Cyber Security Internship

Assignment-1

What is Cyber Security?

- Cyber security, also known as information technology security, is the practice of protecting systems, networks, and programs from **digital attacks**.

Types Of Cyber Security Attacks:

1. Active Attack
2. Passive Attack

Active Attack: Active attacks in cybersecurity are a type of attack where the attacker **directly interacts with the target system or network**.

- Denial-of-service (DoS) attacks
- Man-in-the-middle (MitM) attacks
- SQL injection attacks
- Malware attacks
- Password attacks

Passive Attack:

In contrast to active attacks that directly alter or disrupt systems, **passive attacks** in cybersecurity focus on **gathering information** about a target system or network **without being detected**. They act more like eavesdroppers, listening and observing without interacting with the system itself.

- **Eavesdropping:** Intercepting data transmissions over unsecured networks (e.g., Wi-Fi) to capture information like login credentials or messages.
- **Traffic analysis:** Monitoring network traffic patterns to gain insights into the system's activities, user behavior, or potential vulnerabilities.
- **Shoulder surfing:** Stealing information by observing someone physically using a device or writing down sensitive information.
- **Dumpster diving:** Recovering discarded documents or data storage devices containing sensitive information that hasn't been properly disposed of.
- **Social engineering:** Deceiving users into revealing confidential information through manipulation or exploiting their trust.

HACKERS CATEGORIES

1. White Hat Hackers:
•**Motivation:** Ethical and legal.
•**Intent:** Improve cybersecurity and identify vulnerabilities in systems with permission from the owner.

2. Black Hat Hackers:
•**Motivation:** Malicious and often illegal.
•**Intent:** Gain unauthorized access to systems for personal gain, disrupt operations, steal data, or inflict damage.

3. Gray Hat Hackers:
•**Motivation:** Varies, can be ethical or self-serving.
•**Intent:** Operate in a legal gray area, sometimes using their skills for good (e.g., identifying vulnerabilities without permission but responsibly disclosing them) and sometimes for personal gain (e.g., hacking for personal entertainment or bragging rights).

Essential Terminologies

Threats:

- **Malware:** Malicious software like viruses, worms, ransomware, spyware, and Trojans, designed to harm or exploit computer systems.
- **Phishing:** Social engineering attacks tricking users into revealing personal information through deceptive emails, messages, or websites.

Vulnerabilities:

- **Exploit:** A weakness in a system that attackers can use to gain unauthorized access or control.
- **Patch:** A software update that fixes a known vulnerability.

Security measures:

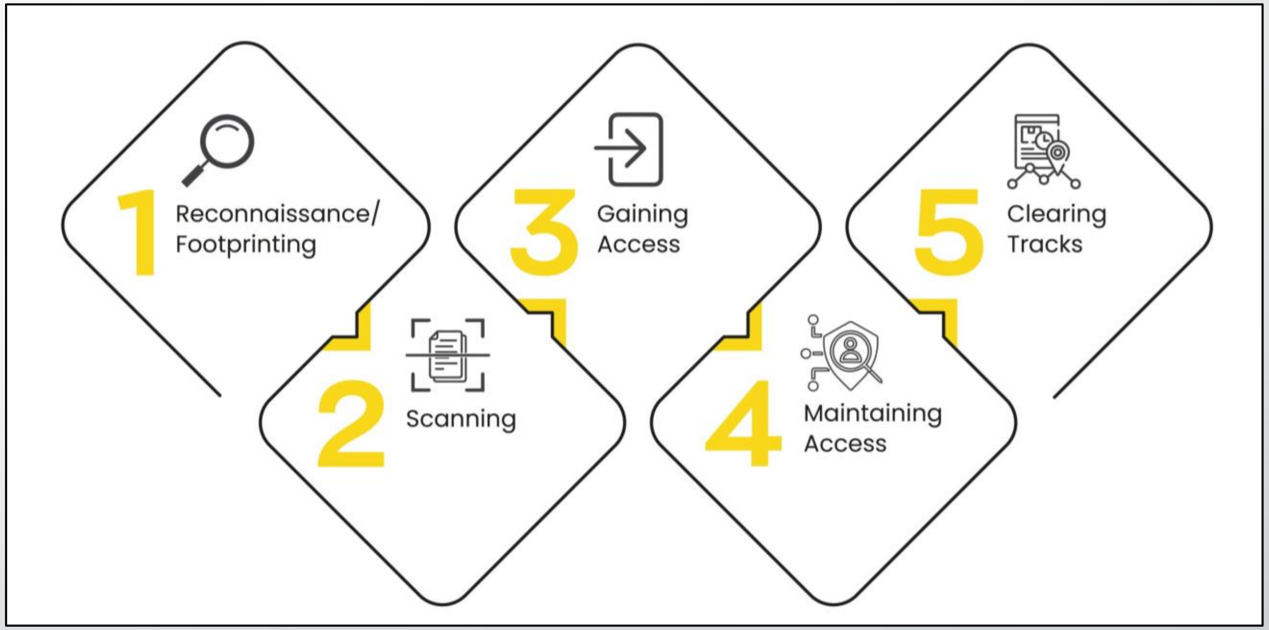
- **Firewall:** A software or hardware device that controls incoming and outgoing network traffic based on security rules.
- **Intrusion Detection/Prevention System (IDS/IPS):** Systems that monitor network activity for suspicious behavior and can either detect or actively block potential threats.
- **Multi-factor authentication (MFA):** Adding an extra layer of security to logins besides passwords, such as fingerprint scans or one-time codes.
- **Encryption:** Transforming data into a scrambled form that only authorized users can decrypt and access.

Top 10 Most Notorious Hackers Of All Time In This Internet World:

1. Kevin Mitnik
2. Anonymous
3. Adrian Lamo
4. Albert Gonzalez
5. Matthew Bevan And Richard Pryac
6. Jeanson James Ancheta
7. Michael Calce
8. Kevin Poulsen
9. Jonathan James
10. Astra

