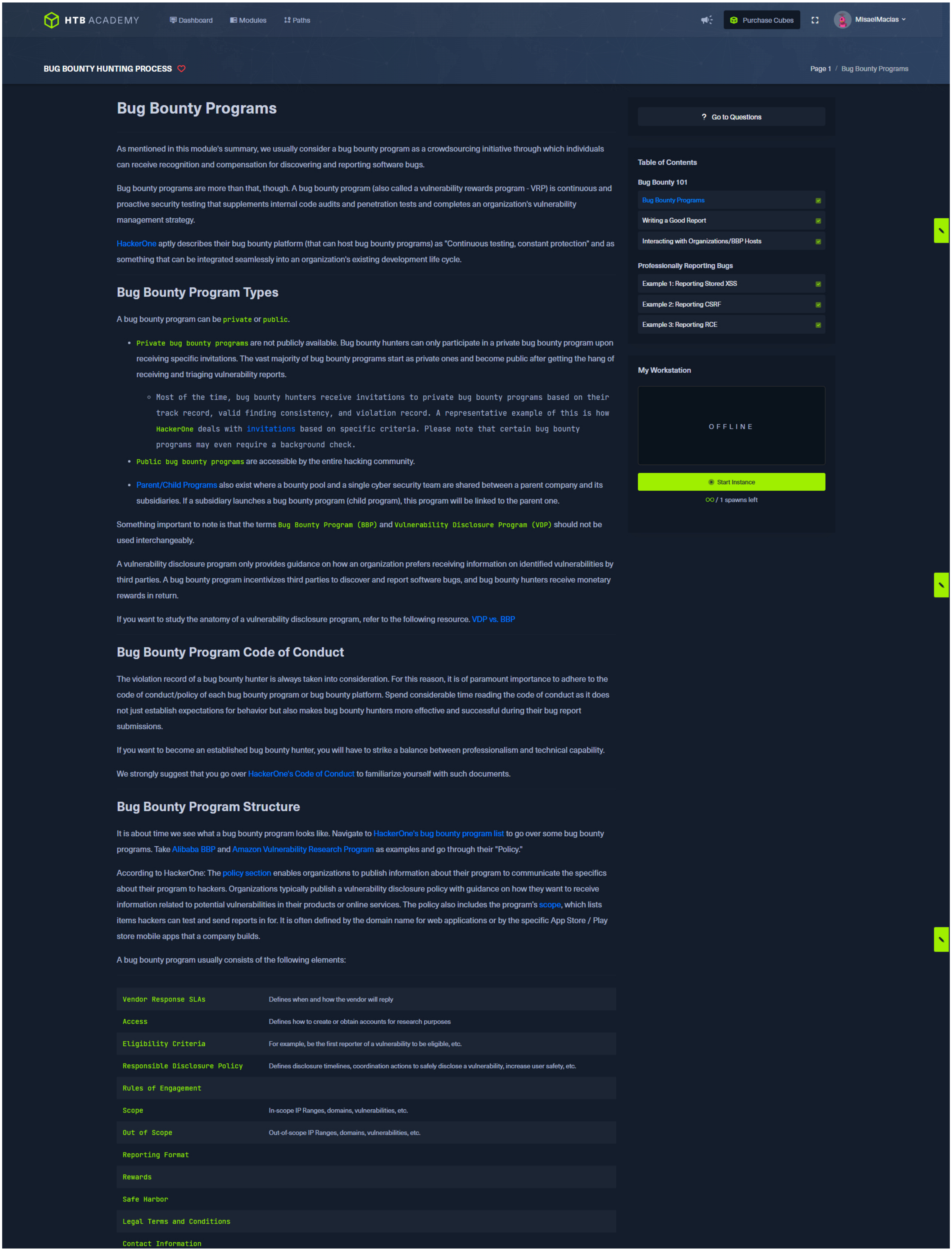


Bug Bounty Programs

As mentioned in this module's summary, we usually consider a bug bounty program as a crowdsourcing initiative through which individuals can receive recognition and compensation for discovering and reporting software bugs.

