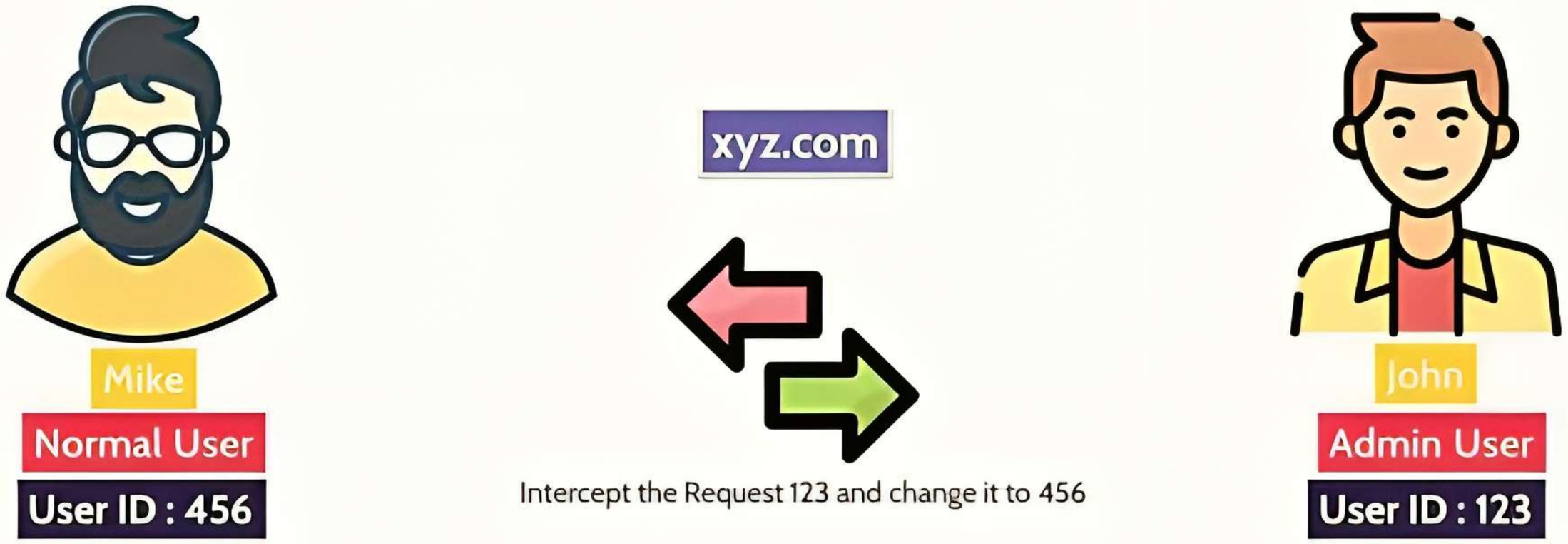
MINISTRY OF SECURITY

OWASP TOP TEN VULNERABILTIES

EXPLAINED EASY

01 BROKEN ACCESS CONTROL

Broken access control occurs when an issue with the access control enforcement allows a user to perform an action outside of the user's limits.



For example, an attacker may be able to exploit a flaw in an application with the intention of gaining elevated access to data to which they are not entitled and can perform unauthorized actions.

