Application Security Interview Questions: Expert Guidance and Insights

Assess your AppSec skills based on these questions.

ToC

Setting up the context

You can assess yourself by checking how many of these application security interview questions are easy for you, how many need finetuning, and how many you have yet to learn and master. Everyone is learning, and a question is easy for you, but it doesn’t mean it’s the same for everyone. However, it depends upon the hiring manager and interviewer's role and expectations.

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

Many questions might not be relevant to your experience or role, as I am sharing mixed questions asked for various roles in the Application Security domain.

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

First thing first

This interview question set is mainly for defensive roles compared to offensive roles, primarily 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 overcome security challenges.

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

Suppose you are new to this domain or planning to make a career in cybersecurity. You should see the study plan before delving into interview questions.

They are:

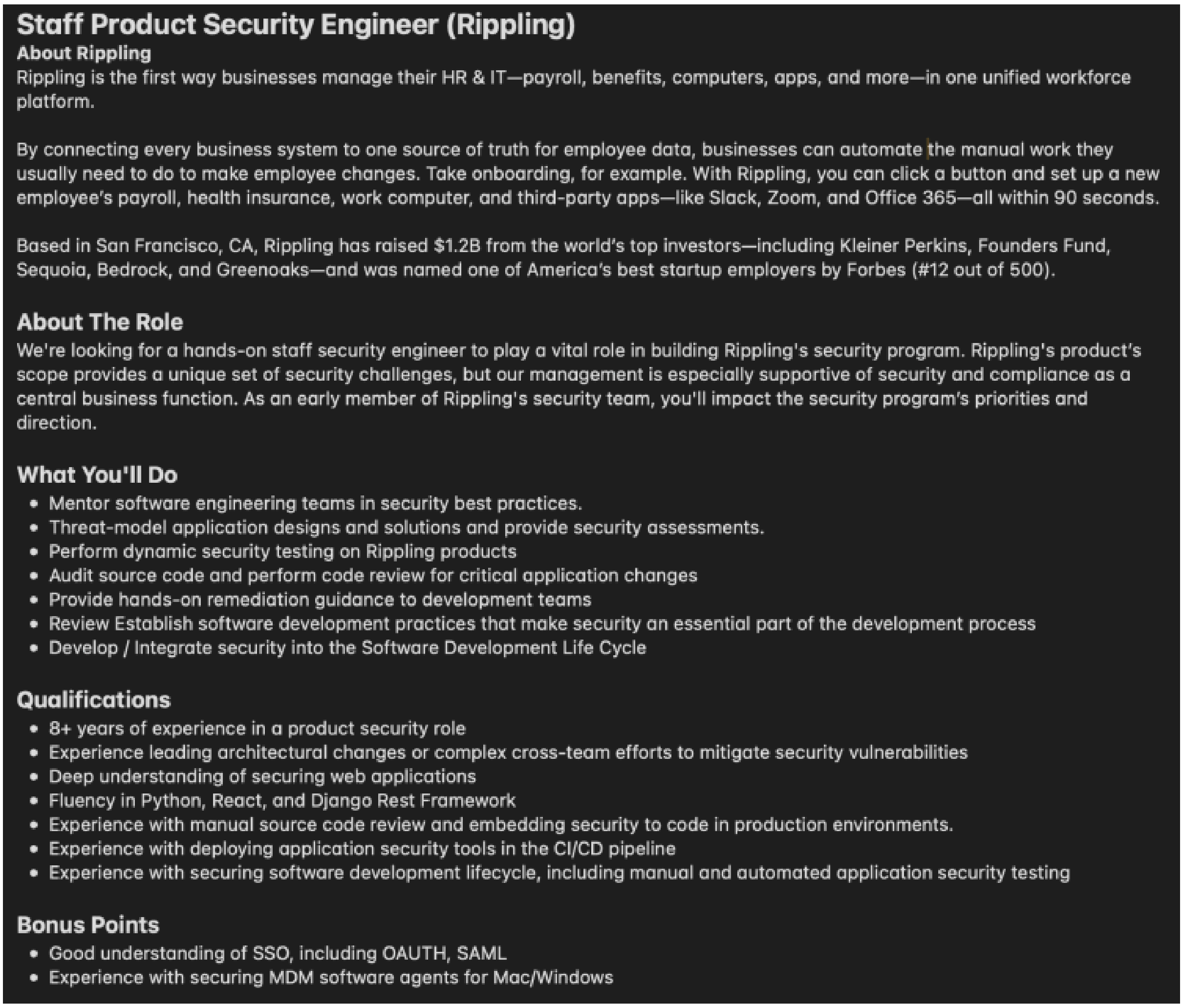
1. Common Skills Study Plan that you can finish within three months
2. 20 Essential books that you should read from the security world
3. Application Security Study Plan (You must go through it before trying for appsec interviews)
4. You can’t ignore API security at present. So, here is your API Security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