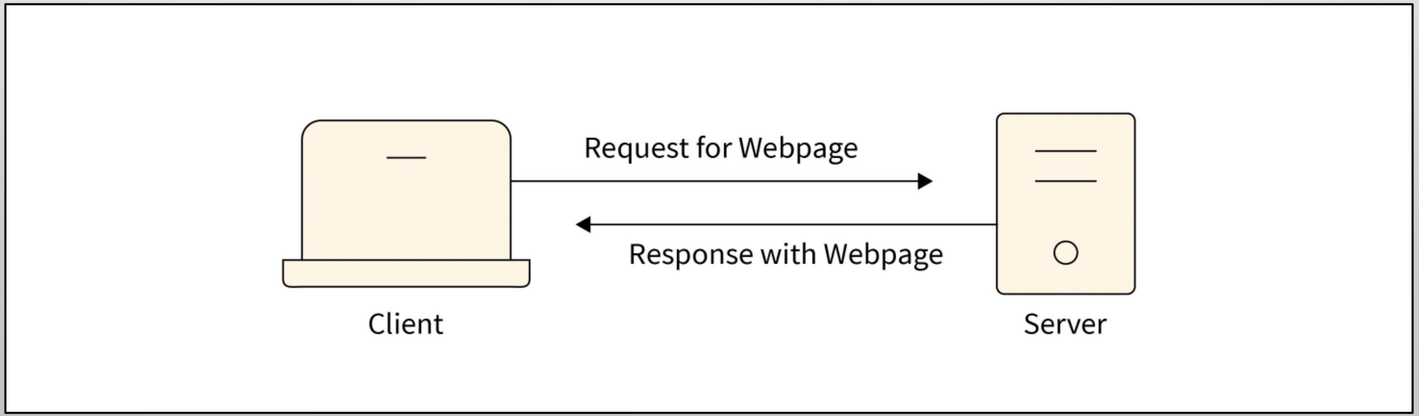
Phases of Hacking

1. Reconnaisance/ Footprinting
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Clearing Tracks

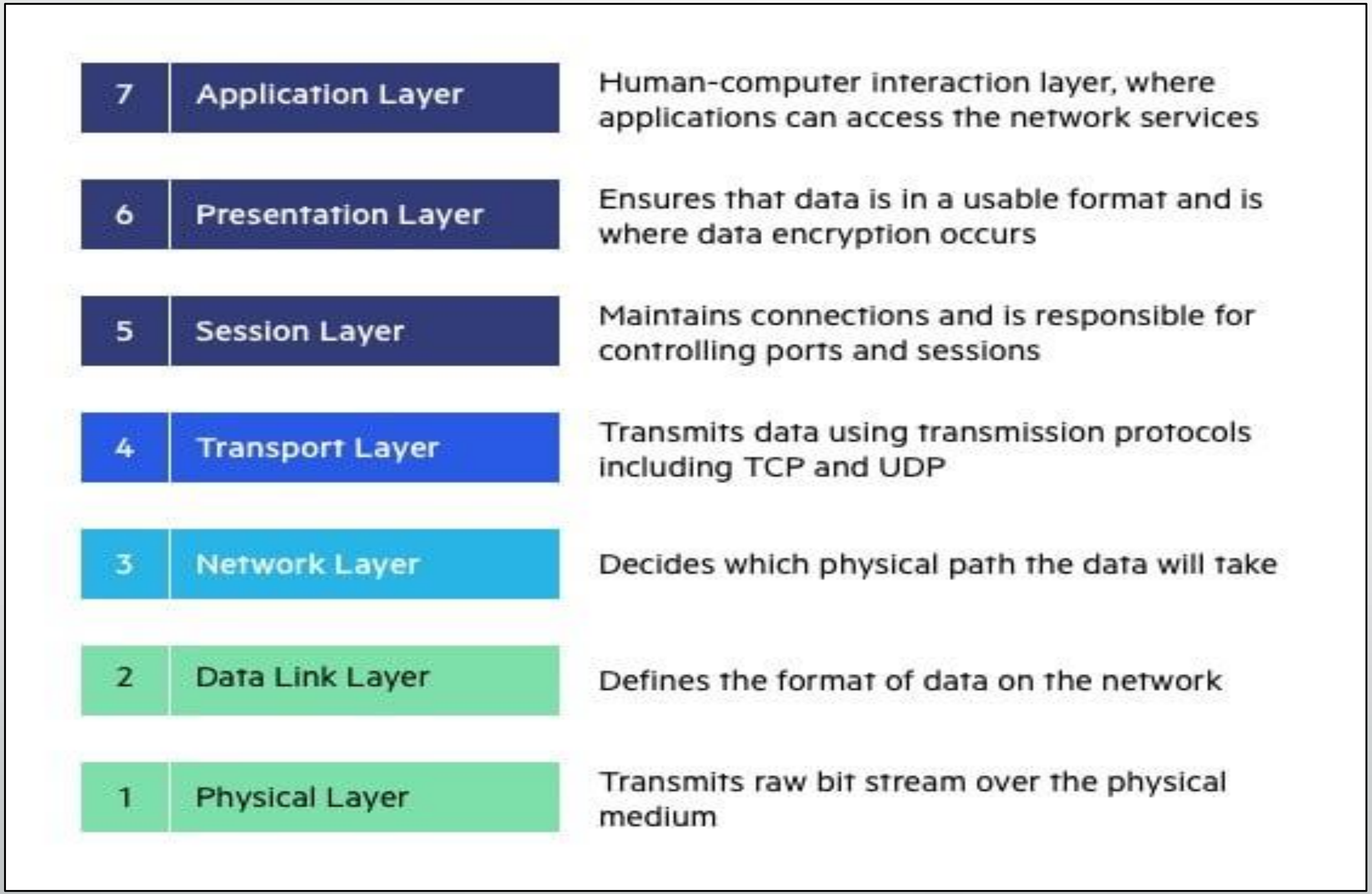


Introduction To Networking

- Client-server architecture, also known as the client-server model or network computing model, is a distributed system architecture that divides tasks and workloads between two distinct types of computer programs:
- Clients: These are user-facing applications that run on personal computers, laptops, mobile devices, or other workstations. They initiate requests for resources or services and display the results received from the server.
- Server: This is a powerful computer program running on a dedicated server machine that manages resources, processes requests from clients, and delivers the requested data or service.



OSI MODELS



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

Application Layer:

•**Function:** Provides network services directly to user applications, such as file transfer, email, web browsing, remote login, and network management.

•**Components:** This layer interacts directly with user applications like web browsers, email clients, and file transfer programs.

Presentation Layer:

•**Function:** Handles data presentation, including encryption/decryption, compression/decompression, and character encoding/decoding, ensuring compatibility between different systems.

•**Components:** Can involve data formatting and translation protocols.

Session Layer:

•**Function:** Establishes, manages, and terminates sessions between communicating applications.

•**Components:** Less commonly used in modern networks, but can be used for session coordination and authorization.

Transport Layer:

•**Function:** Provides reliable communication between applications on different devices by establishing connections, ensuring in-order delivery, and handling flow control.

•**Components:** TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are common transport layer protocols.

Network Layer:

•**Function:** Routes data packets across different networks, determining the most efficient path to reach the destination.

•**Components:** Routers, IP addresses, routing protocols.

Data Link Layer:

•**Function:** Packages data into frames, adds error detection and correction mechanisms, and controls the physical transmission of frames between devices on the same network segment.

•**Components:** Switches, bridges, MAC addresses, error-checking codes (e.g., CRC).

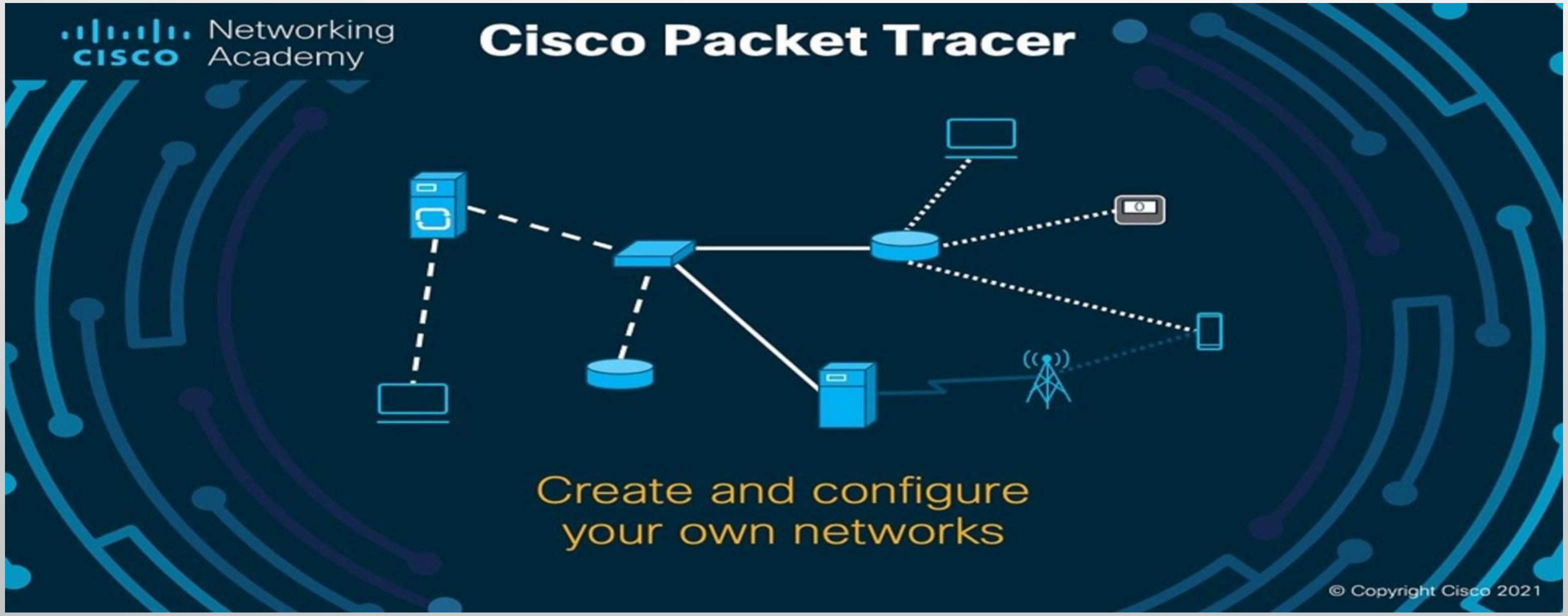
Physical Layer:

•**Function:** Deals with the physical transmission of data bits over a physical medium like cables or wireless signals.

•**Components:** Cables, connectors, network cards (NICs), hubs, repeaters.

DASHBOARD OF CISCO PACKET TRACER

Cisco packet tracer is a network simulation and visualization tool developed by Cisco systems. It allows users to create visual networks and simulate network configuration, devices, and connections.it used for educational purpose, such as teaching networking concepts and practicing network troubleshooting.



