Dealing With Researchers

In this lesson, we'll learn how to deal with reports from ethical hackers as part of a team that handles these reports in a company.

We'll cover the following

Ethical hackers and companies are on the same team

In my personal experience, ethical hackers are some of the most accommodating people in the world. They understand they're dealing with large companies that have their own processes, thus know that they'll have to bend a bit here and there to get a report through. This does not mean it's fine to dismiss them, instead you should feel like a single party working on the report rather than "us vs them".

Evaluating reports

When evaluating a report, make sure you understand it very well and are able to reproduce it. Once that is cleared, let the researcher know that you've been able to reproduce the issue and are working towards identifying whether it can be fixed and if it can be considered a valid submission. Sometimes you won't be able to fix less impactful security flaws, so it's important you're able to justify your decision to the researcher.

Turning hackers down

If you do end up turning down the report, make sure you leave a positive mark in

the conversation. Thank the researcher, invite them to persevere in their work, and leave the conversation on a positive note.

Hackers are generally used to being turned down based on a program's policy, but positivity is a powerful tool to improve collaboration. In some cases, they'll be turned down with a simple "*not in scope, sorry*" after hours of relentless research, so I generally encourage organization to always motivate, thank, and reward these unsung heroes.

Processing a valid report

If you find out the report is valid, understand how your internal team is going to be able to address and fix the issue; more importantly, gather a broad timeline. Once you have a general understanding of how you plan to tackle the issue, let the researcher know. Provide them with a rough timeline and the proposed fix unless confidential information is involved.

This is important for two specific reasons:

1. So that they can help you validate the fix. It might be that the solution you come up with is not the most ideal one, so they could make suggestions on improving the fix.
2. Sharing timelines gives the researcher an expectation on how long they would need to wait for the whole process to be complete. In my experience, waiting weeks is never a problem, and researchers will gladly take a step back and relax to let you do your work. They understand that you're part of an organization that needs its time.

Testing fixes

As time goes on and you start approaching the deadline you've communicated, leave a message for the researcher and let them know whether you're on track or whether there will be delays. Once the fix is rolled out, ask the researcher to take part in the testing phase. I've always made a point of doing both internal testing as well as asking the reporter to double-check that our solution is working as intended.

Paying the hacker

Once the researcher confirms the fix is working, it's time to celebrate! You have made your systems safer, and it's time to pay the hacker. Hit the reward button

and make sure you conclude the conversation with a positive note, thank the

reporter and stress the fact that your organization is safer primarily thanks to their effort.

In the next lesson, we'll look at how to deal with malicious reporters.