This space will focus more on:

1. Secure Code Review
2. Threat Modeling
3. Secure Coding
4. Secure Development
5. And anything defensive in nature and developer-centric. We have another page for everything else related to web security.

How the JD looks for an Application Security role

Here is a JD of a product-based company Rippling for a senior AppSec role



Staff Product Security Engineer (Rippling)

About Rippling

Rippling is the first way businesses manage their HR & IT—payroll, benefits, computers, apps, and more—in one unified workforce platform.

By connecting every business system to one source of truth for employee data, businesses can automate the manual work they usually need to do to make employee changes. Take onboarding, for example. With Rippling, you can click a button and set up a new employee's payroll, health insurance, work computer, and third-party apps—like Slack, Zoom, and Office 365—all within 90 seconds.

Based in San Francisco, CA, Rippling has raised $1.2B from the world's top investors—including Kleiner Perkins, Founders Fund, Sequoia, Bedrock, and Greenoaks—and was named one of America's best startup employers by Forbes (#12 out of 500).

About The Role

We're looking for a hands-on staff security engineer to play a vital role in building Rippling's security program. Rippling's product's scope provides a unique set of security challenges, but our management is especially supportive of security and compliance as a central business function. As an early member of Rippling's security team, you'll impact the security program's priorities and direction.

What You'll Do

- Mentor software engineering teams in security best practices.
- Threat-model application designs and solutions and provide security assessments.
- Perform dynamic security testing on Rippling products
- Audit source code and perform code review for critical application changes
- Provide hands-on remediation guidance to development teams
- Review Establish software development practices that make security an essential part of the development process
- Develop / Integrate security into the Software Development Life Cycle

Qualifications

- 8+ years of experience in a product security role
- Experience leading architectural changes or complex cross-team efforts to mitigate security vulnerabilities
- Deep understanding of securing web applications
- Fluency in Python, React, and Django Rest Framework
- Experience with manual source code review and embedding security to code in production environments.
- Experience with deploying application security tools in the CI/CD pipeline
- Experience with securing software development lifecycle, including manual and automated application security testing

Bonus Points

- Good understanding of SSO, including OAUTH, SAML
- Experience with securing MDM software agents for Mac/Windows

The above JD can give an idea of the concepts and skills you would need to learn.

If you are interviewing someone for an Application Security Engineer role, it could be junior, senior, or architect level. You can always start questions based on the person's experience in AppSec. However, the questions below can always be interesting and will help you understand the candidate better technically. Soft skills, teamwork, presentation skills, and communication skills are out of the scope of this space.

Application Security Interview Questions based on various aspects

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 is TLS important in cybersecurity, and can you explain the use of TLS in detail for a website?
4. How does SSL/TLS make my content secure 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 brute-force attacks on an application. Let's say the login page. Explain everything that comes to your mind.
10. Tell us about a time when you had to learn something new quickly and how you went about it.