What is python

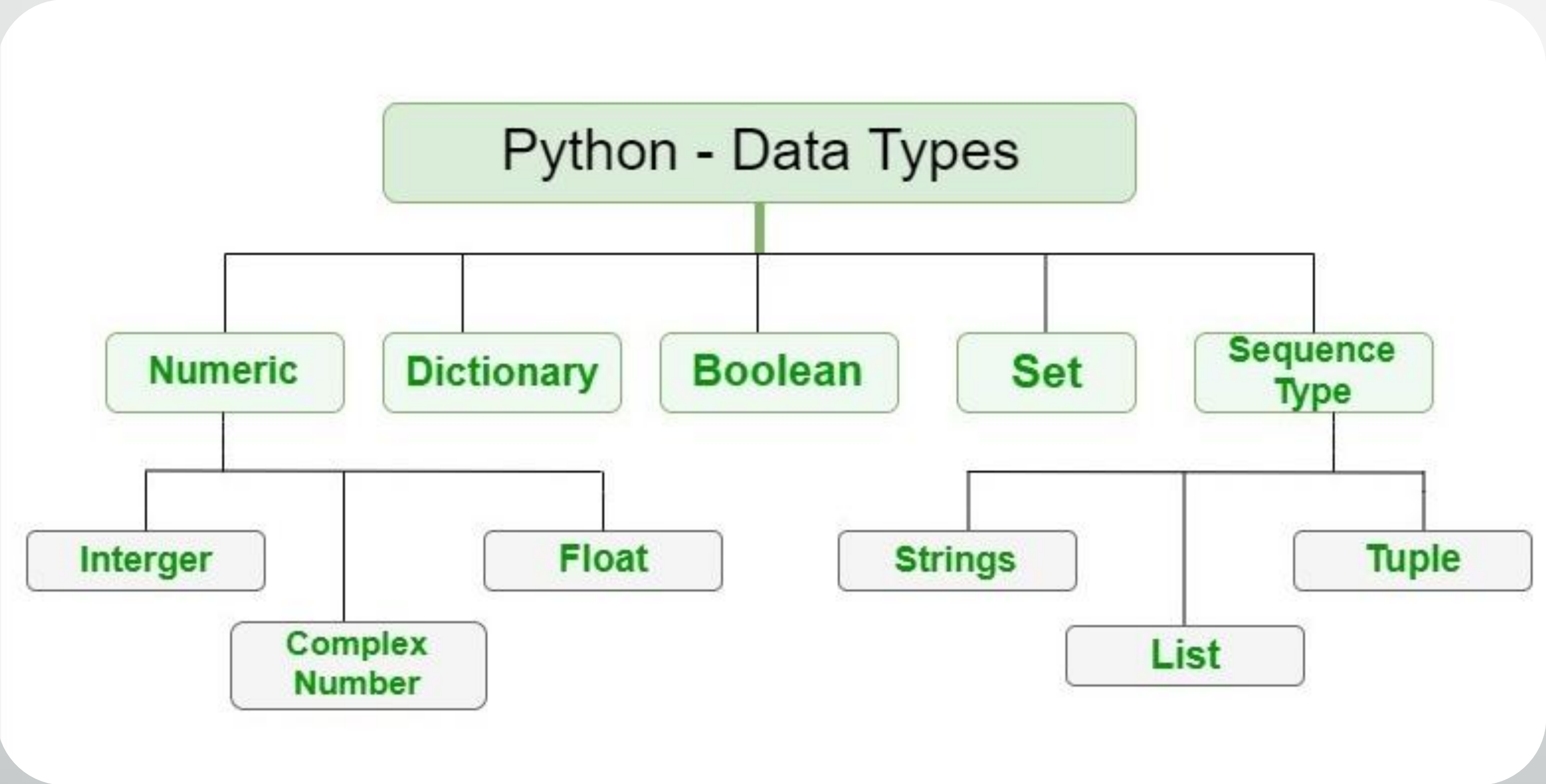
- Python plays a significant role in various aspects of cybersecurity due to its versatility and powerful features and extensive libraries.

Python is popular in cybersecurity:

- **Easy to learn:** Clear and readable code makes it beginner-friendly.
- **Lots of tools:** Many ready-made libraries for security tasks save time.
- **Does many things:** One language for various cybersecurity needs.
- **Free and helpful:** No cost and a large community for support.

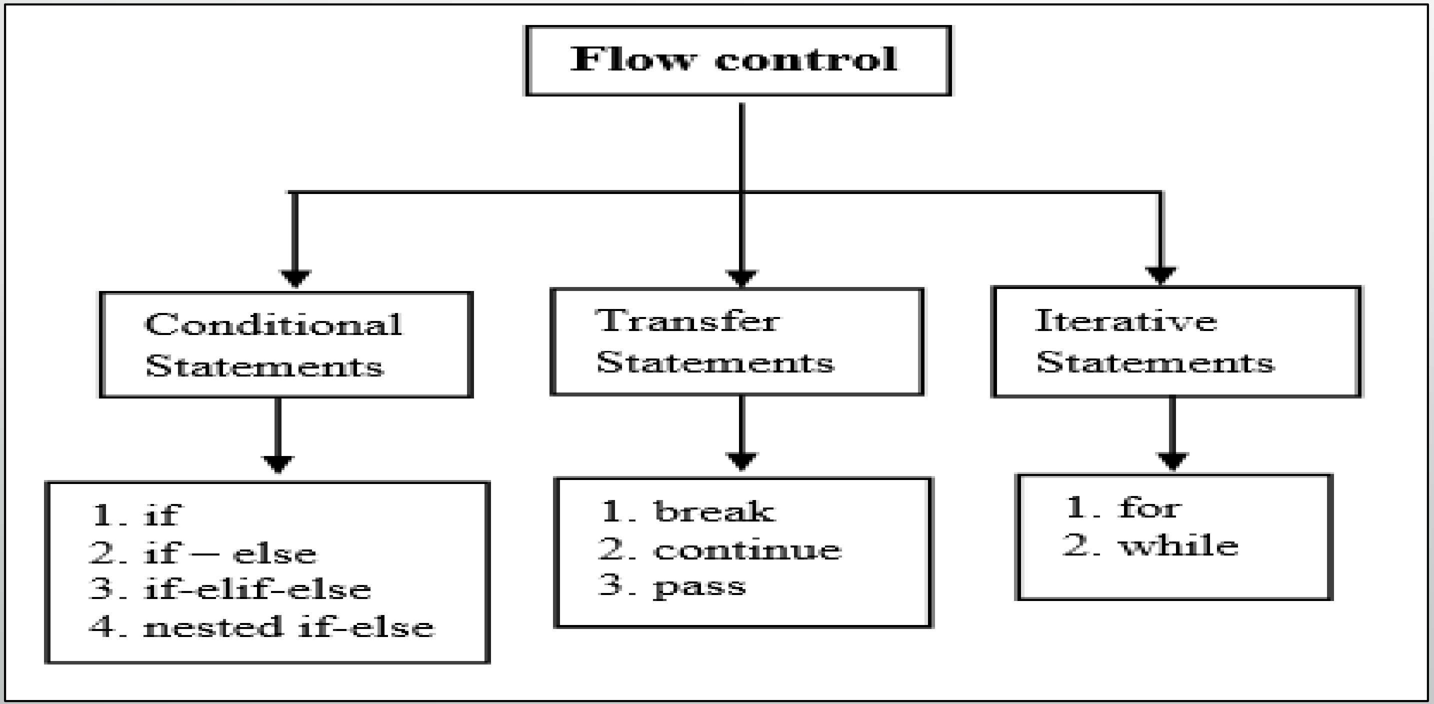
These factors make Python a powerful and accessible tool for many cybersecurity professionals.

DATA TYPES


Python - Data Types
Numeric
Dictionary
Boolean
Set
Sequence Type
Interger
Complex Number
Float
Strings
List
Tuple

CONTROL STRUCTURES

It is provides control structures like if-else statements, loops ,and exception handling for managing program flow.



Flow control

Conditional Statements

1. if
2. if – else
3. if-elif-else
4. nested if-else

Transfer Statements

1. break
2. continue
3. pass

Iterative Statements

1. for
2. while

FUNCTIONS

Functions are reusable blocks of code that can be defined and called multiple times promoting code modularity and reusability.

1.User defined Function

2.Built in Function

3.Lambda Function

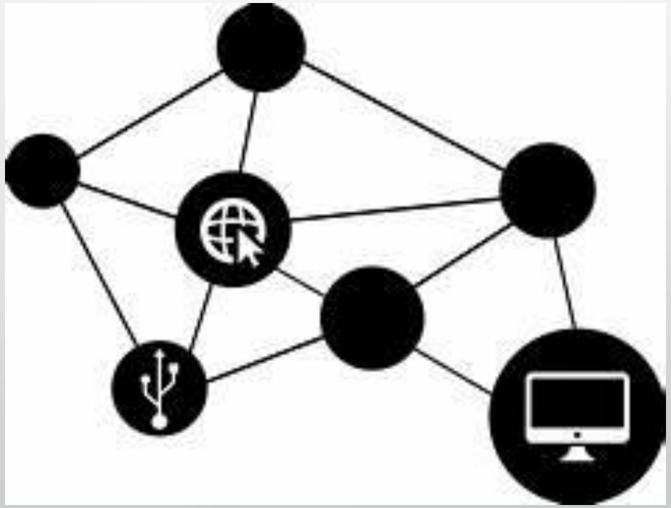
4.Recursion Function

FILE HANDLING:

- Python offers robust file handling capabilities ,allowing hackers to read, write, and manipulate files easily.

NETWORKING

- It is standard library includes modules like ‘socket’ for low-level networking tasks and higher-level libraries like request for HTTP communication.



CRYPTOGRAPHY

Cryptography is the study and practice of **securing information** by transforming it into an **unreadable format** and then back again when needed. It plays a crucial role in protecting sensitive data in the digital world, ensuring confidentiality, integrity, and authenticity.

