What does it take to run a bug bounty program?

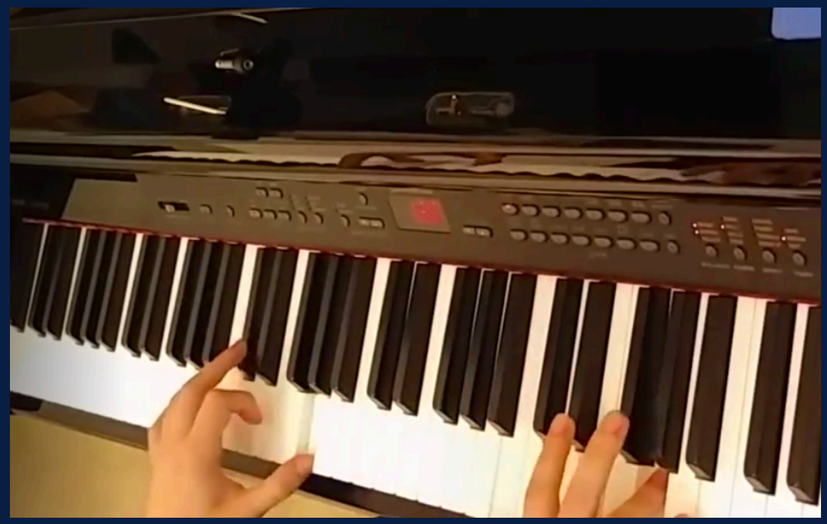
Typical problems and practical solutions

ANTON BLACK | GRADUATE SECURITY ENGINEER, ATLASSIAN | TWITTER.COM/NOQRY

¿Wait, who are you?

Was software engineer,
now at least 50% cyber

Likes both kinds
of keyboard



“

“You should run a bug bounty!”

– everyone, probably

Generally considered a Good Idea

Google	Reddit	Facebook	Microsoft
Apple	Valve	Fitbit	Mastercard
Netgear	Avast	DigitalOcean	Android

(and others)

Agenda

1) Bug bounty considered beneficial

2) Challenges and mitigations

3) Summary

A FORMAL PROGRAM WHERE:

1. Researchers tell you about security bugs in your software

2. You pay them for their efforts

People will attack your software anyway

A bounty lets it happen on your own terms

Tap into international talent

Bounty hunters can work anywhere in the world

Tap into specialist talent

Bounty hunters often specialize in some platform, tool, or framework

Meet security standards

Certifications ask for “vulnerability testing”, “penetration testing”

Publicly declare your commitment to security

You care about security; let people know that

Forgot Password

You must have a valid password in order to access your account(s). If we have not assigned a password for you, please call us or click Contact Support to send a message regarding your problem.

If you have forgotten your password, you can choose to display your Password Hint on this page, or you may choose to have your password e-mailed to you. Please read below to determine which option will work best for you.

Display Your Password Hint

Receive Your Password by E-mail

Enter your account number or user id and the last four digits of your home telephone number, and click the checkbox. If we have an e-mail address on record for you, then your password will be e-mailed to you when you click Submit.

If you have multiple accounts and multiple e-mail addresses for those accounts, your password will be sent to the e-mail address correlating with the account that has the lowest separator (the last three digits of your account number).

Account Number

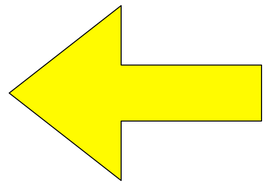
Your account number is printed on your bill. You must enter this number to access information on this site. **If your account number includes a '-', it should be removed. For example, if the account number on your bill is 12345-001, you should enter either 12345 or 12345001 in the account number field.**

Account Number or User ID :

Telephone Number :

(last 4 digits only)