Application Security Role-based questions

1. Explain CORS, SOP, and CSP from a security point of view
2. How is CSRF 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 finding security issues and maintaining development velocity during a secure code review?
13. Describe the STRIDE threat modelling methodology and provide examples of each threat type.
14. How do you prioritise threats identified during a threat modelling exercise?
15. How would you integrate threat modelling 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 sanitisation?
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 must an application developer 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 roles)

1. What step would you plan to ensure developers follow secure coding practices?
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 exciting findings in the 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, primarily when teams work on interdependent components.
8. How would you enforce a secure coding standard in a distributed development team?
9. How would you design a security strategy to protect a microservices architecture from external and internal threats? What are the challenges you might face while developing and implementing it?

10. Describe how you would conduct threat modelling 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 key metrics would you track to measure an SDL program's effectiveness?

Application Security Scenario-based interview questions

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

1. How would you design a safe and secure password mechanism?
2. Can you explain the password hashing function and the importance of salt? Also, how are salting and hashing passwords used in this domain?
3. You use the 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 threats would you consider, and how would you prioritise 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 in implementing a secure solution.
6. A development team is working on a new feature that requires handling and storing user passwords. They plan to store these passwords using a simple hash function (e.g., MD5). 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 handle errors and exceptions properly. For example, stack traces are exposed to end users, which could 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, including a web application, mobile application, and backend APIs. Outline your proposed security architecture, including key components and technologies to ensure robust security across all layers.
10. How would you review an architecture to prevent an automated or dictionary attack attack (think of different brute force attack techniques)?

Secure Code Review round with code snippets

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

Insecure code snippets can be tougher. However, I am adding a few easy ones for practice and to give an idea of how this round can be prepared well, as per the JD.

