Saloni Ghule

21BCE1967

Top 10 hackers in the world

1. Kevin Mitnick, Once the 'Most Wanted Computer Best known for an audacious hacking spree in the 1990s involving the theft of data and credit card numbers, he later became a security consultant and public speaker. Kevin Mitnick is an American computer security consultant, author, and a black hat turned white hat hacker.

2. Anonymous is a global hacker group known for online protests and has faced legal action due to their activities. Their notable events, such as attacks on the Church of Scientology and Russia, often cause controversy due to data leaks and vague political agendas. They are grey hat hackers .

3. Riding Greyhound, couch-surfing, squatting, and using public Internet to compromise high-profile company networks -- and then fix their security problems for free. Lamo was a grey hat hacker who viewed the rise of the World Wide Web with a mixture of excitement and alarm. He felt that others failed to see the importance of internet security in the early days of the World Wide Web.

4. Albert Gonzalez is one of the many poster children for black hat hacking. In 2005, he organized a group of individuals to compromise poorly secured wireless networks and steal information.]

5. Jonathan Joseph James (December 12, 1983 – May 18, 2008) was an American hacker (a gray hat ethical hacker) who was the first juvenile incarcerated for cybercrime in the United States. Jonathan James, also known as c0mrade, was a notorious hacker who gained unauthorized access to NASA's computer systems in 1999. He used a sophisticated technique called "packet sniffing" to intercept data packets traveling over the network and was able to obtain administrator-level access to NASA's computers.

6. Matthew Bevan and Richard Pryce are a team of British hackers who hacked into multiple military networks in 1996, including Griffiss Air Force Base, the Defense Information System Agency and the Korean Atomic Research Institute (KARI). By dumping KARI research into American military networks, the duo of black hat hackers very nearly sparked an international incident.

7. eanson James Ancheta became the first person to be charged for controlling large numbers of hijacked computers or botnets. Jeanson James Ancheta, also known as "Resilient" in the hacking community, was a black hat hacker.

8. Michael Calce, also known by his online handle "Mafiaboy," is famous for being a black hat hacker responsible for a series of high-profile DDoS (Distributed Denial of Service) Michael Calce is a security expert and former computer hacker against large commercial websites, including Yahoo!, Fifa.com, Amazon.com, Dell, Inc., E*TRADE, eBay, and CNN.

9. Kevin Poulsen is a former computer hacker, whose best known hack involved penetrating telephone company computers in the early

1990s to win radio station phone-in contests. Kevin Lee Poulsen is an American black-hat hacker .

10. Astra infiltrated the Dassault Group, a French company with civil and military aviation subsidies, and stole and subsequently sold corporate secrets, including information on weapons systems.They are black hat hackers

Saloni Ghule 21bce1967

TASK 2

PORT AND VULNERABILITIES:

Ports 20 :

FTP –DATA is known for being outdated and insecure. As such, attackers frequently exploit it through: Brute-forcing passwords. Anonymous authentication (it's possible to log into the FTP port with “anonymous” as the username and password)

Port 21:

Businesses need to think about using port 21 FTP to transfer files in their organization due to the unencrypted nature of FTP transmissions. Using FTP can expose sensitive information and network credentials to an attacker when transmitting data across the network or the Internet.

Port 22:

As such, Port 22 is subject to countless, unauthorized login attempts by hackers who are attempting to access unsecured servers. A highly effective deterrent is to simply turn off Port 22 and run the service on a seemingly random port above 1024

Port 23:

Port 23 is a TCP protocol that connects users to remote computers. For the most part, Telnet has been superseded by SSH, but it's still used by some websites. Since it's outdated and insecure, it's vulnerable to many attacks, including credential brute-forcing, spoofing and credential sniffing.

Port 25:

Port 25 is a Simple Mail Transfer Protocol (SMTP) port for receiving and sending emails. Without proper configuration and protection, this TCP port is vulnerable to spoofing and spamming

Port 53:

While using source port equal to 53 UDP packets may be sent by passing the remote firewall, and attacker could inject UDP packets, in spite of the presence of a firewall.

Port 69:

SolarWinds TFTP (Trivial File Transfer Protocol) Server is vulnerable to a denial of service, caused by an error when handling Read Request requests. By sending a specially-crafted Read Request to UDP port 69, a remote attacker could exploit this vulnerability to cause the server process to crash.

