Unit-4:

4.1 Concepts of Cyber Security

4.1.1 Types of Threats

What are Cyber Security Threats?

Cybersecurity threats are acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems. Common categories of cyber threats include malware, social engineering, man in the middle (MitM) attacks, denial of service (DoS), and injection attacks—we describe each of these categories in more detail below.

Cyber threats can originate from a variety of sources, from hostile nation states and terrorist groups, to individual hackers, to trusted individuals like employees or contractors, who abuse their privileges to perform malicious acts.

Common Sources of Cyber Threats

Nation states— hostile countries can launch cyber-attacks against local companies and institutions, aiming to interfere with communications, cause disorder, and inflict damage.

Terrorist organizations— terrorists conduct cyber-attacks aimed at destroying or abusing critical infrastructure, threaten national security, disrupt economies, and cause bodily harm to citizens.

Criminal groups— organized groups of hackers aim to break into computing systems for economic benefit. These groups use phishing, spam, spyware and malware for extortion, theft of private information, and online scams

.

Hackers— individual hackers target organizations using a variety of attack techniques. They are usually motivated by personal gain, revenge, financial gain, or political activity. Hackers often develop new threats, to advance their criminal ability and improve their personal standing in the hacker community

.

Malicious insiders— an employee who has legitimate access to company assets, and abuses their privileges to steal information or damage computing systems for economic or personal gain. Insiders may be employees, contractors, suppliers, or partners of the target organization. They can also be outsiders who have compromised a privileged account and are impersonating its owner.

4.1.2 Advantages of Cyber Security

In simple words, Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Cyber security is very important for today's life. Cyber safety provides enhanced cyberspace security, improves cyber resilience, speeds up cyber, data & information protection for businesses it protects individual private information, it protects networks & resources & tackles

computer hackers and theft of identity. There are a few advantages & disadvantages of cyber security.

ADVANTAGES

- Cyber security will defend us from critical cyber- attacks.
- It helps us to browse the safe website.
- Cyber security will defend us from hacks & virus.
- The application of cyber security used in our PC needs to update every week.
- Internet security processes all the incoming & outgoing data on our computer.
- It helps to reduce computer chilling & crashes.
- Gives us privacy.

DISADVANTAGES

- It was expensive; most of the users can't afford this.
- A normal user can't use this properly, requiring special expertise.
- Lack of knowledge is the main problem.
- It was not easy to use.
- It makes the system slower.
- It could take hours to days to fix a breach in security.

4.2 Basic Terminologies:

4.2.1 IP Address, MAC Address

IP Address:

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.

An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.

MAC Address:

A MAC address (media access control address) is a 12-digit hexadecimal number assigned to each device connected to the network. Primarily specified as a unique identifier during device manufacturing, the MAC address is often found on a device's network interface card (NIC).

A Media Access Control (MAC) address is a string of characters that identifies a device on a network. It's tied to a key connection device in your computer called the network interface card, or NIC. The NIC is essentially a computer circuit card that makes it possible for your

computer to connect to a network. A NIC turns data into an electrical signal that can be transmitted over the network.

Every NIC has a hardware address that's known as a MAC address. Whereas IP addresses are associated with a networking software called TCP/IP, MAC addresses are linked to the hardware of network adapters.

Manufacturers assign a MAC address to a network adapter when it is produced. It is hardwired or hard-coded onto your computer's NIC and is unique to it. Something called the Address Resolution Protocol (ARP) translates an IP address into a MAC address. Think of the ARP as a passport that takes data from an IP address through an actual piece of computer hardware.

Both MAC Address and IP Address are used to uniquely define a device on the internet. NIC Card's Manufacturer provides the MAC Address, on the other hand, Internet Service Provider provides IP Address.

The main difference between MAC and IP address is that MAC Address is used to ensure the physical address of the computer. It uniquely identifies the devices on a network. While IP addresses are used to uniquely identify the connection of the network with that device takes part in a network.

MAC Address	IP Address
MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
MAC Address is a six byte hexadecimal address.	IP Address is either a four-byte (IPv4) or a sixteen-byte (IPv6) address.
A device attached with MAC Address can retrieve by ARP protocol.	A device attached with IP Address can retrieve by RARP protocol.
NIC Card's Manufacturer provides the MAC Address.	Internet Service Provider provides IP Address.
MAC Address is used to ensure the physical address of a computer.	IP Address is the logical address of the computer.
MAC Address operates in the data link layer.	IP Address operates in the network layer.
MAC Address helps in simply identifying the device.	IP Address identifies the connection of the device on the network.
MAC Address of computer cannot be changed with time and environment.	IP Address modifies with the time and environment.
MAC Addresses can't be found easily by a third party.	IP Addresses can be found by a third party.
No classes are used for MAC addressing.	IPv4 uses A, B, C, D, and E classes for IP addressing.

