60+ Application Security Interview Questions

Assess your AppSec skills based on these questions

Setting up the context

You can assess yourself by checking how many of these questions are easy for you, how many need finetuning and how many are yet to learn and master. Remember, every one of us is learning and a question is easy for you doesn't mean it's the same for everyone. However, it depends upon the role, and expectations set by the hiring manager and the interviewer.

The question might look straightforward but your answer speaks more about your experience and hands-on in this domain. Try to analyze the question and answer honestly.

Many questions might not for your experience or role as I am sharing mixed questions asked for various role in Application Security domain.

Also, I am not sharing questions on any programming language specific or even programming based security questions. That can be possibly another series of questions in my next release.

If you are looking for career guidance or learning trending technologies, please contact Flexmind

First thing first

This interview question set is mostly for defensive roles as compared to offensive roles which are mainly called “Penetration Testing or Web Security (sometimes it's used interchangeably) ”. I will concentrate more on how an application is developed, maintained, and deployed and how as a security engineer you would help an engineering team to overcome security challenges.

I will focus more on below topics:

1. Threat Modeling
2. Secure Code Review
3. Secure Coding
4. Secure Development (SDL)
5. And anything defensive in nature and developer-centric.

Note: For API security and offensive security, I will share a separate set of interview questions soon!

Second important note

I am listing questions based on a few criteria:

1. Common to everyone who is in this domain or trying to enter this domain
2. Some questions would be theoretical and you can consider those questions as a starting point to check the candidate’s overall knowledge
3. Some questions are for senior professionals
4. Some questions may have different answers depending on seniority level
5. Some questions can be to check your domain and leadership skills in this domain

One more thing

If you are ne to this domain or planning to make a career in cybersecurity. You should see below study plan before delving into interview questions. They are:

1. Common Skills Study Plan that you can finish within 3 months
2. 20 Essential books that you should read from security world
3. Application Security Study Plan (You must go through it before trying for appsec interviews)
4. You can’t ignore API security at present. So, here is your API Security Study Plan

5. Knowledge of Pentest will be an added advantage for you. Check this out: Web Pentest Study Plan
6. You can star or bookmark Security Study Plan which will give you an insight of what to study for various security domains

List of Application Security Questions

The question might look straightforward but your answer speaks more about your experience and hands-on in this domain. Try to analyze the question and answer honestly.

Application Security Basics Questions

1. Explain your top 3 favorite OWASP Top 10 vulnerabilities and why
2. How does TCP 3-way handshake work?
3. Why TLS is important in cybersecurity and can you explain the use of TLS in detail for a website?
4. How SSL/TLS makes my content secured over the internet
5. What happens when you type google.com in your browser?
6. What's the difference between SAST and SCA?
7. What is SQLi and how would you prevent/mitigate it?
8. Explain XSS with a few examples and how it can be avoided in the current software world.
9. How to avoid bruteforce attack on an application. Let's say login page. Explain everything that comes to your mind.
10. Tell us about a time when you had to learn something new really quickly and how did you go about it?

Application Security Role based questions

1. Explain CORS, SOP, and CSP from security point of view
2. How CSRF is dangerous for an application and what must be done to prevent CSRF in an application?
3. Explain the concept of input validation and why it is crucial for secure coding. Provide examples.
4. How do you approach secure error handling and logging in an application?
5. Discuss the role of encryption in secure coding and some best practices for implementing it.
6. What are some best practices for managing secrets and sensitive information in code?
7. How do you ensure the security of third-party libraries and dependencies in your code?

8. What are the key differences between manual code review and automated static analysis?
9. Describe your approach to conducting a secure code review. What do you look for first?
10. Can you give an example of a security vulnerability you discovered during a code review and how you addressed it?
11. Which secure coding standards do you follow during a code review (e.g., OWASP, CERT)?
12. How do you balance between finding security issues and maintaining development velocity during a secure code review?
13. Describe the STRIDE threat modeling methodology and provide examples of each threat type.
14. How do you prioritize threats identified during a threat modeling exercise?
15. How would you integrate threat modeling into an Agile development process?

Overall Application Security Assessment-based Questions

1. Where do we need security in the SDLC phase?
2. What would you suggest for input sanitization?
3. What should a developer do for secrets management?
4. What are some strategies for ensuring secure session management in web applications?
5. How do you handle security misconfigurations in development and production environments?
6. Discuss the importance of least privilege and role-based access control in application security.
7. How do you ensure that logging and monitoring are implemented securely and do not expose sensitive information?
8. What are the challenges of implementing SDL in a fast-paced development environment, and how do you overcome them?
9. Describe the various phases of SDL and the security activities involved in each phase.
10. How can an attacker exploit SSRF and what an application developer must do to prevent SSRF. This medium article might help you to understand how to bypass SSRF protection?

