



Top 50 VAPT (Vulnerability Assessment & Penetration Testing) Interview Questions.

Round 1

Looking to crack your next **VAPT interview** or improve your hands-on skills in **ethical hacking**?

Here's a curated list of the **most frequently asked questions** that cover everything from fundamentals to real-world testing scenarios:

Core VAPT Concepts

1. What is VAPT, and why is it important?

2. Difference between Vulnerability Assessment and Penetration Testing?
3. What are the main phases of a penetration test?
4. What is reconnaissance in ethical hacking?
5. What is enumeration, and why is it critical to successful exploitation?

Testing Methodologies & Tools

6. Explain black box, white box, and gray box testing.
7. What is a CVE and its purpose in vulnerability management?
8. What is CVSS, and how is its score calculated?
9. What is a vulnerability scanner?
10. List some popular VAPT tools and their use cases.
11. What is Nmap used for and how does TCP vs UDP scanning differ?
12. What is banner grabbing, and what info can it reveal?
13. Explain the use of OpenVAS and Nessus in scanning.
14. What is Metasploit? How is it used during exploitation?
15. What is Burp Suite, and what are its main components?
16. When do you use Nikto, and for what purpose?

Web Application Security

17. What is OWASP, and what does the OWASP Top 10 cover?
18. Explain SQL Injection and methods to prevent it.

19. Define XSS and how it differs from CSRF.
20. Explain command injection and directory traversal vulnerabilities.
21. What is SSRF (Server-Side Request Forgery)?
22. How do you test for insecure file uploads?

Attack & Exploitation Techniques

23. Explain privilege escalation (Windows vs Linux).
24. What is password cracking, and which tools are common?
25. What is a reverse shell, and how is it established?
26. Define post-exploitation—why is it a critical phase?
27. What is vulnerability chaining?
28. Define a zero-day vulnerability and give an example.

Reporting & Risk Management

29. Difference between authenticated vs unauthenticated scans.
30. What is risk rating, and how do you assign it?
31. What should a detailed VAPT report include?
32. What is remediation, and why does it matter?
33. How do you verify if a vulnerability is a false positive?
34. What is responsible disclosure in ethical hacking?

Professional & Ethical Aspects

35. What are common challenges during a pentest?
36. What are the legal and ethical considerations for testers?
37. Explain social engineering and phishing simulation in a pentest.
38. What are the stages of the Cyber Kill Chain?
39. What is exploit development, and when is it used?
40. Which scripting languages are valuable for VAPT automation?
41. Which certifications are ideal for VAPT professionals (CEH, eJPT, OSCP, etc.)?
42. What soft skills are crucial for a penetration tester?
43. How do you stay updated on current vulnerabilities and exploits?

JOIN US -