Port 80:

Port 80 isn't inherently a security risk. However, if you leave it open and don't have the proper configurations in place, attackers can easily

use it to access your systems and data. Unlike port 443 (HTTPS), port 80 is unencrypted, making it easy for cybercriminals to access, leak and tamper with sensitive data.

Port 110:

The issues include: "Buffer Overflows," "Cross-Site Scripting" attacks, "SQL Injection," and many others.

Port 123:

NTP is vulnerable to MitM attacks. These attacks allow unauthorized users to intercept, read, and modify traffic sent between clients and servers. NTP is particularly susceptible to MitM attacks due to the reliance on a small set of servers and the algorithm used to choose a server with which to sync.

Port 143:

One of the biggest security issues with IMAP is that it transmits logins from the client to the server in plain text by default, meaning usernames and passwords are not encrypted. (An encrypted login is obscured using complex mathematical equations so an attacker would not be able to understand it just by reading it.)

Port 443:

What Are the Port 443 Vulnerabilities? Port 443 has the same exposure as the HTTPS and TLS protocols. Vulnerabilities can include the following: Man-in-the-middle (MITM) attacks, where a hacker intercepts the communication between the client and server to steal sensitive information.

TASK 3:

Saloni Ghule

CWE 284 for Broken Access Control:

Description:

The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

Business impact:

Broken access control (CWE 284) can cause unauthorized data leaks, regulatory fines, financial fraud, disrupted operations, and harm to reputation, leading to financial losses, legal trouble, and customer distrust.

CWE 310 for Cryptographic failures:

Description:

Weaknesses in this category are related to the use of cryptography.

Business Impact:

These issues involve weaknesses in how information is encrypted and protected. If not addressed, they can lead to data breaches, unauthorized access, and loss of sensitive information. This can result in damaged customer trust, legal repercussions, financial losses, and harm to the company's reputation. Therefore, it's crucial for businesses to prioritize

strong encryption practices to mitigate these risks and safeguard their operations and customer data.

CWE-89 for Injection:

Description:

CWE-89 is the specific Common Weakness Enumeration (CWE) identifier for "SQL Injection," which is a type of security vulnerability that occurs when an attacker is able to manipulate or inject malicious SQL code into a web application's input fields or parameters.

Business impact:

It allows hackers to sneak malicious code into a website's input fields, leading to unauthorized access of sensitive data like customer information or financial records. This breach of security can harm customer trust, result in legal penalties, cause financial losses, and damage the company's reputation. It's essential for businesses to prevent SQL Injection to safeguard their data and maintain a secure online environment.

CWE for 676 Insecure Design :

Description:

This category encompasses various weaknesses related to the design of software applications that can lead to security vulnerabilities.

Business Impact:

Insecure Application Design, can have significant business impacts. If not addressed, it can lead to security vulnerabilities that attackers exploit to gain unauthorized access, steal sensitive data, or disrupt services. This can result in breaches, financial losses, legal consequences, damage to customer trust, and harm to the company's reputation. Fixing these design flaws early is crucial to prevent these risks and ensure the security of the business's applications and systems.

CWE for 494 Security Misconfiguration:

Description:

CWE-494 is a Common Weakness Enumeration (CWE) identifier that refers to the "Download of Code Without Integrity Check" vulnerability. This weakness occurs when software or data is downloaded from a remote source without verifying its integrity. In other words, the downloaded code or data has not been checked for tampering or unauthorized modifications, allowing potentially malicious content to be executed on the system.

Business impact:

