Book Report Bonus Assignment
Shriram Karpoora Sundara Pandian

The Web Application Hacker’s Handbook (Finding and exploiting the security flaws)
Author : Dafydd Stuttard and Marcus Pinto

This is one of my favorite books, this book is created for bug bounty hunters, in which their sole purpose is to find the vulnerabilities and try to exploit the vulnerabilities. This book is like the bible for bug bounty hunters who focus on web applications. This book has brief content on how to find vulnerabilities on the web application. The author explained the contents deeper in all the topics. The starting chapter with the Web Application (In) security has basics of web application and how it relates to security in the first place.

Then it covers the defense mechanisms of the websites and tech stacks used in the websites. Especially Mapping the application for both front end and back end. Web Application is the most used and interactive application, it revolves around bypassing client side controls and variables that are included in the client side. While the client sees the webpage, lot of backend and API will work together making the application experience seamless. So the author describes Attacking the authentication and how to attack the session management, which manages the user session and the main intention for this is replay session attack. Backend stores all the important data that is used by the front end, so taking control of that is important as an attacker, so author briefs about attacking the back end components and application logics. In cybersecurity cross site scripting and script forgery attacks are common so that here they are discussed in detail along with other techniques, especially the author teaches how to automate some of the interesting attacks and customize them as per the attacker needs.

All applications have basic architecture and server, author explains about the flow of the architecture and how to get access to the server. Teaches about access control and attack tools for finding the vulnerabilities at the base code which is source code of the application. Especially source code that doesn’t have proper input validation and path traversal. At the end the author introduces about the hacker’s toolkit and methodologies attacker should use and evolve about time and application security increase.

This book is written very well and very popular among the bug hunters community because everyone starts bug bounty with web applications and give lot of learning for bug hunters. The author conversed well in this book like he is teaching in person. The special thing about this book is it is beginner friendly and the author didn’t use complex words, even though some of the concepts get complex in this book, the author gives a brief introduction and explanation and stacks up the advanced topics on top, which makes it a good beginner friendly book. Lots of screenshots and appropriate external resources are added here and there for additional clarity and research. This book have good online support and community which makes it special.

Overall these are the reasons and the speciality of the book makes it a popular choice for learning web vulnerabilities and eventually help us learn everything web applicaitions.