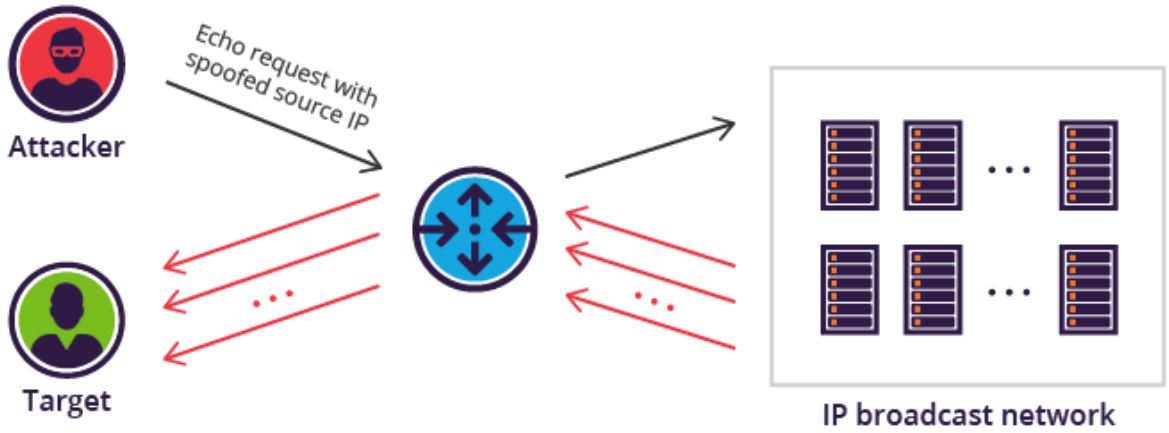
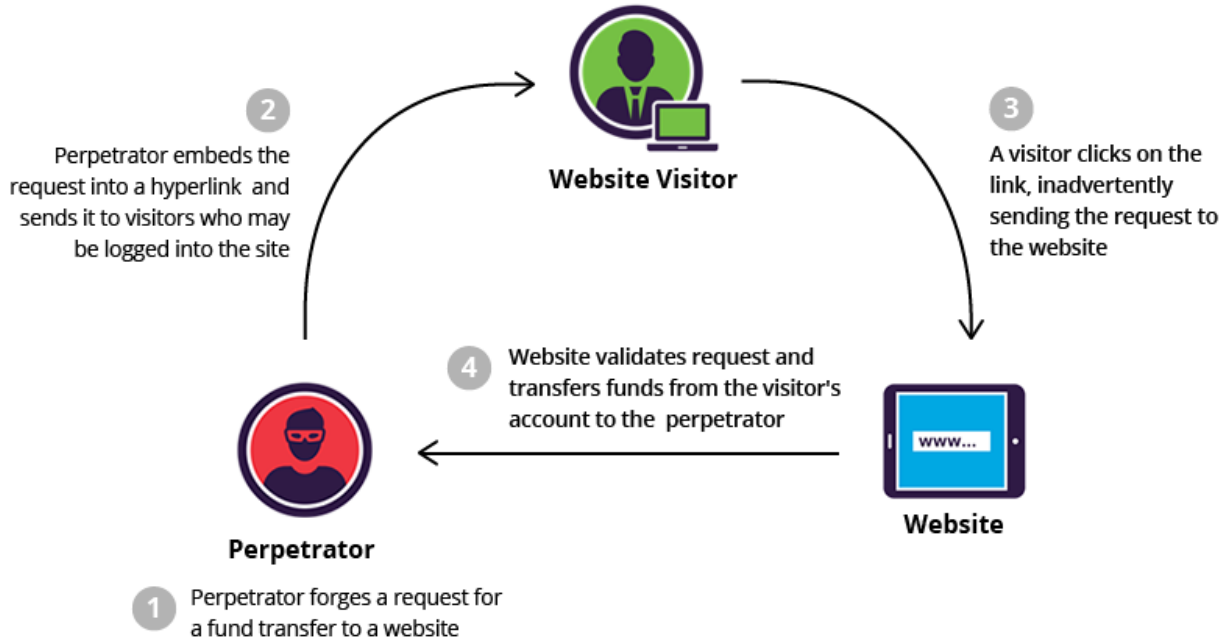
10 Web Application Vulnerabilities

1)Smurf Attack



A Smurf attack is a type of cyber attack that falls under the category of distributed denial of service(DDoS) attacks. DDoS attacks aim to overwhelm a target system,network,or service with a massive amount of traffic,rendering it inaccessible to legitimate users.The Smurf attack is a specific variant of DDoS attack that takes advantage of a flaw in the Internet Control Message Protocol(ICMP),which is used for various network management and diagnostic tasks.