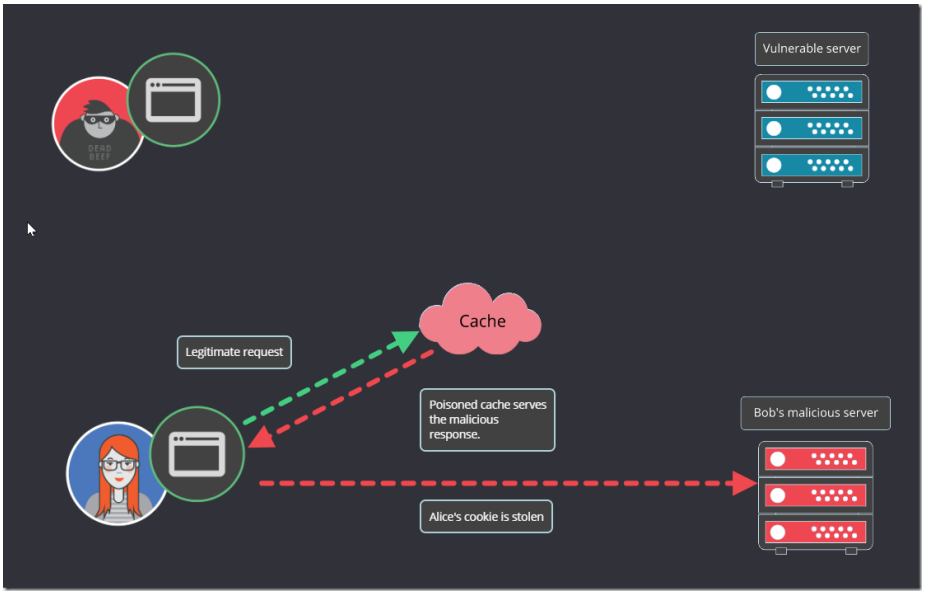
If exploited, malicious code could be introduced into the system during downloads, leading to unauthorized access, data breaches, and potential disruptions. This can result in compromised customer data, financial losses, legal repercussions, and damage to the company's reputation. Implementing integrity checks helps prevent these risks and ensures the security and reliability of the software or system.

Saloni Ghule

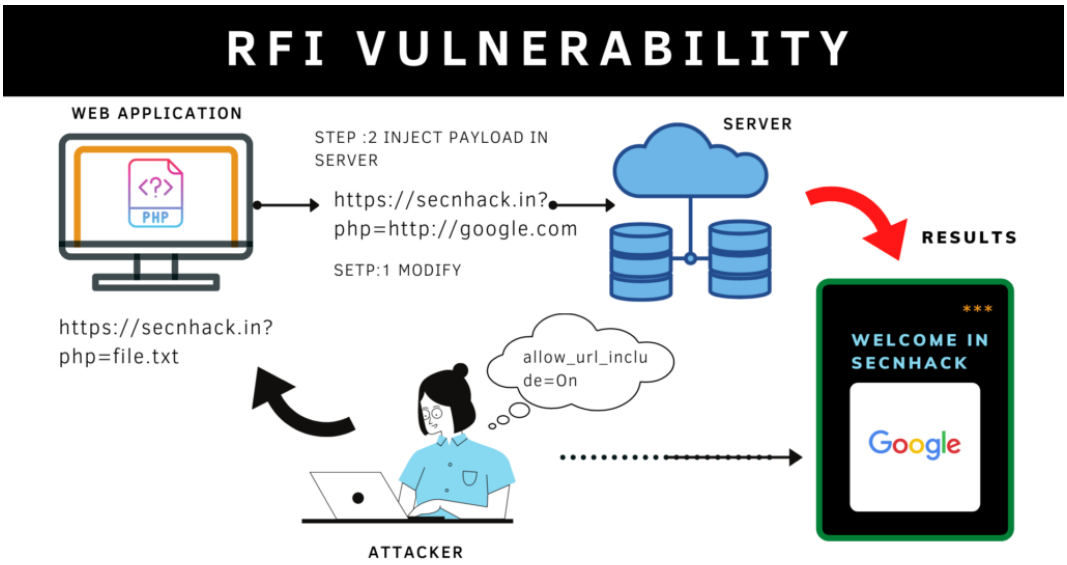
Task 4:

UNDERSTANDING WEB APPLICATION VULNERAILITIES

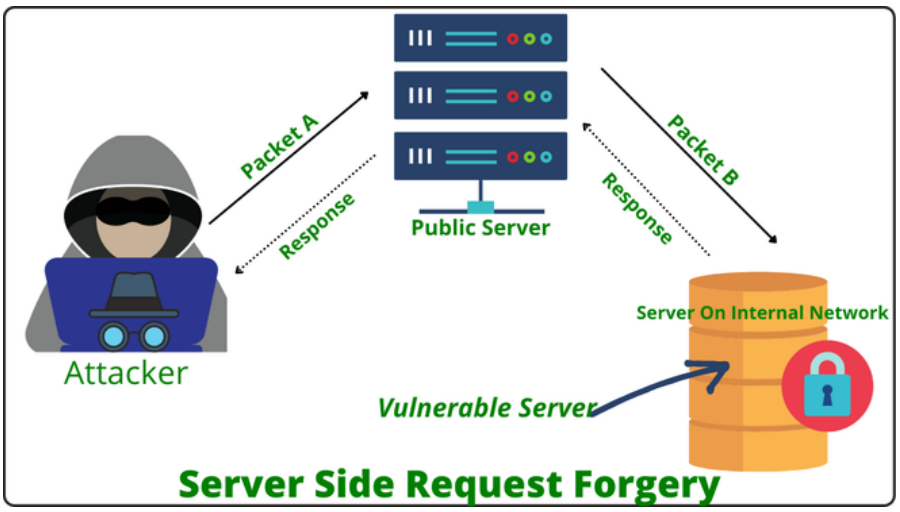
1. **HTTP Response Splitting:** HTTP Response Splitting occurs when an attacker manipulates input to inject newline characters into HTTP responses. This can lead to the creation of multiple responses, allowing them to inject malicious content or headers into the response, potentially bypassing security controls and causing a range of attacks, including cache poisoning and cross-site scripting (XSS).



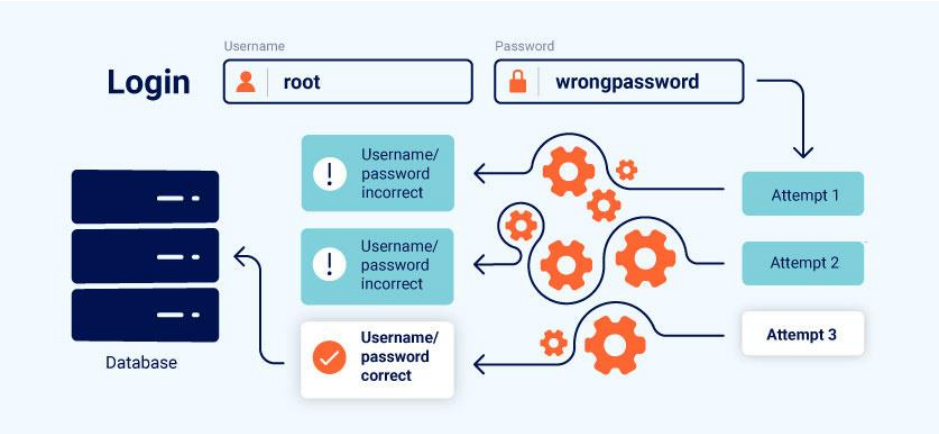
2. **Remote File Inclusion (RFI):** RFI is a vulnerability that occurs when an attacker is able to manipulate the inclusion of files from a remote server. This can lead to remote code execution by loading malicious scripts from an external source, allowing attackers to take control of the targeted system.



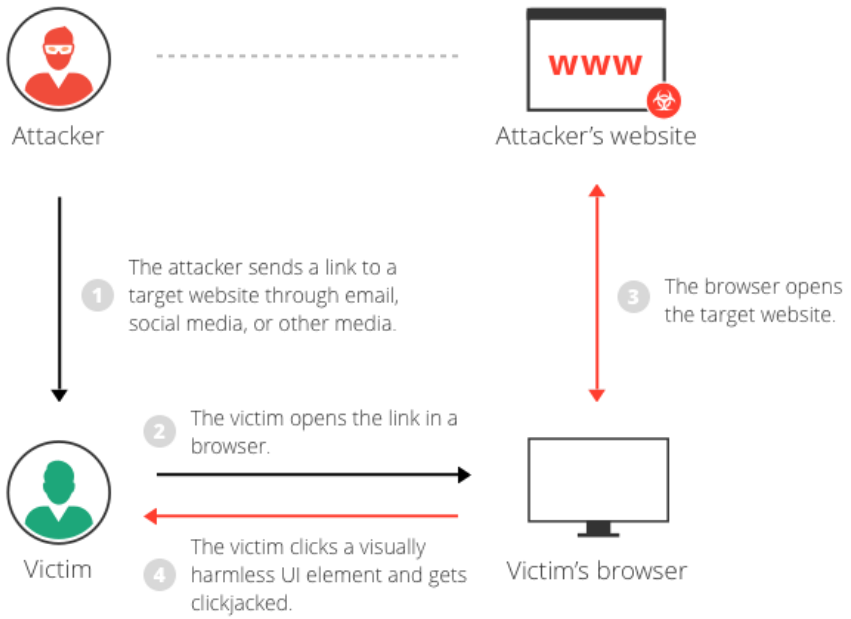
3. **Server-Side Request Forgery (SSRF):** SSRF is an attack that allows an attacker to make unauthorized requests from a vulnerable server to internal resources, potentially leading to data exposure, remote code execution, and further attacks against internal systems.



