**Tech Interview Guide - Security**

For the following roles: Application Security Engineer, Penetration Tester, Security Operations Engineer.

**Overview**
The purpose of this guide is to help you get a taste of what interviewers may be looking for in a technical interview. The questions here are behavioral in nature, designed to get you talking about specific situations and how you handled them. Guidelines are suggested for evaluating the strength of the answers. Remember, these are just sample questions, but you need to start thinking about how you'll answer story-type questions. These questions are designed to see how well you know what you're doing, but also help gauge your commitment to a team environment and whether you'd be a cultural fit for the org.

Remember to be as pleasant and friendly as you can be! Your interviewer is likely looking for confidence, but not over-confidence.

General questions
These questions cover commonalities about all security roles, and are for candidates in all three roles above (Application Security Engineer, Penetration Tester, Security Operations Engineer).

**Tell me about an existing security practice or process that you helped improve.**
What was the situation?
What did you do? Why?
What other options did you consider? Why did you decide on the path you took?
What were the challenges along the way?
What was the outcome? What did you learn?

**Warning Signs:**
Addresses practices/processes on an ad-hoc basis
Can't articulate trade-offs in the chosen approach.
Did not analyze required change methodically
Cannot demonstrate an improved outcome
**Great Signs:**
Understands and articulates how the change improved security posture
Made changes systematically and broadly
Understands and articulates required tradeoffs
Makes methodical, data-driven changes to practice/policy

**Tell me about how you have worked with a team to remediate a security issue.**
What was the issue?
What was the fix? What other approaches did you consider?
How did you communicate with the rest of the team?
How did you and the rest of the team stay aligned on the required work?
What was the outcome? What did you learn?
**Warning signs:**
Did not make sure the problem was clearly understood by the rest of the team
Did not make efforts to explain to the rest of the team, only highlight errors
Failed to get results, or got results by escalating or manipulating the process

Finds faults in teammates, or pulls “hero shifts”, rather than working collaboratively
Adopts an “us and them” mentality between security and other teams

**Great signs:**
Communicated clearly throughout the process
Worked to ensure high alignment continuously
Adopts a team mentality about the fix
Worked to increase the team’s understanding of the issue and fix

**Tell me about an innovative idea (i.e. a tool, practice, or policy) that you helped introduce.**
What was the new idea? What problem did it solve?
How was the new idea an improvement on the previous thing?
How did you manage the change?
What was the outcome? What did you learn?
**Warning signs:**
Idea was implemented without consideration for others
Used role / power rather than persuasion to implement
Improvement was unsuccessful or incomplete
Idea for “new for newness sake”, rather than showing a strong understanding of context
**Great signs:**
Achieved desired outcome
Idea shows sensitivity to context and applicability

**Describe a situation where you disagreed with someone about a security issue.**
What was the issue? What was the disagreement?
What was your point of view? What was theirs?
How did you resolve the disagreement? What was the final decision?
How did you feel about the outcome? How did the other party feel?
What did you learn?
**Warning signs:**
Unable to articulate/empathize with the other point of view
Disagreement not resolved
Disagreement resolved through role power, escalation, or other non-collaborative method
**Great signs:**
Clearly understands and articulates both points of view
Disagreement resolved amicably, to mutual satisfaction

**Questions for Application Security Engineers and Security Operations Engineers**
These questions are specifically for the Application Security Engineer and Security Operations Engineer roles.

**Tell me about a secure development practice (or tool) you helped introduce to an engineering team.**
What was the practice/tool? What problem did it solve?
How was this an improvement on the previous thing?
How did you teach people to use the new practice?
What was the outcome? What did you learn?
**Warning signs:**
Unclear on the problem/issue the practice solved

New practice was implemented without consideration for others
Used role power rather than persuasion to implement

**Great signs:**
Achieved desired outcome
Idea shows sensitivity to context and applicability
Thinks carefully about how engineers learned
Clear goals and measures for adoption

**Tell me about a security-related topic that you helped someone from a non-security background learn.**
What was the topic? How did you teach it?
Who were you teaching? Why?
Where did they get stuck? How did you help unstick them?
What was the outcome? What did you learn?
**Warning signs:**
Does not describe topic clearly
Did not tailor teaching strategy to individuals
Shows disdain or mocks non-technical people
**Great signs:**
Understands and explains topic clearly
Understands how to tailor strategy to different learning styles
Shows empathy and understanding of different knowledge backgrounds

**Questions for Penetration Testers**
These questions are specifically for the Penetration Tester role.

**Tell me about a particularly interesting vulnerability that you discovered.**
What was the vulnerability? How did you find it?
Where did you get stuck while researching the vulnerability? How did you get unstuck?
How did you report the issue? How was the report received?
What was the outcome? What did you learn?
**Warning signs:**
Doesn’t have a systematic approach (“lucked in” to the discovery)
Vulnerability isn’t particularly novel or interesting
Did not analyze in depth
Reported the issue too broadly/narrowly
**Great signs:**
Is animated and excited when talking about the situation
Has a system for discovering vulnerabilities
Analyzed the issue in depth
Vulnerability is especially novel: requires multiple steps, requires “out of the box” thinking, etc
Communicated/reported the issue appropriately and effectively

**Tell me about a time when you reported an issue you discovered to a development team.**
What was the issue?
How did you communicate that issue to the development team?
What remediation steps did you suggest?
What were the actual remediation steps taken? How and why did they differ?

What was the outcome? What did you learn?

**Warning signs:**

Did not make sure the problem was clearly understood by the rest of the team
Did not make efforts to explain to the rest of the team, only highlight errors
Failed to get results, or got results by escalating or manipulating the process
Adopts an “us and them” mentality between security and other teams

**Great signs:**

Communicated clearly throughout the process
Adopts a team mentality about the fix
Worked to increase the team’s understanding of the issue and fix