MAC Address sharing is not allowed.	In IP address multiple client devices can share the IP address.
MAC address help to solve IP address issue.	IP addresses never able to solve MAC address issues.
MAC addresses can be used for broadcasting.	The IP address can be used for broadcasting or multicasting.
MAC address is hardware oriented.	IP address is software oriented.

4.2.2 Domain name Server (DNS)

What is DNS?

Every website on the Internet has its own unique address. It's called an IP address. But unlike the physical street address for a house or building, an IP address consists of a set of numbers strung together and separated by periods. A typical IP address in the IPv4 address space looks like: 123.123.123.2. If customers had to memorize the IP addresses of every website they visited, they wouldn't spend much time on the Internet. Thankfully, we use URLs instead. And behind the scenes, there's an "address book" of sorts that helps convert these user-friendly URLs and web addresses into the IP addresses that computers understand. It's called a Domain Name System, or DNS.

In the simplest form, a DNS is a directory of domain names that align with IP addresses. They bridge the gap between computer language and human language – keeping both servers and people happy.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.

What is DNS Security?

When most people use the Internet, they use domain names to specify the website that they want to visit, for instance checkpoint.com. These domain names are user-friendly addresses which are mapped by the Domain Name System (DNS) to Internet Protocol (IP) addresses that computers and other network infrastructure components use to identify different devices connected to the Internet. In sum, the Domain Name System is the protocol that makes the Internet usable by allowing the use of domain names.

DNS is widely trusted by organizations, and DNS traffic is typically allowed to pass freely through network firewalls. However, it is commonly attacked and abused by cybercriminals. As a result, the security of DNS is a critical component of network security.

4.2.3 DHCP, Router, Bots

DHCP

Dynamic Host Configuration Protocol, or DHCP, is used to provide quick and centralized management of IP addresses and other TCP/IP settings on your network. These are things like host IP address, subnet mask, DNS settings, default gateway address, and so on (I call these "IP configuration settings"). When you power on your computer, a DHCP server likely provides these IP configuration settings to you. Even if you don't have a stand-alone DHCP server, your default gateway likely has its own DHCP server feature.

DHCP really makes network management a lot easier. DHCP eliminates the need for manually assigning IP addresses to our devices. And with this benefit, we decrease the chances of two devices having the same IP address. The following steps describe how DHCP works step-by-step.

Step 1: DHCP Discover: - This first step is a discovery process performed by the workstation. The workstation here refers to the system that currently does not have an IP address. The purpose of this step is to discover any DHCP servers on the network that can hand out IP configuration settings. The workstation accomplishes this task by sending out a broadcast over UDP port 67 that essentially asks, "Hello, are there any DHCP servers available to help me?" This message is referred to as a DHCP Discover message. Importantly, it's a great idea to have multiple redundant DHCP servers on your network. But, this raises an important question: Since routers don't forward broadcasts, will we need to install a DHCP server on every broadcast domain? The answer is no. Routers can forward DHCP broadcast messages if they're configured to do so. Features like "DHCP Relay" and "IP Helper" ensure that DHCP broadcasts can reach other subnets. A relay agent will take a DHCP broadcast and forward it through a router as a unicast transmission to the DHCP server on the other subnet.

Step 2: DHCP Offer: - After step 1 is accomplished and one or more DHCP servers are discovered somewhere on the network, the DHCP servers all reply to the workstation with a broadcast offer to the workstation over UDP port 68. This broadcast contains available IP configuration settings. This message is called a "DHCP Offer."

Step 3: DHCP Request: - In this third step, the workstation receives all the broadcast offers in step 2, and picks one. Whichever IP configuration settings it chooses, the workstation sends another broadcast back out on UDP port 67. Every DHCP server receives this broadcast. This message is called a DHCP Request.

Step 4: DHCP Acknowledgement: - In this final step, the DHCP server that was responsible for the DHCP request responds with one last broadcast to the workstation and all other DHCP servers over UDP port 68. This DHCP Acknowledgement Message tells the other DHCP servers that the new IP configuration settings are owned by this particular workstation and cannot be reused for anyone else.