Submit Reset



Sends passwords in plaintext

More secure products

Your products have measurably fewer bugs


WANTED
WHITE-HAT HACKERS
TO IMPROVE PRODUCT SECURITY
VISIT BUGCROWD.COM/ATLASSIAN
$$$ REWARD

BUT THERE ARE CHALLENGES

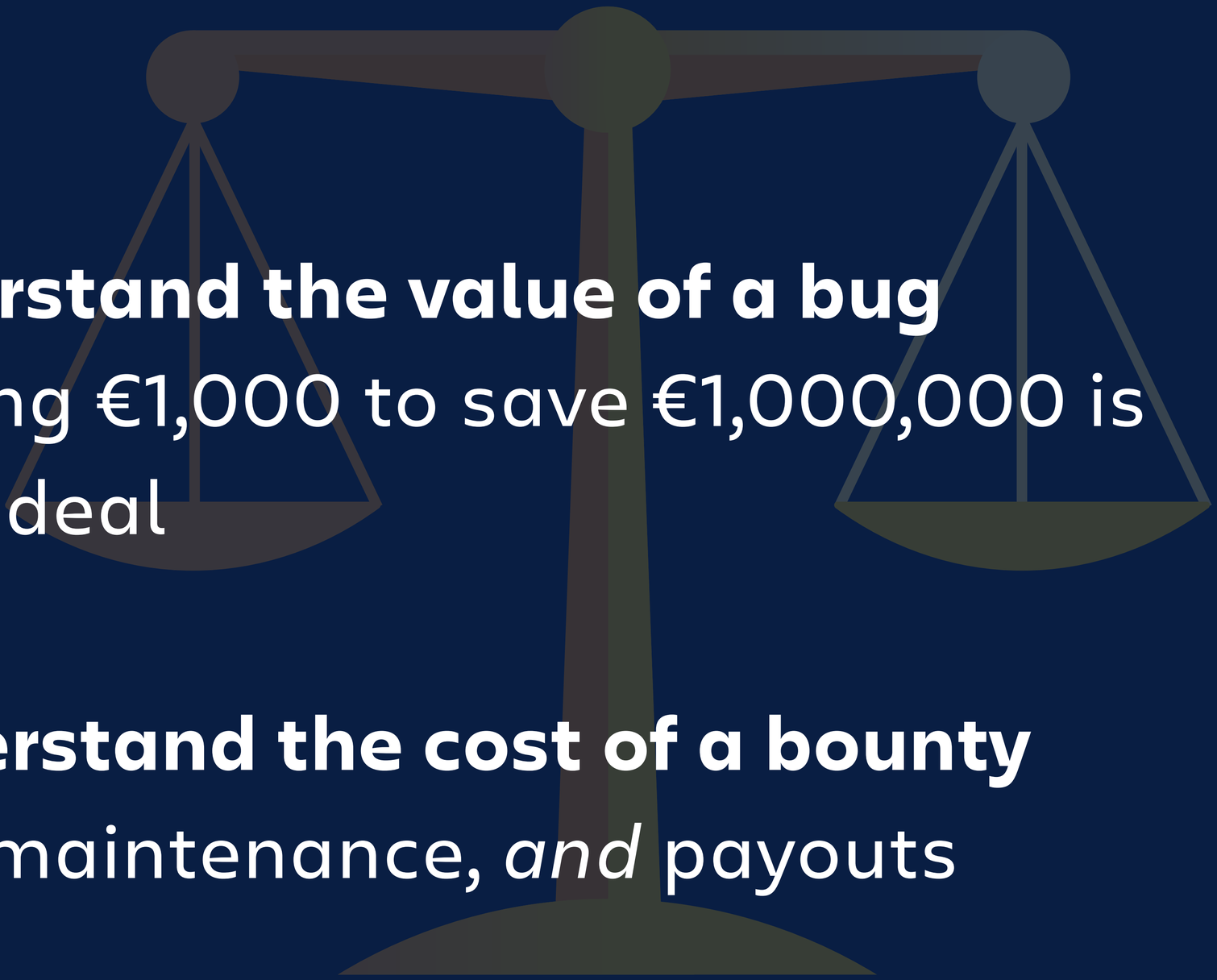
Agenda

1) Bug bounty considered beneficial

2) Challenges and mitigations

3) Summary

Budget



1. Understand the value of a bug

Spending €1,000 to save €1,000,000 is a good deal

2. Understand the cost of a bounty

Setup, maintenance, *and* payouts

Choosing a platform

- **Use an existing bug bounty platform** (STRONGLY RECOMMENDED)
- Or roll your own
- Check the bonus content for a list of platforms

You don’t have experience with bug bounties.

- Limit initial reports
- Make a shared chatroom/forum for your bounty staff to ask each other for help

When should we increase the payouts?

Pull data from your platform:

- # critical bugs found in the last 90 days
- Flow rate (is the dev team overwhelmed?)
- Remaining bounty budget (can you afford it?)

