BISHOP FOX®

# Effectively Operating a Bug Bounty Program

## BEST PRACTICES & RECOMMENDATIONS

(ISC)² PHOENIX CHAPTER, INC

August 13, 2015

# About Me

ZACH JULIAN

- Sr. Security Analyst @ Bishop Fox
- Enterprise Security team
- University of Advancing Technology
- Live in Tempe, AZ
- @tprime_

# What Are Bug Bounties?

DEFINITION

- Bugs exist in all types of software and hardware
- People are going to find vulnerabilities
- Reward researchers for finding vulnerabilities and disclosing them to you privately
- Greater economic incentive to responsibly disclose a vulnerability instead of abusing it

# My Bug Bounty Experience

SOME CREDENTIALS

- Consulted with five different companies' bug bounty programs
  - Four used HackerOne
  - One accepted submissions via HTML form
- Both medium-size and very large companies
  - Some with hundreds of properties
- Range from about 20 to over 100 reports per week

# Benefits of a Bug Bounty Program

THREE REASONS

- Efficient
- Cost-effective
  - Compare Bug Bounty versus security consultants
- Immediate results

# Current Bug Bounty Landscape

WHERE WE'RE AT NOW

- Main bug bounty platforms:
  - HackerOne
  - BugCrowd
- Not every program awards bounties
  - I would recommend it
- Good community of skilled, high-quality reporters
- Chunk of low-quality, spammy reporters

# Where Are We Going?

THE ROAD AHEAD

- LinkedIn private bug bounty program
- Synack – private bug bounty platform
- Increased demand in “vetted” researchers
- Bug bounty may evolve into true freelance pentesting

# LAUNCHING A BUG BOUNTY PROGRAM

Your first priority:
clearly define program scope, qualifying vulnerability types, and non-qualifying vulnerability types.

# First Priority: Scope & Vuln. Definition

AN IMPORTANT FOUNDATION

- If uncertain about program scope, look at other companies HackerOne profiles
- Talk with your security team & developers
- Anticipate low-risk reports and list them as unaccepted as appropriate
- Clearly define price buckets so researchers aren't surprised
- Anticipate some scope changes as the program evolves

# Why Define Scope & Vulns?

AND WHY DO IT FIRST?

- Number one challenge: low-quality, low-risk submissions
  - Will occupy around 50% of your tickets
  - This potential time-waster can be mitigated with planning
- Begin your program by **determining what level risk you are concerned with**
- Spending the time to triage low-risk bugs is not effective cost/benefit
  - Triaged -> Reported -> Fixed -> Validated
  - Consider how many people and hours are involved with each bug fix

Start your scope with well-secured properties, then expand gradually.

# Consider an Initial Security Assessment

PRIOR TO LAUNCHING YOUR BUG BOUNTY PROGRAM

- There may be one vulnerability across many properties
- This will result in **many** tickets once you go public
- Save time
- Keep researchers happy

# Consider an Initial Security Assessment

PRIOR TO LAUNCHING YOUR BUG BOUNTY PROGRAM

The following will likely result in many tickets:

- Rate-limiting
- Password reset logic
- X-Frame-Options
- SSL attacks/weak ciphers
- Crossdomain.xml files
- User enumeration
- Self-XSS

# Suggested Non-Qualifying Vulns.

NOT EFFICIENT TO TRIAGE

- Automated Scans
  - Expect these to increase against your organization
  - Coordinate with firewall/IDS/IPS owners prior to launch
  - You'll likely need to block certain submitters
- SSL reports
- Clickjacking
- 'Possible' in the title
- Self-XSS & other vulnerabilities which require manually intercepting HTTP requests

# Consider Starting as a Private Program

INVITE MORE RESEARCHERS GRADUALLY

- Invite well-known researchers first
  - https://bugcrowd.com/leaderboard
  - https://hackerone.com/thanks
- Acclimate team to BB process
- Lower number of incoming reports
- High-risk vulnerabilities more likely to be addressed
- Invite more researchers gradually, eventually go public

# Select a Bug Bounty Platform

A FEW DIFFERENCES

- HackerOne
  - Most common in my experience
  - Platform is free
  - 20% commission for payouts
- BugCrowd
  - BugCrowd Enterprise
  - Flex Program
  - Managed programs
  - Free to reward points, monthly cost for paid rewards
- Private program or other platform

Start with lower bounty amounts, increase payouts gradually.

