Disclaimer!

The word “hacker” to some means when someone acts maliciously such as hacking into a bank and stealing money. Some will use terms such as “Whitehat” (‘good’ hacker) and “Blackhat” (‘bad’ hacker) to determine the difference however times have changed and the word hacker should not be used to solely describe someone acting in a malicious manner. **This is what you call a criminal. We are not criminals. We are bug bounty hunters**. Throughout this guide you will see the word “hacker” being used and I want to make it clear that when we use the word “hacker” we are not describing someone acting maliciously or illegally.

The information provided in this methodology is intended for legal security research purposes only. If you discover a vulnerability accidentally (these things happen!) then you should attempt to responsibly report it to the company in question. The more detail the better. **You should never demand money in return for your bug** if they do not publicly state they will reward, this is extortion and illegal.

Do **NOT** purposely test on websites that do not give you permission to do so. In doing so you may be committing a crime in your country.

This methodology is not intended to be used for illegal activity such as unauthorised testing or scanning. I do not support illegal activity and do not give you permission to use this flow for such purposes.

The contents of this book are copyrighted to the author Sean Roesner (zseano) and you do not have permission to modify or sell any of the contents.

zseano’s methodology can only be found on https://www.bugbountyhunter.com/