Our payout calculator

- Total Allowable FY19 Average Daily Spend: $XXX.XX
- Current Average Daily Spend: $XXX.XX
- Projected Daily Spend Remaining: $XXX.XX
- Days into the budget period: XXX

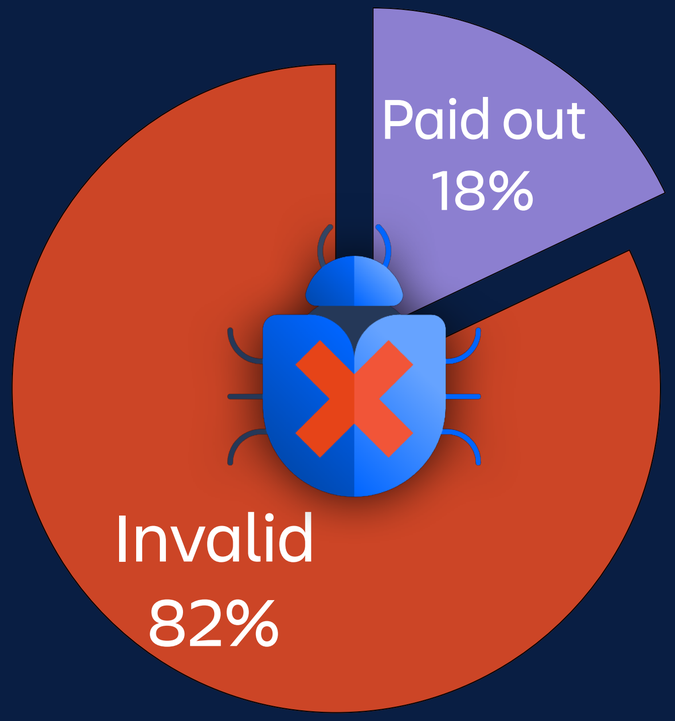
Product 1

- 0 critical issues in the last 90 days
- {0, 0, 0, 1, 0, 1} Issues per Month
  - Slope: 0.17, Intercept: -0.27
- 0.08 Average SLA Violations per week
- 2:1 (Created:Resolved this Quarter)
- 6: Current Issue Severity Metric

Product 2

- 0 critical issues in the last 90 days
- {4, 0, 4, 8, 4, 3} Issues per Month
  - Slope: 0.31, Intercept: 2.73
- 0.08 Average SLA Violations per week
- 15:14 (Created:Resolved this Quarter)
- 30: Current Issue Severity Metric

A huge proportion of all incoming bug reports are invalid.



FY18 bug reports

- Choose a bounty platform which offers filtering services
- Bounty briefing page is your first line of defence

Communication fatigue

- Use standard responses
- Check bonus content for more ideas and situations

e.g. Bug resolved

Hi <researcher>,
Thank you for your report to our bug bounty program.

The issue has been fixed by the development team and should reach production soon.

If you can still reproduce the issue in 2 weeks from today, please let us know and we can investigate further.

Thank you for your continued efforts toward our bug bounty program.

