TASK-5

K. Naveen Abhiram

21BCE7357

Web Server Attacks

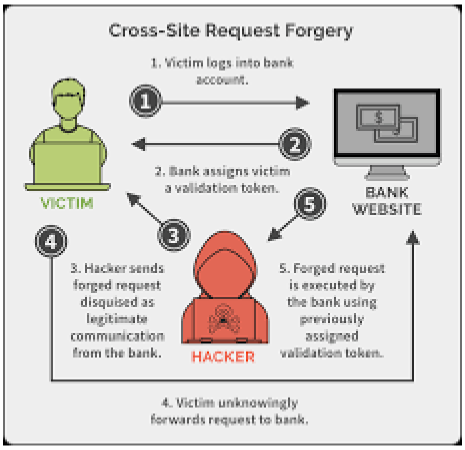
A web server attack is a harmful activity that is directed towards a web server with the goal of exploiting flaws, gaining access without authorization, interrupting services, or jeopardizing the security of the server and the applications it hosts.

1. Cross-Site Request Forgery (CSRF):

Attackers frequently cause accidental modifications to the victim's account by deceiving users into acting inadvertently on a separate website.

Example:

Forcing a person who is already signed in to click a link and unwittingly change their password.

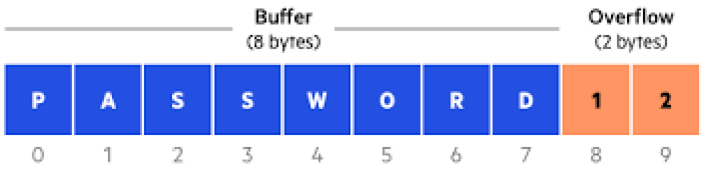

Cross-Site Request Forgery
1. Victim logs into bank account.
1
2
2. Bank assigns victim a validation token.
VICTIM
BANK WEBSITE
5
3
4
3. Hacker sends forged request disguised as legitimate communication from the bank.
HACKER
5. Forged request is executed by the bank using previously assigned validation token.
4. Victim unknowingly forwards request to bank.

2. Buffer Overflow Attacks:

Attackers overwhelm a server's buffer by sending more data than it can manage, perhaps overwriting nearby memory and running malicious code.

<u>Example</u>:

Sending an application with a vulnerability too much data, causing it to crash or run malicious code.

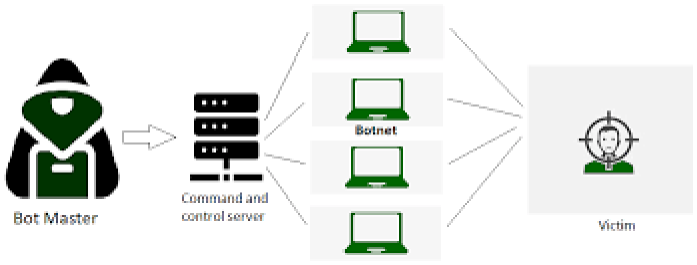


3. Denial of Service (DoS) and Distributed DoS (DDoS):

Attackers overburden a server with requests or traffic, exhausting its resources and blocking access to genuine users. Multiple hacked systems are employed in DDoS assaults.

<u>Example</u>:

Flooding the server with too many requests or traffic.

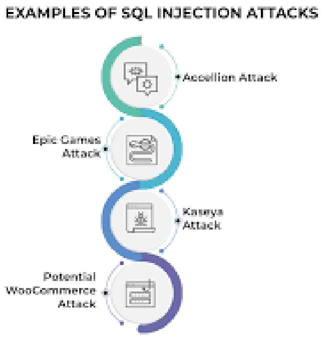


4. SQL Injection (SQLi):

Attackers utilize injected malicious SQL queries into user input fields to take advantage of inadequate input validation. Unauthorized access, data modification, or even total control over a database may result from this.

<u>Example</u>:

Entering 'OR '1'='1 into the login form to get around authentication.