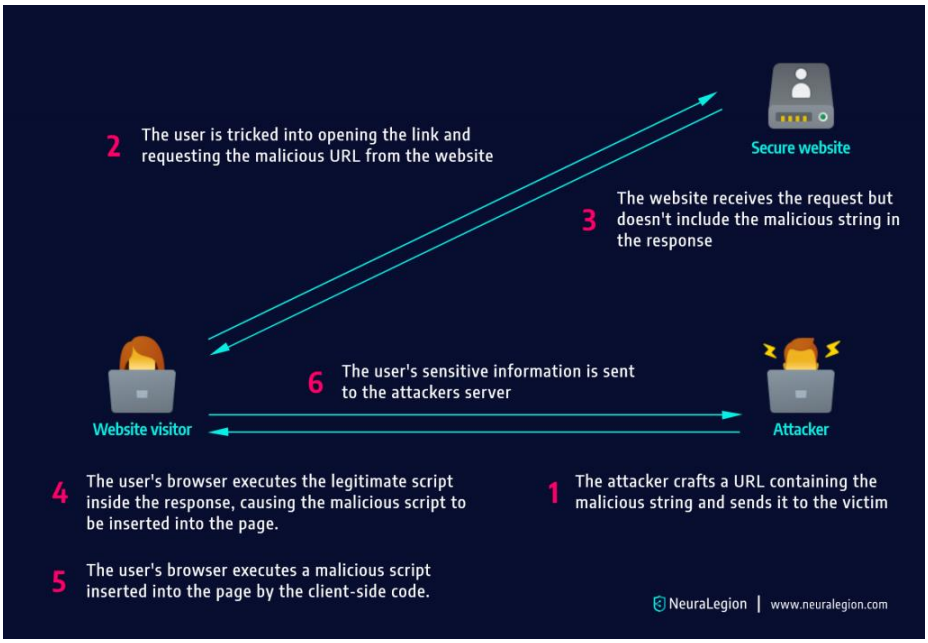
4. **Business Logic Vulnerabilities:** These vulnerabilities stem from flaws in the design and implementation of the application's business logic. Attackers exploit these vulnerabilities to perform actions that violate the intended workflow of the application, such as unauthorized access to restricted features or manipulating transactions.



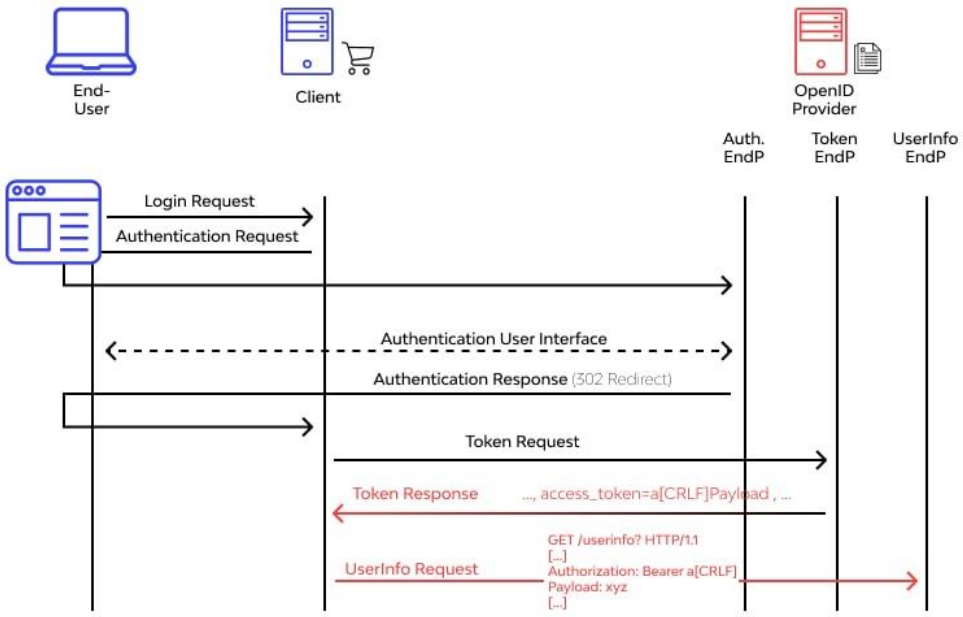
5. **Clickjacking:** Clickjacking involves deceiving a user into clicking on something different from what they perceive. Attackers overlay transparent elements on top of legitimate website elements, tricking users into performing actions they didn't intend, potentially leading to unauthorized actions or data leakage.



