Top 14 OWASP Interview Questions & Answers

1) What is OWASP?

OWASP stands for Open Web Application Security Project. It is an organization which supports secure software development.

2) Mention what flaw arises from session tokens having poor randomness across a range of values?

Session hijacking arises from session tokens having poor randomness across a range of values.

3) Mention what happens when an application takes user inserted data and sends it to a web browser without proper validation and escaping?

Cross site scripting happens when an application takes user inserted data and sends it to a web browser without proper validation and escaping.

4) Mention what threat can be avoided by having unique usernames produced with a high degree of entropy?

Authorization Bypass can be avoided by having unique usernames generated with a high degree of entropy.

5) Explain what is OWASP WebGoat and WebScarab?

- **WebGoat:** Its an educational tool for learning related to application security, a baseline to test security tools against known issues. It's a J2EE web application organized in "Security Lessons" based on tomcat and JDK 1.5.
- **WebScarab:** It's a framework for analysing HTTP/HTTPS traffic. It does various functions like fragment analysis, observer the traffic between the server and browser,

manual intercept, session ID analysis, identifying new URLs within each page viewed

6) List Top 10 OWASP Vulnerabilities

OWASP top 10 security flaws include

- Injection
- Cross site scripting
- Broken Authentication and Session Management
- Insecure cryptographic storage
- Failure to restrict
- Insecure communications
- Malicious file execution
- Insecure direct object reference
- Failure to restrict url access
- Information leakage and improper error handling

7) Explain what threat arises from not flagging HTTP cookies with tokens as secure?

Access Control Violation threat arises from not flagging HTTP cookies with tokens as secure.

8) Name the attack technique that implement a user's session credential or session ID to an explicit value?

Dictionary attack can force a user's session credential or session ID to an explicit value

9) Explain what does OWASP Application Security Verification Standard (ASVS) project includes?

OWASP application security verification standard project includes

- **Use as a metric:** It provides application owners and application developers with a yardstick with which to analyze the degree of trust that can be placed in their web applications

- **Use as a guidance:** It provides information to security control developers as to what to build into security controls in order to meet the application security requirements
- **Use during procurement:** It provides a basis for specifying application security verification requirements in contracts

10) List out the controls to test during the assessment?

- Information gathering
- Configuration and Deploy management testing
- Identify Management testing
- Authenticate Testing
- Authorization Testing
- Session Management Testing
- Data Validation Testing
- Error Handling
- Cryptography
- Business logic testing
- Client side testing

11) Explain what the passive mode is or phase I of testing security in OWASP?

The passive mode or phase I of security testing includes understanding the application's logic and gathering information using appropriate tools. At the end of this phase, the tester should understand all the gates or access points of the application.

12) Mention what is the threat you are exposed to if you do not verify authorization of user for direct references to restricted resources?

You are exposed to threat for insecure direct object references, if you do not verify authorization of user for direct references to limited or restricted resources.

13) Explain what is OWASP ESAPI?

OWASP ESAPI (Enterprise Security API) is an open source web application security control library that enables developers to build or write lower risk applications.

14) Mention what is the basic design of OWASP ESAPI?

The basic design of OWASP ESAPI includes

- A set of security control interfaces
- For each security control there is a reference implementation
- For each security control, there are option for the implementation for your own organization