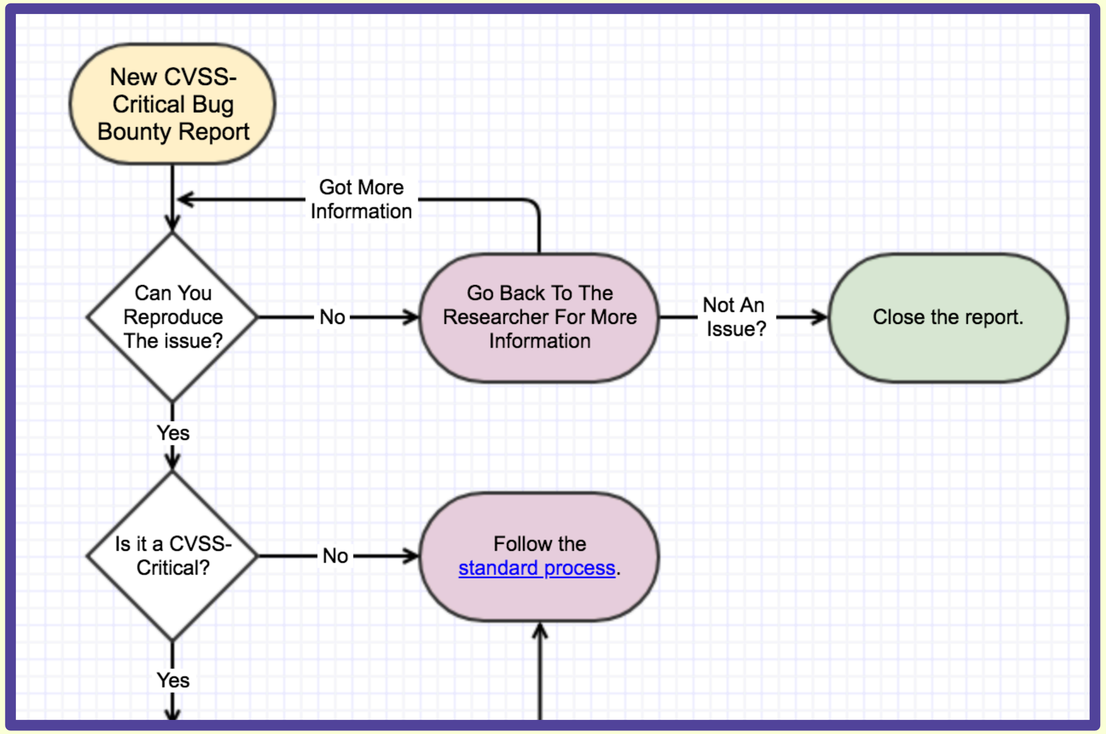

bugcrowd
BUGGY AWARDS
Wednesday, April 18
3 p.m. PT
Local Edition


Atlassian
Program of the Year
Bugcrowd Buggies 2018

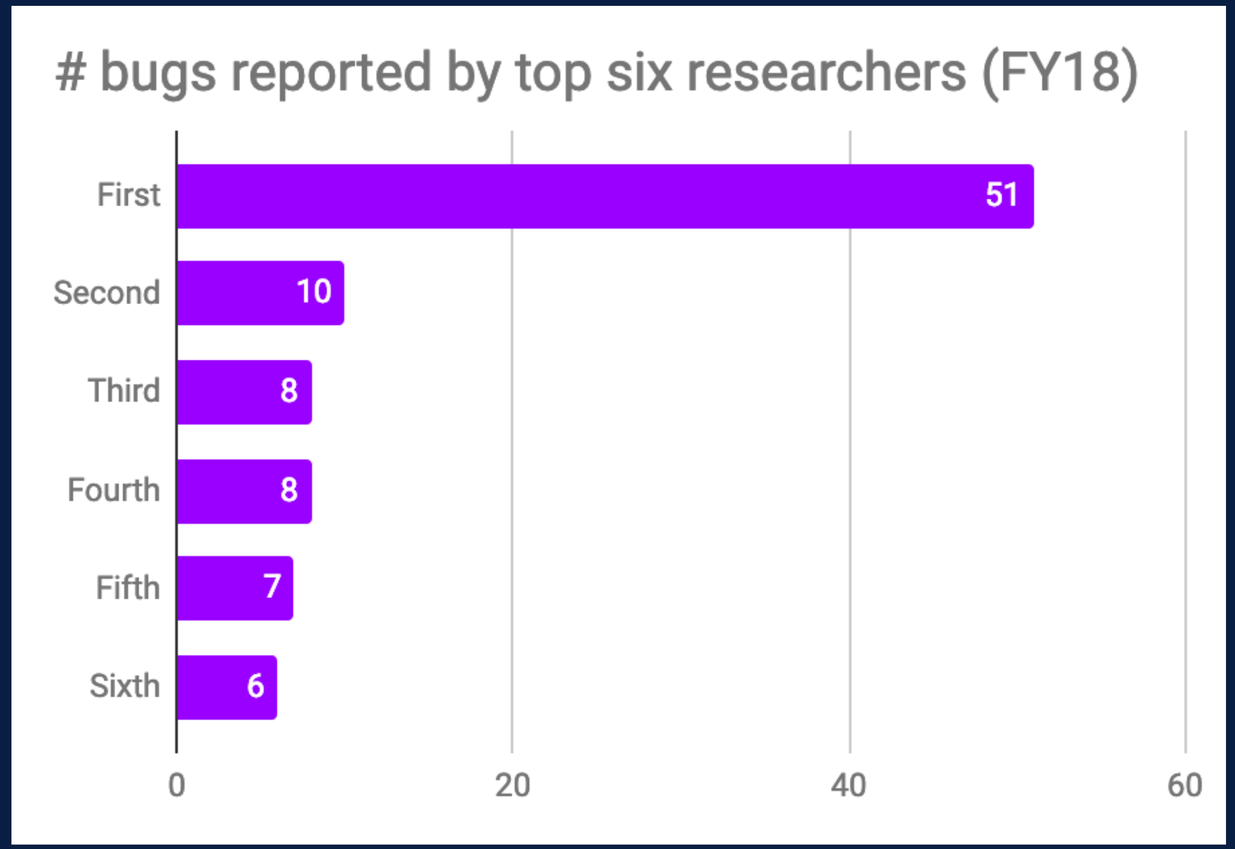
Decision fatigue

- Make a shared page for procedures and protocols
- Every time you have to make a judgement call, update the docs to cover it
- **FLOWCHARTS** 👌

e.g. “How do you handle a Critical bug?”

