1. **Introduction to CIA**

CIA stands for Confidentiality, Integrity and Availability. CIA triad is considered as a basic pillar of cyber security.

*Confidentiality*: sensitive data should be only accessible for authorized persons.

*Integrity*: maintaining the accuracy of data even in the transmission or preventing unauthorized access for data

*Availability*: ensuring that data or resources will be available to authorized user when needed.

1. **Authorization vs Authentication**

|  |  |  |
| --- | --- | --- |
| Context | Authorization | Authentication |
| what is | Confirms the user’s identity | Determine the permission of authorized user |
| Sequence | Pre-requirement | Post-requirement of authorization |
| Access control | No – only validates user | Yes – restricts the user’s access |

1. **Normal website vs Web Application**

|  |  |  |
| --- | --- | --- |
| Context | Normal website | Web application |
| Purpose | Designed to inform or present content | Designed for user interaction and dynamic feature |
| Content-type | Mostly static (HTML CSS) | Mostly dynamic (React, Next) |
| Storage | No needed | Uses databases |
| Complexity | Not complex | More complex |

1. **What is WAS and its importance?**

WAS – Web application security is the technique or process which measures and practices used to protect web application from various cyber-attacks and threats.

* Importance
  + Protects sensitive data
  + Prevent financial loss
  + Maintains user trust
  + Ensures CIA
  + Ensures compliance

1. **What is CVE?**

CVE – common vulnerabilities and exposure is a publicly available database and storage where all common vulnerabilities are stored. Each vulnerability has been assigned with unique CVE Id making it easier to track the security risks and threats.

1. **What is OWASP?**

OWASP – open web application security project is an open-source non-profit organization dedicated to improve software and web application security. It’s an open-source model and community and represents the most critical security risks to web applications.

* TOP 10 OWASP vulnerabilities
  1. Broken access control
  2. Injection attacks
  3. Cryptographic failures
  4. Insecure design
  5. Security misconfiguration
  6. SSRF
  7. Outdated vulnerable components
  8. Integrity failure
  9. Security logging & monitoring failures
  10. Authentication failures

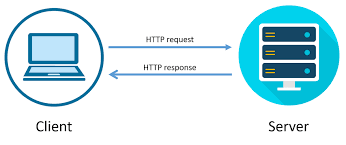
1. **Explain important network protocols.**

Network protocols are set of rules and regulations that determines how data should transmit over network. It enables the communication between multiple devices in or outside of network.

Ex. HTTPS, ARP, DNS, IPsec, etc…

1. **HTTP & HTTPS:**

* Stands for Hypertext transfer protocol which works on request-response model.
* Both protocols used for transmission of data over web pages.
* Https is more secure than Http and use encryption of data.



1. **DHCP**

* Used to assign the IP address to the devices by router.
* Stands for dynamic host configuration

1. **ARP**

* Stands for address resolution protocol which is used for mapping the network.
* When two devices communicate with each other, it needs the MAC addresses of other devices, ARP is used to find MAC address over network

1. **IPSec**

* IP Security refers to the collection of communication rules or protocols used to secure network connections
* Ensures CIA for data transmission

|  |  |  |  |
| --- | --- | --- | --- |
| IPsec header | TCP/IP header | DATA | IPSec trailer |

1. **DNS**

* Domain name system used to translate the human readable for domain names to machine readable IP addresses.

1. **FTP**

* File Transfer Protocol (FTP) is a standard network protocol that allows users to transfer files between computers.

1. **SMTP**

* The Simple Mail Transfer Protocol (SMTP) is a technical standard for transmitting electronic mail (email) over a network.
* SMTP is mainly used to push a mail into mail server.

1. **SSH**

* Secure shell (SSH) is cryptographic protocol used for secure remote activity
* Works on port 22

1. **0Auth 2.0**

* used for third party authentication services
* uses tokens to authenticate the users