Question 1 : What is OWASP? And explain the top 10 OWASP - 10

Answer: OWASP OR Open Web APPLICATION Security Project is an online community dedicated to web application security. The community works towards finding the most critical web application security flaws.

OWASP has many different projects under its umbrella, one of which is the Top 10 project. The goal of the top 10 project is to raise awareness about application security by identifying some of the most critical risks facing organizations. The OWASP Top 10 represents a broad consensus about what the most critical web application security flaws are.

**The Top 10 Vulnerabilities arranged in order of severity:**

1. INJECTION: Injection flaws, such as SQL, OS and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into exciting unintended commands or accessing data without proper authorization.  
     
   Example:   
   An application uses untrusted data when constructing a vulnerable SQL call:  
   The attacker modifies the ‘id’ parameter in their browser to send code.
2. Broken Authentication and Session Management:  
   A web application with broken or weak authentication can be easily detected by attackers and is vulnerable to brute force/dictionary attacks and session management attacks.  
     
   Credential Stuffing : Attackers use lists of known passwords and try them sequentially to gain access. Without automated threat or credential stuffing protection, the application is used by attackers as a validation mechanism for any password they try.

Password Based Attacks: web applications relying only on passwords have inherently weak authentication mechanisms, even if passwords have complexity requirements and are rotated. Organizations should switch to multi-factor authentication.

1. Cross Site Scripting: attackers use XSS to exploit weaknesses in session management and execute malicious code on user browsers.
2. Insecure Direct Object References:  
   Websites often require users to provide values for their applications’ parameters. If these values are not properly vetted, hackers can use them to pass malicious commands to the site.  
   A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
3. Security Misconfiguration:   
   Misconfigured security controls are a common entry point for attackers. For example, a database deployed with a default admin password.
4. Sensitive Data Exposure:   
   Sensitive data is typically the most valuable asset targeted by cyber attacks. Attackers can gain access to it by stealing cryptographic keys, conducting “man in the middle” (MITM) attacks, or stealing cleartext data which may occasionally be stored on servers or user browsers.  
     
   No TLS - If a website does not use SSL/TLS for all pages, an attacker can monitor traffic, downgrade connections from HTTPS to HTTP and steal the session cookie.
5. XML External Entities:   
   If a web application uses a vulnerable component processing XML, attackers can upload XML or include hostile content, commands or code within an XML document.
6. Insufficient Logging and Monitoring - attackers rely on the lack of monitoring and timely response to succeed with any other attack vector.
7. Insecure Deserialization -- deserialization is a complex technique, but if executed correctly, it allows attackers to execute malicious code on a server.
8. Broken Access Control: Broken access control means that attackers can gain access to user accounts and act as users or administrators, and that regular users can gain unintended privileged functions. Strong access mechanisms ensure that each role has clear and isolated privileges.

Question 2: Differentiate between SQL and No-SQL. - 5

Answer : SQL Database :

* RELATIONAL DATABASE MANAGEMENT SYSTEM (RDBMS)
* These databases have fixed or static or predefined schema.
* These databases are not suited for hierarchical data storage.
* These databases are best suited for complex queries.
* Vertically Scalable.
* Follows ACID property

NoSQL Database:

* Non-relational or distributed database system.
* They have dynamic schema.
* These databases are best suited for hierarchical data storage.
* These databases are not so good for complex queries.
* Horizontally scalable.
* Follows CA (Consistency, availability, partition tolrence).

Question 3: What is the CAP theorem? Give examples of each – 5

Answer : Consistency

Consistency means that all clients see the same data at the same time, no matter which node they connect to. For this to happen, whenever data is written to one node, it must be instantly forwarded or replicated to all the other nodes in the system before the write is deemed ‘successful.’

Availability

Availability means that that any client making a request for data gets a response, even if one or more nodes are down. Another way to state this—all working nodes in the distributed system return a valid response for any request, without exception.

Partition tolerance

A partition is a communications break within a distributed system—a lost or temporarily delayed connection between two nodes. Partition tolerance means that the cluster must continue to work despite any number of communication breakdowns between nodes in the system.

Question 4 : How do you stop a DDoS attack?

Answer: Identify the DDoS attack early: If you run your own servers, then you need to be able to identify when you are under attack. That’s because the sooner you can establish that problems with your website are due to a DDoS attack, the sooner you can stop the DDoS attack.

To be in a position to do this, it’s a good idea to familiarize yourself with your typical inbound traffic profile; the more you know about what your normal traffic looks like, the easier it is to spot when its profile changes. Most DDoS attacks start as sharp spikes in traffic, and it’s helpful to be able to tell the difference between a sudden surge of legitimate visitors and the start of a DDoS attack.

Question 5: What is the difference between a process and a thread?

Answer: Process:

* A process is a program under execution that is an active program
* Processes require more time for context switching as they are more heavy.
* Processes are totally independent and don’t share memory.

Thread:

* A thread is a lightweight process that can be managed independently by a scheduler.
* Threads require less time for context switching as they are lighter than processes.
* A thread may share some memory with its peer threads.

Question 6: ) What is the difference between exec and fork

Answer : The fork() returns the PID of the child process. If the value is non-zero, then it is parent process’s id, and if this is 0, then this is child process’s id.

The exec() system call is used to replace the current process image with the new process image. It loads the program into the current space, and runs it from the entry point.

So the main difference between fork() and exec() is that fork starts new process which is a copy of the main process. the exec() replaces the current process image with new one, Both parent and child processes are executed simultaneously.

Question 7: What is "nohup" used for?

Answer: Nohup, short for no hang up is a command in Linux systems that keep processes running even after exiting the shell or terminal.

Nohup prevents the processes or jobs from receiving the SIGHUP (Signal Hang UP) signal. This is a signal that is sent to a process upon closing or exiting the terminal. In this guide, we take a look at the nohup command and demonstrate how it can be used.

Question 8: What is swap and what is it used for?

Answer: Swap is hard disk space used as RAM. It is **very** slow, but stops computers from crashing when they are trying to deal with more data then their RAM can handle.

Swap is used to give processes room, even when the physical RAM of the system is already used up. In a normal system configuration, when a system faces memory pressure, swap is used, and later when the memory pressure disappears and the system returns to normal operation, swap is no longer used.

Question 9: What Unix/Linux commands will alter a files ownership, files permissions?

Answer: chown − The chown command stands for "change owner" and is used to change the owner of a file.

Chmod - The chomod command stands for "change mode" and is used to change the permission of a file.