# Define Payment Buckets

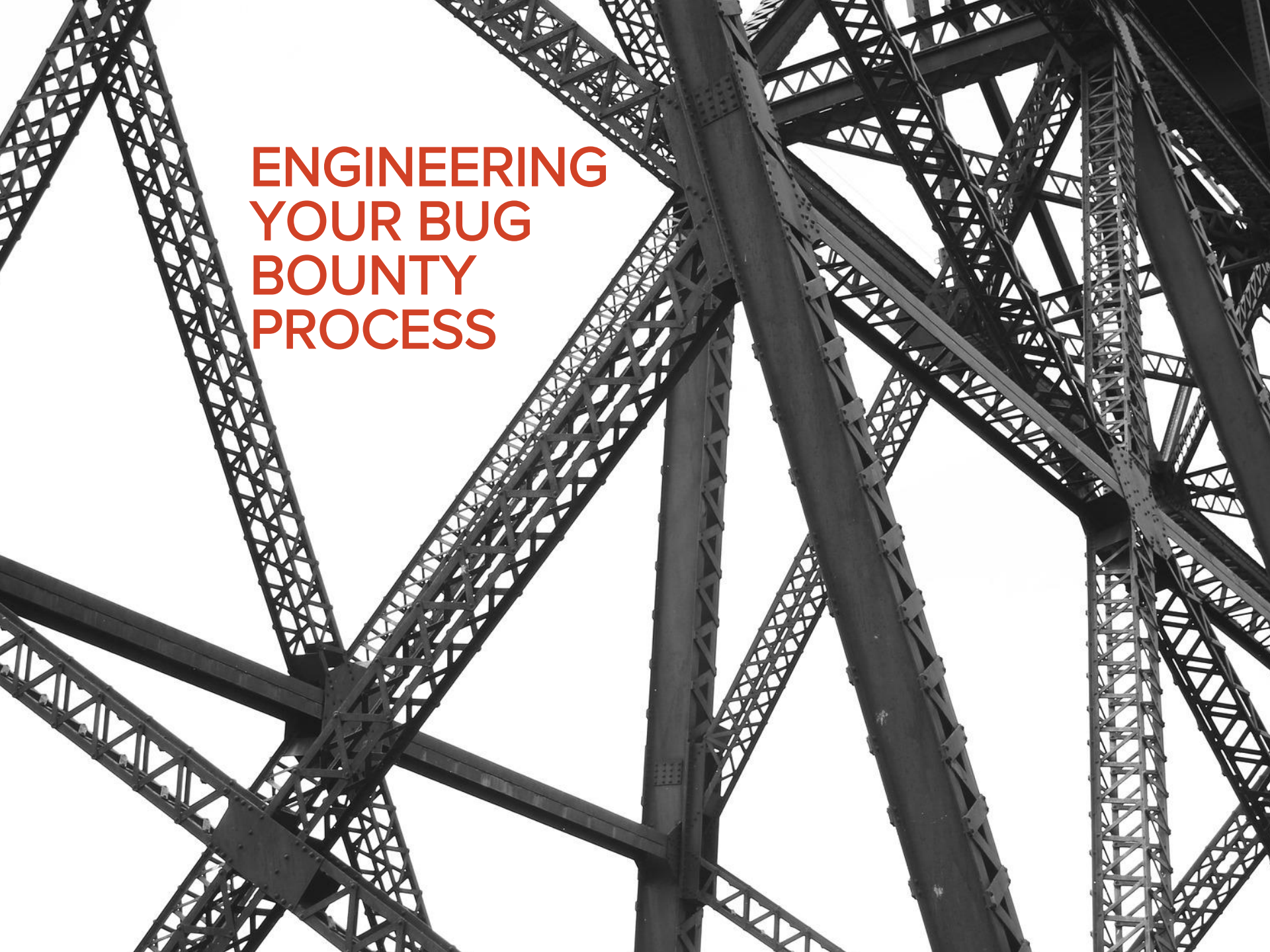
SOME EXAMPLES

| Type | Low | Medium | High |
|---|---|---|---|
| Open Redirect | $50 | $50 | $50 |
| CSRF | $50 | $100-$500 | $500+ |
| Info. Disclosure | $50 | $100-$500 | $500+ |
| XSS | $100 | $250-500 | $500+ |
| Broken Auth./Session | $100 | $250-$1k | $1k+ |
| SQL Injection | $1k+ | $1k+ | $1k+ |
| RCE | $1k+ | $1k+ | $1k+ |