Benefits of DHCP.

Reliable IP address configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.

Reduced network administration. DHCP includes the following features to reduce network administration:

- Centralized and automated TCP/IP configuration.
- The ability to define TCP/IP configurations from a central location.
- The ability to assign a full range of additional TCP/IP configuration values by means of DHCP options.
- The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable devices that move to different locations on a wireless network.
- The forwarding of initial DHCP messages by using a DHCP relay agent, which eliminates the need for a DHCP server on every subnet.

Router

What is a router?

A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

There are several types of routers, but most routers pass data between LANs (local area networks) and WANs (wide area networks). A LAN is a group of connected devices restricted to a specific geographic area. A LAN usually requires a single router.

A WAN, by contrast, is a large network spread out over a vast geographic area. Large organizations and companies that operate in multiple locations across the country, for instance, will need separate LANs for each location, which then connect to the other LANs to form a WAN. Because a WAN is distributed over a large area, it often necessitates multiple routers and switches.

How does a router work?

Think of a router as an air traffic controller and data packets as aircraft headed to different airports (or networks). Just as each plane has a unique destination and follows a unique route, each packet needs to be guided to its destination as efficiently as possible. In the same way that an air traffic controller ensures that planes reach their destinations without getting lost or suffering a major disruption along the way, a router helps direct data packets to their destination IP address.

In order to direct packets effectively, a router uses an internal routing table — a list of paths to various network destinations. The router reads a packet's header to determine where it is going, then consults the routing table to figure out the most efficient path to that destination. It then forwards the packet to the next network in the path.

Bots

A 'bot' – short for robot – is a software program that performs automated, repetitive, pre-defined tasks. Bots typically imitate or replace human user behavior. Because they are automated, they operate much faster than human users. They carry out useful functions, such as customer service or indexing search engines, but they can also come in the form of malware – used to gain total control over a computer.

Internet bots can also be referred to as spiders, crawlers, or web bots.

A bot is a software application that is programmed to do certain tasks. Bots are automated, which means they run according to their instructions without a human user needing to manually start them up every time. Bots often imitate or replace a human user's behavior. Typically they do repetitive tasks, and they can do them much faster than human users could.

A bot is a small piece of software that automates web requests with various goals. Bots are used to perform tasks without human intervention, including everything from scanning website content to testing stolen credit card numbers to providing customer service support. A bot can be used in both helpful and harmful ways, while "bot attack" always refers to an attacker with a fraudulent goal.

A bot attack is the use of automated web requests to manipulate, defraud, or disrupt a website, application, API, or end-users. Bot attacks started out as simple spamming operations and have branched into complex, multinational criminal enterprises with their own economies and infrastructures.

Bot attacks are automated, ranging from individual cyber criminals to vast hacking organizations. Sophisticated attackers write custom code to vary frequency and length of an automated attack, designed to circumvent security monitoring.

Bots usually operate over a network; more than half of Internet traffic is bots scanning content, interacting with WebPages, chatting with users, or looking for attack targets. Some bots are useful, such as search engine bots that index content for search or customer service bots that help users. Other bots are "bad" and are programmed to break into user accounts, scan the web for contact information for sending spam, or perform other malicious activities. If it's connected to the Internet, a bot will have an associated IP address.

Bots can be:

Chatbots: Bots that simulate human conversation by responding to certain phrases with programmed responses

Web crawlers (Googlebots): Bots that scan content on WebPages all over the Internet

Social bots: Bots that operate on social media platforms

Malicious bots: Bots that scrape content, spread spam content, or carry out credential stuffing attacks

4.3 Common Types of Attacks:

4.3.1 Distributed Denial of Service

DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.

Motivations for carrying out a DDoS vary widely, as do the types of individuals and organizations eager to perpetrate this form of cyberattack. Some attacks are carried out by disgruntled individuals and hacktivists wanting to take down a company's servers simply to make a statement, have fun by exploiting cyber weakness, or express disapproval.

Other distributed denial-of-service attacks are financially motivated, such as a competitor disrupting or shutting down another business's online operations to steal business away in the meantime. Others involve extortion, in which perpetrators attack a company and install hostageware or ransomware on their servers, then force them to pay a large financial sum for the damage to be reversed.