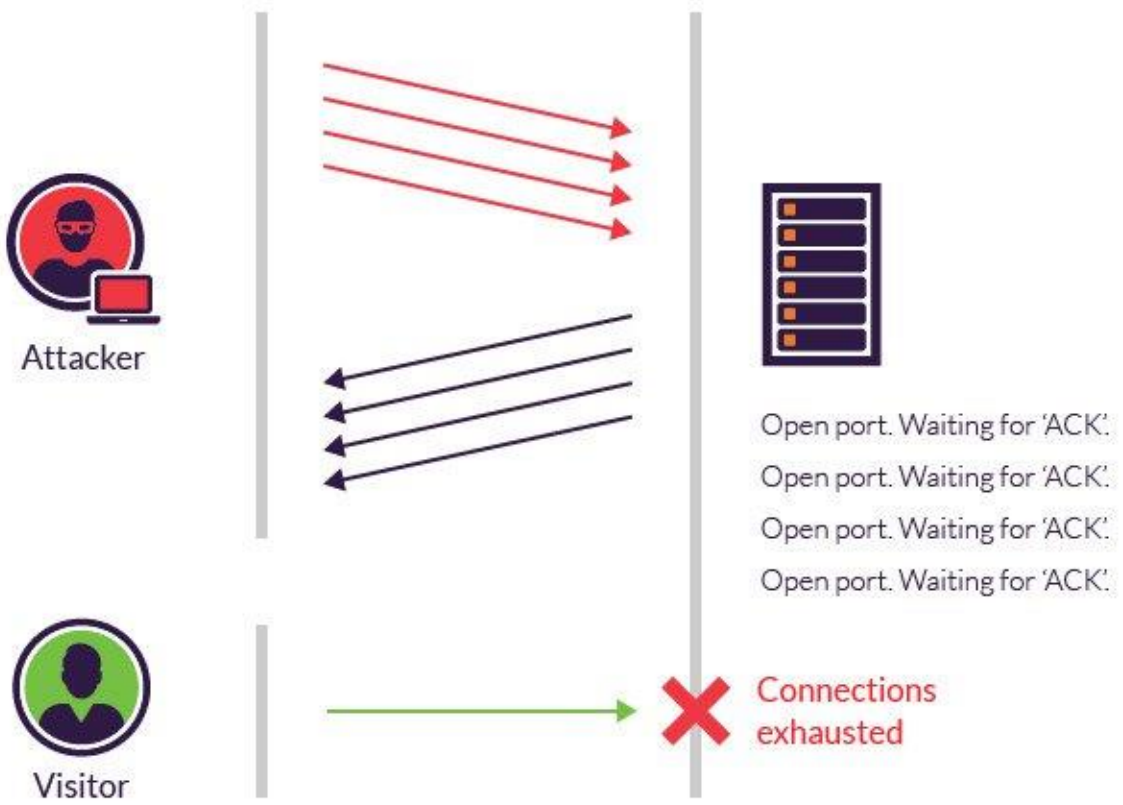
2)Cross-site request forgery



Cross Site Request Forgery is a type of cyber attack that targets the trust realationship between a user and a website they are logged into.Also known as a one click attack or session

