Anatomy of a Bug Bounty Brief

A handy infographic that guides you when developing your brief

1 Organization name

3 Focus areas

This is a great opportunity to let hackers know what's important to you and draw attention to it.

Focus areas highlight:

- Areas of concern or critical functionality
- New features/functionalities
- Overlooked or complex targets

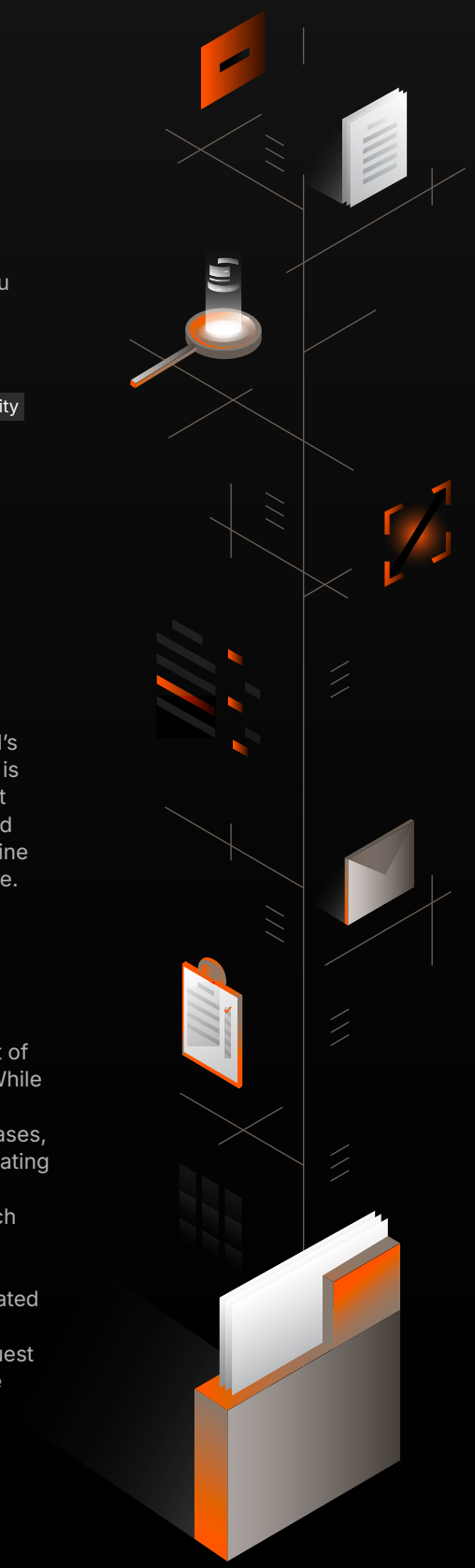
5 Exclusions

Guide hackers in the right direction by clearly stating any exclusions to your engagement's scope. Bugcrowd's Vulnerability Rating Taxonomy (VRT) is a great resource for vulnerability best practices. We specifically recommend adding P5 vulnerabilities as the first line under your exclusions to reduce noise.

7 Disclosure and rules

Public disclosure is an important part of the vulnerability reporting process. While we respect each customer's specific disclosure policies and unique use cases, we nonetheless recommend collaborating with hackers to transparently share resolved vulnerabilities. This approach fosters goodwill and strengthens relationships within the hacker community. That being said, coordinated disclosure is the default policy for all new engagements. Hackers can request to disclose their submission once the vulnerability has been fixed.

bugcrowd



2 Scope

It's critical to define a clear and available scope, leaving nothing open to interpretation. Ensure your engagement stands out by evaluating your attack surface and unique goals and creating a compelling bounty scope that motivates hackers. Design a compelling bounty brief by:

- Opting for a wide scope
- Offering large rewards
  (ideally with wildcarded domains)
- Answering questions before they can be asked; it's best to be as informative as possible

4 Out of scope

What is out of scope is just as critical as what is in scope. Mention:

- Third-party services
- Areas of your scope that may be exceptions to in scope
- Similarly named/geographically operated locations

6 Rewards

To meet your organization's unique goals, aim to pique hackers' interest—increase brand recognition, create interesting targets, build rapport with the community, offer leaderboard recognition, and of course, give cash rewards.

We strongly encourage all customers to offer cash rewards, combined with a strong, well-thought-out scope, for an ideal engagement. Don't know where to start with reward payouts? Check out our recommended bounty reward ranges.

Ultimately, your bounty brief is a work agreement between you and the hacker. Make sure it's complete to ensure a successful engagement.