Agenda

- History of Bounty Programs
- Mozilla Web Bounty Results
- Launching a Web Bounty Program
- Common Bounty Concerns
- Conclusion
Agenda

- History of Bounty Programs
- Mozilla Web Bounty Results
- Launching a Web Bounty Program
- Common Bounty Concerns
- Conclusion
History of Bounty Programs

- 1995 - Netscape
- 2002 - iDefense
- 2004 - Mozilla Firefox
- 2005 - ZDI
- 2007 - Pwn2Own

- 2010
  - Google Chromium
  - Deutsche Post E-Postbrief
  - Google Web
  - Mozilla Web
  - Barracuda

- 2011
  - Hex Rays
  - Facebook
Types of Programs

- Open to all - Reported direct to software maker
  - (1995) Netscape
  - (2004) Mozilla Firefox
  - (2010) Google Chromium
  - (2010) Google Web
  - (2010) Mozilla Web
  - (2010) Barracuda
  - (2011) Hex Rays
  - (2011) Facebook

- Central “Clearing House”
  - (2002) iDefense
  - (2005) ZDI TippingPoint

- Pre-Approved Teams / Competition
  - (2007) Pwn2Own
  - (2010) Deutsche Post E-Postbrief
Programs for the Web

- Mozilla Web Bounty
  - $500 - $3000

- Google Web Bounty
  - $500 - $3137

- Facebook Security Bounty
  - Typically $500, paid up to $5000

General Policies
- Select web sites in scope
- Critical issues
- Paid for new issues (not dupes)
Bounty Programs - Why?

- User & user data safety is #1
- Productive relationship with community
- Work directly with researchers
- Consistent security at scale is hard
- Not competing with black market
Agenda

- History of Bounty Programs
- Mozilla Web Bounty Results
- Launching a Web Bounty Program
- Common Bounty Concerns
- Conclusion
Mozilla Web Bounty - Scope

- Goal: Protect Users
- Critical issues such as xss, csrf, code injection, authentication flaws

Sites In Scope

- bugzilla.mozilla.org
- *.services.mozilla.com
- getpersonas.com
- aus*.mozilla.org
- www.mozilla.com/org
- www.firefox.com
- www.getfirefox.com
- addons.mozilla.org
- services.addons.mozilla.org
- versioncheck.addons.mozilla.org
- pfs.mozilla.org
- download.mozilla.org
Mozilla Web Bounty - Submission Timeline

Bugs By Date

- November-10: 3
- December-10: 87
- January-11: 42
- February-11: 7
- March-11: 10
- April-11: 13
- May-11: 13
- June-11: 15
- July-11: 19
- August-11: 12
- September-11: 3

Monday, September 26, 2011
Mozilla Web Bounty - Bugs Reported

Reported Bugs - New vs Duplicate

- New Bugs: 79%
- Duplicates: 21%

Monday, September 26, 2011
Mozilla Web Bounty - Types of Issues Reported

Bugs by Category

- XSS: 60%
- Other: 13%
- CSRF: 10%
- Input: 7%
- SQLInject: 5%
- Auth: 3%
- TLS: 2%

Monday, September 26, 2011
## Mozilla Web Bounty - The Reporters

### How Many Bugs Are People Submitting?

<table>
<thead>
<tr>
<th>Number of Bugs Submitted</th>
<th>Percentage of Reporters</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Bug</td>
<td>47%</td>
</tr>
<tr>
<td>2-5 Bugs</td>
<td>33%</td>
</tr>
<tr>
<td>6+ Bugs</td>
<td>20%</td>
</tr>
</tbody>
</table>

Top 11% of bug finders contribute 56% of bugs
Mozilla Web Bounty - What is Submitted

- Failure in design patterns - ex: image uploads
- Procedural gaps / forgotten servers
- Smaller traditional bugs
Mozilla Web Bounty - The Bounties

$104,000* Total Paid (since Dec, 2010)
175 Bugs Submitted
64 Qualifying bugs
24 Paid Contributors