DDoS attacks are on the rise, and even some of the largest global companies are not immune to being "DDoS'ed". The largest attack in history occurred in February 2020 to none other than Amazon Web Services (AWS), overtaking an earlier attack on GitHub two years prior. DDoS ramifications include a drop in legitimate traffic, lost business, and reputation damage.

How DDoS Attacks Work

A DDoS attack aims to overwhelm the devices, services, and network of its intended target with fake internet traffic, rendering them inaccessible to or useless for legitimate users.

DoS vs. DDoS

A distributed denial-of-service attack is a subcategory of the more general denial-of-service (DoS) attack. In a DoS attack, the attacker uses a single internet connection to barrage a target with fake requests or to try and exploit a cybersecurity vulnerability. DDoS is larger in scale. It utilizes thousands (even millions) of connected devices to fulfill its goal. The sheer volume of the devices used makes DDoS much harder to fight.

Botnets

Botnets are the primary way distributed denial-of-service-attacks are carried out. The attacker will hack into computers or other devices and install a malicious piece of code, or malware, called a bot. Together, the infected computers form a network called a botnet. The attacker then instructs the botnet to overwhelm the victim's servers and devices with more connection requests than they can handle.

Types of DDoS Attacks

Volume-Based or Volumetric Attacks

This type of attack aims to control all available bandwidth between the victim and the larger internet. Domain name system (DNS) amplification is an example of a volume-based attack. In this scenario, the attacker spoofs the target's address, then sends a DNS name lookup request to an open DNS server with the spoofed address.

When the DNS server sends the DNS record response, it is sent instead to the target, resulting in the target receiving an amplification of the attacker's initially small query.

Protocol Attacks

Protocol attacks consume all available capacity of web servers or other resources, such as firewalls. They expose weaknesses in Layers 3 and 4 of the OSI protocol stack to render the target inaccessible.

A SYN flood is an example of a protocol attack, in which the attacker sends the target an overwhelming number of transmission control protocol (TCP) handshake requests with spoofed source Internet Protocol (IP) addresses. The targeted servers attempt to respond to each connection request, but the final handshake never occurs, overwhelming the target in the process.

Application-Layer Attacks

These attacks also aim to exhaust or overwhelm the target's resources but are difficult to flag as malicious. Often referred to as a Layer 7 DDoS attack—referring to Layer 7 of the OSI model—an application-layer attack targets the layer where web pages are generated in response to Hypertext Transfer Protocol (HTTP) requests.

A server runs database queries to generate a web page. In this form of attack, the attacker forces the victim's server to handle more than it normally does. An HTTP flood is a type of application-layer attack and is similar to constantly refreshing a web browser on different computers all at once. In this manner, the excessive number of HTTP requests overwhelms the server, resulting in a DDoS.

DDoS Attack Prevention

Even if you know what a DDoS attack is, It is extremely difficult to avoid attacks because detection is a challenge. This is because the symptoms of the attack may not vary much from typical service issues, such as slow-loading web pages, and the level of sophistication and complexity of DDoS techniques continues to grow.

Further, many companies welcome a spike in internet traffic, especially if the company recently launched new products or services or announced market-moving news. As such, prevention is not always possible, so it is best for an organization to plan a response for when these attacks occur.

4.3.2 Man in the Middle, Email Attack

A MITM attack is a form of cyber-attack where a user is introduced with some kind of meeting between the two parties by a malicious individual, manipulates both parties and achieves access to the data that the two people were trying to deliver to each other. A man-in-the-middle attack also helps a malicious attacker, without any kind of participant recognizing till it's too late, to hack the transmission of data intended for someone else and not supposed to be sent at all. In certain aspects, like MITM, MitM, MiM or MIM, MITM attacks can be referred.

If an attacker puts himself between a client and a webpage, a Man-in-the-Middle (MITM) attack occurs. This form of assault comes in many different ways.

For example, In order to intercept financial login credentials, a fraudulent banking website can be used. Between the user and the real bank webpage, the fake site lies "in the middle."

How does MITM work

There are several reasons and strategies for hackers to use a MITM attack. Usually, like credit card numbers or user login details, they try to access anything. They also spy on private meetings, which may include corporate secrets or other useful information.

Types of Attacks

Although ARP poisoning is commonly known as a MitM attack, other forms of data interception also give attackers the ability to read private communications between two parties.