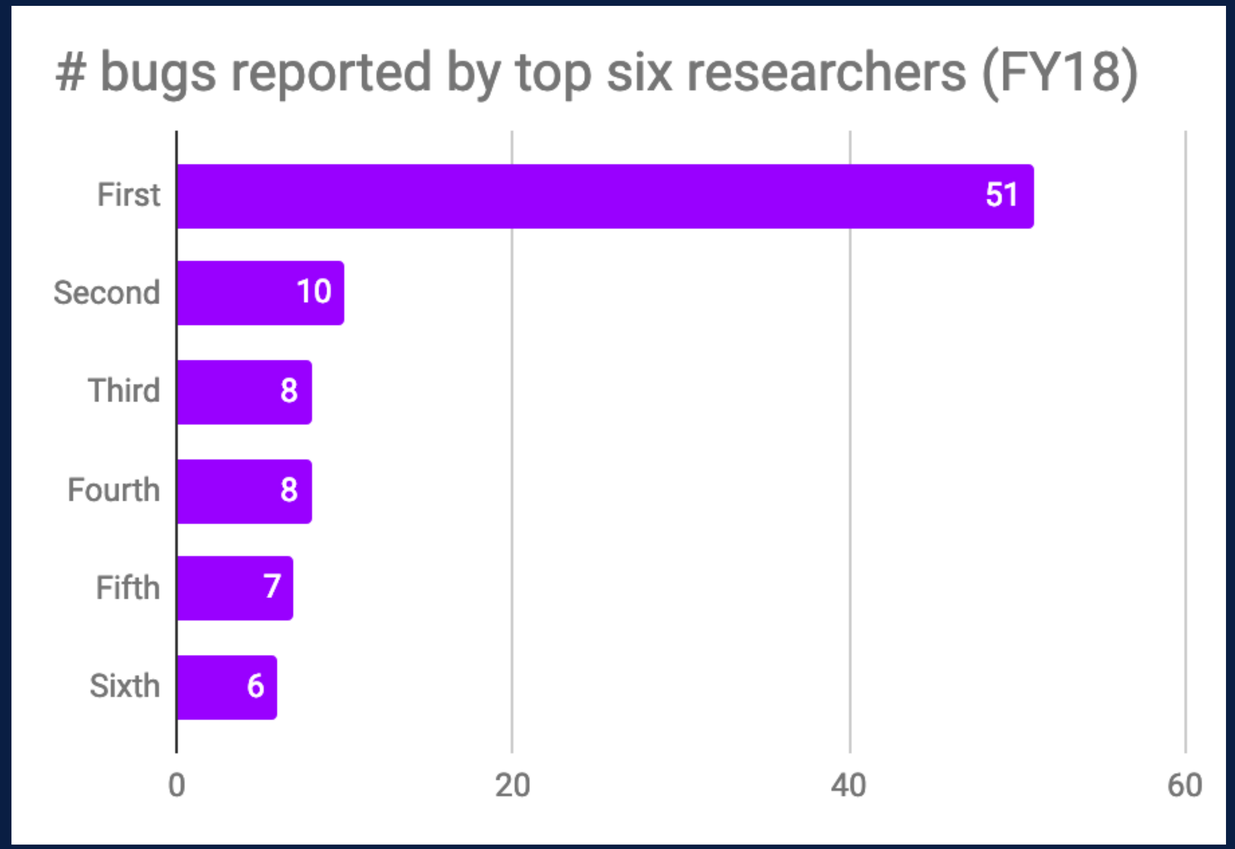


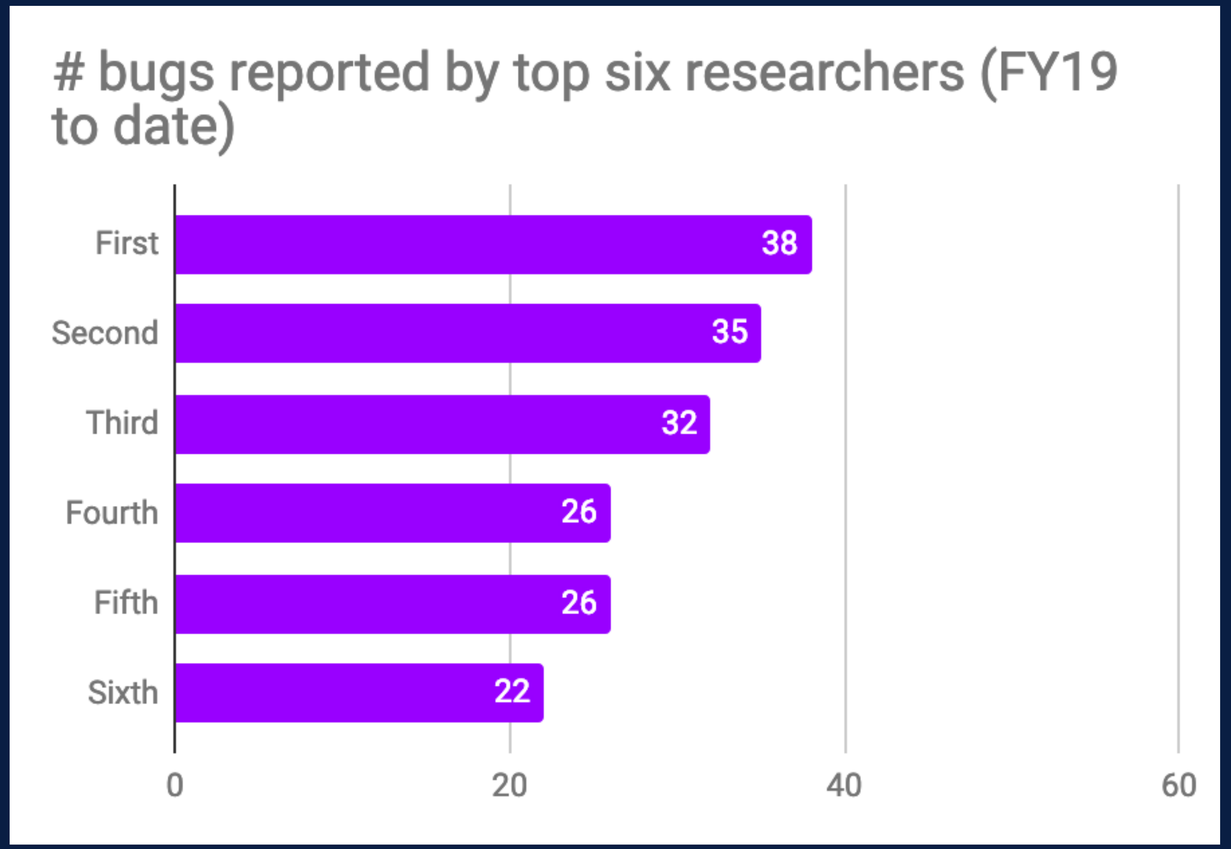
You’re dependent on a small group of researchers.



- Increasing the bounty ≠ more researchers
- Advertise and hold hacking events

Broader researcher base!





Boring, repetitive admin tasks

- Choose a platform with an API
- *Make the robots do it for you*

Agenda

1) Bug bounty considered beneficial

2) Challenges and mitigations

3) Summary

Run a bug bounty!

Choosing your platform:

Filtering services

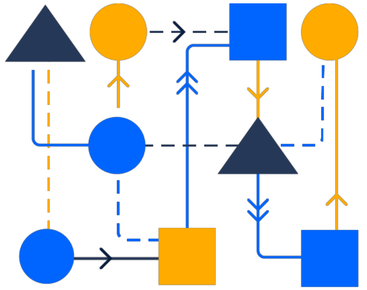
Reports + stats

Control via API

Preventing problems:

Start small

Use filtering services



Document procedures

Pull data to inform decisions

Advertise

Automate!

Atlassian's bounty program: bugcrowd.com/atlassian

For more info, check out the bonus doc:

tinyurl.com/dublin-bsides-2019-bugbounty

ANTON BLACK | GRADUATE SECURITY ENGINEER, ATLASSIAN | TWITTER.COM/NOQRY