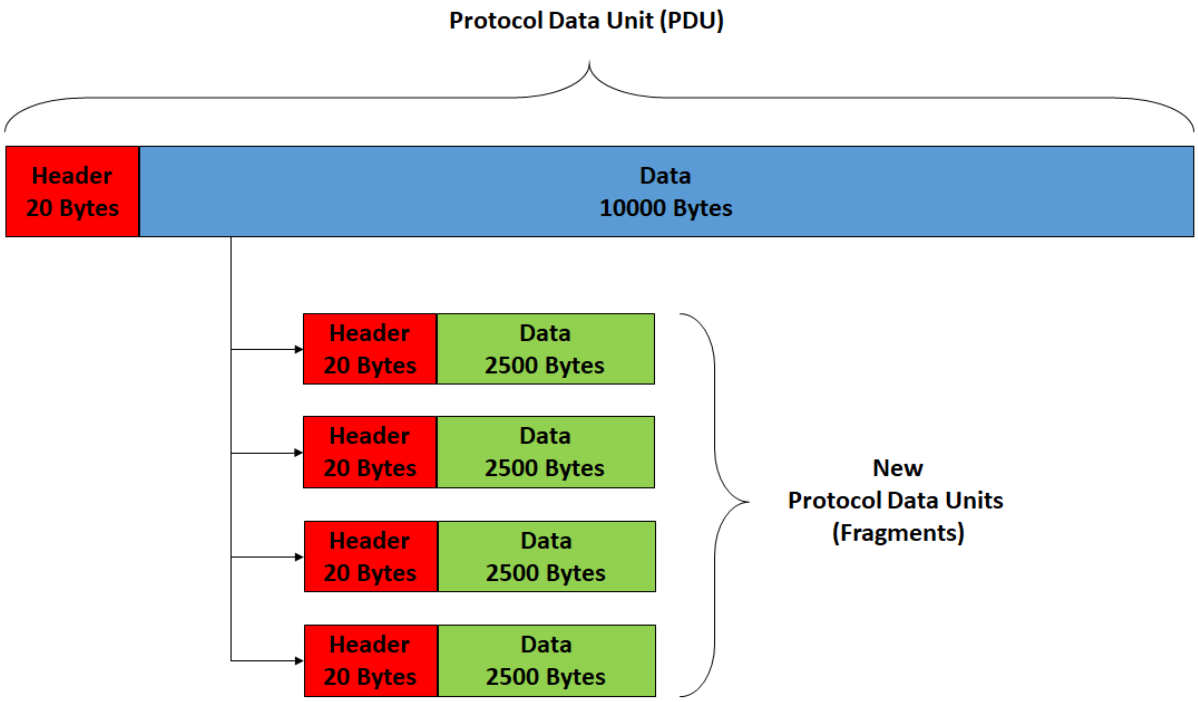
riding,CSRF,attacks occur when an attacker tricks the user's browser into making an unintended and unauthorized request to a different website on which the user **is authenticated.**

3)<u>SYN Flood Attack</u>



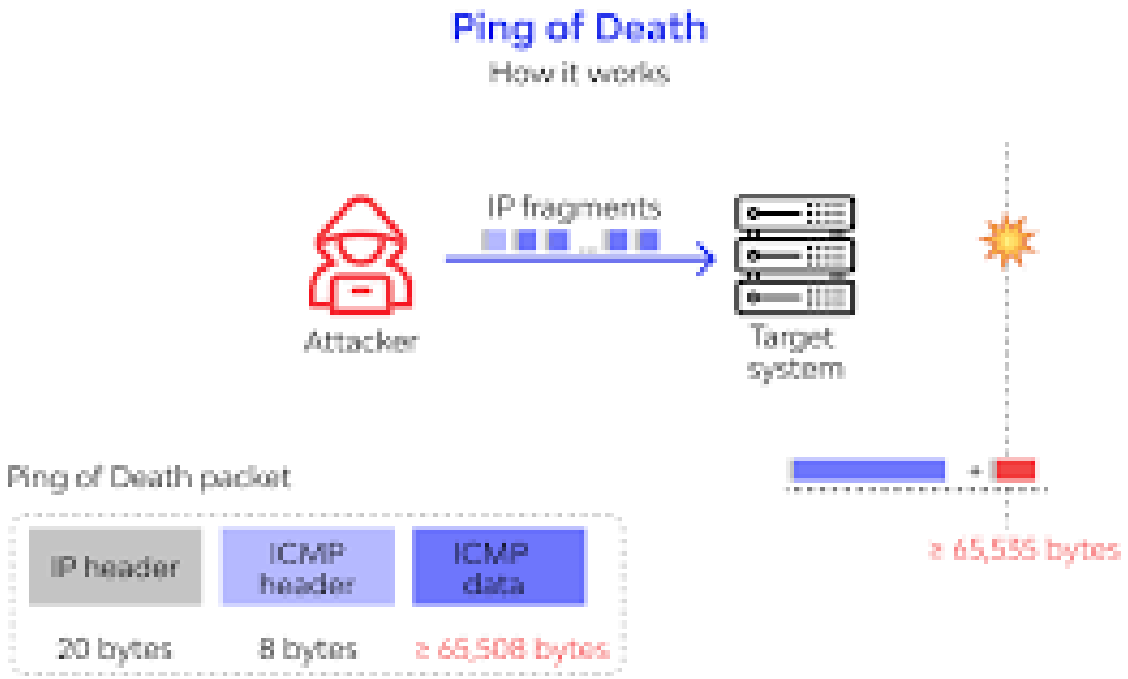
A SYN flood attack is a type of cyber attack that targets the three way handshake process in the transmission control protocol, a fundamental protocol used for establishing connections between devices over the internet. This type of attack is a subtype of Distributed Denial of Service(DDoS) attacks, which aim to overwhelm a target system or network with a large volume of malicious traffic ,rendering it inaccessible to legitimate users.

