# **Anatomy of a Bounty Brief**

The bounty brief outlines the rules of engagement for a bounty program, setting expectations for the program owner and researchers throughout the process. It's your responsibility to write a concise, unambiguous brief, and the researcher's responsibility to read and understand it before working on the program.

Your Bugcrowd team will guide you through the brief development process, but in the meantime, this guide will help you get you started.

# Scope

The single most important thing that you can do to ensure a successful program is to define a clear scope, leaving nothing open to interpretation. A bounty's scope informs the researchers what they can and cannot test, and points them to key targets. There's a careful balance to strike when considering how permissive your program's scope should be - start by evaluating your attack surface, your unique goals and these considerations:

- · Too narrow of a scope may result in coverage and testing gaps (creating a false sense of security), or may signal to researchers that it's not worth their time.
- A vague or incomplete scope may lead to lost testing time while researchers ask verification questions, or worse, create conflict and disagreement regarding the acceptability of valid submissions.
- An overly broad scope may create unwanted noise, and may distract resources and time constrained researchers from focusing on what you really care about.

#### Focus

Let the researchers know what's important to you and draw attention to it. Many of our customers running ongoing programs offer additional bonuses for valid submissions on these critical targets. Focus areas may include specific bug types, specific functionality, new features, or whatever you feel needs special attention. For complex or unintuitive targets, be sure to provide documentation for the target - so as to assist researchers in working on the targets guickly and effectively.

# 

It's also important to explicitly call out what is not in scope, or you may end up with frustrated researchers who expect to get paid for a vulnerability found on an otherwise "In Scope" target. The most common example listed as "Out-of-Scope" are hosts that resolve to third-party services. Researchers are penalized for making Out-of-Scope submissions, so it is important to set accurate expectations of what is not reward-able before they begin testing.

# Exclusions

Encourage good behavior and guide researchers in the right direction by accurately articulating any exclusions to your program's scope. Bugcrowd's templated 'out-of-scope' list excludes many vulnerabilities that can be easily picked up by scanners or automated testing methods that you're likely already using as part of your development process. Also, be sure to mention things that might be intended functionality (e.g. XSS via an HTML editor), things that are accepted business risks, known issues, and whether or not you'll accept issues that result from pivoting. Also, remember to review and modify the 'standard exclusions' list to include any low hanging fruit (spf records, etc) that you don't want included in findings.

Ultimately, what you choose to exclude is your call, but keep in mind that it's worth reviewing your standard exclusions upfront, as your bounty brief is a work agreement between you and the researcher. Make sure it is complete to ensure a successful program!

### 000



### **Program Details**

We strive to keep abreast on the latest state-of-the-art security developments by working with security researchers and companies and appreciate the community's efforts in creating a more secure world.

#### Targets

*.domain.com	1		
API			
MISC applica	tions		

Please explain your listed targets. Leave nothing to interpretation - and be sure you know and understand your attack surface.

#### Focus Areas

Use this space to draw attention to the things you care about. For instance, if you want researchers to focus on testing the API, mobile app, specific functionality (e.g. payment processing), or targets

#### Out-of-Scope

Use this area to talk about what you don't care about. Be sure to mention things that might be intended functionality (e.g. XSS via an HTML editor), things that are accepted business risks, known issues, and whether or not you'll accept issues that result from pivoting

#### The following finding types are specifically excluded from the bounty:

Please be sure to review these standard exclusions to ensure that they're things that you don't care about -- additionally, you're free to add to this list as you see fit

- Descriptive error messages (e.g. Stack Traces, application or server errors)
- HTTP 404 codes/pages or other HTTP non-200 codes/pages.
- Fingerprinting / banner disclosure on common/public services.

- etc.

#### Rewards:

Rewards are administered according to the following guidelines:

- XSS: \$XXX-\$XXX
- CSRF: \$XXX-\$XXX
- SQL: \$XXX-\$XXXXX

- Etc

#### 

This bounty follows Bugcrowd's standard disclosure terms

### •Rewards

In order to meet your organization's unique goals, there are a variety of ways to peak the interest of researchers - brand recognition, interesting targets, leaderboard recognition, and of course, cash rewards

We encourage all customers to offer cash rewards, as in general, programs with higher minimum rewards and/or higher reward ranges are more likely to receive more attention. Our Defensive Vulnerability Pricing Model provides baseline recommendations on what to pay based on security maturity and submission priority.

For more mature programs, we also encourage defined program rewards for vulnerability types based on priority. For guidance, see the Bugcrowd Vulnerability Rating Taxonomy.

## ··Disclosure + Rules

• •

• • • •

• •

. .

. .

• •

While Bugcrowd believes public disclosure to be • an important part of the vulnerability reporting ecosystem and encourage our customers to work with researchers to disclose issues once a fix is • released, we support our customers' individual disclosure policies.

Coordinated Disclosure is the default recommended policy for all new public programs, and is strongly recommended but optional for ongoing private bounty programs. In this model, program owners commit to allowing researchers to publish mutually agreed information about the vulnerability after it has been fixed. With Coordinated Disclosure, researchers can externally disclose limited or full disclosures approved by program owners.

 Lastly, consider your business' unique use cases • For example, do you need to add additional rules to your program that don't fall into one of the aforementioned categories?