HACKING WEB SERVER INTERVIEW QUESTIONS

1.What are some common web server attacks?

Answer: Common web server attacks include Distributed Denial of Service (DDoS) attacks, SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), directory traversal, and remote file inclusion.

2.What is a Distributed Denial of Service (DDoS) attack?

Answer: A DDoS attack overwhelms a web server with a massive amount of traffic from multiple sources, causing it to become slow, unavailable, or crash.

3.How does an SQL injection attack work?

Answer: SQL injection involves inserting malicious SQL code into a web application input field, allowing attackers to manipulate the database, extract data, or execute administrative operations.

4.What is cross-site scripting (XSS)?

Answer: XSS is an attack where malicious scripts are injected into trusted websites. When users visit the compromised page, the script executes in their browser, potentially stealing cookies, session tokens, or other sensitive data.

5.What is a cross-site request forgery (CSRF) attack?

Answer: CSRF tricks a user into performing actions they did not intend by exploiting their authenticated session with a web application, potentially changing user settings or executing transactions.

6.What is directory traversal and how does it affect web servers?

Answer: Directory traversal (or path traversal) attacks manipulate web server inputs to access directories and files outside the intended web root, potentially exposing sensitive information.

7.Explain the remote file inclusion (RFI) attack.

Answer: RFI occurs when an attacker exploits a web application to include a remote file, which can lead to the execution of malicious scripts on the server.

8.What is a web shell and how is it used in web server attacks?

Answer: A web shell is a script that allows attackers to execute arbitrary commands on the server through a web interface, providing remote access and control over the compromised server.

9.Describe the impact of an HTTP response splitting attack.

Answer: HTTP response splitting involves manipulating HTTP headers, allowing attackers to inject malicious content or set custom headers, leading to XSS, cache poisoning, or other attacks.

10.What are some signs that a web server has been compromised?

Answer: Signs include unusual traffic patterns, unauthorized changes to web pages, unexpected server crashes, alerts from security tools, and unauthorized user accounts or files.

11.What is a vulnerability assessment in the context of web server security?

Answer: A vulnerability assessment involves systematically identifying, evaluating, and prioritizing security weaknesses in a web server infrastructure to improve its security posture.

12.What tools are commonly used for web server vulnerability scanning?

Answer: Common tools include Nessus, OpenVAS, Nikto, Burp Suite, OWASP ZAP, and Qualys Web Application Scanner.

13.How does penetration testing differ from vulnerability scanning?

Answer: Penetration testing involves actively exploiting vulnerabilities to assess the security of a system, while vulnerability scanning identifies and reports potential vulnerabilities without exploiting them.

14.What is the role of the OWASP Top Ten in web server security auditing?

Answer: The OWASP Top Ten is a list of the most critical web application security risks, providing guidelines and best practices for identifying and mitigating common vulnerabilities.

15.Explain the concept of attack surface analysis in web server security.

Answer: Attack surface analysis involves identifying all the potential points of entry (e.g., ports, services, and interfaces) that an attacker could exploit, helping to prioritize areas for security improvement.

16.What is the importance of patch management in web server security?

Answer: Patch management ensures that all software and components on the web server are up-to-date with the latest security patches, reducing the risk of exploitation from known vulnerabilities.

17.How can configuration management improve web server security?

Answer: Proper configuration management ensures that web servers are set up securely, following best practices and guidelines, minimizing the attack surface and reducing the risk of misconfigurations.

18.What is the role of intrusion detection systems (IDS) in web server security?

Answer: IDS monitor network traffic and system activities for signs of malicious behavior, alerting administrators to potential security incidents in real-time.

19.Why is it important to conduct regular security audits on web servers?

Answer: Regular security audits help identify new vulnerabilities, verify the effectiveness of existing security measures, and ensure compliance with security policies and regulations.

20.What are some best practices for securing web servers?

Answer: Best practices include using strong authentication and access controls, enabling HTTPS, regularly updating and patching software, using security headers, implementing web application firewalls (WAFs), and regularly performing security assessments.