HOW TO GET STARTED IN BUG BOUNTY (9+pro tips)

STÖK Follow
Jan 27 · 5 min read

If you are a infosec beginner or a “bounty curious” leet hacker. This is the post for you! Iv been asked this question more than once and decided to answer it in a vlog simply by telling my story, and sharing tips that i found usefull along the way.

text is cool, video is cooler..

March 2018, india,…

So there I was in a hotel room, after a few beers, somewhere in India primarily the Goa region for the annual Nullcon conference. I was there to vlog, not to hack. So I asked Jobert (one of the founders of HackerOne) Who was hacking away on a target with Frans Rosén (one of the founders of Detectify) in Ted Kramer’s room.

Jobert! How do you do you get started in this web hacking thing?

And for the first time in my life, he showed me a 100mb big chunk of a jar file that from that day on would change my life forever. The application he then showed me was Portswiggers Burp Suite, and I fell love with it, head over heals. A tool that I have been using more or less on a daily basis ever since.

While i was staring at the application with all its tabs and weird code content, he said.

“*Pick one bug and learn as much as you can about that vulnerability and start looking for it, everywhere*”

So I looked up the owasp top 10, and some other sites and decided, since I know A lot about infrastructure design, but can’t code for shit, il choose race conditions. And in a few weeks i found my first ever race condition bug. And I was nervous, i didn’t know how or what a successful report looked like.

> ***But I had been told that "POC och GTFO".***

In other words.

Show how you can exploit the bug in easy and reproduceable steps, so that the triage'er that's going to verify your finding and that might not have your level of expertise in this precise area, can follow your step by step instructions to reproduce the bug.

I can't express this enough. Before you submit a bug always ask yourself:

> ***"How can an attacker use this against the organization"***
> *What's the real impact here. And how can I exploit it?*

Triagers (who are humans aswell, yeah I know its weird, but they are, and guess what, they are kinda cool ppl too) are daily being saturated with "crap" reports, and to make sure that your report stands out, Always create a "proof of concept" where you explain AND show how you can exploit the bug , and in some chases even chain it into something.. well terrible..

Because if you are reporting a "bug" that a disclosed version of a service (lets say apache) has "whatever" kind of known CVE's, without any proof on how you would exploit them.

Its kinda more or less like saying:

> **“An attacker could potentially steal all the money in this banks vault since the clerk is running Windows XP on their cashier box.”**

YES, We all know how crappy XP is and how easy it is to pwn, if left unhardened, but simply seeing is that its XP and knowing that its potentially pwnable, doesn’t mean that the bank hasn’t hardened and isolated that cashiers box from the vault infrastructure..

And without any expoit-chain or actual impact, your report, that you worked really hard on producing, will turn informative. That means that you will loose valuable rep/kudos and since its super important especially if you want to get some private invites. A good report with a easy step by step and a real world attack scenario, is key..

Choosing your targets…

So how do I choose my targets? Well im not mayflowering anything anymore. I used to do that in the beginning, totally useless for me. I know for sure that leet haxx0rs like frans that’s been around for years easily can jump around on progams and find epic bugs. But not me, im still in the learning phase. So iv choosen a few programs with big enough scopes to keep me busy for the next year or so. And i have decided to stay loyal to those programs, learning how their development cycles works, learning how their infrastructure is designed, and learn as mutch as I can about their codebase and staying updated when then push code or release new features.

Takeaway. If your serious in getting into bounty's, and you want to have the chance to show your skills on some of the most hardened targets on the market. Then get yourself a paid burp pro license. "Don't larry lau that shit" And remember, there is no silver bullet, there is no easy fix. You are the one that have to do all the work. So Invest in yourself!.

Study others reports, rest, study writeups, rest, hack on cool targets and rest.

Also do remember, karmas a bitch, if you gained something from the community, if you learned anything worth sharing. Then give back, and the community will give back to you..

This are the tips/pointers I give to anyone that's new to webapptesting.