4)<u>IP fragmentation</u>:



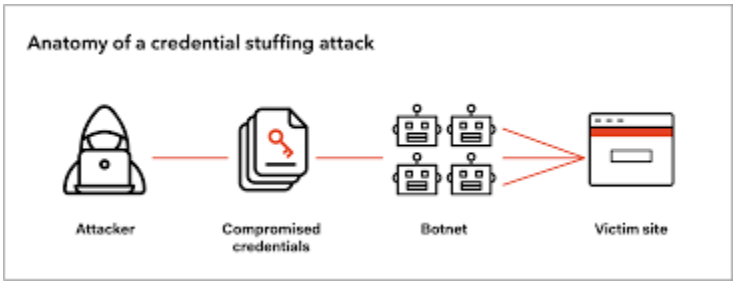
IP fragmentation attacks are a kind of computer security attack based on how the IP requires data to be transmitted and processed. Specifically,it invokes IP fragmentation, a process used to partition messages from one layer of a network into multiple smaller payloads that can fit within the lower layers protocol data unit.

5)<u>Ping of death</u>



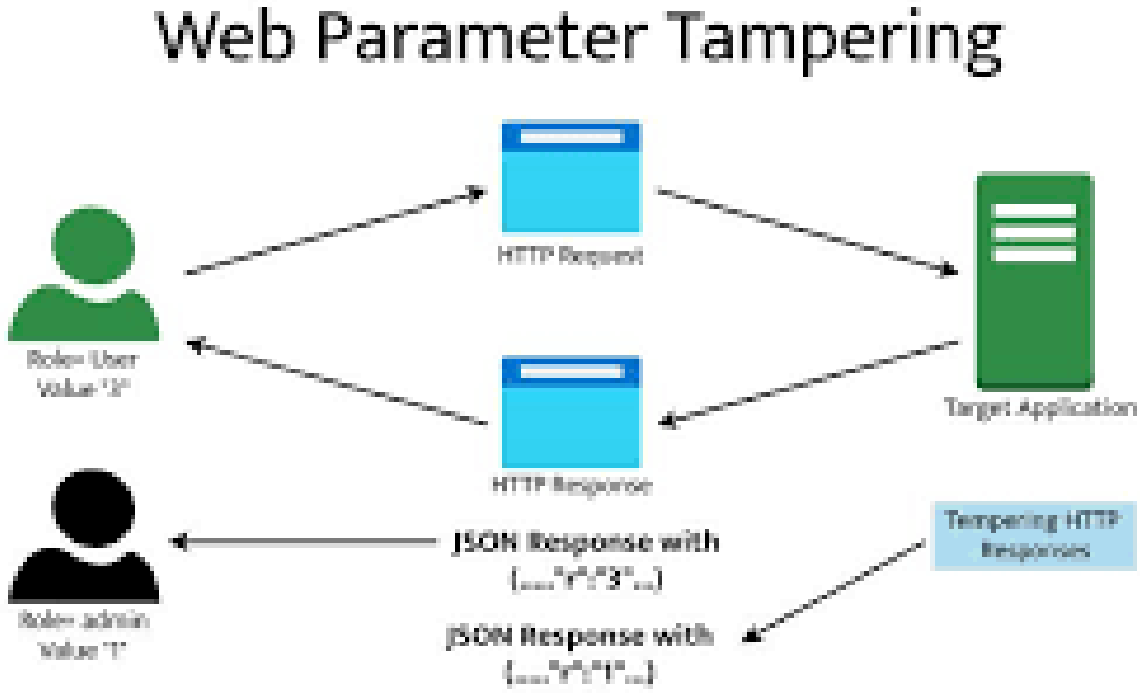
It is a type of cyber attack that targets networked computer systems,particularly those using the Internet Control Message Protocol for communication.ICMP is a protocol used by network devices to send error messages and operational information about network conditions.One of the functions of ICMP is to send “echo request” messages,commonly known as “pings”,”to check if a remote host is reachable and responsive.

