Hacking APIs: Breaking Web Application Programming Interfaces
BY: Corey J. Ball
Date: 04/29/2024

"Hacking APIs" by Corey J. Ball is a comprehensive guide that focuses on the security of Web Application Programming Interfaces (APIs). The book covers various aspects of API security, from understanding how web applications work to exploring common vulnerabilities and sophisticated attack techniques. It is divided into four main parts: understanding API security basics, building an API testing lab, attacking APIs, and applying real-world hacking techniques on APIs.

Ball's book is exceptional in both its depth and breadth of content. It covers the entire life cycle of APIs, giving readers the necessary tools and knowledge to conduct effective penetration testing against APIs. What sets this book apart is its hands-on approach, which includes numerous practical exercises and examples that simulate real-world scenarios.

The book is meticulously organized, with a logical flow that benefits both beginners and experienced professionals. Each chapter builds on the previous one, gradually increasing in complexity, making the material accessible and allowing readers to develop their skills progressively.

One of the book's strengths is its detailed explanation of essential tools like Postman, Burp Suite, and various other utilities critical for API testing. Ball not only lists these tools but also explains their importance in the context of API security and provides step-by-step guides on how to use them effectively.

However, the book may have some minor flaws. Some readers might find certain sections overly detailed, which could be slightly overwhelming for beginners. Additionally, while the book covers a wide range of topics, the rapid evolution of technology means that readers will need to supplement this book with up-to-date resources to keep up with the latest developments in API security.

The book "Hacking APIs" by Corey J. Ball is an excellent resource for people who want to enhance their knowledge of API security. It provides a comprehensive examination of theoretical concepts along with practical advice to take action. Cybersecurity experts and enthusiasts will find it essential reading. Although the book has a few minor drawbacks, its strengths surpass its weaknesses, making it highly recommended for any cybersecurity library.