Email hijacking:

Email messages sent in clear text are open to eavesdropping, but an attacker can also read messages should they obtain a targeted user's username and password to the email account. The attacker may wait silently reading messages until sensitive information is transferred such as a financial transaction, and then use the targeted user's email address to send a message that will reroute money transfers to the attacker's bank account.

Wi-Fi eavesdropping:

A poorly secured Wi-Fi connection could be subject to a MitM using a method called ARP poisoning. The attacker's device is used as the default gateway between the sender and the Wi-Fi router where data can be intercepted and read. Attackers also use malicious hotspots of their own to trick users into connecting and routing communication through the attacker-controlled hotspot.

Session hijacking:

When users connect to a server, a unique session is created that identifies the user on the server. Attackers with access to this session token can impersonate the user and read data on a web application.

IP spoofing:

Using a fraudulent IP address, an attacker can reroute traffic from an official site to an attacker-controlled server.

DNS spoofing:

Similar to IP spoofing, DNS spoofing alters a website's address record to divert traffic to an attacker-controlled server. Any information sent to this server is intercepted by the attacker unbeknownst to the tricked users.

How to Prevent MitM Attacks

Because MitM attacks are invisible and silent to the targeted user, it's essential that users take the necessary precautions to prevent them. It's also the responsibility of the application developer to ensure that their software is not vulnerable to MitM attacks. In some cases, users would be unable to prevent a man-in-the-middle attack due to the way an application is coded.

Some methods to prevent becoming a victim of a MitM attack:

Use two-factor authentication on email accounts. Should an attacker obtain email credentials for your account, successful authentication would not be possible as the attacker would not have access to the 2FA PIN.

Use traffic analytical tools on the network. These tools help administrators identify suspicious traffic and provides analytics into ports and protocol usage across users and devices.

Use certificate pinning on mobile apps. Certificate pinning whitelists approved certifications, which blocks any attacker-controlled certificates from being used with the application. Certificate pinning is the responsibility of the application developer.

Use VPN on public Wi-Fi networks. With VPN, an attacker may intercept data but would be unable to read data or downgrade to a weaker encryption protocol as the VPN uses its own encryption algorithm to package data and transfer it across the internet.

Educate employees about the dangers of phishing. Some MitM and malware attacks start with phishing attacks. Educate employees to identify phishing attacks so that they do not install malware or send credentials to attackers.

Integrate email security. Email filters will detect a majority of phishing emails or messages with malicious attachments and send them to a safe quarantine storage where they can be reviewed by an administrator.

Never connect to an unknown Wi-Fi hotspot. Attackers use malicious hotspots with names similar to an official source. Users should never connect to a public Wi-Fi without first verifying that it is indeed owned by the official provider.

4.3.3 Password Attack, Malware

Password attacks involve exploiting a broken authorization vulnerability in the system combined with automatic password attack tools that speed up the guessing and cracking passwords. The attacker uses various techniques to access and expose the credentials of a legitimate user, assuming their identity and privileges. The username-password combination is one of the oldest known account authentication techniques, so adversaries have had time to craft multiple methods of obtaining guessable passwords. Additionally, applications that use passwords as the sole authentication factor are vulnerable to password attacks since the vulnerabilities are well understood.

Password attacks have far-reaching consequences since malicious users only require unauthorized access to a single privileged account or a few users accounts to compromise the web application. Depending on the data hosted by the application, compromised passwords can pave the way for the exposure of sensitive information, distributed denial-of-service, financial fraud, and other sophisticated attacks.

.

4.4 Hackers:

The basic definition of a hacker is someone who uses a computer system to gain unauthorized access to another system for data or who makes another system unavailable. These hackers will use their skills for a specific goal, such as stealing money, gaining fame by bringing down a computer system, or making a network unavailable -- even sometimes destroying them. However, there are three different types of hackers, each with a particular goal, and not all are the bad guys.

A hacker is a person who breaks into a computer system. The reasons for hacking can be many: installing malware, stealing or destroying data, disrupting service, and more. Hacking can also be done for ethical reasons, such as trying to find software vulnerabilities so they can be fixed.

4.4.1 Various Vulnerabilities:

Vulnerabilities are flaws in a computer system that weaken the overall security of the device/system. Vulnerabilities can be weaknesses in either the hardware itself, or the software that runs on the hardware. Vulnerabilities can be explorrited by a threat actor, such as an attacker, to cross privilege boundaries (i.e. perform unauthorized actions) within a computer system. To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerabilities are also known as the attack surface.