MINISTRY OF SECURITY

02 CRYPTOGRAPHIC FAILURE

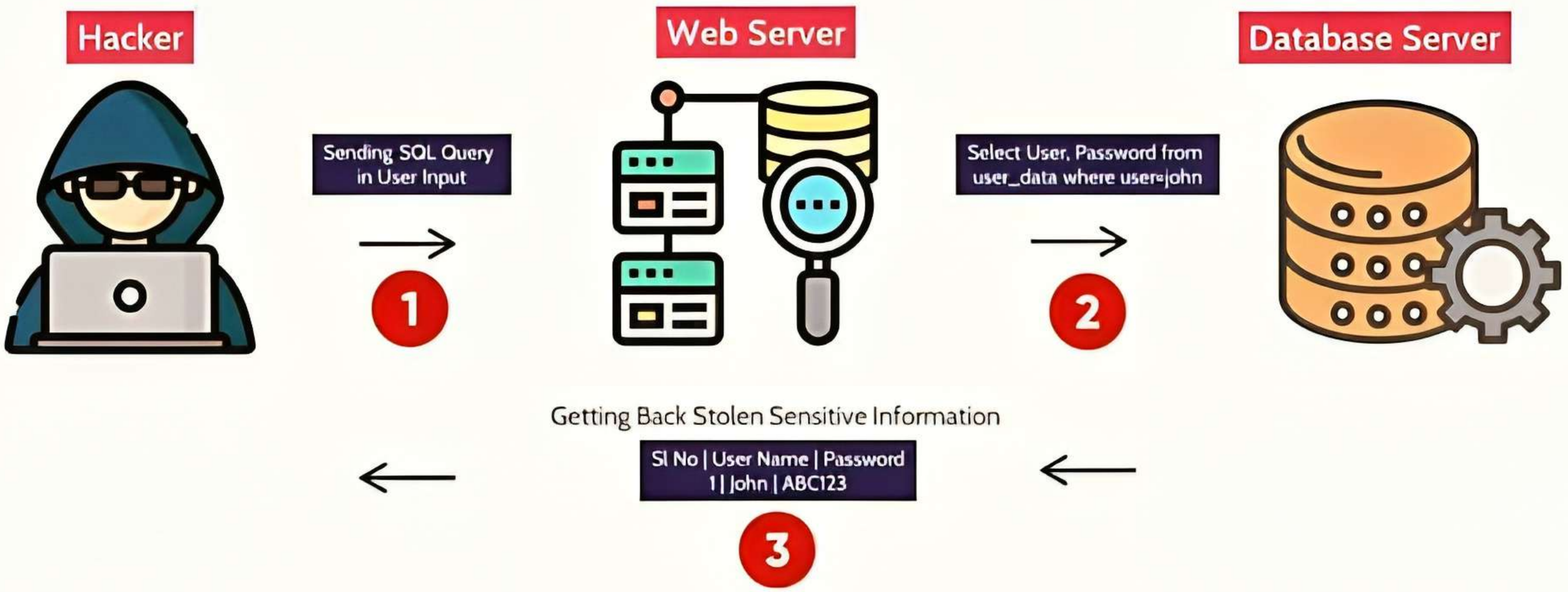
A cryptographic failure flaw can occur when you store or transmit data in clear text or try to protect data with old or weak encryption.

For example, consider a site that doesn't enforce TLS for all pages. An attacker steals the user's session cookie and then replays this cookie and hijacks the user's (authenticated) session, accessing or modifying the user's private data.

MINISTRY OF SECURITY

03 INJECTION

Injection attacks are a type of security vulnerability that arises when an application takes user input and uses that input in an unsafe way.



Injection attacks are one of the most dangerous attacks where an attacker simply sends malicious data to make the application process it and do something it is not supposed to do.