# Define Payment Buckets

CONTINUED

- Look at other companies' payout amounts if unsure
- twitter.com/disclosedh1
- Typically only the minimum to maximum payout is listed publicly


ENGINEERING
YOUR BUG
BOUNTY
PROCESS

# Select  Ticket Management Software

MANAGE BUGS THROUGH A SECONDARY TICKET MANAGEMENT SYSTEM

- Use BugZilla, JIRA, or another ticket management software
- Consciously select which fields and information are included in each ticket
  - Ensure this is part of your triaging process documentation
- Every click in your process adds time, decreases efficiency.

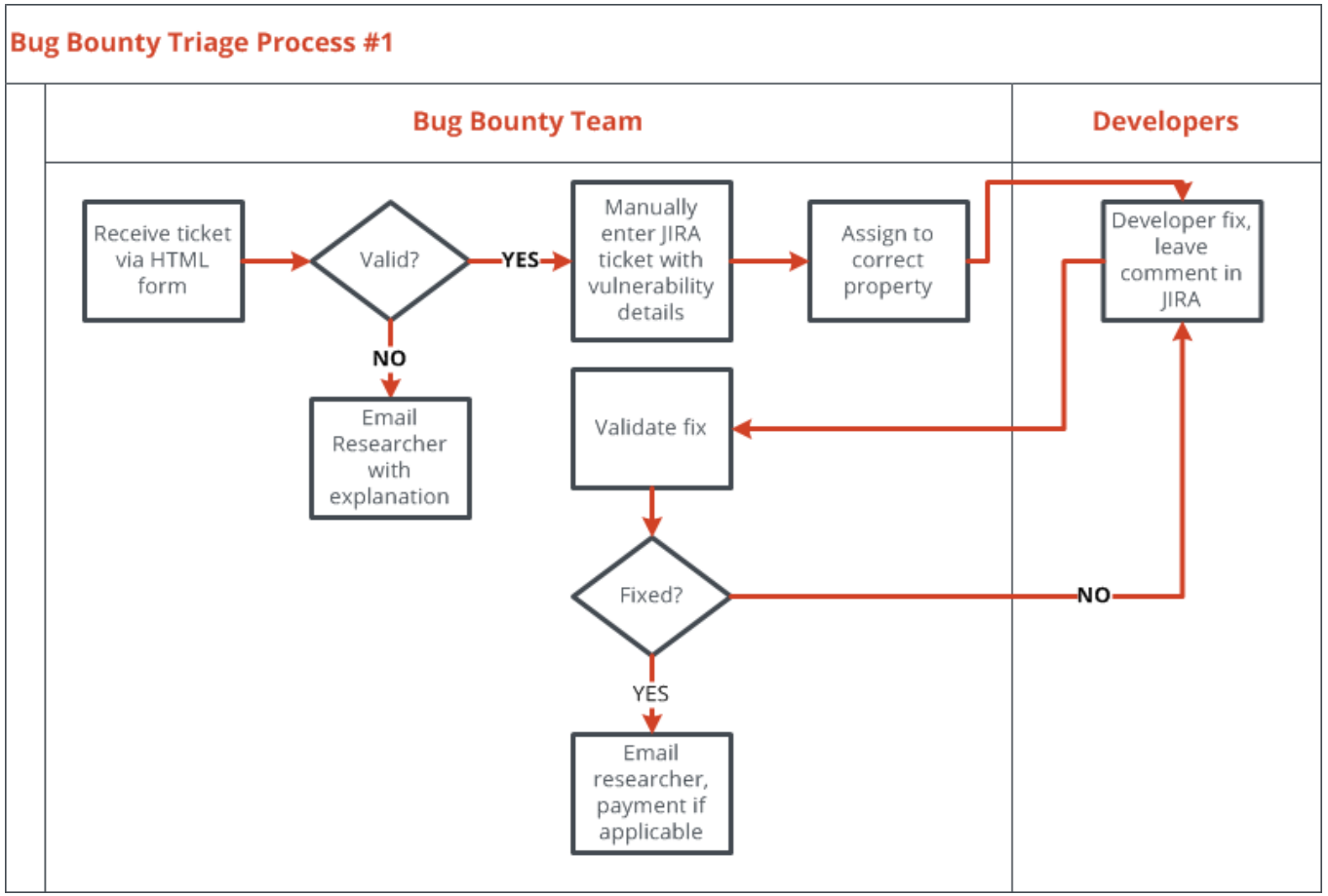
# Establish Your Triage Process

DEFINE AND DOCUMENT PROCESSES AT THE BEGINNING

- Define and document your triage/ticketing process before you open your bug bounty program
- Define and document appropriate contacts:
  - Manager for each property
  - Who creates user accounts?
- Define and document payment process:
  - Many companies seem to be vague about this
  - Who performs the verification?
  - When is payment made?
- Define ticket turnaround times

