Bug Bounty at my Org?

It's more likely than you think

Presented By: Ashley Rider
Andrew Durgin

Disclaimer

➢ The views and opinions expressed here represent our own and not those of the people, institutions or organizations that we may or may not be associated with, unless stated explicitly.

Introductions

Ashley Rider

- Ashley has worked at Paychex since graduating college in 2005, with 14 years' experience across multiple disciplines within Information Security, including Security Identity Management, Security Engineering, and Vulnerability Assessment and Management. She is currently responsible for managing the Security Assessment team. Ashley graduated from Rochester Institute of Technology in 2005 with a Bachelor's degree in Information Technology. Ashley works hard to build strong cross-functional partnerships to continuously improve Security across the entire organization in a complex and continuously changing threat landscape.

Introductions

Andrew Durgin

➢ Andrew joined the USAA Information Security team in December 2017 to focus on Web Application security. Prior to this, Andrew worked over a decade at Paychex, Inc. serving various roles in Information Security, including Security Engineering, Security Assessment, and Security Operations Management. Andrew graduated from Rochester Institute of Technology in 2005 with a Bachelor's degree in Information Technology. Andrew finds satisfaction in providing realistic solutions that enables the organization while at the same time strengthening their security posture.

Overview

- What is Bug Bounty?
- Potential Benefits
- Things to Consider
- Where to Start?
- Private vs. Public Programs
- Vulnerability Management
- Performance Metrics
- Cost Analysis
- Lessons Learned
- Conclusions
- Q & A

What is “Bug Bounty”?

“**Bug Bounty**” is a concept where researchers can be rewarded, via recognition and/or compensation, for responsible disclosure of security vulnerabilities and exploits.

= $

Does this fit within Corporate InfoSec?

- **Security Assessment:** Automated scanning tools to access the posture of a system and/or application

- **Penetration Test:** An authorized manual attack against a system or application, used to identify security vulnerabilities and exploits, allowing the attacker to gain access to the system and/or data

- **Bug Bounty:** Crowdsourced penetration testing, offering monetary rewards to anyone who can find and report a vulnerability or exploit

- **Responsible Disclosure:** For an Organization, this means accepting ***and acting*** on notifications of vulnerabilities without legal action against the researcher

The “Crowd”

- Who are the researchers?
  - Located worldwide - anyone with an Internet connection
  - Novice to Expert skill level

- Vetting process
  - Depends on the type of program and/or vendor framework, you may have some ability to “filter” researchers

Potential Benefits

- Cost
  - Per vulnerability is less than a traditional penetration-test
- Quality
  - May exceed a traditional penetration-test
- Resources
  - 1-to-many testers with varying skill sets and background
- Coverage
  - Target coverage can be defined as wide or narrow as desired

Things to Consider

- Resources
  - Difficult to anticipate *your* resource commitment
- Coverage
  - No guarantee of what gets tested
- Timeliness
  - Submissions may not align with your timeline
- Risk of Public Disclosure
  - *A researcher can go public with or without a bug bounty program*

Where to Start?

- Research!
  - Multiple vendors within the Bug Bounty space
  - Potential applications to target
- Build Senior Leadership and Legal Support
  - Use business terms that leadership understands
- Start with a SMALL PoC
  - Limit the PoC to a single web application target
  - Start with the lowest bounty payouts

Private vs. Public Programs

- Private
  - **Pro**: Invite Only: Ability to limit the number of researchers
  - **Pro**: Refine your internal process without the public watching
  - **Con**: Interest and submissions can dwindle over time

- Public
  - **Pro**: Any security researcher is welcome to participate
  - **Pro**: Great coverage
  - **Con**: Can quickly overwhelm if your application does not have a strong security posture
  - **Con**: Difficult with managed services and subscriptions that require significant set-up for user accounts
  - **Con**: Bogus/irrelevant findings

Should I self-manage Bug Bounty?

- ***Proceed with CAUTION!***

- Many companies are not staffed to handle the influx of submissions, triage, and communication to the researchers
  - The current “in-the-moment” fire always takes priority over normal BAU work

- Limited to a Public Bug Bounty Program
  - No established connections to security researchers

Vulnerability Management

- ➢ **If your organization is not prepared to remediate findings timely, do not invest in a Bug Bounty Program!**

- A vulnerability reported through Bug Bounty should be validated by internal resources prior to acceptance and reward payment

- Look to build efficiencies that move an accepted finding into your VM process automatically, using API Integrations

Performance Metrics

- Essential to measure the success of your Bug Bounty program
  - Keep researchers engaged
    - Processing time to validate submissions and approve payment
    - Average cost per vulnerability by Severity
    - Accepted Submissions vs. Total Submissions
    - YTD spend on Bug Bounty reward payouts

  - Prove value to your Organization
    - Mean-time-to-fix
    - Discovery & Remediation trends
    - Relative risk by Application

Cost Analysis

Bug Bounty Maturity Model*			
Payout by Severity	**Basic**	**Progressive**	**Advanced**
Critical	$1,500	$5,000	$15,000
High	$900	$1,800	$2,700
Medium	$300	$600	$900
Low	$100	$200	$300
Minimal	$0	$0	$0
Payout Range	**$100 - $1,500**	**$200 - $5,000**	**$300 - $15,000**

*Bugcrowd: What’s a Bug Worth? Defensive Vulnerability Pricing Model

Type	Testers	Duration	Cost	Critical	High	$ per C/H Finding	Medium	Low
Traditional Penetration Test	2	11 weeks	$29,000	2	3	$5,800	10	**37**
Bug Bounty	**7**	**12 days**	$60,000	**12**	**29**	**$1,500**	18	4

Lessons Learned

- Resource requirements
- Timely triage
- Each instance of XSS is a unique “bug”

Researcher Behavior

- ➢ Tips for **_*those*_** researchers
  - Potential phishing by researcher
  - Non-issues/misrepresentation
  - Multiple submissions for variations of the same vulnerability
  - Disagreement on severity or payout
  - Adjustment of severity AFTER the payout

- Lean on your vendor resources to deal with problematic researchers

Conclusions

- ➢ Bug Bounty is a companion, not a replacement, of your existing dedicated security testing resources
- ➢ Consider it one of many channels that can feed your Vulnerability Management program
- ➢ Monitor for submission trends
  - Pursue any areas of opportunity discovered
  - Unknown Unknowns

Q & A

Ashley Rider
aeh4945@gmail.com
LinkedIn: www.linkedin.com/in/ashley-rider

Andrew Durgin