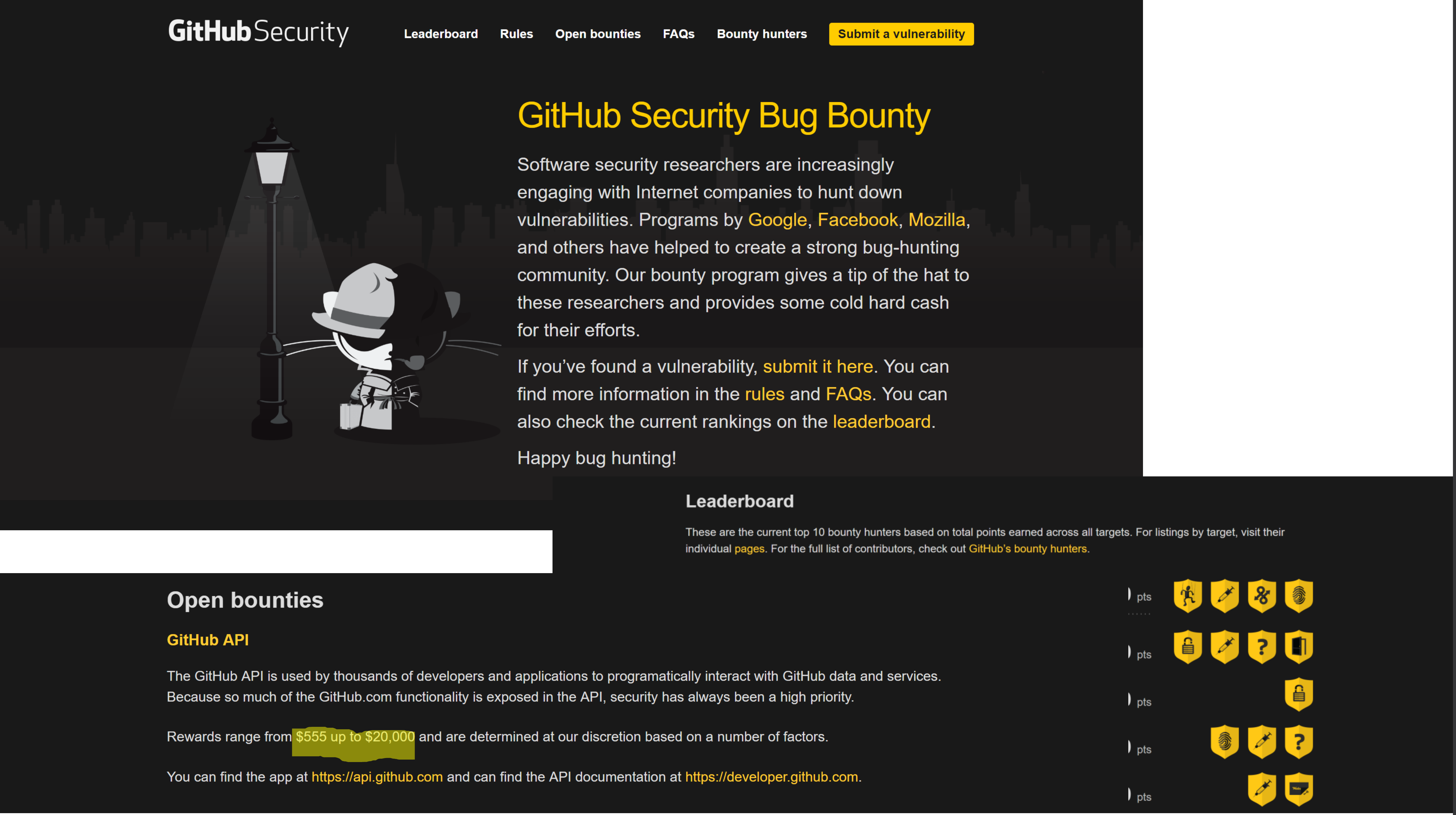
Disclosing Software Vulnerabilities

Discovered a Vulnerability – What to do?

- Do nothing.
- Exploit or sell.
- Make sure you found it legally.
- Tell the vendor.
- Tell everyone.
- Disclose responsibly

Why you should do something.

Why you might consider selling.



GitHub Security Bug Bounty

Software security researchers are increasingly engaging with Internet companies to hunt down vulnerabilities. Programs by Google, Facebook, Mozilla, and others have helped to create a strong bug-hunting community. Our bounty program gives a tip of the hat to these researchers and provides some cold hard cash for their efforts.

If you've found a vulnerability, submit it here. You can find more information in the rules and FAQs. You can also check the current rankings on the leaderboard.

Happy bug hunting!

Leaderboard

These are the current top 10 bounty hunters based on total points earned across all targets. For listings by target, visit their individual pages. For the full list of contributors, check out GitHub's bounty hunters.