MINISTRY OF SECURITY

04 INSECURE DESIGN

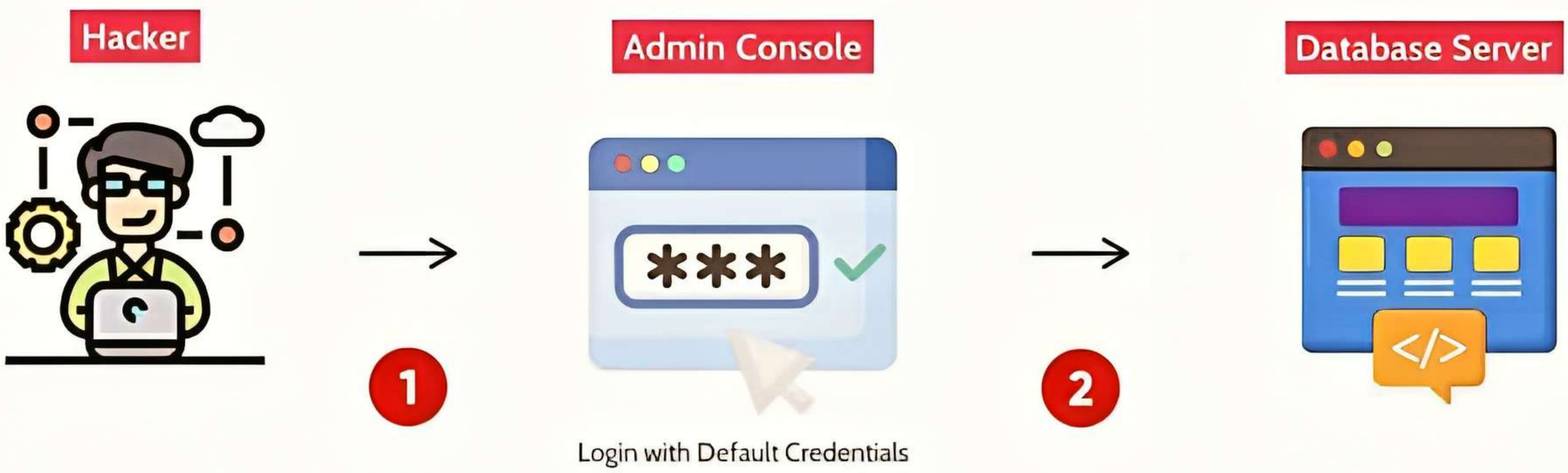
Insecure design expressed as “missing or ineffective control design.” If a system or product design is not secure, it can be considered an insecure design.

For instance, a malicious actor could reserve 600 movie tickets for a specific timeframe, preventing genuine buyers from reserving any. This situation could have been prevented if the system design had limited reservations to just 15 tickets.

MINISTRY OF SECURITY

05 SECURITY MISCONFIGURATION

Misconfiguration vulnerabilities are configuration weaknesses that may exist in software components or may have unneeded services enabled, such as remote administration functionality.

