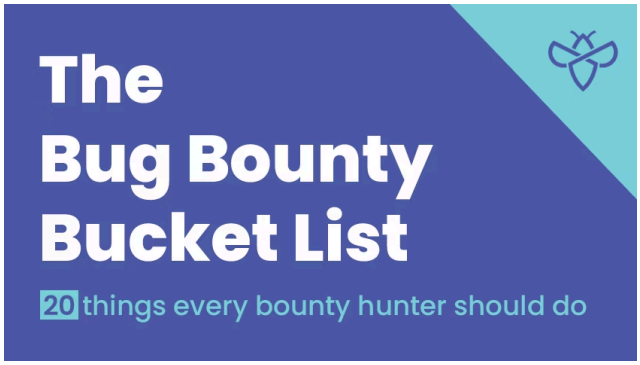
The Bug Bounty Bucket List

BY INTIGRITI · JULY 1, 2019 · LAST UPDATED ON MARCH 6, 2025



Summer vacation has started and this is the ideal moment to sharpen some of your bug bounty skills. We've made a bucket list with 20 actionable goals for the summer break – how many can you scratch off?

1. **Find a blind XSS in something else than a contact form.** There are lots of potential vectors to insert your blind XSS payloads: your user agent, an e-mail, a file, … Instead of testing with standard payloads, always test with blind payloads because you never know where they end up!

2. **Revisit your old reports and celebrate the improvements you've made. It is sometimes hard to notice your own personal growth and achievements, so take a moment to look back. At the same time, you can retest the vulnerabilities you have submitted and see if there are any regressions!**

3. **Get a bug chain involving at least three vulnerabilities.** There is nothing more fulfilling as successfully chaining a couple of low-severity bugs into a high impact chain. If open redirects are out of scope, do keep track of them! You might need them later when exploiting an SSRF vulnerability.

4. **Find at least one zero day.** Do you see an application running open source software? Remember that every software has bugs and this will be no exception. Try to score at least one CVE this summer – you may be able to score multiple bounties with it!

5. **Go for a hacker movie night. If you've been looking at Burp Suite for hours in a row, then remember that hacking does not have to be boring! An ideal break in between hacking sessions is a hacker movie night, with movie classics like Who Am I, Untraceable, Blackhat, The Matrix, Hackers, Swordfish & Mr Robot.**

6. **Learn GraphQL. GraphQL is an amazing query language from Facebook, but due to its complexity, it is often a challenge to implement it in a secure manner. We would recommend everyone to read this Detectify article on GraphQL abuse.**

7. **Learn how to pwn some buckets**. This goal can't be missing on a bucket list! AWS access control settings are complex and are susceptible to a wide range of attacks. Make sure to read Detectify's "A Deep Dive in AWS S3 Access Controls" and educate yourself!

8. **Learn a new programming language**. As the software development landscape evolves, bounty hunters have to adapt. New programming languages are introduced every year and new types of vulnerabilities emerge with them. The early bird catches the worm, so always be on the lookout for security issues in new products!

9. **Find a postmessage XSS.** Once you're aware of their existence, PostMessage XSS'es are relatively easy to spot and fun to exploit. Read Detectify's post on the pitfalls of PostMessage, pick a random bug bounty program and take a look through their javascript files!

10. **Give a presentation at a conference.** Even if it's just a local OWASP chapter meeting, giving a presentation at a conference can help order your thoughts, research and boost your self-confidence. Check https://www.cfptime.org for a list of available conferences to apply for!

11. **Attend a conference.** If you don't feel comfortable speaking at a conference, just go as an attendant! Don't forget to socialise with other hackers, the best way to learn new skills is to talk and listen to people that are passionate about it!

12. **Participate in a CTF.** Very often, you will encounter scenarios from CTF's in the wild. Capture the flag contests are a fun way to sharpen your skills and to learn to collaborate. We would recommend it to every bug bounty hunter!

13. **Drop your tools for a day.** If you're stuck on a target, close Burp for a day and see what you can get from manual recon! Limiting your toolset can force you to look at your target from a different perspective and get more creative, resulting in more unique vulnerabilities!

14. **Write a blog article.** Sharing is caring! Help your peers by sharing unique or interesting findings you have found. Always make sure you get a program's permission before you do a blogpost!

15. **Bingewatch** LiveOverflow & PwnFunction. Both channels offer great explainer videos on hacking and are very effective to learn more about information security in a fun and accessible way!

16. **Create a tool**. Why would you spend your valuable bug bounty time on things that can easily be automated? Write a tool or fork one on GitHub — nothing pays off as much as getting bounties from tools you have written!

17. **Read a book.** It's a great way to get your eyes off the screen for a second. We recommend the Web Application Hackers Handbook, Web Hacking 101 and Real-World Bug Hunting: A Field Guide to Web Hacking

18. **Work out.** Working out can be a great source of fresh inspiration! Stimulate your brain during your workout sessions by listening to podcasts from Pentesterland.

19. **Try some whitebox testing**. Decompile an Android app using Dex2Jar and start debugging with Frida, or take a look at some of the open source bug bounties hosted by the European Commission.

20. **Go for business logic.** Business logic flaws are often overseen in security audits as they are often complex and unique for every asset. Give yourself a moment to read the documentation and understand the business processes behind the application. Not a lot of bug bounty hunters look into business logic flaws, so it could be a good idea to spend some time researching them!

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com