Types of Cryptography:

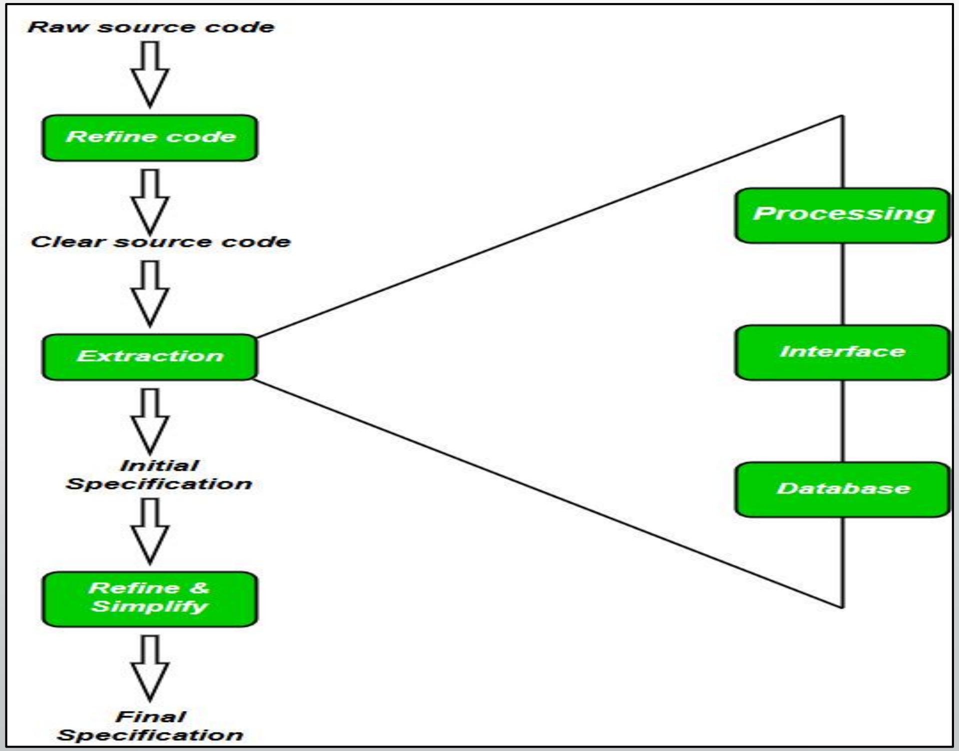
- **Symmetric Key Cryptography:** Uses a **single secret key** for both encryption and decryption. This method is efficient but requires secure key exchange between parties.
- **Asymmetric Key Cryptography:** Uses a pair of keys: a **public key** for encryption and a **private key** for decryption. The public key is widely distributed, while the private key is kept secret. This allows anyone to encrypt messages using the public key, but only the holder of the private key can decrypt them.

WEB SCRAPING

- Python’s libraries such as ‘Beautiful soup’ and ‘scrapy’ facilitate web scraping, extracting data from websites for analysis for manipulation.

REVERSE ENGINEERING

Python along with tools like ‘IDA Pro’ and ‘Ghidra’, aids in reverse engineering tasks such as analyzing and understanding binary executables.



PENETRATION TESTING

- **Penetration testing (pen testing)**, also known as **ethical hacking**, is a simulated cyberattack performed on a computer system, network, or application to identify vulnerabilities that malicious actors could exploit. It's essentially a legal and controlled way to **proactively** discover weaknesses in your security defenses before attackers do.

WEB APPLICATION SECURITY:

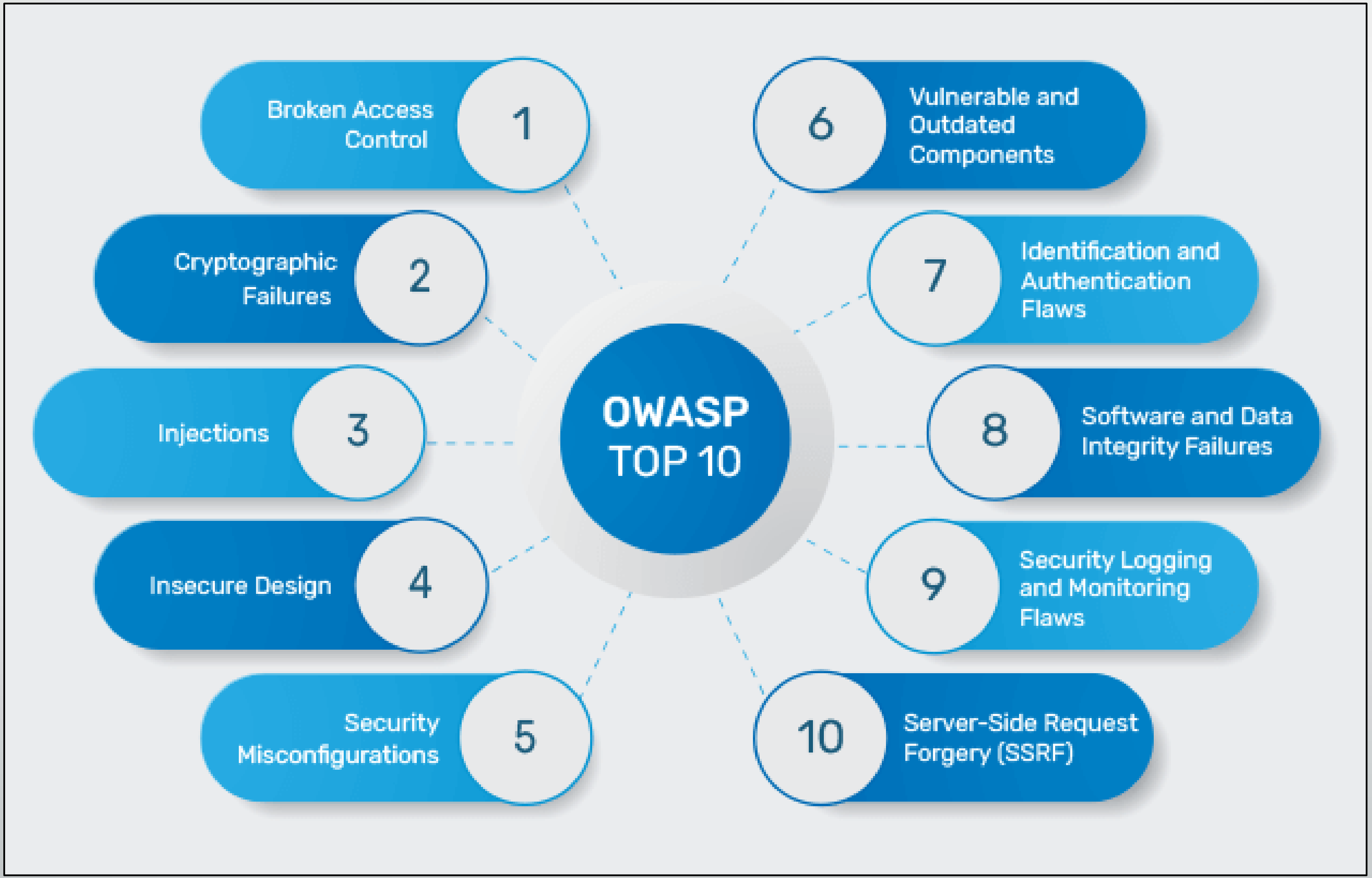
- Python frameworks like Django band flask help secure web applications against common vulnerabilities like SQL injection ,XSS and CSRF.

PASSWORD CRACKING:

- Password cracking refers to the process of **recovering** a password from its encrypted or disguised form. This can be done through various methods, some more sophisticated than others, with the ultimate goal of gaining unauthorized access to a system, account, or data. It's important to understand that password cracking is **illegal and unethical** when used without proper authorization.

OWASP
TOP 10 WEB APPLICATION SECURITY RISKS

- A01:2021:Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and outdated components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data integrity Failures
- A09:2021-Security Logging and monitoring failures
- A10:Server-side Request Forgery