) pts

) pts

) pts

) pts

) pts

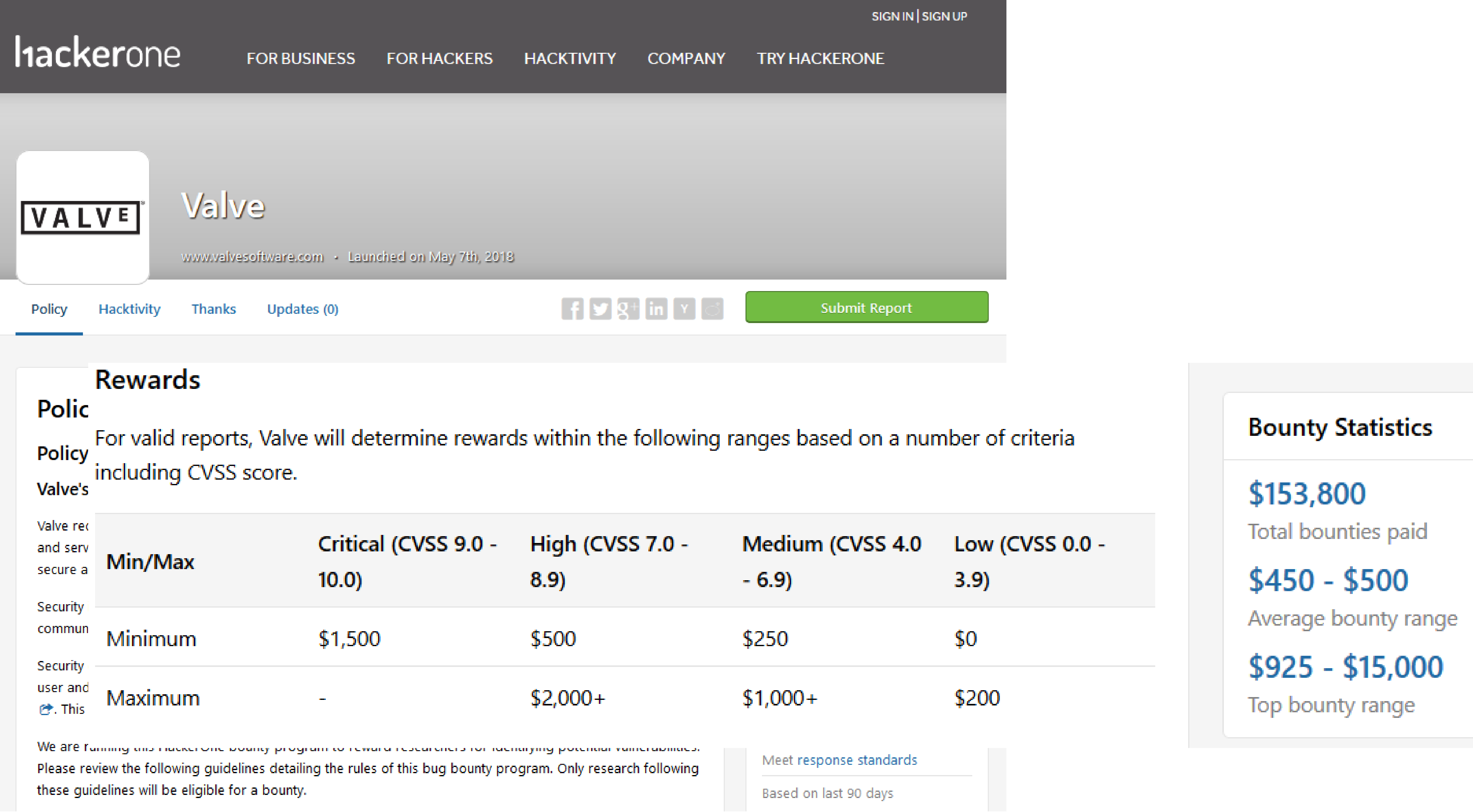
Open bounties

GitHub API

The GitHub API is used by thousands of developers and applications to programatically interact with GitHub data and services. Because so much of the GitHub.com functionality is exposed in the API, security has always been a high priority.

Rewards range from $555 up to $20,000 and are determined at our discretion based on a number of factors.

You can find the app at https://api.github.com and can find the API documentation at https://developer.github.com.



Valve

www.valvesoftware.com · Launched on May 7th, 2018

Polic

Policy

Valve's

Valve rec
and serv
secure a

Security
commun

Security
user and
. This

We are running this HackerOne bounty program to reward researchers for identifying potential vulnerabilities. Please review the following guidelines detailing the rules of this bug bounty program. Only research following these guidelines will be eligible for a bounty.

Meet response standards

Based on last 90 days

Rewards

For valid reports, Valve will determine rewards within the following ranges based on a number of criteria including CVSS score.