6)Broken Authentication Attack



This attack are a type of cybersecurity threat that attacks vulnerabilities in the authentication and session management mechanisms of web applications. Authentication is the process of verifying the identity of a user, and session management involves maintaining a users authenticated state during their interaction with a web application.when these mechanisms are improperly implemented or configured,attackers can exploit the weaknesses to gain unauthorized access to accounts or manipulate user sessions.

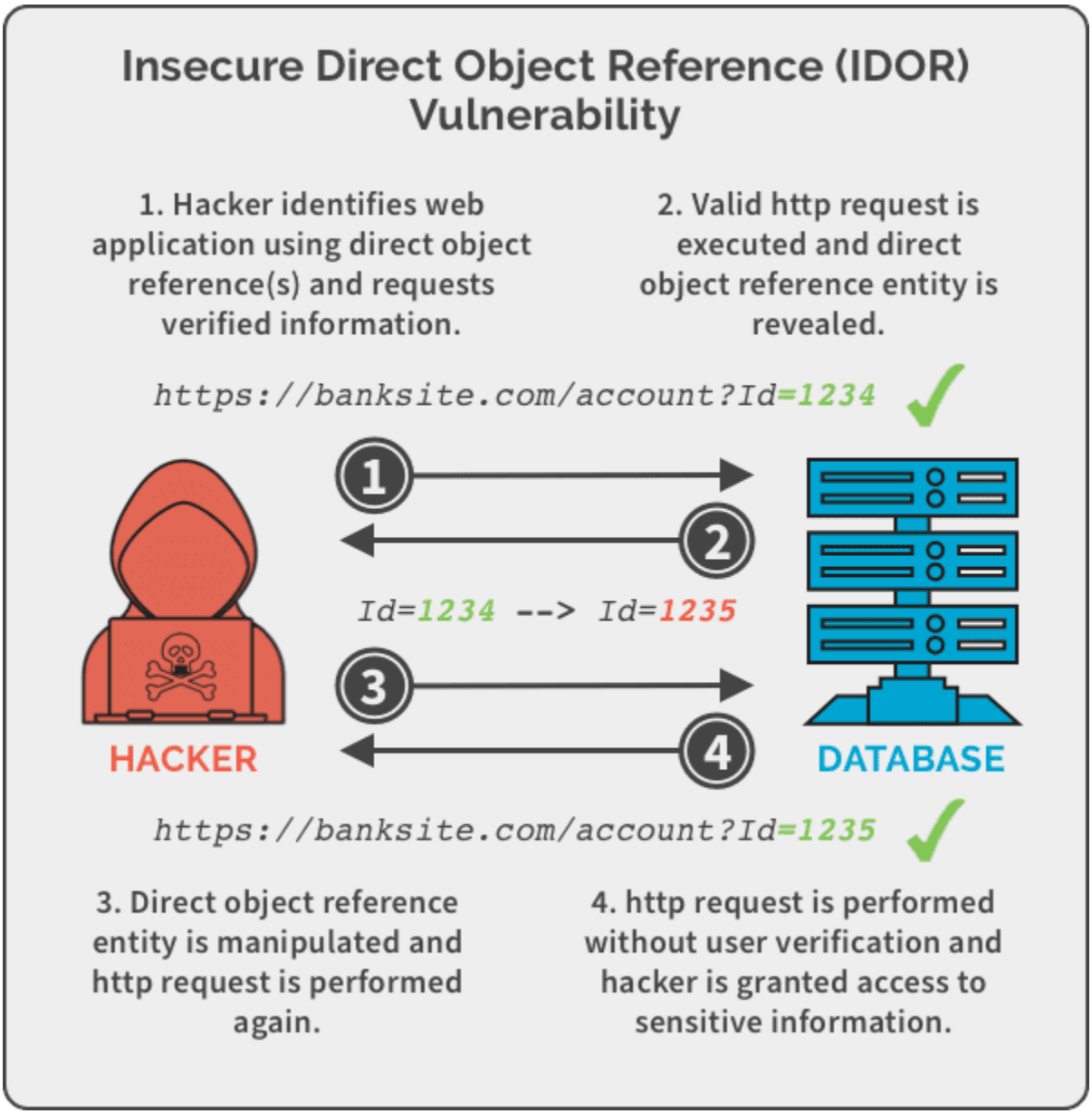
7)Character Generator protocol