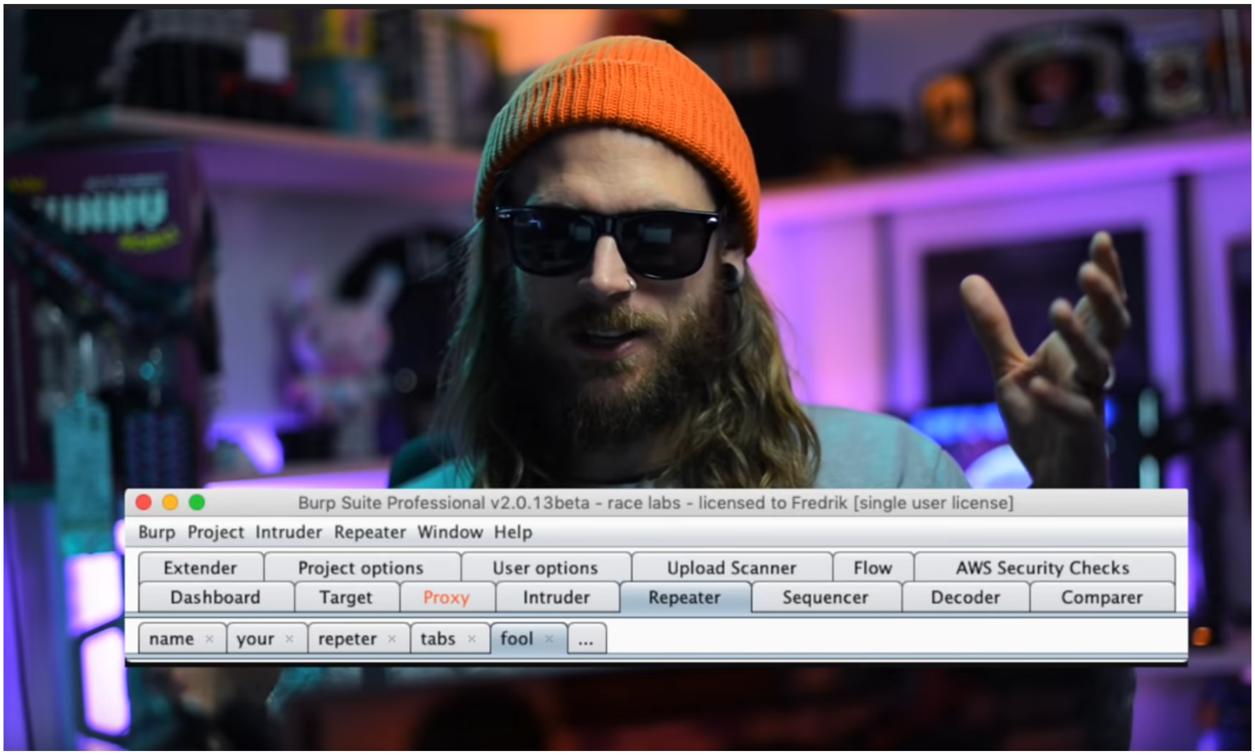
1. **Buy peters book: https://leanpub.com/web-hacking-101**
2. **Check out my website for loads of cool educational videos. https://www.stokfredrik.com**

3. **Watch anything you can from Jason haddix just google it.**
4. **Watch all the tutorials and do the ctf on https://hacker101.com**
5. **Watch everything on www.bugcrowd.com/university**
6. **Sign up for Pentesterslabs https://pentesterlab.com/referral/0gk6uq0ajrd38Q**
7. **Sign up for Hackerone.com, Bugcrowd.com or any other BB platform.**
8. **Get a Burp pro license, its way better than getting a "ethical hacker course"**
9. **Find a program that you like and vibe with, its more fun to hack on a program or brand you like.**
10. **Don't waste time on VDP's**
11. **Don't be discouraged that everyone else has automated everything, its just not true.**
12. **Always approach a target like you're the first one there. Your view is unique.**
13. **Remember, Zero days can be new bugs in old code. Tavis has shown that over and over again.**
14. **BE PROUD OF YOURSELF! YOU DID THIS!**

Also.. we are all just a bunch of hackers that loves to haxx and wants to make a buck, so no need for the drama.

Until we meet again. I love you ❤

//STÖK



i just added this picture as a easteregg, you do label you repeter tabs right? And to get a ”cool thumbnail” yeah, yeah,. i know,.,. ❤