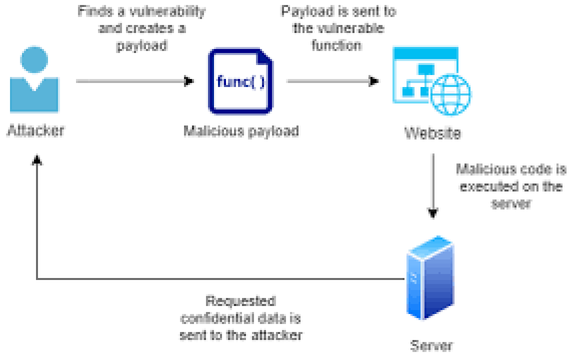

EXAMPLES OF SQL INJECTION ATTACKS
Accellion Attack
Epic Games Attack
Kaseya Attack
Potential WooCommerce Attack

5. Remote Code Execution (RCE):

Attackers use flaws as an opportunity to execute arbitrary code on a server, possibly taking over the entire network. When paired with lax server security, this is very risky.

Example:

Putting harmful code in a file and getting the server to run it.

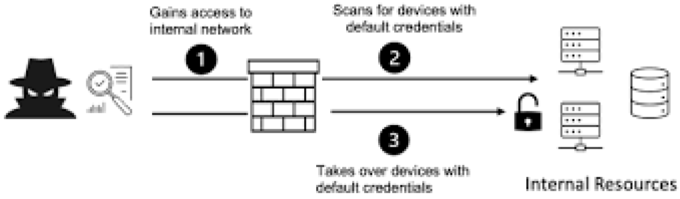

Finds a vulnerability and creates a payload
Payload is sent to the vulnerable function
Attacker
func( )
Malicious payload
Website
Malicious code is executed on the server
Requested confidential data is sent to the attacker
Server

6. Server Misconfiguration:

Attackers locate servers that are misconfigured in order to take advantage of security flaws, which frequently arise from carelessness or a lack of security awareness.

Example:

Since directory listing is enabled, accessing private files.

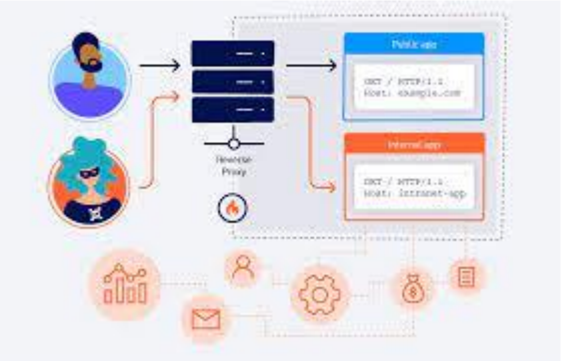

Gains access to internal network
1
Scans for devices with default credentials
2
3
Takes over devices with default credentials
Internal Resources

7. HTTP Header Injection:

Attackers change HTTP headers to fool servers into processing erroneous or malicious commands, which may result in unauthorized access or data leakage.

Example:

Altering headers to route users to a phishing website.

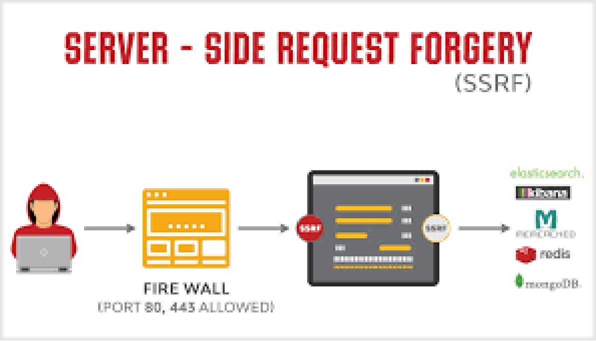


8. Server-Side Request Forgery (SSRF):

A web application is tricked by an attacker into sending queries to internal resources that shouldn't be reachable from the outside. Internal services or sensitive data may be exposed as a result.

Example:

That requests be sent to internal databases or services by the server.



9. Directive Traversal:

Inadequate input validation is used by attackers to traverse across directories and access restricted files. This might compromise the system as a whole or reveal private configuration files.

Example:

Accessing files outside the specified directory by altering a URL.

10. XML External Entity (XXE) Attacks:

Attackers include external entities that can reveal sensitive information by taking advantage of ineffective XML parsers.

Example:

uploading an XML file to the server to get private information.