* Mozilla Web Bounty, not including Firefox Bounties
Mozilla Web Bounty - Bounty Payments

Count By Bounty

- $500: 20
- $1,000: 11
- $1,500: 4
- $3,000: 25

Monday, September 26, 2011
Mozilla Web Bounty - Bounty Payments

Total Payout & Count By Submitter

- $25,000: 9
- $20,000: 11
- $15,000: 5
- $10,000: 5
- $5,000: 4
- $0: 3

Unqiue Contributor

Monday, September 26, 2011
Mozilla Web Bounty - Benefits

- Engages community
- Produces many high value bugs
- Bounty is not purchasing silence
- Security at huge scope
- Identifies clever attacks & edge cases
Mozilla Web Bounty - Lessons Learned

- Initial spike of work load
- Prepare necessary teams
- Response time & communication is critical
- Researchers & directions - not always a perfect match
Mozilla Web Bounty - Worth It?

YES!
Agenda

- History of Bounty Programs
- Mozilla Web Bounty Results
- Launching a Web Bounty Program
- Common Bounty Concerns
- Conclusion
Bounty Programs - Why?

- User & user data safety is #1
- Productive relationship with community
- Consistent security at scale is hard
- Not competing with black market
Launching Your Own Web Bounty Program

Bug bounties are an enhancement, not a substitute for any portion of a secure SDLC
Bounty Programs - Preparation

- Gain developer & team lead support
- Check your code
- Define clear reporting process
- Define scope and types of issues
- Build team to respond to reports & establish response time goals
- Announce program
- Root cause analysis
- Learn & adjust
Agenda

- History of Bounty Programs
- Mozilla Web Bounty Results
- Launching a Web Bounty Program
- Common Bounty Concerns
- Conclusion
Bounty Concerns

- Common concerns with web bounty programs
  - Encourages attackers
  - Too expensive
  - Veil of cover for attackers
  - Bounty program duplicates internal security work
  - Can’t compete with black market

We’ll address why these concerns aren’t necessarily valid
Bounty Concerns - Encourages attackers

- Bad guys already attacking you
- Without bounty program good guys afraid to test or report
- Bounty program enables participants that will help you
Bounty Concerns - Too Expensive

- Very high value
- Compare bounty payout with equivalent 3rd party testing
- Provides continual testing
- Use individual bugs to identify root cause flaws
- What percentage of profit spent on security?
Bounty Concerns - Veil of cover for attackers

- Goal is to identify flaws, not identify bad guys
- One possible deployment:
  - Full security controls & active blocking in prod
  - Setup public stage for testing with dummy data
  - Configure production to actively blocks attackers
  - Stage area could be next revision of code for prod
Bounty Concerns - Duplicates Internal Security Work

- You don’t know what you don’t know
- Identifies process breakdowns
- Identifies areas for training in secure sdlc
- Another tactic to protect users & critical data
Bounty Concerns - Can’t Compete with Black Market

- Bounty programs and black market target different audiences
- Some people are bad, but many people are good
- Many don’t want hassle or questionable ethics/legalities of black market
Bounty Concerns - Can’t Compete with Black Market

- Black market process
  - Identify critical issue
  - Weaponize exploit
  - Find buyer on underground market
  - Negotiate price
  - Give bank account info for wire transfer? Arrange meeting for large cash exchange?
  - File appropriate tax returns?

- Bug bounty process
  - Identify critical issue
  - Report issue to reputable program
  - Receive bounty from organization
  - Feel happy you’ve helped the world be safer
Agenda

- History of Bounty Programs
- Mozilla Web Bounty Results
- Launching a Web Bounty Program
- Common Bounty Concerns
- Conclusion
Conclusion

Web Bounty Program works great for Mozilla

Recommend exploring how this may work for you

Leverage lessons learned & evaluate risk/benefit
Question?

@_mwc
michael-coates.blogspot.com