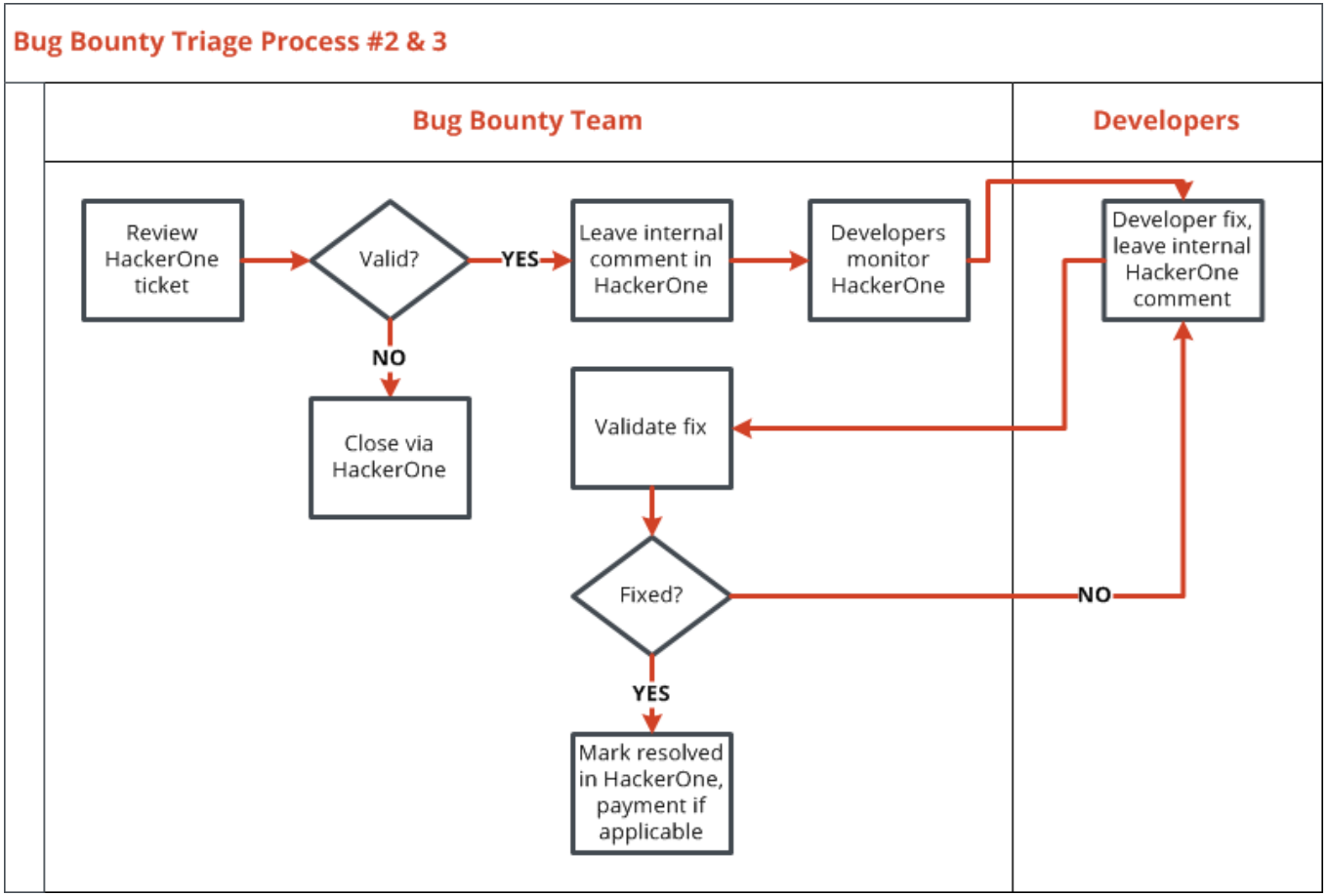
# Bug Bounty Processes

EXAMPLE #1



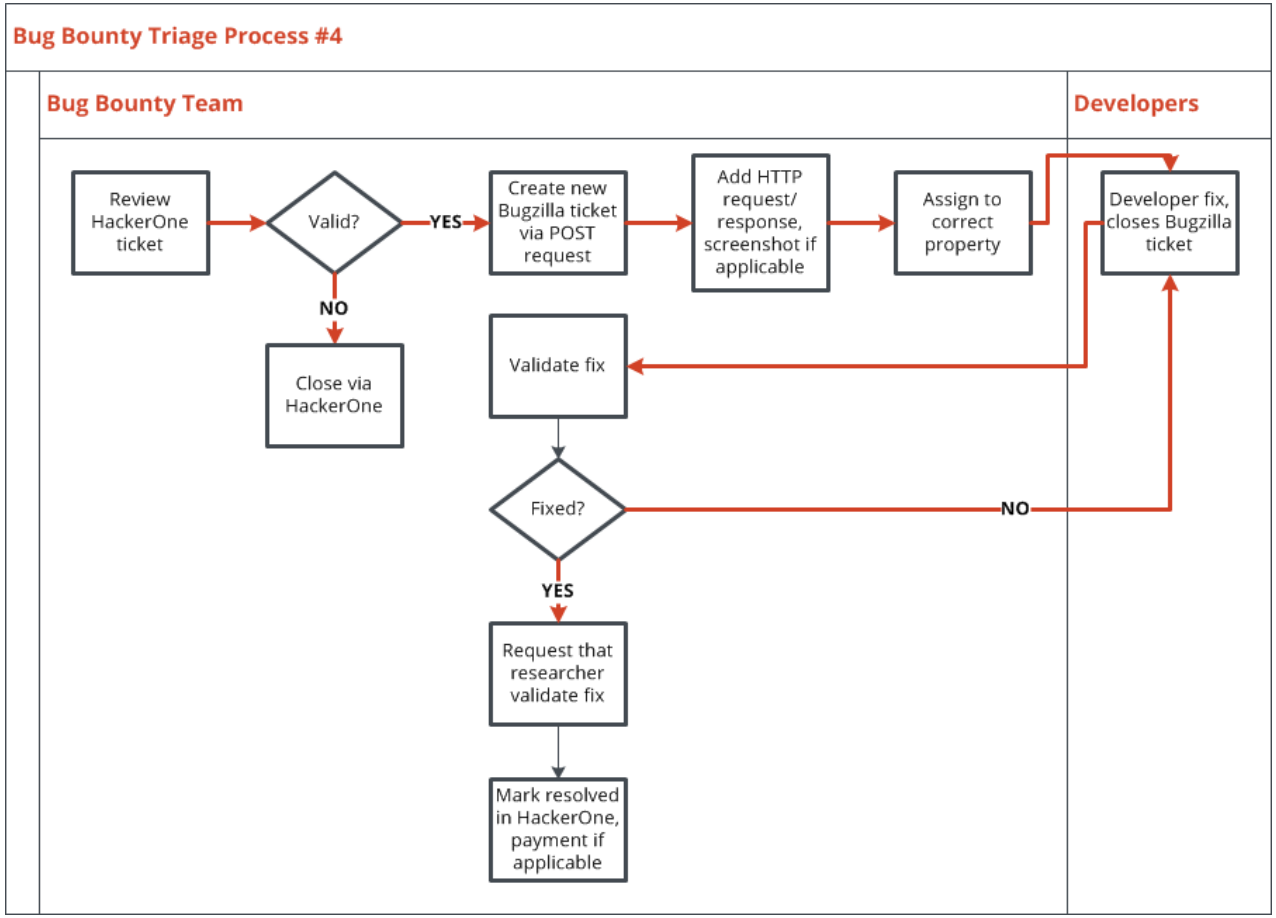
# Bug Bounty Processes

EXAMPLE #2 & 3



# Bug Bounty Processes

EXAMPLE #4



# Consider Outsourcing Initial Triage

CONTRACT YOUR BUG BOUNTY TEAM

- Outsource the point between researchers and developers
- Helpful in quickly launching a bug bounty program
- Can be cost effective opposed to hiring