It is a simple network protocol that was originally defined in the early days of the internet.it’s a protocol designed for testing and debugging purposes and is not intended for actual application use due to its potential security vulnerability.It operates on port 19 and is typically implemented

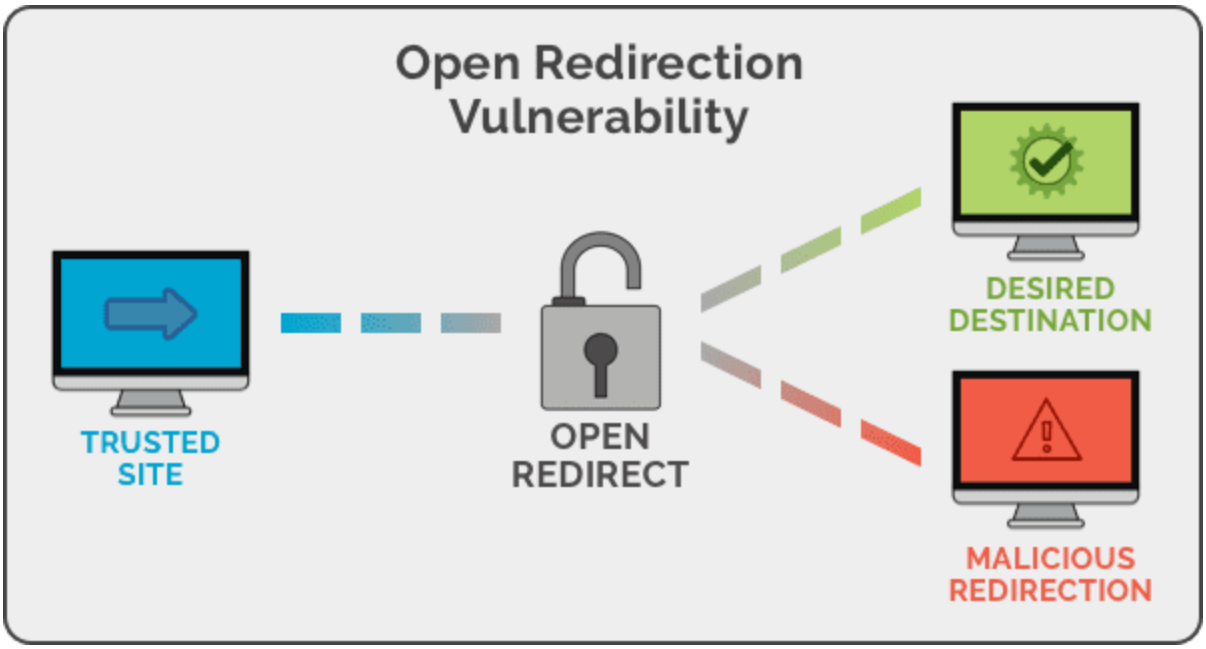
as a service network device.It’s main purpose is to respond to requests by sending a stream of characters back to the requester.This can be useful for testing network connectivity, measuring data transmission rates, and diagnosing network issues.

