Malicious Reporters

In this lesson, we'll look at how a malicious reporter might behave and how to deal with them.

We'll cover the following

Ignore malicious reporters... usually

From time to time you might bump into a security researcher that doesn't play by the traditional rules. They might demand a payout before revealing what the vulnerability is. My suggestion, in these cases, would be to ignore the reporter or simply re-iterate the program's rules. It might not always be possible to play hardball though, as your organization's existence might be under threat. Please make a very reasoned choice and act to the best of your judgement.

ℹ Father, I have sinned!

One of the reasons I wouldn't want to categorically ask you to turn malicious researchers down is because that would be hypocritical of me. Unfortunately, in one instance I felt I had to bow down to a researcher's demands.

The story is extremely simple: an "ethical hacker" claimed he could log into customer accounts on a portal we managed, sending plaintext emails and passwords as proof. We, unfortunately, realized their claim was valid and proceeded to ask him to disclose the issue so that we could address it properly. He wouldn't budge, asking us to first proceed with the payment before disclosing the issue instead.

Luckily, one of the engineers I was working with understood what had happened: a simple case of *password reuse gone wrong*. The hacker got a hold of a credentials dump for a different website from the dark web and tried the same user accounts on other services. We actually tried those credentials on

> other popular services and realized that was what had happened, but couldn't be sure unless we got an explicit confirmation from the hacker. In a move that I live to regret, we decided to pay this person off, at which point he confirmed what we thought. Luckily, we had already forced a password reset of user accounts targeted in this other website's leak, and no further action needed to be taken.
>
> I still regret how we gave in on this issue but, in the heat of the moment, I thought that was the only possible course of action.

We're about to wrap it up

Now that we've touched on a very important mechanism to test your applications' security posture, it's time to move on to the next chapter in this course: the final one.

Before we do, let's take a quick quiz on how bug bounty programs work in the next lesson.