Ensure your company has an established escalation process.

# Prepare Researcher Responses

YOU'RE GOING TO NEED THEM

- Researcher communication will be frequent and repetitive
- Prepare responses for common statuses:
  - Not Applicable
  - Duplicate
  - Valid
  - Working as Designed
- HackerOne has built-in responses
- Define who is doing the responding

# Talk With Legal

GET APPROVAL ON SCOPE & RESPONSE LANGUAGE

- Recommend legal approval for scope language
- Consider clearing other public-facing language
- I’m not a lawyer

# Miscellaneous Concerns

NON-ESSENTIALS

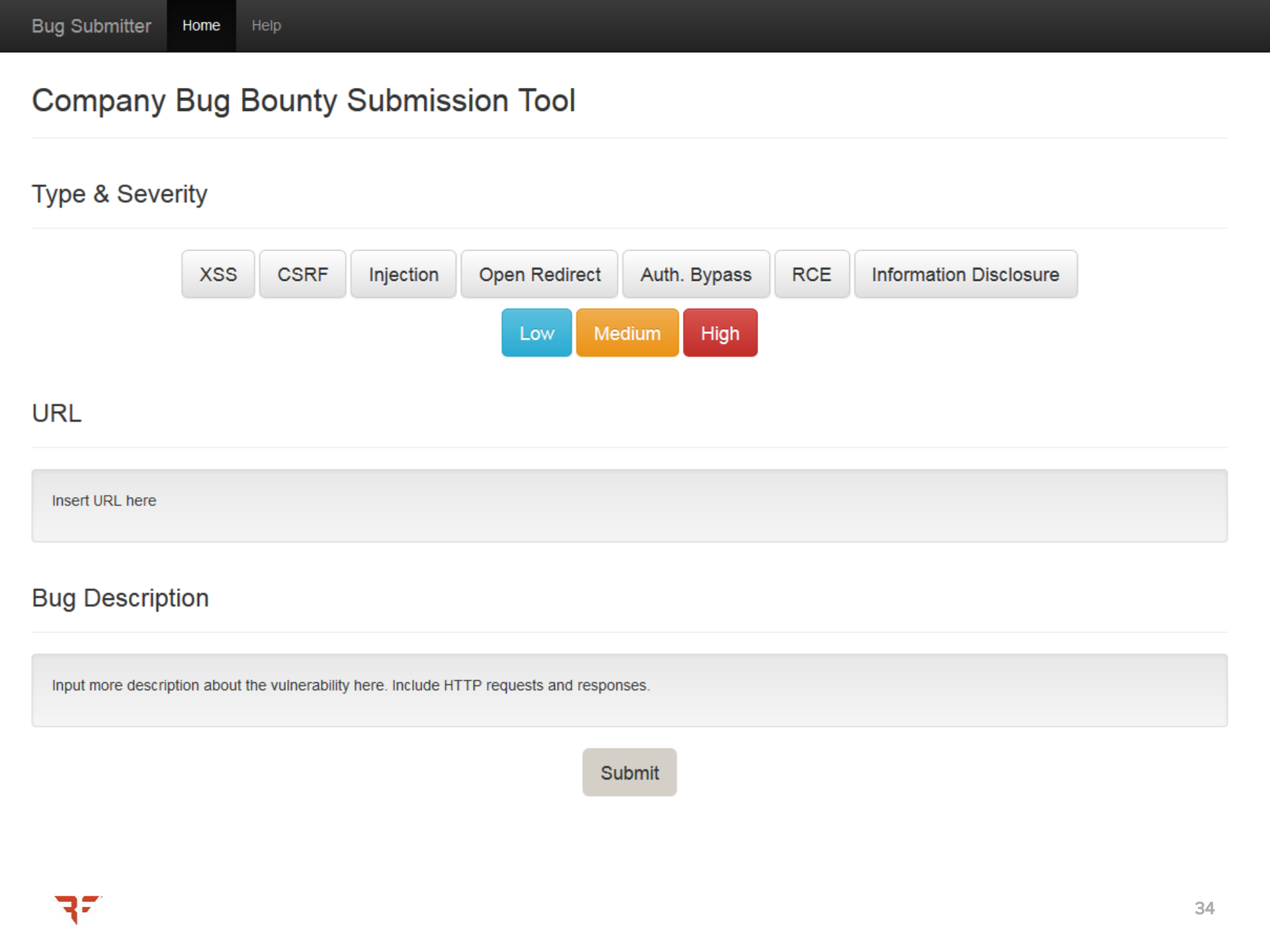
- Work with front-end team for **Wall of Fame**
- Consider offering **job opportunities** for quality researchers
- Consider assigning a project manager to your bug bounty program launch