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

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

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

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 a hint I suppose. What issue this code snippet would cause and how would you help the 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);
```

Topics or concepts that are subjective and can check your in-depth knowledge regarding that area

1. What do you think about a good password?

This question looks very similar, but it can help the interviewer understand whether the person has experience with password management skills.

This question will help you to drill down to more specific questions to understand the competence of the candidate:

1. What is a complex password
2. Should the password complexity be the same for the admin and user
3. How do you save the password in a Database, encrypted or hashed or plain text
4. Do you use salt? Is it the same for all the passwords? Is it random per user?
5. How do you make your code safe from password attacks?

2. How do you stop brute force attacks on login/signup/forgot password page(s)?

This question helps you to understand if the person is aware of secure code development and secure design for such features and how far he/she can think. Check if the person talks about:

1. Captcha
2. CSRF token
3. Rate Limiting
4. MFA
5. Alert and Monitor for such strange behaviour
6. Account Lockout after n failed attempts

3. What happens when you type google.com on the browser

This question checks if the person understands the behind-the-curtain scene, such as URL to IP conversion, DNS involvement, server response, etc. Listen to the interviewee and see if he/she mentions the following:

1. How DNS resolves the URL
2. TCP 3-way handshake
3. How does HTTPS work, and what are its advantages
4. How to prevent the application from MiTM (Man in The Middle Attack)

4. How SSL/TLS makes my content secured over the internet

This question is the extension of the previous question to understand if the person understands:

1. How client server Hello established
2. How key exchange happens, i.e. public key or certificate
3. Is it symmetric or asymmetric encryption or both, and when is it used
4. Talks about Certificate Signing Request (CSR)
5. What are weak ciphers, and what are good SSL Cipher Suites
6. Able to use openssl command to see the details of SSL information
7. Can explain ssl format like this:
   TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
8. TLS 1.2 or TLS 1.3, and why?
9. What is PFS (Perfect Forward Secrecy), and why is it used?
10. Why is the enabled website still getting hacked?

5. How would you make developers aware and involved in secure code development?

This question would help you to understand if the person has delivered any training, presented slides, given demos, or delivered secure coding practices workshops. See if a person talks about:

1. OWASP ASVS (Application Security Verification Standard)
2. OWASP Top 10 2017/2021
3. OWASP Secure Review with some examples
4. Secure Design Principles
5. Then, you can go a little deeper, like sharing what difficulties you faced while training them on secure code design, principles, etc.
6. How do you ensure developers follow what you teach or make them aware of, such as IDE plugins, git actions, SAST tools, etc.?

6. Which one would you prefer and why? Manual secure code review or automated or both?

7. Which tools have you used for SAST?

8. What is the difference between SAST and SCA?

9. How well do you understand SQLi (SQL Injection)?

See if the person can explain:

1. When data becomes code and how to test it
2. Any specific tool to fasten SQL Injection
3. Can you spot SQLi from the code review
4. Experience of any SAST tool through which you can verify and validate SQLi
5. Mitigation for SQLi
6. Prepared statement in SQL injection

10. Do you understand the key difference between encryption, hashing, salt, obfuscation and encoding?

11. What you should check if the website is damn slow suddenly?

12. Explain how you handle AuthN and AuthZ.

An interviewer can assess whether the candidate has a robust and comprehensive understanding of authentication and authorization and their practical application in ensuring application security.

Depth of Understanding:

Does the candidate understand the fundamental differences and purposes of authentication and authorisation? Can they explain common methods and protocols for both AuthN and AuthZ?

Practical Knowledge:

1. Can the candidate discuss specific implementations and technologies (e.g., OAuth, SAML, RBAC)?
2. Do they mention industry best practices and why they are important?

Security Focus:

1. Is the candidate aware of common security risks and how can they be mitigated in both AuthN and AuthZ?
2. Do they highlight the importance of monitoring and logging?

Experience:

1. Can the candidate provide examples from past experience where they have implemented or improved AuthN and AuthZ mechanisms?
2. Are they able to discuss challenges faced and how they overcame them?

Current Trends:

1. Is the candidate up-to-date with current trends and emerging technologies in authentication and authorisation?
2. Do they mention advanced methods like biometrics, adaptive authentication, or zero-trust models?

13. How do you implement CSP? Does it add extra security for a web application? How?

Go as much deep as you can. Use this article to understand the details of CSP

14. What are the benefits of using SoP, CORS, and CSP?

Explain the basics of these concepts with one or two real-world examples. Also, explain why and where to use these with a few scenarios.

15. How do you handle typical developer and security clash situations?

16. List out the techniques used to prevent web server attacks

Check what points one can cover, and then you can deep dive based on the answer:

1. Patch management
2. Web Server hardening
3. Scanning system vulnerability
4. Custom vs default port
5. Firewall and other server settings avoiding default settings
6. Proper alerting and monitoring mechanism
7. Server log settings

17. List out the steps to successful data loss prevention controls.

See if the interviewee can explain below points:

1. Information risk profile
2. Assign roles and responsibilities to the technical administrator, incident analyst, auditor and forensic investigator.
3. Develop the technical risk framework
4. Expand the coverage of DLP controls
5. Monitor the results of risk reduction
6. Incident Response, risk severity, playbook etc.

18. Where do we need security in the SDLC phase?

19. What would you suggest for input sanitisation?

20. What have you done so far for API Security?

You can't think of application security without API security at present. However, I will cover more API security Interview Questions on another page.

21. Why is XoR very important in the Crypto world?

It's a basic but untouched topic in cryptography, and I recommend that every AppSec engineer learn the basics.

22. How OAuth works?

23. What is SCA, and how do you perform SCA?

24. What should a developer do for secrets management?

25. What is your exciting finding in a secure code review?

Summary

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

I will also try to add more security interview questions for specific roles. Please share in the comments which one you want to see next. Some examples are senior or Lead AppSec Engineer, AppSec Architect, DevSecOps engineer, and Product Security Engineer roles.

The updated version will be available on GitHub repo

Further reading 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

Follow us for cybersecurity guidance and study materials:

1. Twitter
2. Medium
3. Telegram
4. Whatsapp
5. Linkedin