Working with Hackers

A (brief) look at implementing Vulnerability Disclosure Policies & Bug Bounties

GLITCHWITCH.IO

NO PHOTOS / VIDEO PLEASE

Please respect my privacy and refrain from taking photos.

Slides and overview available at **glitchwitch.io/blog/**

Thank you :)

glitchwitch@longcon:~$ whoami

- GlitchWitch (they/them)
- Currently a Freelance Information Security Researcher
- Working in IT for over a decade
  - IT Admin & Manager
  - Web Developer
  - Server Admin
  - Freelance Consultant
  - Wearer of many hats
- Occasional backyard auto mechanic

More information about services: **glitchwitch.io/services/**

What you will learn... (hopefully)

Vulnerability Disclosure & Reporting

- Why you should have a policy in place
- Best practices for implementing a policy
- Resources for starting your own

Bug Bounties

- The benefits of running a bug bounty
- How to prepare for launching a bounty program

What is a Vulnerability Disclosure Policy?

“A vulnerability disclosure policy is intended to give hackers & researchers clear guidelines for submitting potentially unknown and harmful security vulnerabilities to organizations.” --HackerOne

A good Vulnerability Disclosure Policy (VDP) will...

- Provide a way for external parties to report security issues
- Define clear guidelines for scope, communication, and legal requirements
- Ensure safe harbour for researchers and program owners
- Ultimately improve the overall security posture of your organization

Why you need a Vulnerability Disclosure Policy

If you have a publicly accessible website or products, you should have a VDP!

Why?

- Nothing is 100% secure, there will be bugs
- Provides a clear path leading to quicker remediation
- Encourages hackers to tell you, rather than ignore, sell, or exploit the issue
- Helps quell fears from researchers who have faced legal threats in the past

Your VDP should include…

- Communication
    - Contact information (security@company.tld, PGP key, etc)
    - Expected response times
    - Information to include in report
    - Acknowledgment, Hall of Fame, Rewards, etc
- Scope
    - Domains, products, IPs
    - Restrictions (no DoS, don’t steal user data, no phishing, etc)
- Disclosure
    - Set terms and expectations around potential full disclosure
- Legal
    - Promise to not take legal action against researchers who act in good faith

Vulnerability Disclosure Policy Resources

- Open Source Vulnerability Disclosure Framework
  - Maintained by BugCrowd and CipherLaw
  - Designed to prepare your organization to work with independent security researchers
- Disclose.io
  - Expands on the work done by Bugcrowd and CipherLaw
  - Attempts to standardize best practices around safe harbour for good-faith security research
- ISO/IEC 29147
  - Provided for free by the International Organization for Standardization
  - Gives guidelines for the disclosure of vulnerabilities in products and online services
- Other Companies' VDPs
  - Popular examples include Google, Cloudflare, Dropbox

Common Pitfalls

Communication

- Not having a timely response
- No internal communication or documentation path

Resources & Staffing

- Lack of customer service skills
- Inability to validate and prioritize findings
- Inability to fix the bugs that are reported to you

What about bug bounties?

A bug bounty differs from a Vulnerability Disclosure Policy in a few ways.

Bug bounties expand on VDPs by offering incentives and financial rewards for vulnerabilities discovered by researchers.

Bug bounties are typically set up after you already have good security posture.

Bug bounties are not for everyone!

Bug Bounty Program Preparation

Before you launch a successful bug bounty program, you’re going to want to have a few things down first.

- An existing Vulnerability Disclosure Policy
- A budget for paying researchers
- Good security posture
- Security testing

Bug Bounty Considerations

Rewards

- How will you reward researchers?
- What information are you willing to pay for?
- How much are you willing to pay?

Platform

- Where will you host your bug bounty?
- Will it be public or invite only?

Pros/Cons Bug Bounty Platforms

Pros

- International financial and tax paperwork is handled for you
- Managed bounties reduce internal workload
- Recognition and immediate response from hacker community

Cons

- Expensive (upwards of 20% of bounty payout)
- Third-party responsible for keeping vulnerability information secure
- Lots of submissions, often low quality ones

Conclusion

- Vulnerability Disclosure Policies help improve overall security
- VDPs encourage researchers to report findings they might not have
- VDPs take a lot of work to implement, but often are worth it
- Bug bounties are not for everyone
- Communication is key

Thank you for your time. Any questions?

Submit Questions at **goo.gl/slides/rxhsn2**

Need help launching a Vulnerability Disclosure Policy or doing security testing before a bug bounty? I’m available for hire!

Learn more at **GlitchWitch.io**