OWASP TOP 10

1 Broken Access Control

2 Cryptographic Failures

3 Injections

4 Insecure Design

5 Security Misconfigurations

6 Vulnerable and Outdated Components

7 Identification and Authentication Flaws

8 Software and Data Integrity Failures

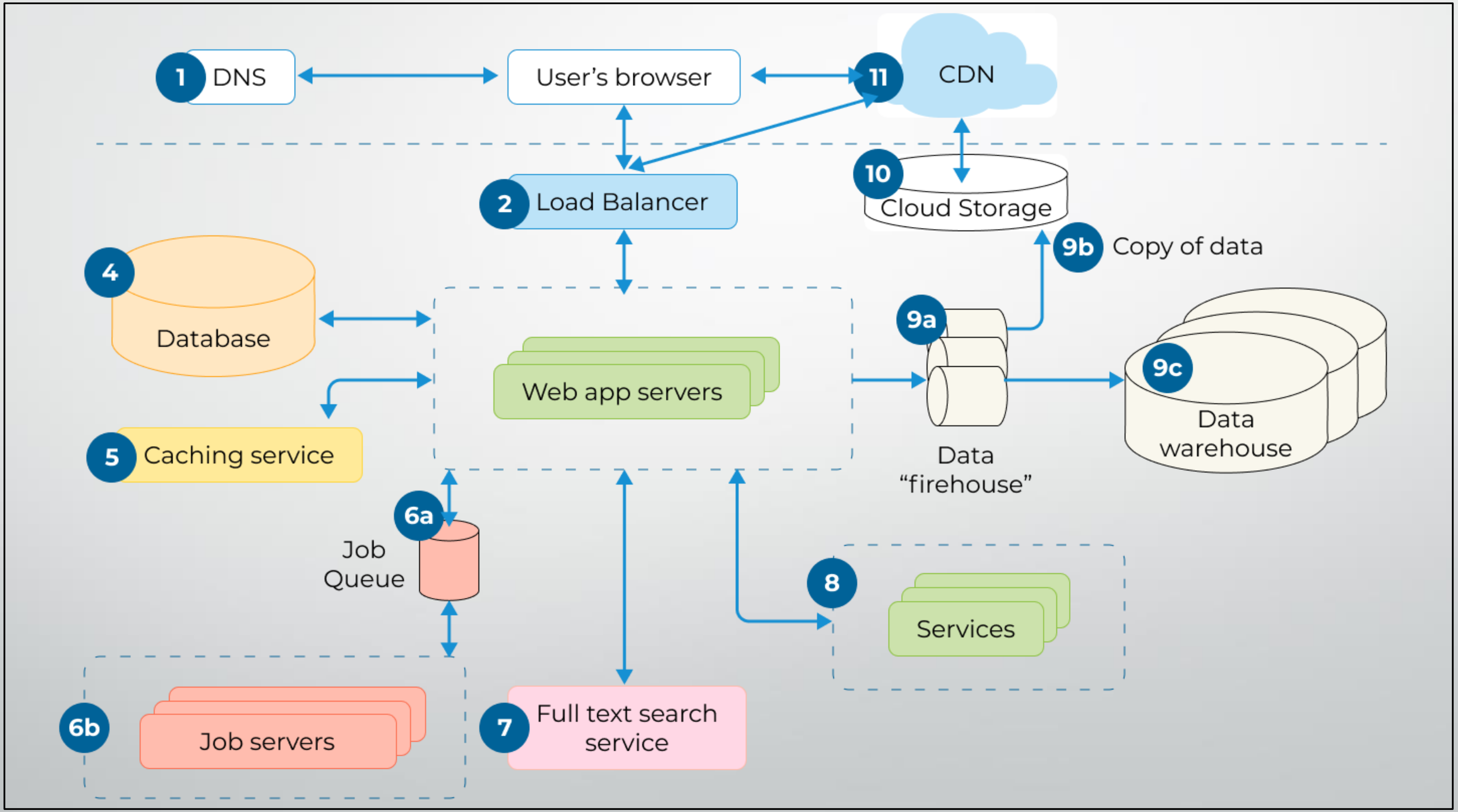
9 Security Logging and Monitoring Flaws

10 Server-Side Request Forgery (SSRF)

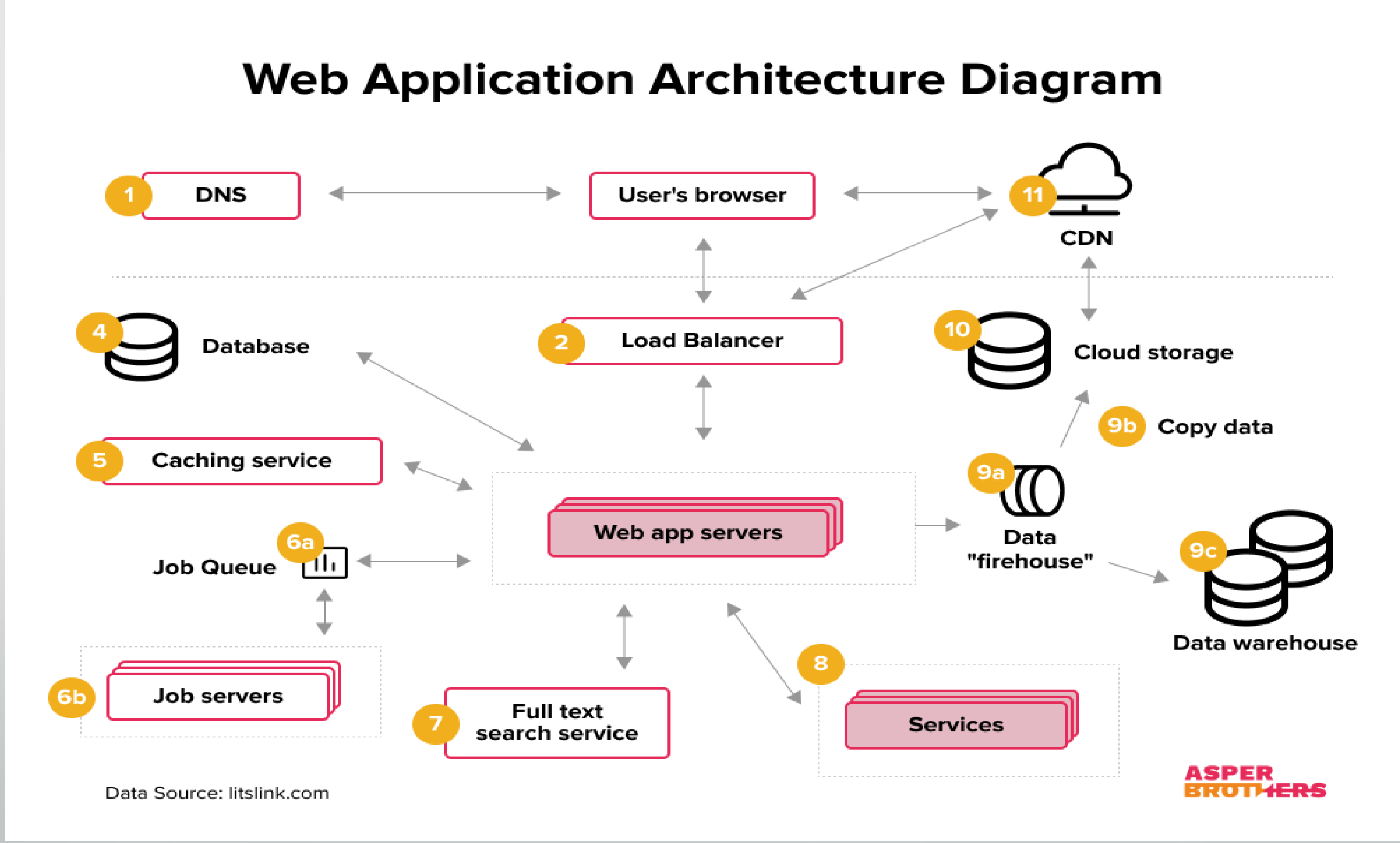
Introduction To Web Applications…

- Web applications, often abbreviated as **web apps**, are software programs that run within a web browser. Unlike traditional desktop applications that need to be downloaded and installed, web apps are accessed through the internet using a web browser like Chrome, Firefox, or Edge. This makes them **platform-independent**, meaning they can be accessed from any device with a web browser and internet connection, regardless of the operating system (Windows, Mac, Linux, etc.).