Bug bounty programs are more than that, though. A bug bounty program (also called a vulnerability rewards program - VRP) is continuous and proactive security testing that supplements internal code audits and penetration tests and completes an organization's vulnerability management strategy.

HackerOne aptly describes their bug bounty platform (that can host bug bounty programs) as "Continuous testing, constant protection" and as something that can be integrated seamlessly into an organization's existing development life cycle.

Bug Bounty Program Types

A bug bounty program can be `private` or `public`.

- `Private bug bounty programs` are not publicly available. Bug bounty hunters can only participate in a private bug bounty program upon receiving specific invitations. The vast majority of bug bounty programs start as private ones and become public after getting the hang of receiving and triaging vulnerability reports.
    - Most of the time, bug bounty hunters receive invitations to private bug bounty programs based on their track record, valid finding consistency, and violation record. A representative example of this is how `HackerOne` deals with invitations based on specific criteria. Please note that certain bug bounty programs may even require a background check.
- `Public bug bounty programs` are accessible by the entire hacking community.
- Parent/Child Programs also exist where a bounty pool and a single cyber security team are shared between a parent company and its subsidiaries. If a subsidiary launches a bug bounty program (child program), this program will be linked to the parent one.

Something important to note is that the terms `Bug Bounty Program (BBP)` and `Vulnerability Disclosure Program (VDP)` should not be used interchangeably.

A vulnerability disclosure program only provides guidance on how an organization prefers receiving information on identified vulnerabilities by third parties. A bug bounty program incentivizes third parties to discover and report software bugs, and bug bounty hunters receive monetary rewards in return.

If you want to study the anatomy of a vulnerability disclosure program, refer to the following resource. VDP vs. BBP

Bug Bounty Program Code of Conduct

The violation record of a bug bounty hunter is always taken into consideration. For this reason, it is of paramount importance to adhere to the code of conduct/policy of each bug bounty program or bug bounty platform. Spend considerable time reading the code of conduct as it does not just establish expectations for behavior but also makes bug bounty hunters more effective and successful during their bug report submissions.

If you want to become an established bug bounty hunter, you will have to strike a balance between professionalism and technical capability.

We strongly suggest that you go over HackerOne's Code of Conduct to familiarize yourself with such documents.

Bug Bounty Program Structure

It is about time we see what a bug bounty program looks like. Navigate to HackerOne's bug bounty program list to go over some bug bounty programs. Take Alibaba BBP and Amazon Vulnerability Research Program as examples and go through their "Policy."