Some common "test your problem-solving skills" Application Security questions (mostly for senior role)

1. What step would you plan to make sure that secure coding practices are being followed by developers?
2. How would you make developers aware and involved in secure code development?
3. How do you handle typical developer and security clash situations?
4. What were your interesting findings in secure code review?
5. What are the common vulnerabilities you have experienced so far?
6. How would you approach identifying and mitigating security risks in a large, legacy codebase that hasn't been regularly maintained for security?
7. Describe a strategy to ensure secure coding practices in a multi-team development environment, especially when teams are working on interdependent components.
8. How would you implement and enforce a secure coding standard in a globally distributed development team?
9. How would you design a security strategy to protect a microservices architecture from both external and internal threats? What are the challenges you might face while designing and implementing it?
10. Describe how you would conduct a threat modeling for a cloud-native application. What specific security concerns are most critical in any cloud native application?
11. Can you provide an example of how you have implemented SDL in a past project?
12. What are some key metrics you would track to measure the effectiveness of an SDL program?

Application Security Scenario based interview questions

Consider this section as the toughest one and mainly for senior appsec professional.

1. How would you design a safe and secured password mechanism?
2. Can you explain password hashing function and importance of salt. Also, how salting and hashing passwords are used in this domain?
3. You use SCA tool to find vulnerabilities in 3rd party libraries. How would you mitigate those vulnerabilities found and risks associated with third-party libraries and frameworks?
4. Your company is developing a new financial application that handles sensitive customer data, including banking information. Describe how you would

approach threat modeling for this application. What specific threats would you consider, and how would you prioritize and mitigate them?

5. You are tasked with performing a secure code review for a web application that has been recently developed. During the review, you find several instances where user inputs are directly concatenated into SQL queries. Explain how you would address this issue and guide the development team to implement a secure solution.
6. A development team is working on a new feature that requires handling and storing user passwords. They plan to use a simple hash function (e.g., MD5) to store these passwords. As a security architect, how would you advise them on securely handling and storing passwords? Provide a detailed explanation of best practices.
7. During a code review, you discover that the application does not properly handle errors and exceptions. For example, stack traces are exposed to end users, which could potentially reveal sensitive information. Describe how you would rectify this situation and implement secure error handling and logging practices.
8. A critical vulnerability is discovered in a third-party library used extensively in your company's application. Explain the process you would follow to assess the impact, communicate with stakeholders, and implement a fix. How would you prevent similar issues in the future?
9. You are designing the architecture for a new e-commerce platform that includes a web application, mobile application, and backend APIs. Outline the security architecture you would propose, including key components and technologies to ensure robust security across all layers.
10. How would you review an architecture to prevent an automated bruteforce attack or dictionary attack?

Secure Code Review round with code snippets

Many companies won’t have this round, but I feel one should involve few code snippets in an interview to check the candidate’s indirect coding knowledge from security point of view, at least for the senior role like lead or staff role.

Insecure code snippets can be on a tougher note. Hoever, I am adding few easy one for practice and to give an idea that how this round can be prepared well as per the JD.

I would a hint for your practice, but in an interview you won’t be given any hint.

1. Identify the security issue in this code snippet and explain how you would fix it. [Hint: Can you spot CSRF issue here?]

   ```
   if ($_SERVER['REQUEST_METHOD'] === 'POST') {
       $userId = $_POST['userId'];
       $newEmail = $_POST['newEmail'];
       updateEmail($userId, $newEmail);
   }
   ```

2. Identify the security issue in this code snippet and explain how you would fix it. [Hint: Insecure desrialization]

   ```
   ObjectInputStream in = new ObjectInputStream(new
   FileInputStream("data.ser"));
   Object obj = in.readObject();
   in.close();
   ```

3. Identify the security issue in this code snippet and explain how you would fix it. [Hint: password hashing issue]

   ```
   import hashlib
   def store_password(password):
       hashed_password =
   hashlib.md5(password.encode()).hexdigest()
       save_to_database(hashed_password)
   ```

4. Which security issue it can cause? [Hint: XSS]

   ```
   const userInput = request.query.userInput;
   const output = "<div>" + userInput + "</div>";
   response.send(output);
   ```

5. Most common question asked in a secure coding round. It doesn't need hint I suppose. What issue this code snippet would cause and how would you help developer in fixing it?

   ```
   String userId = request.getParameter("userId");
   String query = "SELECT * FROM users WHERE user_id = '" +
   userId + "'";
   Statement stmt = connection.createStatement();
   ResultSet rs = stmt.executeQuery(query);
   ```

Summary

I have tried to cover all the possible questions from basics to advanced from various topics under AppSec domain like Threat Modeling, Secure Code Review, OWASP Top 10, Secure Design, Cryptography (basics), Overall understanding of application from a security perspective, dealing few scenarios with agile development, developers etc. All the best for your bright future and hope these set of questions would help you to excel in an interview.

I will try to add more security interview questions for specific role as well. Please share in comment which one you want to see next. Some examples are Sr. or Lead AppSec Engineer, AppSec Architect, DevSecOps engineer, Product Security Engineer role.

Don't forget to like, share, comment if you found it helpful for you.
Follow us on Linkedin: Sanjeev Jaiswal and Flexmind
Join our **whatsapp group for cybersecurity discussions**

References:

1. Security Study Plan
2. Cybersecurity Career Roadmap
3. Security Interview Questions
4. Appsec Interview questions by appsecengineer team
5. AppSec questions by startup jobs
6. Questions from Synopsys