8)Insecure Direct Object References(IDOR):



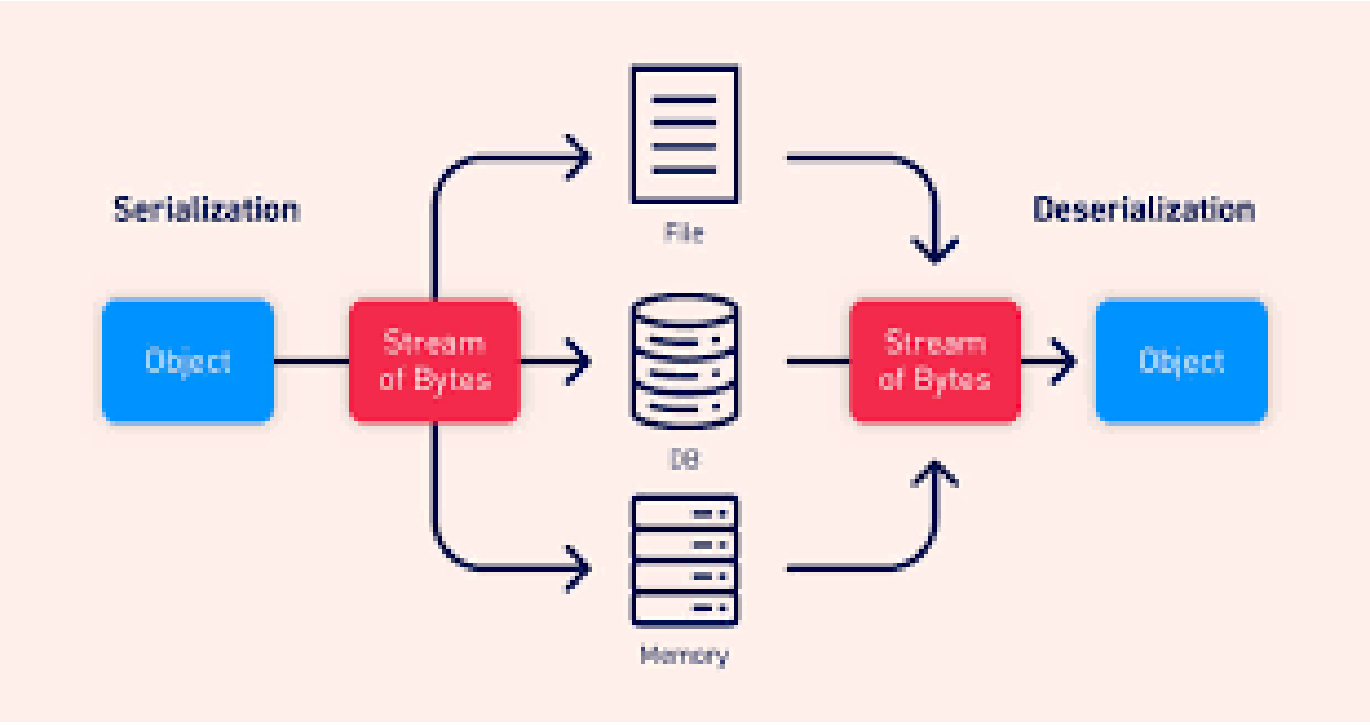
It is a type of web application vulnerability that occurs when an attacker is able to manipulate input parameters that reference internal objects such as files,database records,or resources,in a way that allows them to access unauthorized data or perform unauthorized actions. In simpler terms an IDOR attack allows an attacker to access information or perform actions that they should not have permission to access information or perform actions that they should not have permission to access, by manipulating input parameters like URLs or form fields.

9)Unvalidated Redirects and Forwards:



Unvalidated Redirects and Forwards is a web application vulnerability that occurs when an application allows users to navigate to different pages or websites using redirection or forwarding mechanisms without properly validating to redirect users to malicious websites or phishing pages,leading to potential data theft,phishing attacks, or other malicious activities.

10)Insecure Deserialization



Insecure Deserialization is a type of cybersecurity vulnerability that occurs when an application improperly handles data that is being deserialized. Serialization is the process of converting data structures or objects into a format that can be easily stored, transmitted, or reconstructed later. Deserialization is the reverse process, where serialized data is transformed back into its

original form. Insecure Deserialization vulnerabilities can be exploited by attackers to execute arbitrary code, bypass security controls, or perform other malicious actions. This is possible because deserialization can involve the reconstruction of complex data structures or objects, and if the application doesn't properly validate and sanitize the deserialized data, attackers can inject malicious code or manipulate the data in harmful ways.