Dosh4Vulns: Google's Vulnerability Reward Programs

Adam Mein
Chris Evans
Who?

- Chris Evans, Google
  - Engineer, researcher, troublemaker
  - Leads Chrome Security Team
- Adam Mein, Google
  - Program Manager, troublemaker
  - Central Google Security Team
  - PM for the Google Web initiative
- Both: cashiers
Agenda

- History
- Chromium
- Google Web
- Recommendations
- Conclusion
Agenda

- History
- Chromium
- Google Web
- Recommendations
- Conclusion
Agenda

- History
- Chromium
- Google Web
- Recommendations
- Conclusion
Chromium

- Program launched Jan 2010
  - Reward levels $500, $1000, $1337
- Program refreshed July 2010
  - New $3133.7 level for critical bugs; $1000 used for good quality reports
Total payout over $120,000
- Across 140 qualifying bugs
See the "Chromium Hall of Fame"
- Top reporter pocketed $28,000 (Serg Glazunov)
All open-source (good, bad and ugly)
- A public and consistent track record
Participants include people from China, Finland, France, Italy, Japan, Netherlands, Poland, Russia, Spain, Sri Lanka, USA, Vietnam, etc.
- Lot of money in some countries
Chromium :: positives

- Many fewer bugs in Chromium
  - Getting harder to find bugs
- Better value for money than contracted audits
- Sense of community
- Hiring opportunities
- Huge diversity of talents and bug classes
- Seen as industry leaders in associated PR
- Benefits to other software: Safari, iPhone, Android, Blackberry, Windows 7, Flash, libxml
Chromium :: negatives

- None really?
  - I couldn't be happier
- Hard work
  - We have resource and buy-in to handle the load
- Lesser quality reports
  - Laugh them off
Agenda

- History
- Chromium
- Google Web
- Recommendations
- Conclusion
Google Web :: preparation

- feedback/support from:
  - security team
  - legal
  - budget
  - all Google engineers

- panel formation
- war room
- clarification about in/out of scope
Google Web :: scope

- web properties, no clients apps
- vulns: XSS, XSRF, etc
- excluded:
  - DoS, corp infrastructure, SEO
  - blackhat
  - acquisitions (if < 6 months)
$500, $1000, $1337 or $3133.70
may aggregate vulnerabilities in "common" locations
increase based on:
  ○ severity of vuln, not value of data (one exception...)
  ○ novel / interesting
Google Web :: eligibility

- reasonable notice
- private disclosure
- appropriate testing
- first in, best dressed
• immediate increase in reports
  ○ decent signal-to-noise ratio
• increased breadth
• clever bugs
• fun bugs
Bugs filed / week
What types of bugs do they find?
Are they new or old finders?

- Existing: 14.8%
- New: 85.2%
Where do they live?

- USA: 13.6%
- Rest of the World: 86.4%
• Top 20% of people are responsible for how many bugs?
● top 20% of people are responsible for how many bugs?

~80%
how much have we paid?
How much have we paid?

$3,552,465,750
how much have we paid?

$3,552,465,750

(Vietnam Dong)
how much have we paid?

$170,178

(US dollars)
Donating to charity

- Donated: 98.6%
- Didn't donate: 1.4%
Google Web :: benefits

- more bug reports = more bug fixes
- compelling value for money
- relationships with new bug reporters
Google Web :: challenges

- low quality reports looking for cash
- dealing with unsavory characters
- resources to triage and administer
- new addition to the "not a bug" argument
Google Web :: challenges

● some dislike cash for vulnerabilities
● what if low quality exceeds the high?
● harder for everyone else?
● can we ever stop?
Agenda

- History
- Chromium
- Google Web
- Recommendations
- Conclusion
Recommendations

- must love bugs
- need to run a tight ship
- get your resources sorted
  - 1000% increase first 2 weeks
  - 200-300% after
- get buy-in from the bug fixers
Recommendations

● proactively communicate common "non-issues"
● think global
  ○ language translation
  ○ PR
● look after the best
Agenda

- History
- Chromium
- Google Web
- Recommendations
- Conclusion
Conclusion

- Has it been a success for Google?
  - Yes!

- Should you start a VRP?
  - Maybe...
Questions...