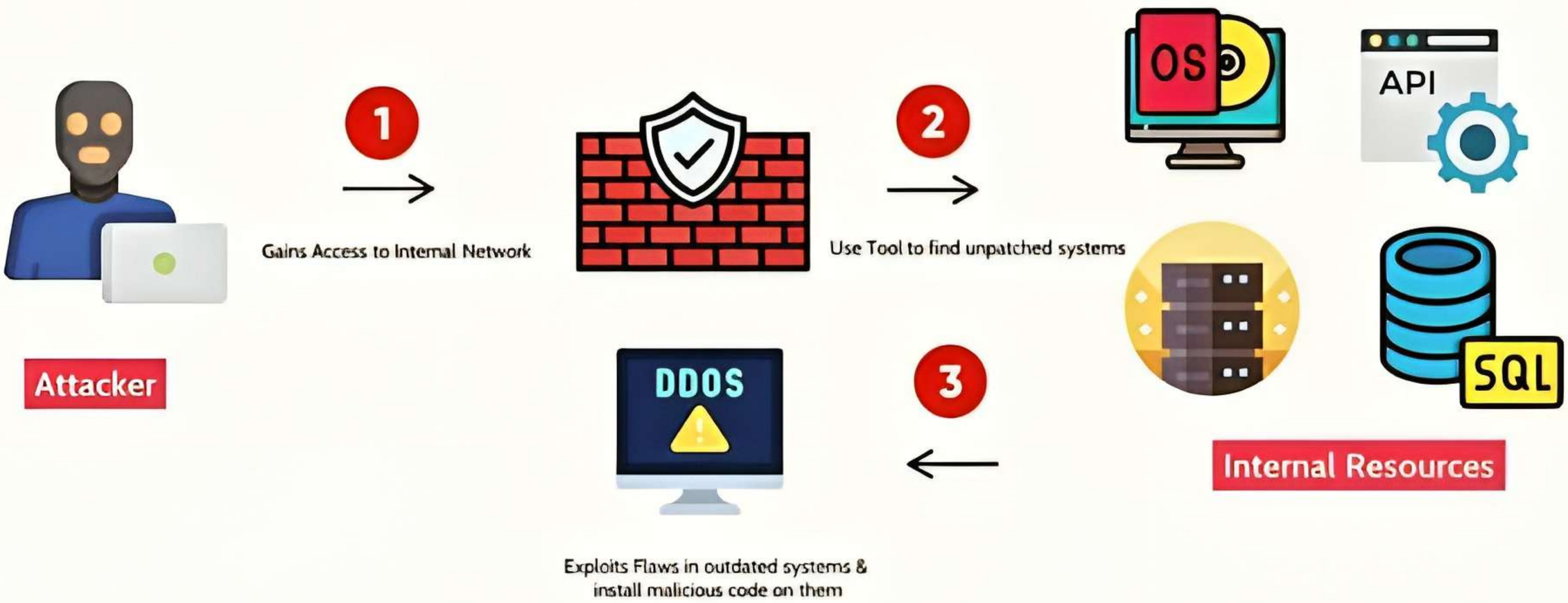


For example, web server software may ship with default user accounts that an attacker can use to access the system, or the software may contain sample files, such as configuration files and scripts that an attacker can exploit.

MINISTRY OF SECURITY

06 VULNERABLE COMPONENTS

The term “vulnerable” or “outdated” components is used to describe software susceptible to being breached, hacked, or otherwise compromised.

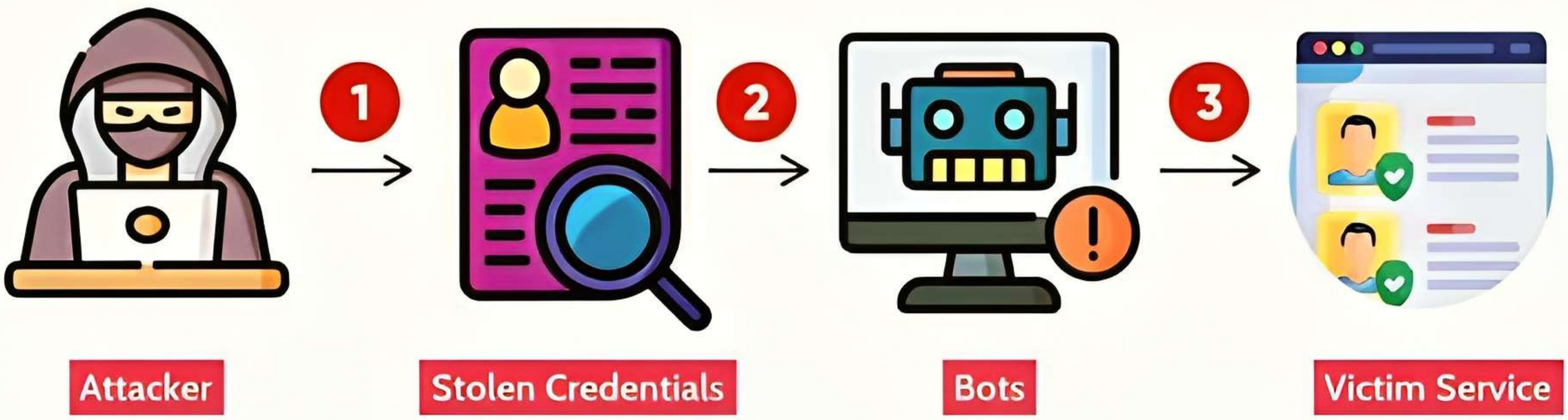


An attacker may exploit component vulnerabilities and then gain access to unauthorized information, modify data, or cause a denial of service (DoS). Components can include OS, Database, API and Server etc.

MINISTRY OF SECURITY

07 IDENTIFICATION & AUTHENTICATION FAILURES

Identification and authentication failures can occur when functions related to a user's identity, authentication, or session management are not implemented correctly.