In Short, security vulnerability is an unintended characteristic of a computing component or system configuration that multiplies the risk of an adverse event or a loss occurring either due to accidental exposure, deliberate attack, or conflict with new system components.
The Difference among Vulnerabilities, Threats and Risks

Many people may use the terms vulnerability, threat and risk interchangeably. However, in the cybersecurity world, these terms have distinct and specific meanings.

As noted above, a vulnerability is a weakness that can be exploited by a malicious actor. For example, unpatched software or overly permissive accounts can provide a gateway for cybercriminals to

access the network and gain a foothold within the IT environment.
A threat is a malicious act that can exploit a security vulnerability.
A risk is what happens when a cyber threat exploits a vulnerability. It represents the damage that could be caused to the organization in the event of a cyberattack.

4.4.1.1 Injection attacks, Changes in security settings

Injection attacks: Injection attacks refer to a broad class of attack vectors. In an injection attack, an attacker supplies untrusted input to a program. This input gets processed by an interpreter as part of a command or query. In turn, this alters the execution of that program.

Injections are amongst the oldest and most dangerous attacks aimed at web applications. They can lead to data theft, data loss, loss of data integrity, denial of service, as well as full system compromise. The primary reason for injection vulnerabilities is usually insufficient user input validation.

Types of Injection Attacks

SQL injection (SQLi) and Cross-site Scripting (XSS) are the most common injection attacks but they are not the only ones. The following is a list of common injection attack types.

Injection attack	Description	Potential impact
Code injection	The attacker injects application code written in the application language. This code may be used to execute operating system commands with the privileges of the	Full system compromise

Injection attack	Description	Potential impact
	user who is running the web application. In advanced cases, the attacker may exploit additional privilege escalation vulnerabilities, which may lead to full web server compromise.	
CRLF injection	The attacker injects an unexpected CRLF (Carriage Return and Line Feed) character sequence. This sequence is used to split an HTTP response header and write arbitrary contents to the response body. This attack may be combined with Cross-site Scripting (XSS).	Cross-site Scripting (XSS)
Cross-site Scripting (XSS)	The attacker injects an arbitrary script (usually in JavaScript) into a legitimate website or web application. This script is then executed inside the victim's browser.	Account impersonation Defacement Run arbitrary JavaScript in the victim's browser
Email Header Injection	This attack is very similar to CRLF injections. The attacker sends IMAP/SMTP commands to a mail server that is not directly available via a web application.	Spam relay Information disclosure
Host Header Injection	The attacker abuses the implicit trust of the HTTP Host header to poison password-reset functionality and web caches.	Password-reset poisoning Cache poisoning
LDAP Injection	The attacker injects LDAP (Lightweight Directory Access Protocol) statements to execute arbitrary LDAP commands. They can gain permissions and modify the contents of the LDAP tree.	Authentication bypass Privilege escalation Information disclosure
OS Command Injection	The attacker injects operating system commands with the privileges of the user who is running the web application. In advanced cases, the attacker may exploit additional privilege escalation vulnerabilities, which may lead to full system compromise.	Full system compromise
SQL Injection (SQLi)	The attacker injects SQL statements that can read or modify database data. In the case of advanced SQL Injection attacks, the attacker can use SQL commands to write arbitrary files to the server and even execute OS commands. This may lead to full system compromise.	Authentication bypass Information disclosure Data loss Sensitive data theft Loss of data integrity Denial of service Full system compromise.
XPath injection	The attacker injects data into an application to execute crafted XPath queries. They can use them to access unauthorized data and bypass authentication.	Information disclosure Authentication bypass

Changes in security settings: Security misconfiguration is the lack of proper security in server or web apps, opening up your business to cyber threats. This kind of misconfiguration runs rampant,

commonly occurring when levels of the application stack are upgraded while others are left untouched, as the default settings may have included insecurities that go unaddressed.

- Running an application with debug enabled in production
- Having directory listing (which leaks valuable information) enabled on the server
- Running outdated software (think WordPress plugins, old PhpMyAdmin)
- Running unnecessary services
- Not changing default keys and passwords (which happens more frequently than you'd believe)
- Revealing error handling information (e.g., stack traces) to potential attackers

4.4.1.2 Expouser of Sensitive Data

Exposure of Sensitive Data: Sensitive data exposure can happen in several ways. Sheer human negligence can cause data to be uploaded to a public website or a commonly accessed database. Inappropriate access controls might lead to a single employee owning control over a huge database of sensitive information. Unlike a data breach, there isn't always malicious intent behind such scenarios. Human errors or system misconfigurations cause sensitive data (intellectual property, user credentials, personally identifiable information, payment details, etc.) to end up in the wrong place where it is vulnerable to exploitation.