Min/Max	Critical (CVSS 9.0 - 10.0)	High (CVSS 7.0 - 8.9)	Medium (CVSS 4.0 - 6.9)	Low (CVSS 0.0 - 3.9)
Minimum	$1,500	$500	$250	$0
Maximum	-	$2,000+	$1,000+	$200

Bounty Statistics

$153,800
Total bounties paid

$450 - $500
Average bounty range

$925 - $15,000
Top bounty range

Why you should not sell to third-parties.

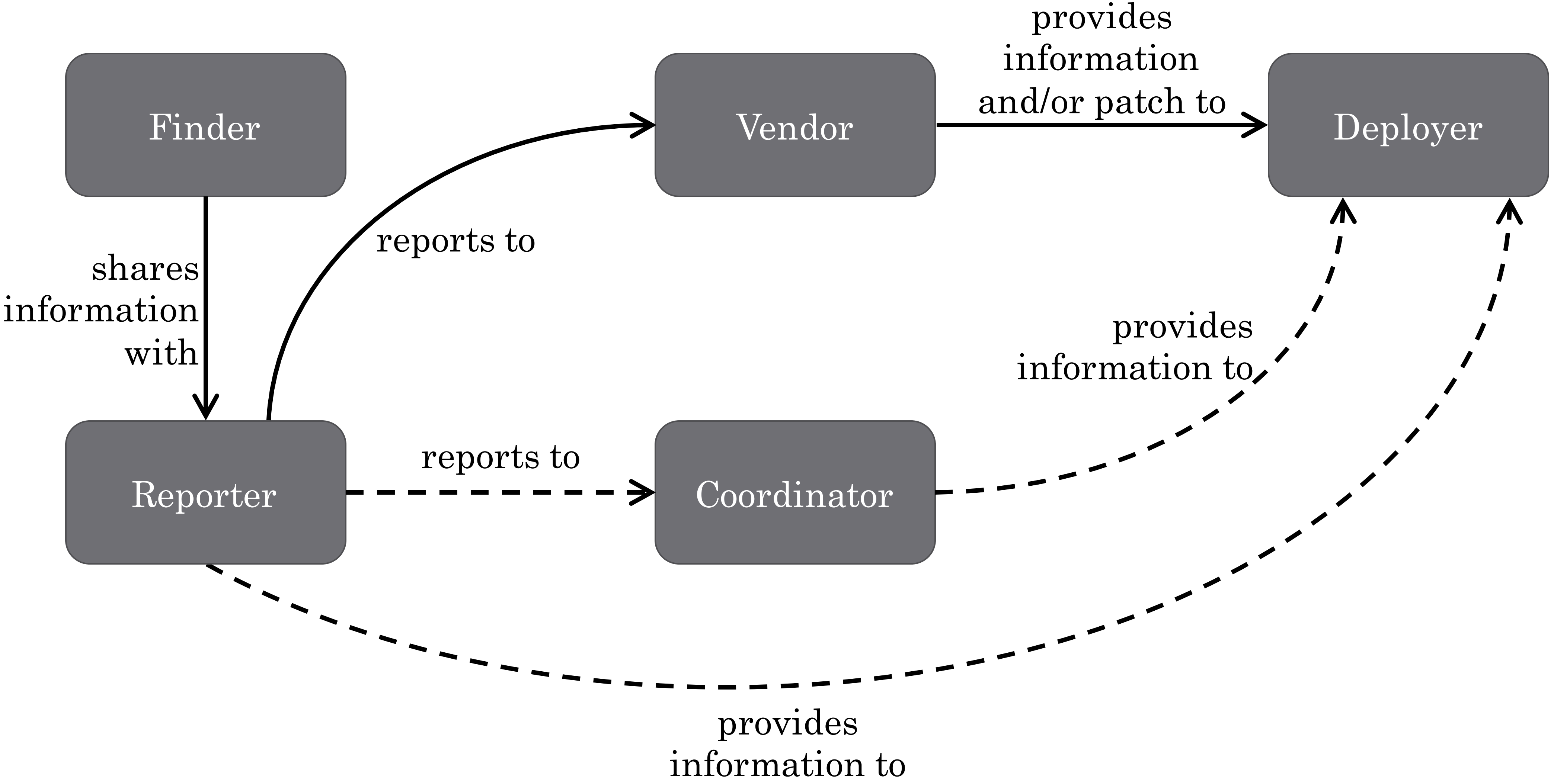
Make sure you won't get sued.

Why only telling the vendor is suboptimal.

Why telling everyone is suboptimal, too.

How everyone can profit.

How to disclose vulnerabilities with CERT/CC.



So what to do now?

- Do nothing. - **No!**
- Exploit or sell. - **Don't exploit, only sell to the vendor.**
- Make sure you found it legally. - **Don't risk getting sued.**
- Tell the vendor. - **Only if it is critical.**
- Tell everyone. - **Only when the vendor is unresponsive.**
- Disclose responsibly - **Do that!**