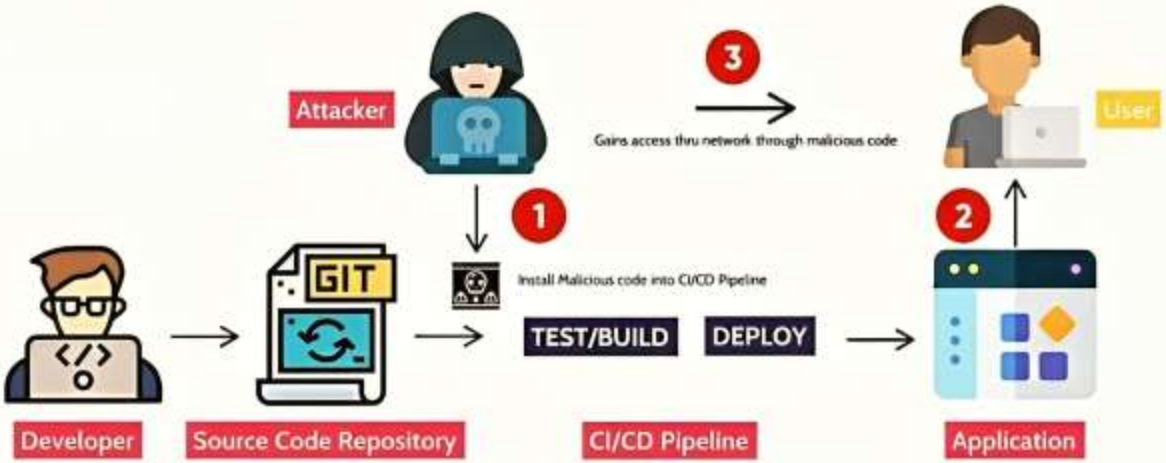


Attackers may be able to exploit identification and authentication failures by compromising passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.

MINISTRY OF SECURITY

08 SOFTWARE AND DATA INTEGRITY FAILURES

Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations or use software from untrusted sources.



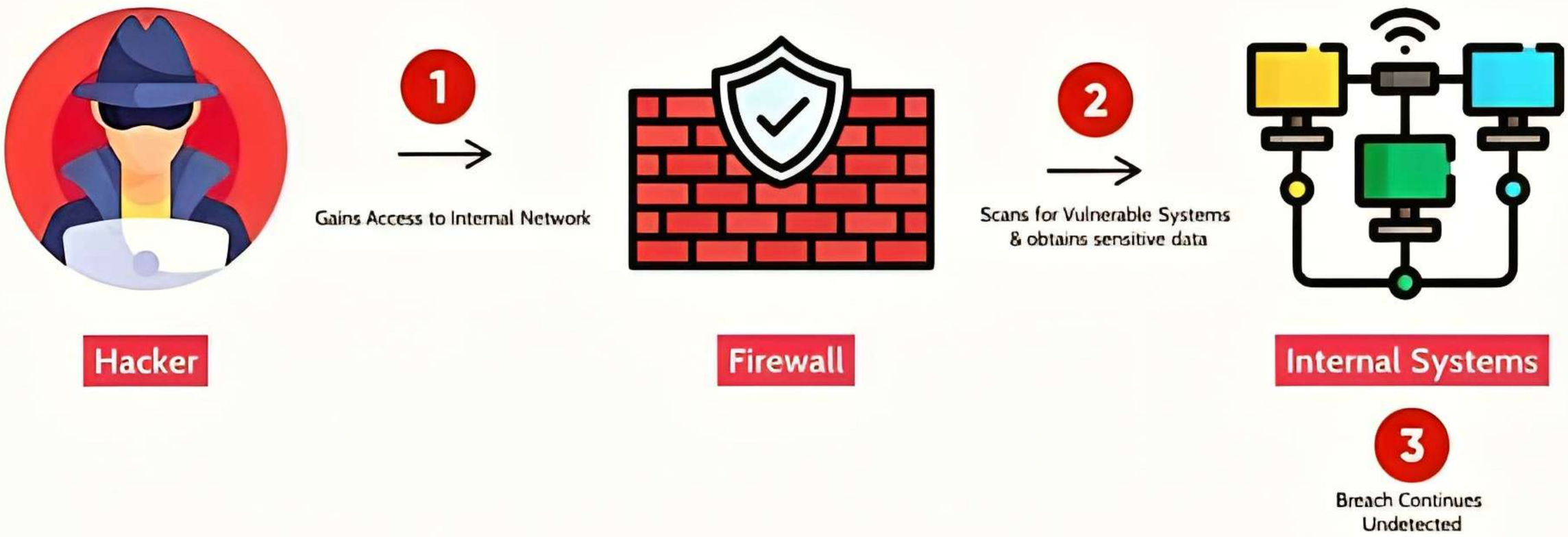
An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code, or system compromise.