This web security vulnerability is about crypto and resource protection. Sensitive data should be encrypted at all times, including in transit and at rest. No exceptions. Credit card information and user passwords should never travel or be stored unencrypted, and passwords should always be hashed. Obviously, the crypto/hashing algorithm must not be a weak one. When in doubt, web security standards recommend AES (256 birts and up) and RSA (2048 bits and up).

It cannot be overemphasized that session IDs and sensitive data should not travel in URLs. Cookies with sensitive data should have the "secure" flag on.

4.4.1.3 Breach in authentication protocol

Breach in authentication protocol: Broken authentication is an umbrella term for several vulnerabilities that attackers exploit to impersonate legitimate users online. Broadly, broken authentication refers to weaknesses in two areas: session management and credential management. Both are classified as broken authentication because attackers can use either avenue to masquerade as a user: hijacked session IDs or stolen login credentials.

Attackers employ a wide variety of strategies to take advantage of these weaknesses, ranging from huge credential stuffing attacks to highly targeted schemes aimed at gaining access to a specific person's credentials

Session Management Flaws Open the Door to Attacks. Session management is part of broken authentication, but the two terms are often listed side by side so people don't assume that "authentication" refers only to usernames and passwords. Since web applications use sessions and credentials to identify individual users, attackers can impersonate them using either mechanism.

Attackers Exploit Weak and Compromised Credentials. Malicious actors use various methods to steal, guess, or trick users into revealing their passwords. It includes various ways such as password spraying, Phishing Attacks etc. Password spraying is a little like credential stuffing, but instead of working off a database of stolen passwords, it uses a set of weak or common passwords to break into a user's account. Attackers typically phish by sending users an

email pretending to be from a trusted source and then tricking users into sharing their credentials or other related information. It can be a broad-based attempt that hits everyone at an organization with the same phony email, or it can take the form of a “spear phishing” attack tailored to a specific target.

4.4.2 Types of Hackers: White hat and Black hat

Main types of hackers: Black hat hacker, White hat hacker and Gray hat hacker.

1) Black Hat Hacker - Evil Doer

The black hat hacker is the one who hacks for malicious intent - he is the bad guy. This type of hacker uses his or her skills to steal money or data, knock a computer system offline, or even destroy them. Some of these hackers love to see their work and name in the news, so they would try to target big name organizations and companies. For instance, they might change the front page of a company website.

Black hats also try to break into computer systems to steal credit card information and possibly steal valuable information to sell on the black market. They may even lock out the computer and network system from the owners and then hold them for ransom.

The black hat works outside of the law. This is the hacker that we as a society are most familiar with. Some black hats have cost companies hundreds of millions of dollars in damages for credit card and social security information theft. They can work alone, in that case known as a lone wolf, or with a team. They work slowly and methodically, since the black hat knows it takes patience to compromise a computer or a network system in order to a hit a big payoff and not be caught.

2) White Hat Hacker – Ethical Hacker

White hat hackers are cyber security professionals who are authorized or certified to hack organizational networks and computer systems. They use their expertise and skills to find vulnerabilities in systems. A white hacker is also known as Ethical Hacker.

Typically, large organizations, businesses, and governments hire white hat hackers to identify security vulnerabilities before black hat hackers can. White hat hackers spot and fix the weaknesses in the security systems and safeguard them against external attacks and data breaches. They are also known as ethical hackers.

Ethical hackers, thus, do not intend to harm a system. Instead, they find loopholes in a system as a part of penetration testing and vulnerability assessments.

White hat hackers usually have a good degree of technical expertise and broad skills in programming, networking, and IT.

3) Gray hat hackers

Gray hat hackers may not have the criminal or malicious intent of a black hat hacker, but they also don’t have the prior knowledge or consent of those whose systems they hack into. Nevertheless, when gray hat hackers uncover weaknesses such as zero-day vulnerabilities, they report them rather than fully exploiting them. But gray hat hackers may demand payment in exchange for providing full details of what they uncovered