HACKING WEB APPLICATIONS INTERVIEW QUESTIONS

1.What are some common web application attacks?

Answer: Common web application attacks include SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), broken authentication, session fixation, local file inclusion (LFI), remote file inclusion (RFI), and command injection.

2.How does an SQL injection attack work?

Answer: SQL injection occurs when an attacker inserts malicious SQL code into a web application's input fields, manipulating the database to access, modify, or delete data, or execute administrative operations.

3.What is cross-site scripting (XSS) and its types?

Answer: XSS is an attack where attackers inject malicious scripts into web pages viewed by other users. Types include Stored XSS, Reflected XSS, and DOM-based XSS.

4.Explain a cross-site request forgery (CSRF) attack.

Answer: CSRF tricks a user into performing unwanted actions on a web application where they are authenticated, potentially leading to unauthorized state changes like changing passwords or making transactions.

5.What is the difference between Local File Inclusion (LFI) and Remote File Inclusion (RFI)?

Answer: LFI allows an attacker to include files from the server's local file system, while RFI includes files from remote servers, potentially executing malicious code hosted externally.

6.What is command injection?

Answer: Command injection is an attack where the attacker executes arbitrary commands on the host operating system via a vulnerable application, often by manipulating input fields.

7.What is a session fixation attack?

Answer: Session fixation involves an attacker setting a user's session ID before they log in, allowing the attacker to hijack the session after the user authenticates.

8.What is a broken authentication attack?

Answer: Broken authentication occurs when application functions related to authentication and session management are implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens.

9.Explain what a security misconfiguration attack is.

Answer: Security misconfiguration involves improperly configured security controls, such as default accounts, misconfigured permissions, or exposed debug information, which attackers can exploit.

10.What are injection flaws?

Answer: Injection flaws occur when untrusted data is sent to an interpreter as part of a command or query, allowing attackers to execute unintended commands or access data without proper authorization.

11.What is the purpose of web application security testing?

Answer: The purpose is to identify, evaluate, and mitigate security vulnerabilities in web applications to protect against potential attacks and ensure the integrity, confidentiality, and availability of the application and its data.

12.What are the main phases of a web application penetration test?

Answer: The main phases include planning and reconnaissance, scanning and enumeration, vulnerability assessment, exploitation, and reporting.

13.What tools are commonly used in web application security testing?

Answer: Common tools include Burp Suite, OWASP ZAP, Nikto, SQLmap, Acunetix, and Nessus.

14.How is reconnaissance conducted in web application hacking?

Answer: Reconnaissance involves gathering information about the target application, such as identifying domain names, IP addresses, technologies used, open ports, and publicly available information.

15.What is vulnerability scanning and how is it performed?

Answer: Vulnerability scanning uses automated tools to identify known vulnerabilities in a web application by sending probes to the application and analyzing the responses.

16.How do ethical hackers exploit vulnerabilities in web applications?

Answer: Ethical hackers simulate attacks to exploit identified vulnerabilities, such as executing SQL injections, XSS payloads, or command injections, to understand their impact and validate their existence.

17.What is post-exploitation in web application hacking?

Answer: Post-exploitation involves activities after successfully exploiting a vulnerability, such as data extraction, privilege escalation, maintaining access, and covering tracks.

18.What is the role of reporting in web application penetration testing?

Answer: Reporting documents the findings, including identified vulnerabilities, their severity, potential impact, and recommended remediation measures, providing a comprehensive assessment of the application's security posture.

19.What are some best practices for securing web applications?

Answer: Best practices include validating and sanitizing user inputs, implementing strong authentication and session management, using HTTPS, keeping software and libraries updated, performing regular security assessments, and employing security headers.

20.How can the risk of SQL injection be mitigated?

Answer: The risk can be mitigated by using prepared statements and parameterized queries, validating and sanitizing user inputs, and employing web application firewalls (WAFs).