

What You Need To Know About Bug Bounties

BY UNCLE RAT



Agenda

- ▶ Bug bounties is not hunting bugs
- ▶ Bug bounties is not the same is hacking or pentesting
- ▶ Bug Bounties are not a reliable way of getting money
- ▶ Bug Bounties is NOT exploitative of researchers



Bug bounties is
not hunting bugs

<https://t.me/learningnets>



Bug bounties is not hunting bugs

- ▶ Bug bounty hunting is the wrong name
- ▶ More relevant: Testing a target against an advanced hunters skill
- ▶ What we don't do
 - ▶ Hunt for bugs
 - ▶ Hunt for money
- ▶ What we do
 - ▶ Test a target
 - ▶ That has already been tested before
 - ▶ Against our skill level and methods



Bug bounties is
not the same is
hacking
or pentesting

<https://t.me/learningnets>



Bug bounties is not the same is hacking or pentesting

- ▶ Pentesters are the first to test a target
- ▶ Bug bounty hunters come last in line
 - ▶ Sometimes very late if a program has existed for a long time
- ▶ We can't think the same way as a pentester
 - ▶ Pentesters CAN use a set methodology
 - ▶ We can not
 - ▶ We need to adept and overcome
- ▶ Our hacking skills WILL fill in the gaps where other hackers failed



Bug Bounties are
not a reliable
way of getting
money

<https://t.me/learningnets>



Bug Bounties are not a reliable way of getting money

- ▶ Even if you are the best hunter ever
- ▶ Even if you are finding consistent bugs
- ▶ Even if you are finding consistent non duplicates
- ▶ Even then, the company can take a while to pay out

- ▶ If you want to go full time
 - ▶ First test your skill
 - ▶ Think in bigger timeframes, monthly wages are no more
 - ▶ Be prepared to make less than when you were full time employed



Bug Bounties is
NOT exploitative
of researchers

<https://t.me/learningnets>



Bug Bounties is NOT exploitative of researchers

- ▶ You don't have a contract with the company to pay you
- ▶ You don't have to test your target
- ▶ You are not hunting for bugs

- ▶ You are hacking a live target, this is a priviledge
- ▶ You are testing your skills against a real product
- ▶ You are getting rewarded for securing your target