MINISTRY OF SECURITY

09

LOGGING AND MONITORING FAILURES

Failure to sufficiently log, monitor, or report security events, makes suspicious behavior difficult to detect and greatly increases the chances of an attacker successfully taking advantage of your application.



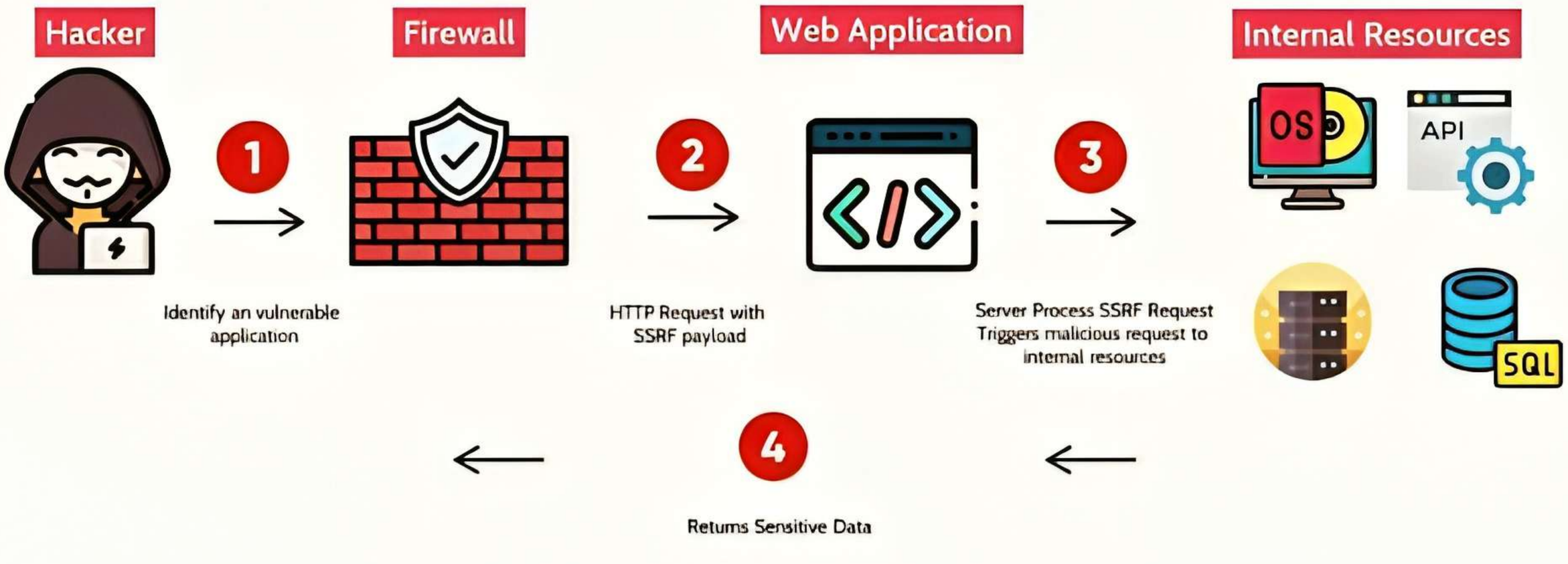
A children's health plan provider's website operator couldn't detect a breach due to a lack of monitoring and logging. The attacker had accessed and modified thousands of sensitive health records.

MINISTRY OF SECURITY

10

SERVER-SIDE REQUEST FORGERY

Server Side Request Forgery (SSRF) attacks are used to target internal systems that are behind firewalls and are not accessible from the external network.



In a normal SSRF attack the attacker might cause the server to make a connection to internal services by exploiting internally running services like SSH, localhost, FTP etc and steals the data.

MINISTRY OF SECURITY