Alice & Bob Learn Application Security

By Tanya Janca

www.wiley.com/en-us/Alice+and+Bob+Learn+Application+Security-p-9781119687405

First of all, who are Alice and Bob? Alice and Bob are fictional characters created by RSA Security in 1978 to illustrate how the RSA encryption method worked. Since then, they've been used in countless security-related talks, publications, tutorials, etc.

Next, who is Tanya Janca? Tanya is the foremost expert in application security. With years of experience in software development and cyber security as well as countless conference talks, webcasts, YouTube videos, and blog posts, it's no wonder she literally wrote the book on application security. Tanya is an excellent communicator. She is an expert in application security, and she knows how to reach her audience regardless of their levels of expertise.

I have to say that this book was long overdue. There has never, to my knowledge, been anything else like this. I learned most of what I know of application security through various scattered resources from certification guides to YouTube videos to web-based articles. Sure, there's a lot of info, but until now there was nothing that tied it all together. *Alice & Bob* is the first of its kind. I'm sure there'll be plenty of copycats. On to the review!

Alice & Bob is not just a collection of information, nor is it a *do it this way, not that way* sort of guide. Tanya does explain the correct way to accomplish a task, but she also gives you the reasons behind her statements, and those reasons are backed up with solid references and real-life examples. *Alice & Bob* is presented similarly to a college course, where each successive chapter builds on the previous chapters. And like a college course, each chapter contains a quiz.

Most reference guides are not meant to be read front-to-back. It's usually easier just to search for the information you need. In this case, you should read it start-to-finish and then keep it on hand to access information as necessary. The book is divided into three main parts and 11 logically ordered chapters. By logically ordered, I mean that it takes you from beginner-level security concepts through incident handling and threat modeling (nice breakdown of threat types, by the way), secure coding, and defense in depth/layered security (and how web application security applies) and then shows you how to create a learning plan to help you grow as an analyst. Many of us have more or less followed the *make it up as we go* philosophy with no real plan, so having a structured learning plan is extremely helpful.

Some of the material in this book has already been published in Tanya's many blogs and YouTube videos. However, *Alice & Bob* expands on that information with relatable examples that really drive her points home and then builds on them with so much new, complementary material.

This book was written specifically for anyone interested in securing their web applications. Note that web application security is not strictly the domain of the security department. Software developers should read it. And if you're a penetration tester (or want to be), you should have a firm understanding of how web applications work and how they can be exploited. *Alice & Bob* covers the most common vulnerabilities (i.e., OWASP Top 10) and gives advice on how to mitigate them. Application developers specifically need to understand how their code could be vulnerable and then plan ahead (i.e., ensure that their code is not vulnerable). Penetration testers need to understand the tech behind these flaws so they can try to exploit them. Essentially, you need to know how your adversary thinks in order to defeat them. This book is also useful for anyone working in or considering a career in DevSecOps.

A couple of years ago, my employer needed someone on our security team to start testing our web applications. I was already learning penetration testing, so I jumped on the opportunity. I have done plenty of web development throughout my career, and I really enjoyed it, so application security was a natural fit. I also needed to learn about secure coding. Penetration testers can't just hand developers a list of findings and 500-page scan results and hope for the best. That's an easy way to lose the support of the development staff. Instead, they need to offer suggestions on how to remediate vulnerabilities and then educate developers on the proper ways in which to write secure code. I research the vulnerabilities I discover so I can present our developers with ways in which they can correct the flaws. The research also helps me to state my case when trying to convince a developer, and more importantly senior management, that a vulnerability must be addressed. My research led me more and more to Tanya's blogs. That's when I realized just how great a resource she is. I started using and referring to her blog posts when making recommendations to the developers.

Part I: What You Must Know to Write Code Safe Enough to Put on the Internet
This section emphasizes the importance of developing a solid understanding of information security concepts while giving you a basic security education. Topics include the CIA Triad, threat modeling, defense in depth, and the characteristics of a good application security program. If you work in security, essentially, your job boils down to protecting the **C**onfidentiality, **I**ntegrity, and **A**vailability (CIA) of your data. CIA is referenced throughout the book with examples of how it should be protected.

Other topics in this section include software project requirements as they relate to security, encryption, input validation, third-party components, cookie security, and insider threats; very descriptive depictions of cross-site request forgery (CSRF) and server-side request forgery (SSRF); secure coding and design; a detailed description of OWASP and its offerings; session management, etc.

One very important topic that Tanya spends a lot of time on is the need to use security headers. This section goes into amazing detail on ALL of the security headers and how to configure them.

Part II: What You Should Do to Create Very Good Code
This section takes things a step further with discussions on the importance of secure code review and especially peer review including descriptions of the many types of code review and testing types (e.g., SAST, DAST, SCA, etc.). Also covered is the need to test your applications, database, and infrastructure via manual and automated methods followed by proper (i.e., secure) deployment.

Chapter 7 contains a particularly helpful dissection of a mature application security program, covering essential topics such as application inventory (Can't secure what you don't know exists!), developer education, fully integrating security into the SDLC, and incident response. There's even a brief discussion on the proper tools to use when testing.

Chapter 8 provides an extremely in-depth narrative on what encompasses modern web applications and how to secure them.

Part III: Helpful Information on How to Continue to Create Very Good Code
Alice & Bob culminates with general tips on password management, multi-factor authentication, application inventory, incident response, and other items you can use in your everyday work and life, followed by the appropriately titled *Chapter 10 Continuous Learning*, which emphasizes just that. It gives advice on how to continue your education and grow as a security analyst. It also includes a great template for creating your learning plan. And of course, no guide on security and advancing in the profession would be complete without a mention of soft skills. I've worked with too many people who were technical geniuses but couldn't relate to their co-workers. Having worked as a technical writer for many years, I learned that one of the most important aspects of technical communication is to play to your audience. It's so important that you, as a security analyst, find the proper methods in which to communicate with the other members of your staff (especially senior management) and your clients.

Finally, Chapter 11 ties everything together and correctly states that security is the job of the entire organization and not just the security team. Every member of the organization has a part to play. If you work in security, you have to convince your team, staff, clients, etc., using facts, demonstrations (i.e., proof of concept) and numbers (i.e., costs), that your findings are real and important. There has to be substance behind your motives. Otherwise, you won't be taken seriously.

TL;DR AKA Conclusion
Alice & Bob Learn Application Security is a very well-thought out study guide that will help you learn the many intricacies of application security. I highly recommend it for anyone working (or anyone who wants to work) in web application development, DevOps, DevSecOps, or penetration testing.

You may look at all of this and feel overwhelmed. That's why *Alice & Bob Learn Application Security* was written in such a logical sequence. If you're new, just start at the beginning and work your way through at your own pace. And don't be afraid to ask questions. If you already have experience, take what you need to fill in the gaps.

If you like this book, check out Tanya's website and her YouTube channel.