What's in a Program?

In this lesson, we'll study what a bug bounty program looks like.

We'll cover the following

What is a bug bounty program?

A BBP is a call for help from an organization, reaching out to security researchers worldwide. The organization lays out the scope and terms of the program, fundamentally allowing security researchers to probe their systems and software in exchange for a financial reward.

If researchers find a vulnerability in an application, they can submit it and, if the organization finds the submission acceptable, receive a bounty as a reward.

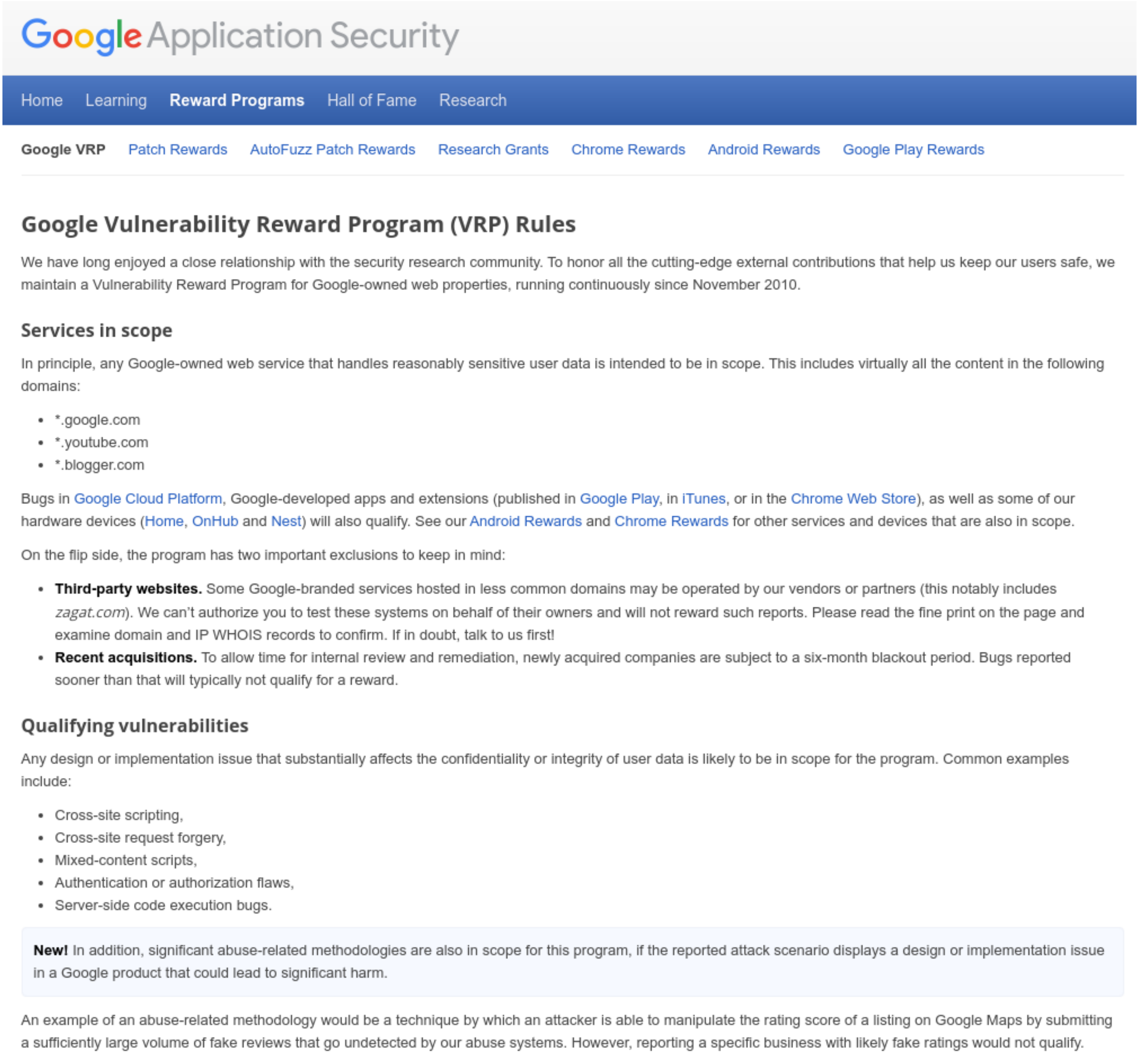
What is a valid submission?

It is worth noting that there is no general definition of what makes a submission acceptable, as each program has different rules and terms for valid submissions. For example, Google has a program named *"Google Vulnerability Reward Program (VRP) Rules"* which states valid reports could include:

- Cross-site scripting
- Cross-site request forgery
- Mixed-content scripts
- Authentication or authorization flaws
- Server-side code execution bugs

While it unequivocally states exclusions, which are alleged vulnerabilities that do not qualify as valid submissions, meaning researchers will be turned down when submitting them. Some examples include vulnerabilities in `*.bc.googleusercontent.com` or `*.appspot.com` as well as flaws affecting the users of out-of-date browsers and plugins.