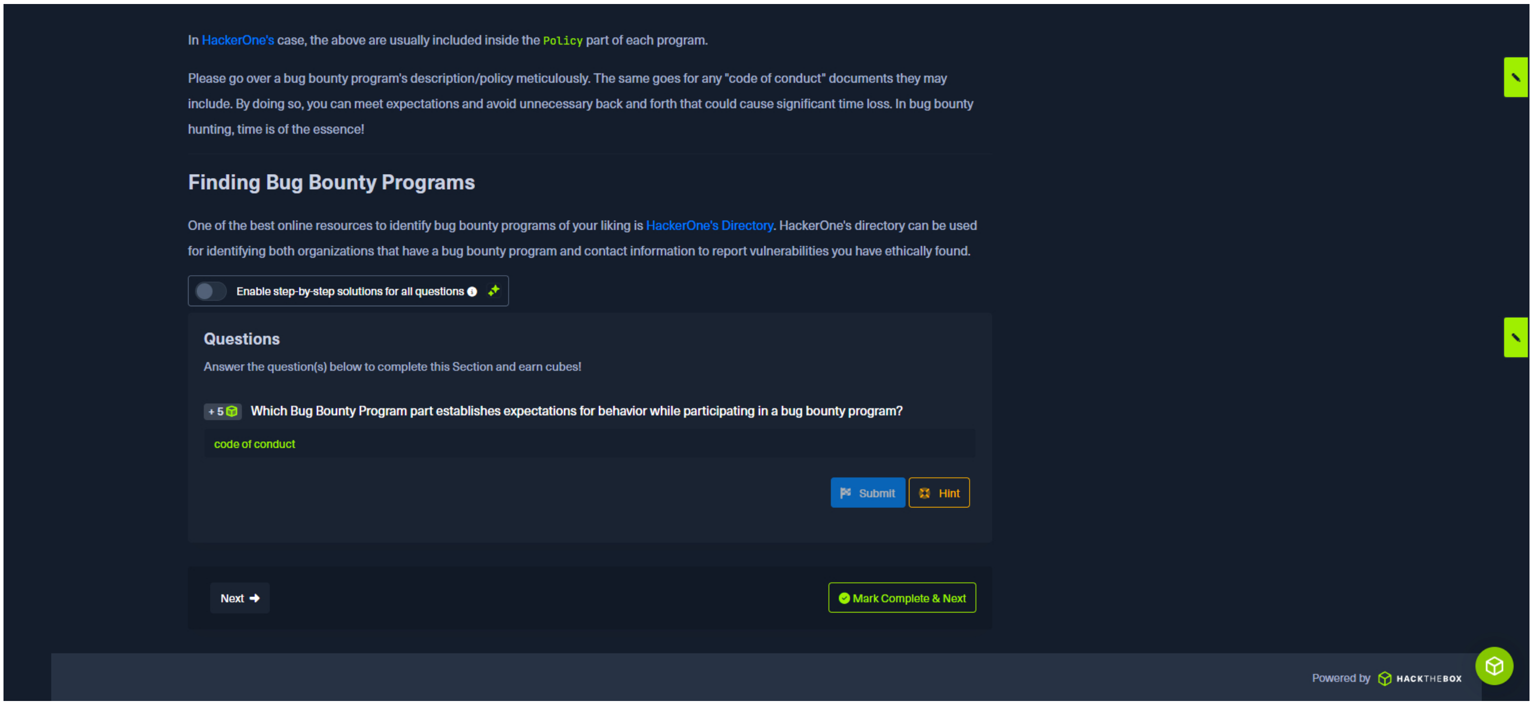
According to HackerOne: The policy section enables organizations to publish information about their program to communicate the specifics about their program to hackers. Organizations typically publish a vulnerability disclosure policy with guidance on how they want to receive information related to potential vulnerabilities in their products or online services. The policy also includes the program's scope, which lists items hackers can test and send reports in for. It is often defined by the domain name for web applications or by the specific App Store / Play store mobile apps that a company builds.

A bug bounty program usually consists of the following elements:

`Vendor Response SLAs`	Defines when and how the vendor will reply
`Access`	Defines how to create or obtain accounts for research purposes
`Eligibility Criteria`	For example, be the first reporter of a vulnerability to be eligible, etc.
`Responsible Disclosure Policy`	Defines disclosure timelines, coordination actions to safely disclose a vulnerability, increase user safety, etc.
`Rules of Engagement`	
`Scope`	In-scope IP Ranges, domains, vulnerabilities, etc.
`Out of Scope`	Out-of-scope IP Ranges, domains, vulnerabilities, etc.
`Reporting Format`	
`Rewards`	
`Safe Harbor`	
`Legal Terms and Conditions`	
`Contact Information`	

Table of Contents

My Workstation



In HackerOne's case, the above are usually included inside the `Policy` part of each program.

Please go over a bug bounty program's description/policy meticulously. The same goes for any "code of conduct" documents they may include. By doing so, you can meet expectations and avoid unnecessary back and forth that could cause significant time loss. In bug bounty hunting, time is of the essence!

Finding Bug Bounty Programs

One of the best online resources to identify bug bounty programs of your liking is HackerOne's Directory. HackerOne's directory can be used for identifying both organizations that have a bug bounty program and contact information to report vulnerabilities you have ethically found.

○ Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

+5 Which Bug Bounty Program part establishes expectations for behavior while participating in a bug bounty program?

code of conduct