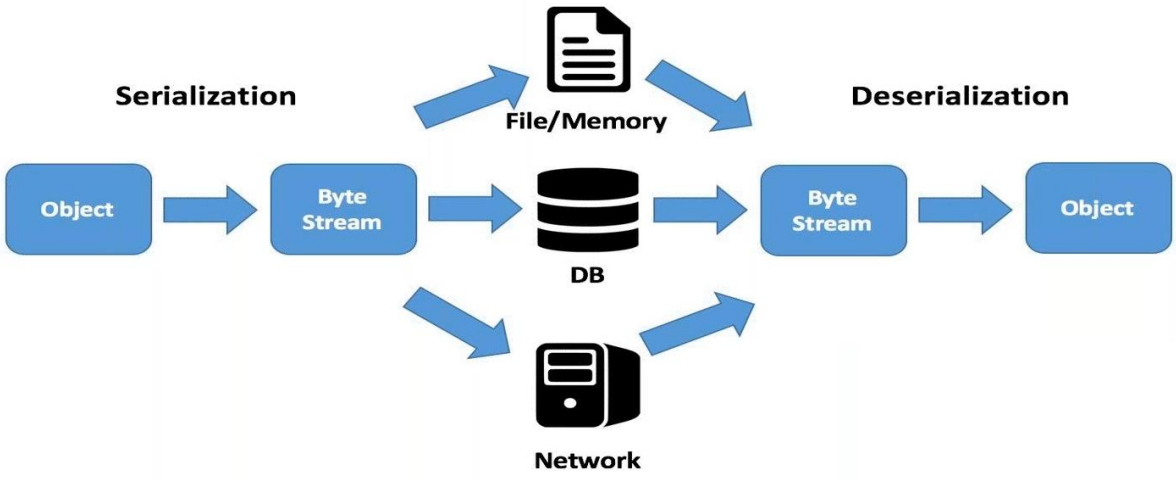
6. **DOM-based Cross-Site Scripting (DOM XSS):** DOM XSS occurs when an attacker manipulates the Document Object Model (DOM) of a web page to execute malicious scripts in the victim's browser. Unlike traditional XSS, which relies on server-side vulnerabilities, DOM XSS attacks manipulate the client-side code directly.



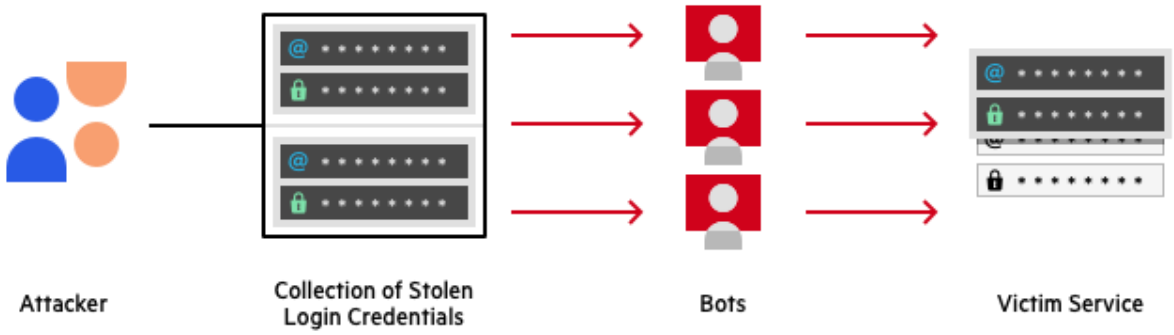
7. **CRLF Injection:** Carriage Return Line Feed (CRLF) injection is a vulnerability where an attacker injects CRLF characters into application input, potentially leading to HTTP header manipulation, HTTP response splitting, or other attacks that exploit the improper handling of newlines.