Google goes beyond simply listing the exclusions, as it also provides the reasoning behind their choice. For example, vulnerabilities in `*.bc.googleusercontent.com` are excluded because, "*these domains are used to host applications that belong to Google Cloud customers. The Vulnerability Reward Program does not authorize the testing of Google Cloud customer applications. Google Cloud customers can authorize the penetration testing of their own applications, but testing of these domains is not within the scope of or authorized by the Vulnerability Reward Program.*"



Google Vulnerability Reward Program (VRP) Rules

We have long enjoyed a close relationship with the security research community. To honor all the cutting-edge external contributions that help us keep our users safe, we maintain a Vulnerability Reward Program for Google-owned web properties, running continuously since November 2010.

Services in scope

In principle, any Google-owned web service that handles reasonably sensitive user data is intended to be in scope. This includes virtually all the content in the following domains:

- *.google.com
- *.youtube.com
- *.blogger.com

Bugs in Google Cloud Platform, Google-developed apps and extensions (published in Google Play, in iTunes, or in the Chrome Web Store), as well as some of our hardware devices (Home, OnHub and Nest) will also qualify. See our Android Rewards and Chrome Rewards for other services and devices that are also in scope.

On the flip side, the program has two important exclusions to keep in mind:

- **Third-party websites.** Some Google-branded services hosted in less common domains may be operated by our vendors or partners (this notably includes *zagat.com*). We can't authorize you to test these systems on behalf of their owners and will not reward such reports. Please read the fine print on the page and examine domain and IP WHOIS records to confirm. If in doubt, talk to us first!
- **Recent acquisitions.** To allow time for internal review and remediation, newly acquired companies are subject to a six-month blackout period. Bugs reported sooner than that will typically not qualify for a reward.

Qualifying vulnerabilities

Any design or implementation issue that substantially affects the confidentiality or integrity of user data is likely to be in scope for the program. Common examples include:

- Cross-site scripting,
- Cross-site request forgery,
- Mixed-content scripts,
- Authentication or authorization flaws,
- Server-side code execution bugs.

New! In addition, significant abuse-related methodologies are also in scope for this program, if the reported attack scenario displays a design or implementation issue in a Google product that could lead to significant harm.

An example of an abuse-related methodology would be a technique by which an attacker is able to manipulate the rating score of a listing on Google Maps by submitting a sufficiently large volume of fake reviews that go undetected by our abuse systems. However, reporting a specific business with likely fake ratings would not qualify.

A screenshot of the Google Vulnerability Reward P

A screenshot of the Google Vulnerability Reward Program

This is a high-level explanation of how a BBP works, your organization can publish a program such as Google's inviting researchers to test their services, and mention additional information such as:

- **scope of the program**- which domains & applications researchers can test
- **disclosure policy**- how should researchers get in touch with the organization and how far they should test before submitting a report
- **eligibility criteria**- which reports qualify, or what are the terms under which a report must be submitted
- **exclusion list**- vulnerability the organization will likely dismiss, or behavior that might disqualify a submission

Terms and conditions to include

There might be additional terms to your program, but the above points are generally good for kicking a program off. For example, a legal note stating you won't be able to process payments to a researcher from a country that your own country has declared sanctions towards.

If you're in doubt of what you should include in the terms and conditions of your program you should have a chat with your legal department and look at what other big companies have mentioned in their own programs, as they're usually a good source of inspiration, not to mention the fact that they've probably been doing it for years and their experience is invaluable.

How to attract more researchers

You might question whether you're going to be able to attract as many researchers as Google does, and the truth is that ethical hackers are generally attracted to programs that are very comprehensive and well-explained, and ones that have generous rewards.

If you're planning to offer $100 for a database breach you might be out of luck here. Make sure your organization has some budget to kick the program off with and you have enough resources to deal with the submissions. There should always be someone available to verify submissions and engage with researchers should they report a vulnerability.

Researchers are patient

In my experience, I’ve noticed researchers to be extremely patient, meaning their submission could be ignored for a week without them following-up with the organization. Try to keep the turnaround time as short as possible, but my recommendation would be to try to address reports within 48-72 hours of their submission. Remember, you don’t have to fix the vulnerability within that timeframe, simply acknowledge the submission and let the researcher know what the next steps are going to be.

Going back to the original question, how you will be able to attract researchers?, there are two ways to make sure your program ends up on the radar of ethical hackers; by publishing a `security.txt` and joining a BBP platform such as HackerOne.

Let’s study what `security.txt` is in the next lesson.