How web application works



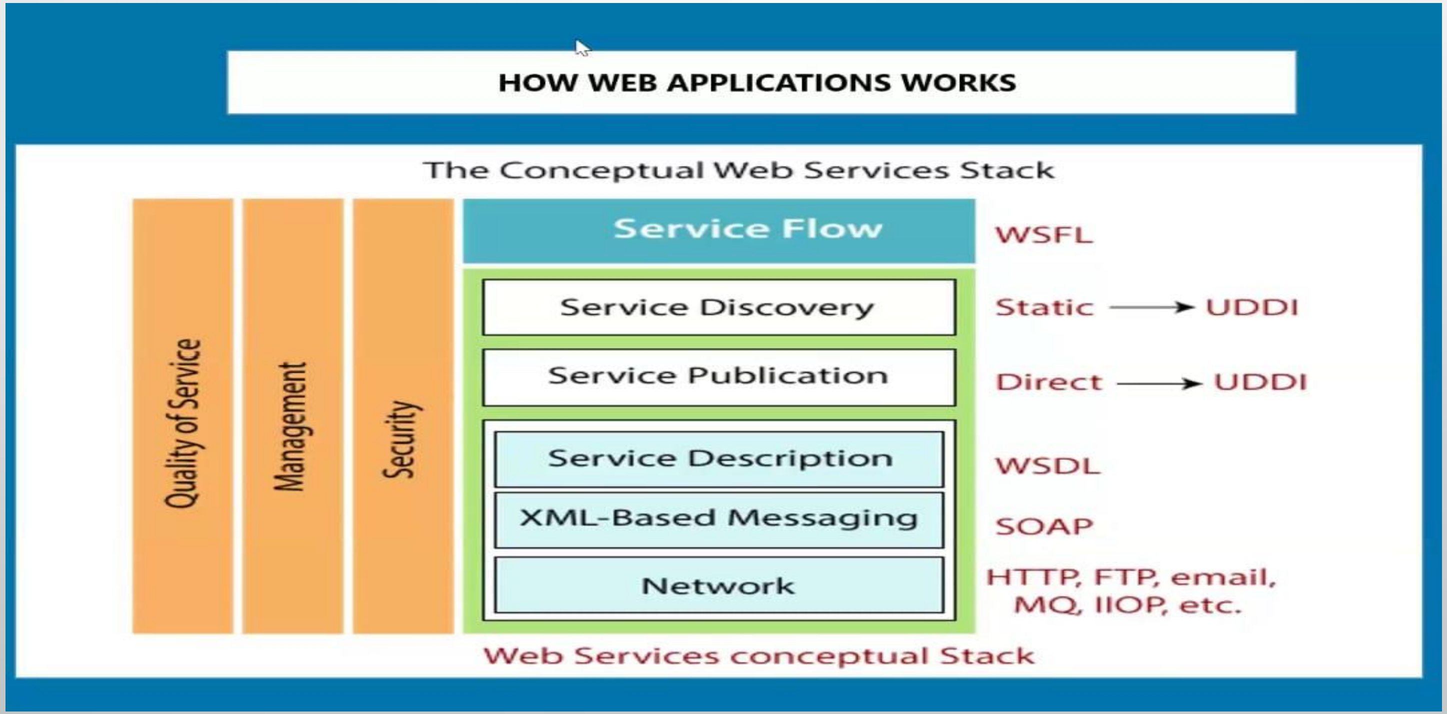
Web Application Architecture



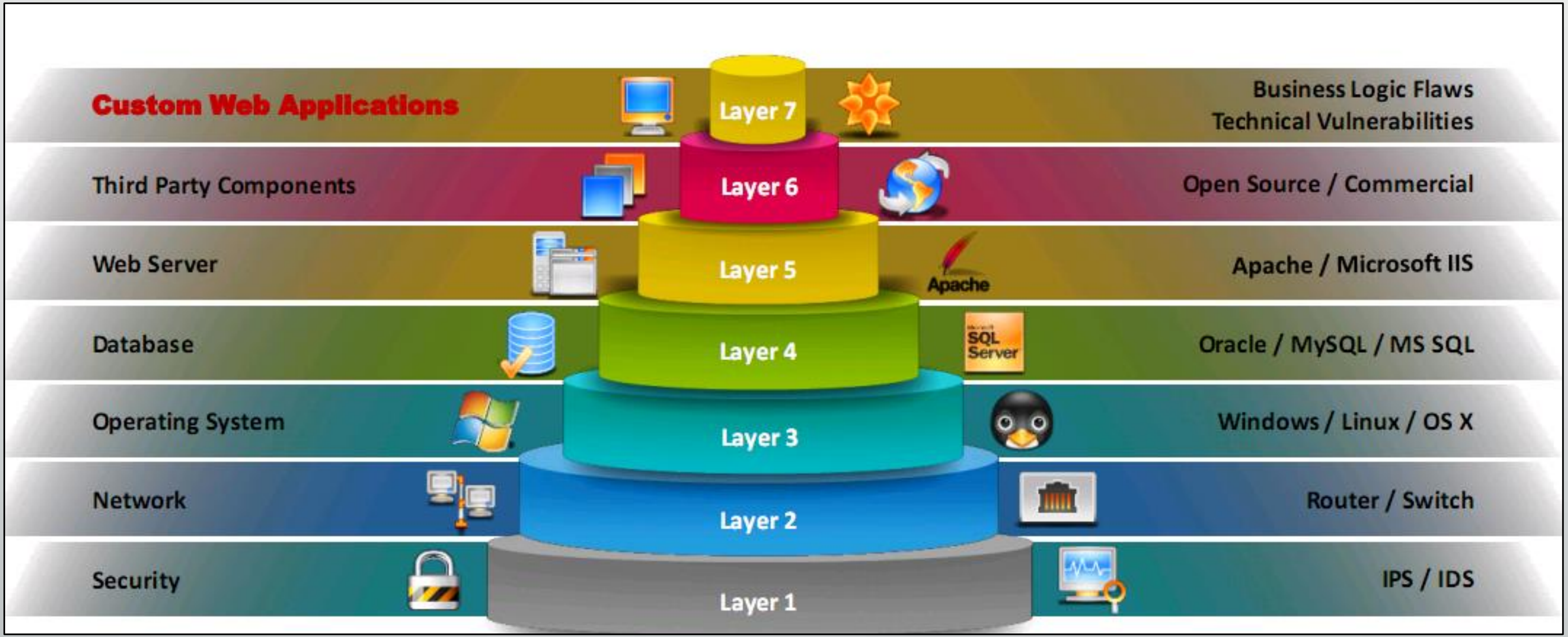
Data Source: litslink.com

Web services

- Web services are a fundamental concept in the world of **distributed computing** and **network communication**. They enable applications to **communicate and exchange data** over the internet, regardless of the underlying programming languages, platforms, or operating systems used.



Vulnerability Stack



Custom Web Applications	Layer 7	Business Logic Flaws Technical Vulnerabilities
Third Party Components	Layer 6	Open Source / Commercial
Web Server	Layer 5	Apache / Microsoft IIS
Database	Layer 4	Oracle / MySQL / MS SQL
Operating System	Layer 3	Windows / Linux / OS X
Network	Layer 2	Router / Switch
Security	Layer 1	IPS / IDS

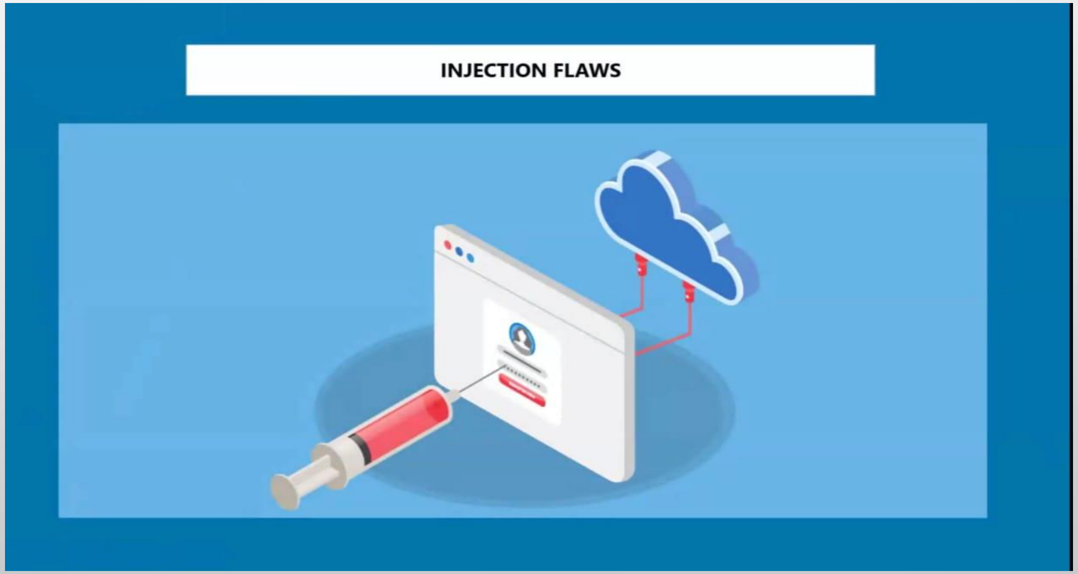
OWASP Top 10 Applications security Risks

- A1:Injection
- A2:Broken Authentication
- A3:Sensitive Data Exposure
- A4:XML External Entity
- A5:Broken Access Control
- A6: Security Misconfigurations
- A7:Cross-site Scripting(XSS)Attack
- A8:Insecure Deseralization

A1-Injection:

A1 injection, also known as **SQL injection (Structured Query Language injection)**, is a type of **web security vulnerability** that allows an attacker to inject malicious code into a website's database queries. This can lead to a variety of serious security consequences, including:

- Data theft
- Data manipulation
- Website takeover



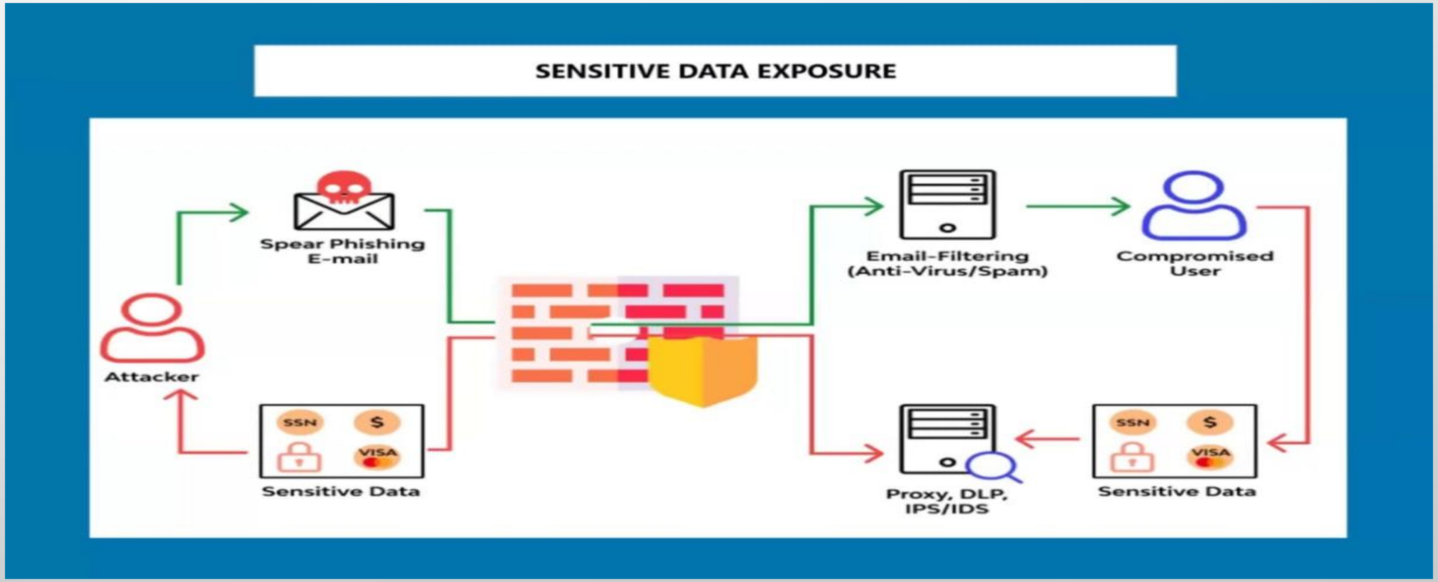
A2-Broken Authentication:

A2: Broken Authentication refers to vulnerabilities in an application's authentication and session management mechanisms. These vulnerabilities can allow unauthorized users to gain access to accounts, data, or functionalities they shouldn't have

A3-Sensitive Data Exposure

A3 in the context of OWASP Top 10 refers to **Sensitive Data Exposure**. It encompasses vulnerabilities that can lead to the exposure of sensitive data, such as:

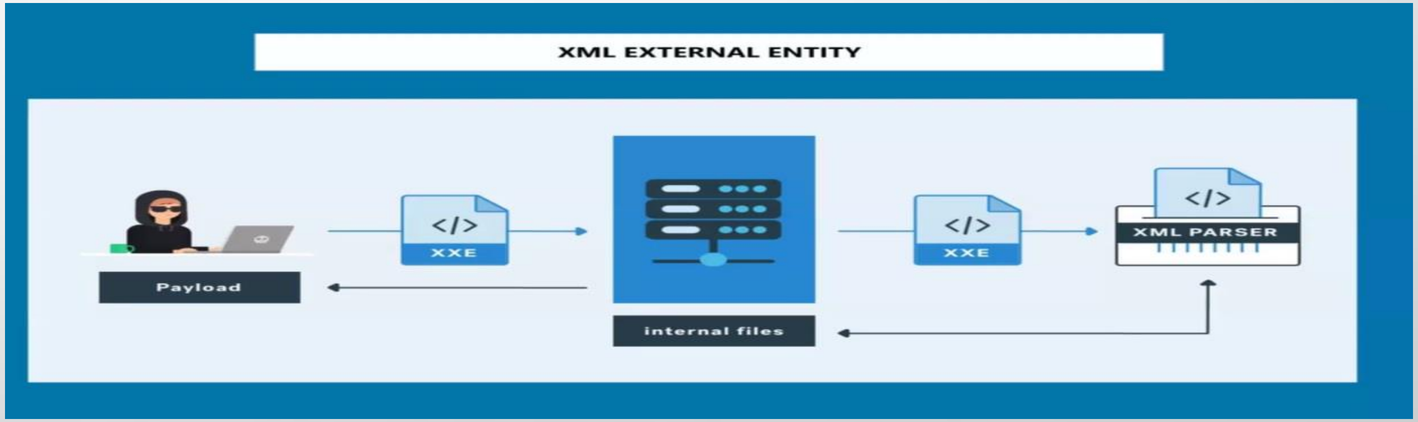
- Personal information
- Financial data
- Medical data
- Trade secrets



A4-XML External Entity

A4 in the context of OWASP Top 10 refers to **XML External Entities (XXE)**. It encompasses vulnerabilities that can lead to an attacker exploiting an application's processing of XML data to:

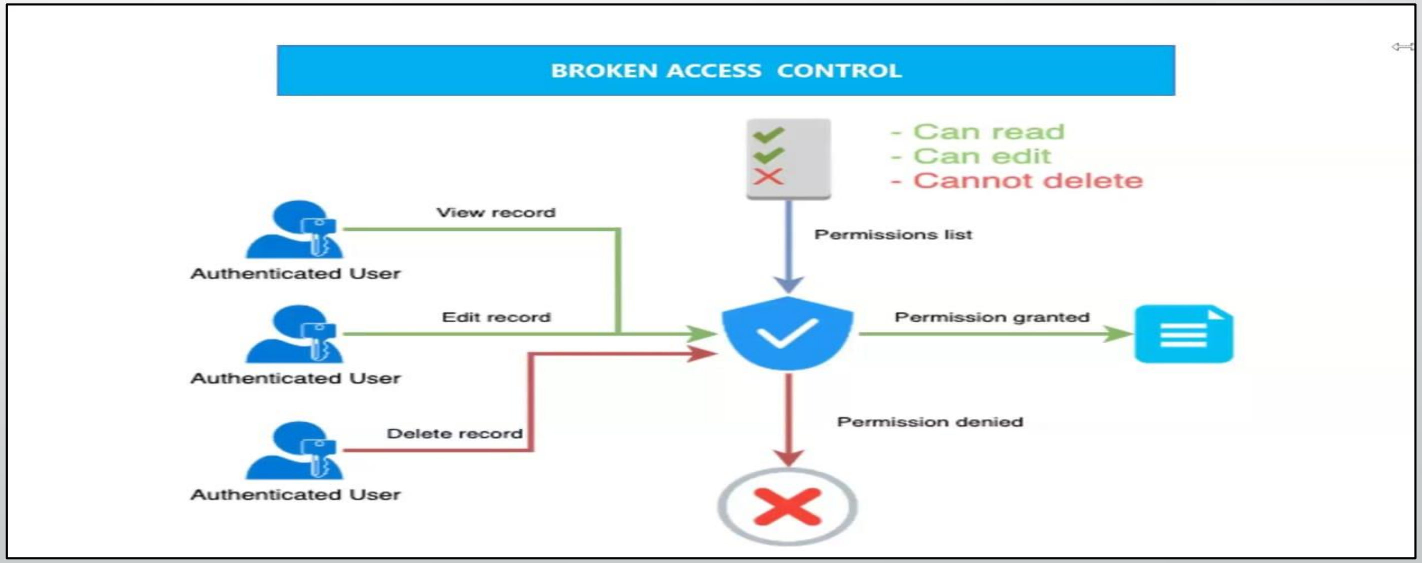
- Read sensitive files
- Denial of service
- Remote code execution



A5-Broken Access Control

Broken Access Control in the 2021 OWASP Top 10, is a critical web security risk highlighted in the OWASP Top 10 list. It encompasses vulnerabilities that allow unauthorized access to resources or functionalities within an application. This can lead to severe consequences, including:

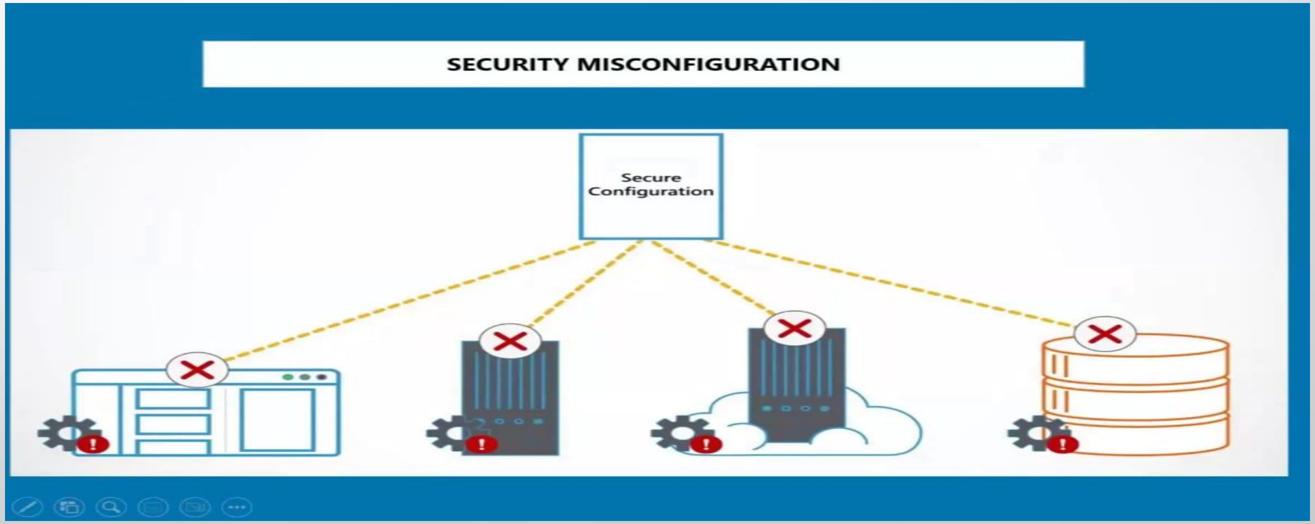
- Data breaches
- Unauthorized modifications
- System takeover



