Organizing a BUG Bounty program

GetClouder

Marian Marinov < mm@1h.com >
What will I tell you?

- Why?
- How?
- The most interesting thing by now

GetClouder
Organizing a BUG Bounty program
I’m confident that we can not find all possible bugs in our software

Having a bounty program gives us higher credibility
  - people understand that we want to be secure... we don’t simply say we are
  - people like companies that think about customers issues

It made the people from our teams think more about security and write better code
First and most important, dedicate a person(s) that will handle the communication

Define the rules of engagement
- what is considered a bug
- what is not
- what is eligible for award

Verify each disclosure

Keep track of all disclosures

Create a Hall of Fame page

Award only the first disclosure
How?

- Dedicate time from each Dev team which will be reserved only for fixing bugs found through the Bug Bounty program.
- There will be bugs that are either invalid or are handled in a way that would be invisible to the researchers, prepare a template that explains this in a polite manner.
- Allow researchers to publish the information they have found, after you have fixed the problem.
- If anyone asked who was the first to find a specific bug, be prepared to point them to a link from the Hall of Fame page.
- If possible create a reward program.
Jakub Zoczek - DNS issues

- Hijacking our DNS cluster inserted NIMBUS.GETCLOUDER.COM and CUMULUS.GETCLOUDER.COM and pointed them to his own DNS server
- Inserted root-servers.net on our DNS cluster affected only local resolver
Thank you!

- https://www.getclouder.com/bounty
  - 
- Marian Marinov
- mm@1h.com
  - 
- Find me around, if you have any questions