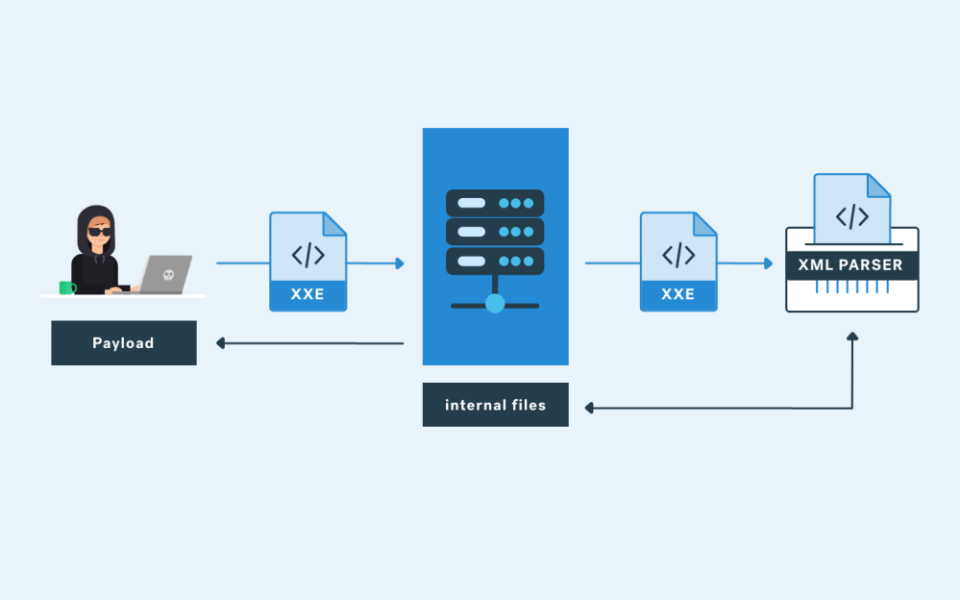
8. **Insecure Deserialization:** Description: Insecure deserialization occurs when an application processes untrusted serialized data, which can lead to remote code execution, authentication bypass, or other security issues.



9. **Credential Stuffing:** Credential stuffing occurs when attackers use leaked username and password pairs from one service to gain unauthorized access to other accounts, exploiting users who reuse passwords across multiple platforms.



10. **XML External Entity (XXE) Injection:** XML External Entity (XXE) Injection is a vulnerability that occurs when an application processes XML input from an untrusted source without proper validation and safeguards. XML (eXtensible Markup Language) is a widely used format for structuring and sharing data between different systems. XXE attacks exploit the way XML parsers process external entities, which are references to data outside of the XML document itself.


XXE
XXE
XML PARSER
Payload
internal files

TASK 9:

LOCAL SECURITY POLICY

Local Security Policy in Windows is a management tool that allows administrators to configure and enforce security settings on a local computer. It is primarily used to control the security of a single Windows computer, as opposed to Group Policy, which is used to manage security settings for multiple computers within a domain.

Here are some key points about Local Security Policy:

Security Settings: Local Security Policy provides a graphical user interface for configuring security-related settings on a Windows computer. These settings cover a wide range of security aspects, including user account policies, audit policies, security options, and more.

User Account Policies: It allows you to define password policies, account lockout policies, and other settings related to user accounts. For example, you can set password complexity requirements or specify how many failed login attempts trigger an account lockout.

Audit Policies: Local Security Policy lets you configure auditing policies to track events and activities on the computer. This is crucial for monitoring and analyzing security-related events, helping you identify potential security breaches.

Security Options: You can control various security-related options, such as requiring Ctrl+Alt+Delete for login, disabling guest accounts, and configuring interactive logon settings.

Local Policies: It includes settings for user rights assignments, which determine what actions users and groups are allowed to perform on the computer. Examples include the right to shut down the system, change system time, or manage auditing and security logs.

Local Security Policy vs. Group Policy: While Group Policy allows centralized management of security settings across multiple computers in a network domain, Local Security Policy is limited to a single computer. Group Policy is typically used in enterprise environments, while Local Security Policy is more suitable for standalone computers or small networks.

Local Security Policy is used to enhance the security of a Windows computer by configuring and enforcing security policies and settings. It helps administrators tailor security measures to meet their specific requirements and protect the local system from unauthorized access, malicious activities, and other security threats. By defining and enforcing security policies through Local Security Policy, administrators can reduce vulnerabilities and improve the overall security posture of the Windows computer.