Ethical Student Hackers

Bug Bounties

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

- Relevant UK Law: https://www.legislation.gov.uk/ukpga/1990/18/contents

Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf

What are Bug Bounties?

Basic Flow

Pick a Program

Find a Bug

Write a Report

Submit

Get Rewarded

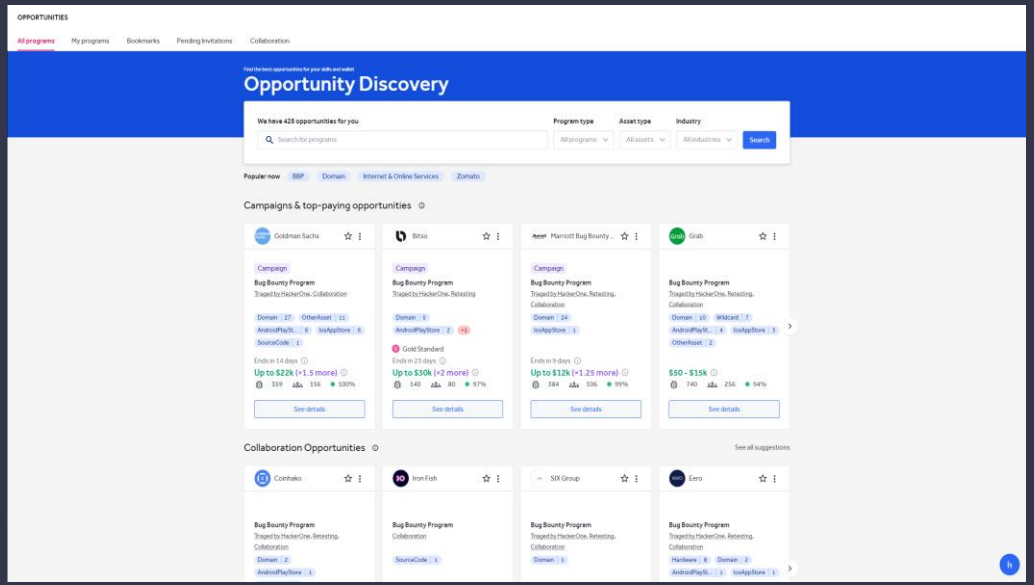
And stay in scope the whole time

A lot of companies, most of them you use on a daily have these bug bounty programs.