TUNING YOUR
BUG BOUNTY
PROGRAM

# Automate Wherever Possible

EVERY CLICK COSTS MONEY

- Seek to reduce every required mouse click
- For instance, BugZilla tickets can be created via GET or POST request.
- Work with HackerOne to find a solution for your ticketing software


Bug Submitter
Home
Help
Company Bug Bounty Submission Tool
Type & Severity
XSS
CSRF
Injection
Open Redirect
Auth. Bypass
RCE
Information Disclosure
Low
Medium
High
URL
Insert URL here
Bug Description
Input more description about the vulnerability here. Include HTTP requests and responses.
Submit

Rotate your bug bounty analysts to avoid burnout.

# Record Bug Bounty Metrics

A USEFUL SET OF DATA

- Analyze bug bounty data
  - How many bugs are submitted per day?
  - What % of bugs are valid?
  - Who are the most/least efficient researchers?
  - What properties are most affected?
  - What vulnerability types are most common?
  - How much are we paying?
- Automate regular retrieval of this data, if desired
- This data can be used to make larger security decisions

# Social Situational Awareness

KEEP AN EYE ON PUBLIC OPINION

- Twitter is the main forum for bug bounty discussion - #bugbounty
- Consider creating a Twitter account @<company>Security
- Monitor the #bugbounty hashtag
- Become aware of, and address, issues before they grow
- Low-quality researchers may threaten disclosure
  - Be transparent

# Bug Bounty Campaigns

GUIDE RESEARCHERS TO YOUR ADVANTAGE

- Focus researchers on key properties
- Focus researchers on vulnerability types
- Promote campaigns on Twitter, other web properties

# TIPS FOR TEAM MEMBERS

## PERFORMING INITIAL TRIAGE

# Take Advantage of Reputation

ENCOURAGE QUALITY SUBMISSIONS

- HackerOne researchers are sensitive to **reputation score**
- Effective way to reinforce program rules and scope
- Consider marking **Not Applicable** if the following applies:
  - Out of scope
  - Automated report
  - Wrong company
  - Inaccurate title
  - Poor quality
- This does not include reporter's English abilities

# Communicate With Management

KEEP EVERYONE INFORMED

- Weekly or monthly meetings are recommended
- Necessary for continued efficiency
- Important for critical vulnerabilities – think Heartbleed
- Management should be open to analyst's observations & input

# AN APPEAL

TO THE BUG BOUNTY COMMUNITY

# Demand Quality

LET'S IMPROVE THE BUG BOUNTY MODEL

- The largest obstacle facing bug bounties right now are 'beg bounty' hunters
  - Submit as many reports as possible
  - Consistently low-quality, inaccurate, copied from a scanner
- Companies so far have not addressed this issue
- My appeal to bug bounty community:

**State that researchers who consistently submit low-quality reports will not be invited to continue.**

# References

USEFUL SOURCES

- *Bounty Launch Lessons* - https://medium.com/@magoo/bounty-launch-lessons-c7c3be3f5b

# Thank you – Questions?

- @bishopfox / www.bishopfox.com
- zjulian@bishopfox.com
- @tprime_

(ISC)² PHOENIX CHAPTER, INC

BISHOP FOX®