A6-Security Misconfigurations

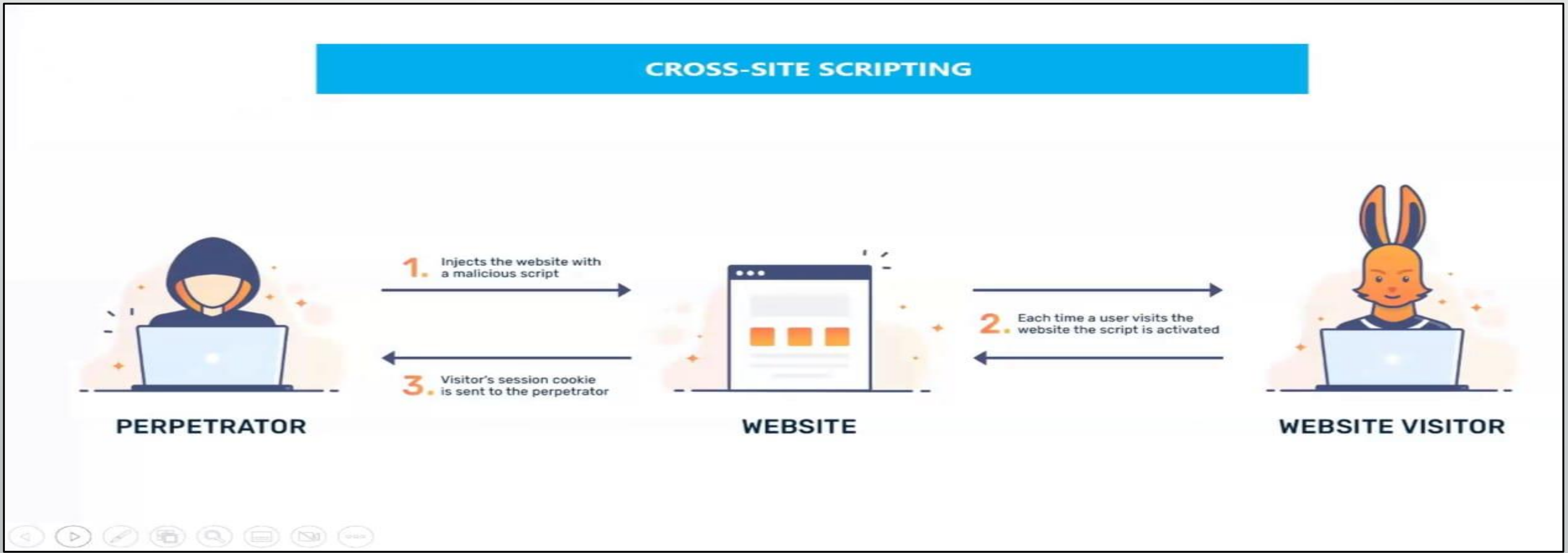
A6 in OWASP refers to **Security Misconfiguration**. It encompasses vulnerabilities that can lead to an attacker exploiting an application's insecure configuration to:

- Gain unauthorized access
- Elevate privileges
- Disrupt or disable functionality



A7-Cross -site Scripting(XSS)Attack:

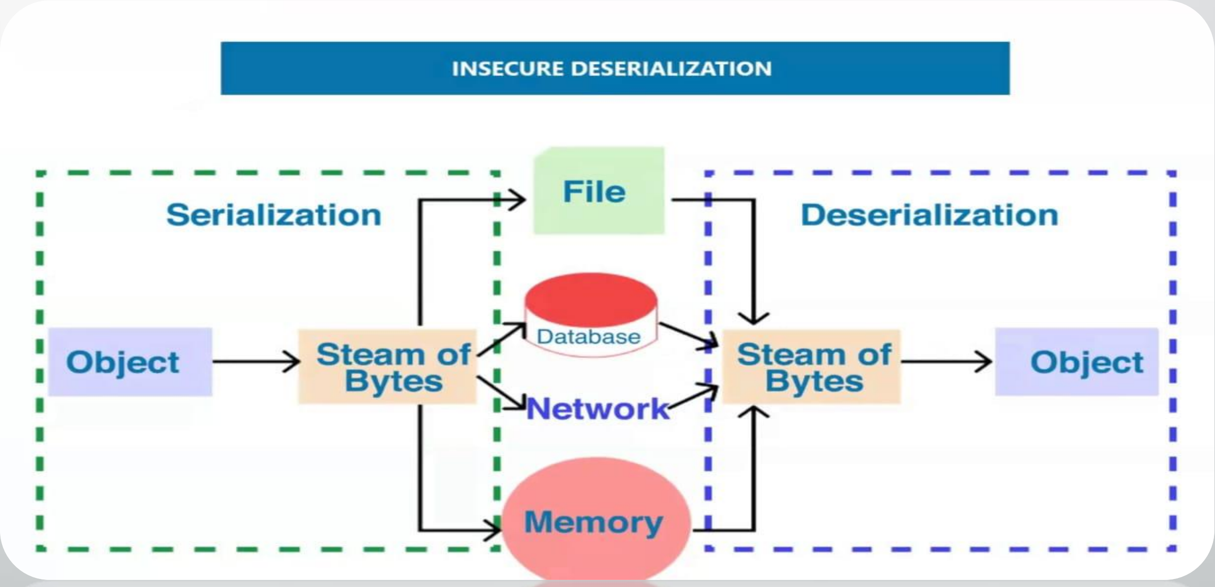
- **Cross-Site Scripting (XSS)**, classified as **A7: Cross-Site Scripting** in the OWASP Top 10, is a web security vulnerability that allows attackers to inject malicious code into web pages. This code, typically in the form of JavaScript, runs within the victim's browser, potentially leading to various security breaches.content.


CROSS-SITE SCRIPTING
1. Injects the website with a malicious script
2. Each time a user visits the website the script is activated
3. Visitor's session cookie is sent to the perpetrator
PERPETRATOR
WEBSITE
WEBSITE VISITOR

A8-Insecure Deserialization

A8 in OWASP refers to **Insecure Deserialization**. It encompasses vulnerabilities that can lead to an attacker exploiting an application's insecure deserialization process to:

- **Gain unauthorized access**
- **Elevate privileges**
- **Disrupt or disable functionality**



Components with known vulnerabilities

- Components with known vulnerabilities, also referred to as **vulnerable components**, are software components that contain security flaws or weaknesses that have been identified and publicly disclosed. These vulnerabilities can be exploited by attackers to gain unauthorized access to systems, steal sensitive data, or disrupt operations.

Web Application Hacking Methodology

1.foot printing web infrastructure

2.analyze web application

3.by pass client inside controls

4.Attack Authentication mechanism

5.Attack Authorization schemes

6.Attack Access Controls

7.Attack Session Management Mechanism

8.Perfor Injection Attacks

9.Attack Application Logic Flaws

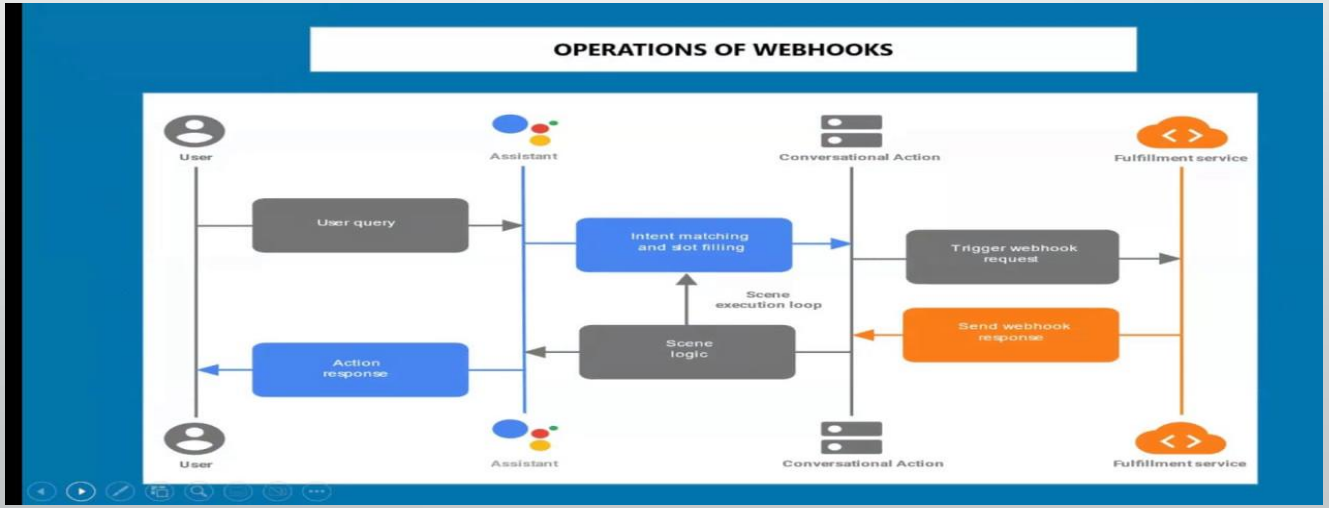
10.Attack Shared Environments

11.Attack Database Connectivity

12.Attack web client

What is webhook

- A webhook is a lightweight communication method that allows applications to exchange information in real-time. This allows the receiving system to react and perform an action based on the received data.
- Ex: A webhook could be used to notify a third-party Service whenever a new order is placed on an e-commerce website.



OPERATIONS OF WEBHOOKS

- **CYBER SENSE+ COMMON SENSE=<u>CYBER SECURITY</u>**