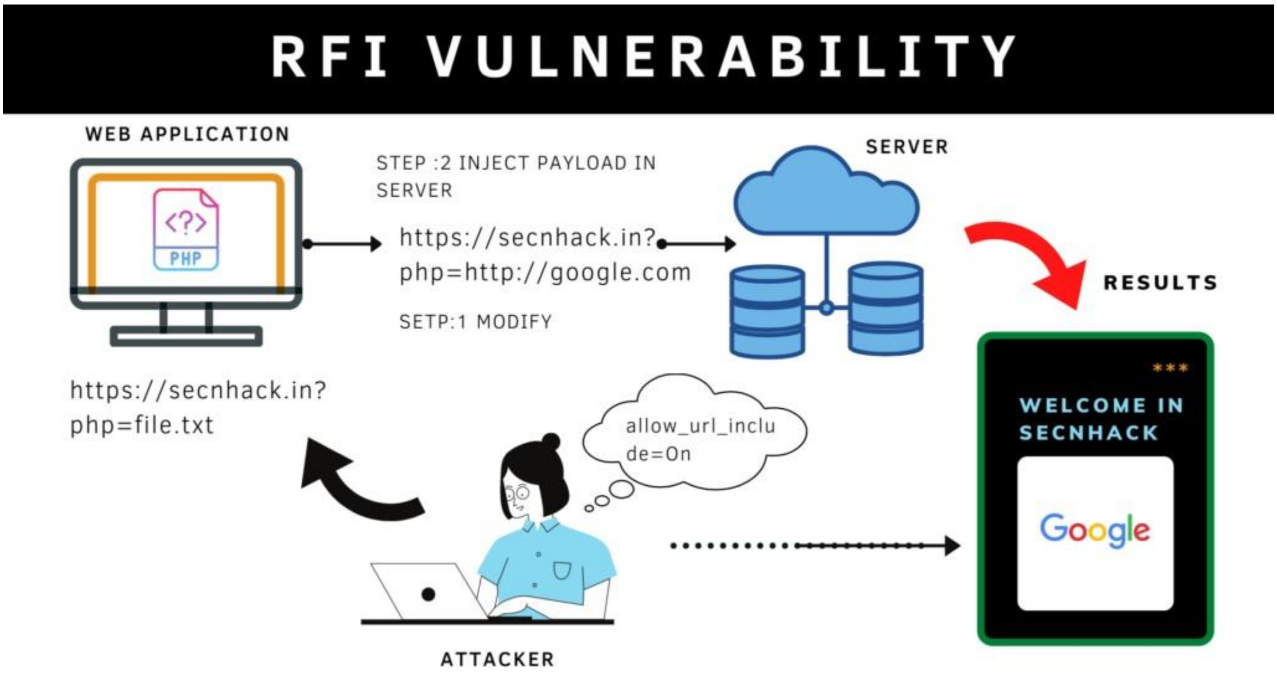
```
startup.io/public/../../etc/passwd
wwwroot/public/../../etc/passwd
/etc/passwd
```

```
root:x:0:0:root:/root:/
bin/bash
bin:x:1:1:bin:/bin:/user/
bin/nologin
sys:x:2:2:sys:/dev:/user/
bin/nologin
```

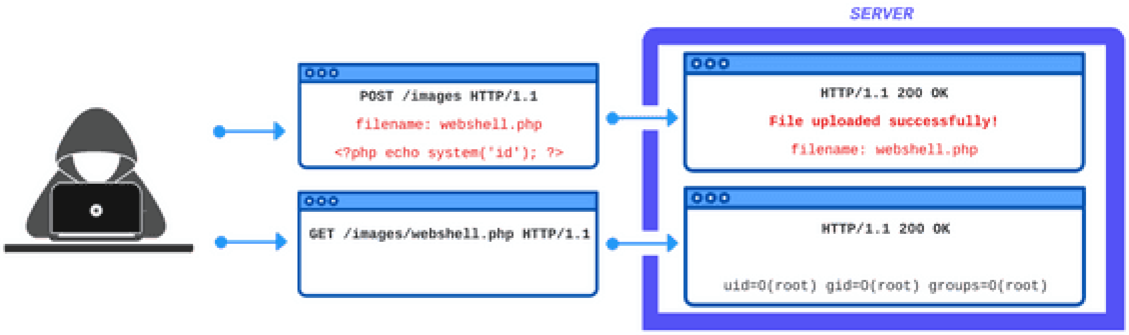
7) Server-SideRequestForgery(SSRF): Attackers manipulate a web server into making requests to internal or external resources, potentially leading to data exposure, unauthorized access, or information leakage.



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



9) File Upload Exploits: Attackers upload malicious files via vulnerable input fields, which, when executed, canlead to unauthorized access,databreaches,oreven full server compromise.



```
POST /images HTTP/1.1
filename: webshell.php
<?php echo system('id'); ?>
```

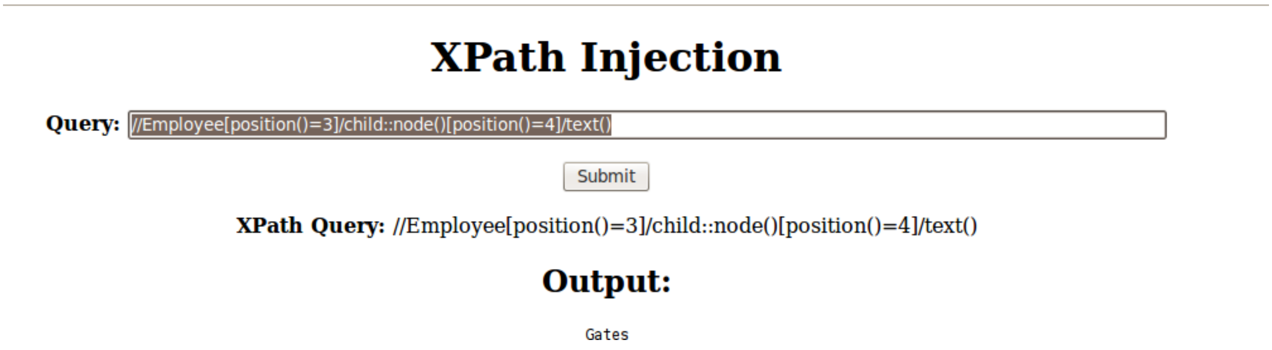
```
GET /images/webshell.php HTTP/1.1
```

```
HTTP/1.1 200 OK
File uploaded successfully!
filename: webshell.php
```

```
HTTP/1.1 200 OK

uid=0(root) gid=0(root) groups=0(root)
```

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



XPath Injection

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

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

Output:

```
Gates
```