

## 25 Questions Every Application Security Engineer Must Know!

Follow us @ scspcommunity 📿 💼 😭 🔞 💟 🛗











- 1.) On a high traffic website, how would you implement a secure login field? Keeping performance in consideration.
- 2.) What are the ways to mitigate a brute force attacks?
- 3.) In what ways site administrators can detect incoming CSRF attacks?
- 4.) What happens when you enter any website address in your browser's address bar and press enter?
- 5.) In what ways can you pentest a web application covering the following narratives:
  - a.) Unauthenticated testing on login page.
  - b.) Authenticated testing via user account.
  - c.) Authenticated testing via multiple user accounts.







- 6.) Explain the Same Origin Policy? How is Cross Origin Policy different? Also define CORS.
- 7.) How can you run SSHD securely on an online server?
- 8.) What are the possible details that should not be exposed by a web server if something goes wrong?
- 9.) How are 3 legged and 2 legged OAuth different?
- 10.) Deleting data does not actually erase it, why?

Follow us @ scspcommunity ( ) fin ( ) ( ) ( )

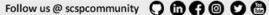








- 11.) Code reviewers should watch out for which kind of anti-security patterns?
- 12.) Differentiate between tcpdump and FWmonitor?
- 13.) A DB with one round of sha256 with static salt was exfiltrated! What should be the immediate action? Is the DB at any risk of being read?
- 14.) For a repo of source code to be audited, what's the first few things that need to be done?
- 15.) How can hackers leverage off Host header injection vulnerability?











- 16.) How would you mitigate XXE injection attacks for an application which requires the use of external entities to be called because of business needs.
- 17.) Is CSRF attack mitigated by SOP?
- 18.) Explain Web cache deception attack?
- 19.) Explain HTTP Request smuggling?
- 20.) How would you test a file upload functionality in an application?











- 21.) An API needs to fetch credentials, what will be the secure way to store those secrets and make them available for API calls?
- 22.) How would you investigate if an exisiting vulnerability has been exploited by an attacker or not?
- 23.) How logs can be poisoned using LFI/RFI?
- 24.) Where would credentials for a script be saved on a system that are needed to be used by the script?
- 25.) Explain Double-Submit cookie?

Follow us @ scspcommunity ( ) ( ) ( ) ( ) ( ) ( )