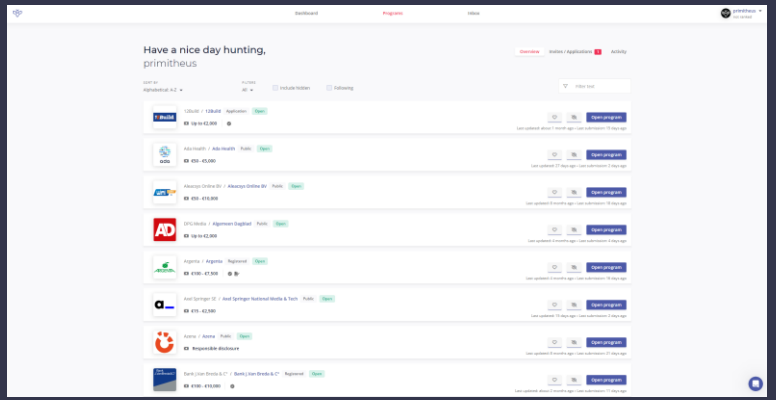
…And so on

Platforms

Hackerone



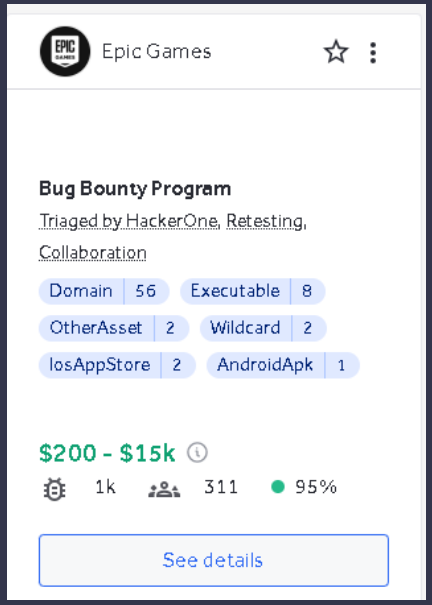
Intigriti

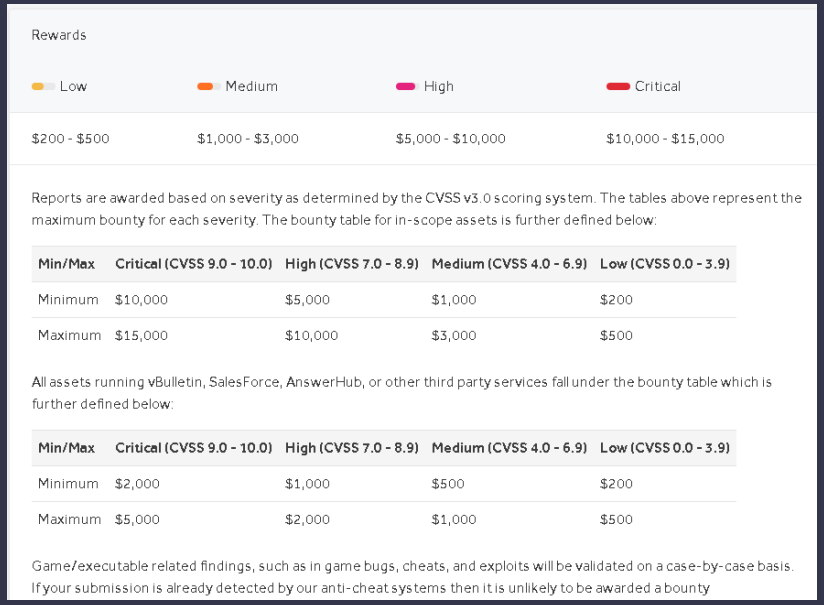


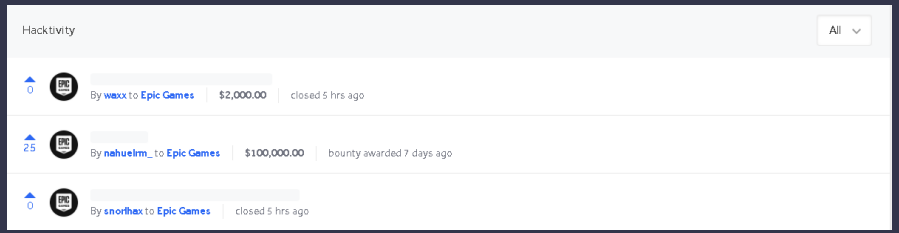
Among a selection of other platforms such as Bugcrowd

Example of A Bounty

- Lists the Assets such as Domains, Executable, Android APKs etc.
- Reports are split into severity of the bug.
- You can see the “Hacktivity” tab which displays the most recent bug reports. Sometimes they will disclose what was submitted, most of the time they won’t (for obvious reasons)







Misconceptions and Mistakes

“There are millions of hackers and they’re all more skilled than me, I’ll never find a bug.”
“These companies are so big, they would’ve plugged up any easy vulnerabilities to find.”

Going for the money

Money is great, but never go for the money.
Build up your skills. Learn and understand the
The vulnerabilities, develop a workflow that works for you.
If you make money that’s just a plus.

SCOPE !

- The important thing we have is consent! And we want to keep it.
- As long as you stay in scope, you're safe. Stepping out of scope, even with good intentions, you're just breaking the law.

- Example of the scope of Eero https://hackerone.com/eero?type=team

Finding a Bug

Reconnaissance

In this stage, you're finding assets or points of exploitation such as subdomains, parameters or queries. You want to know where you're exploiting, but also, you're wanting to take a deeper look into the actual product you're trying to exploit. Understanding how it works is essential.

Finding an Exploit

Know you're exploits https://owasp.org/www-project-top-ten/ try to stay specific.

Escalation

If you can escalate the bug you have found, wonderful! But stay in the scope. If not then explain how this bug might lead to an escalated problem in your report.

You've Found a Bug

- Write a detailed report.

Your report is the most important thing in this process. You want your report to be very easy to follow and allow anyone reading it to be able to reproduce the bug you have found. And if you want to be rewarded, you must explain the severity and significance of what you have found.

You want to convince them that what you have found is a problem and it is worth fixing.

Doesn't necessarily have to be a long report.

Example

Abdelrhman Badr <mb.abdelrhman@gmail.com>
to admin

Thu, Jun 30, 2022, 7:50 AM

Good Morning,

Parameter "ReturnUrl" is vulnerable to CRLF, allowing an attacker to inject their own headers in a server response.

An example is shown below.

The filter on ReturnUrl is bypassed by using "%E5%98%8A".

Kind Regards,
Abdelrhman

CraignDave <admin@craigndave.co.uk>
to me

Thu, Jun 30, 2022, 1:36 PM

Hi Abdelrhman,

Every day's a school day :)
Many thanks for exposing that one for us. We have a patch in test now that will be going live tonight unless something unforeseen occurs.
I'll drop you a note when it's live and if you could give it a poke for us to double check that would be very much appreciated.

We don't have an official bug-bounty scheme but if there's anything that takes your fancy on our merch store (a hoody and a mug for example) then please let us know and we'll sort that out for you.
https://shop.craigndave.org/product-category/merchandise

Alternatively we can offer you an equivalent value in amazon vouchers if you prefer.

Many thanks,
Mark

Tools & Resources

- https://github.com/tomnomnom/assetfinder Great for Recon.
- https://portswigger.net/burp BurpSuite is your best friend for testing on domains.
- Time! Learning and testing could take up a lot of time so don't be discouraged if you feel like you'll never find a bug. You'll eventually find something because there are infinitely many bugs out there.

- https://hackerone.com Most popular bug bounty platform & Great CTFs to get you started.
- https://owasp.org/ Learn about most common vulnerabilities and their uses.
- https://www.youtube.com/@STOKfredrik STÖK – Informative Guides (quit but still great)
- https://www.youtube.com/@NahamSec NahamSec – Informative Guides
- https://www.youtube.com/@LiveOverflow LiveOverflow – Deep dives into reports and vulnerabilities.

Make Your Account

https://hackerone.com/sign_up

Any Questions?

www.shefesh.com

Thanks for coming!