BUILD IT BREAK IT FIX IT

A security-minded programming contest

Run by professors and students at the

University of Maryland, College Park USA

Funding provided by

National Science Foundation
WHERE DISCOVERIES BEGIN

MOTIVATING A NEW SECURITY CONTEST

- Today's contests reward those who can **break** systems by finding vulnerabilities
  - DEFCON CTF, Collegiate Cyber defense challenge (CCDC), Pwn to Own, …
- But we also want the opposite: reward those who can **build more secure systems**
  - Not the same skillset set as breaking things
  - Of direct relevance to companies, and society

BUILD IT, BREAK IT, FIX IT CONTEST

- Contestants can participate in two ways
  - **Build-it teams**: build security-sensitive software
  - **Break-it teams**: find flaws in built software
    - Build-it teams fix flaws found by break-it teams
- Separate winners for building and breaking
  - Individuals (or teams) can do both
- Open to US college student participants nationwide
  - Participation is remote, on-line
- Scheduled this fall starting 8/28/2014

BUILD IT, BREAK IT, FIX IT: OVERVIEW

Round 1:
Build-it team
Contestants build software to specification

72 hours

Must satisfy basic correctness and performance requirements
Starts 8/28/2014

Round 2:
Break-it team
Contestants report bugs in submissions

72 hours

Bug reports are (failing) executable test cases, including exploits
Starts 9/4/2014

Round 3:
Build-it team
Fixes bugs in their software found by break-it teams

48 hours

Doing so may wipe out many bug reports in one go: all count as the same bug
Starts 9/12/2014

Last: Judges tally final results

GOALS

- Empirically assess what actually works by correlating features of submission with team performance
  - Programming language, framework, library, …
  - Developer experience, S/W process, …
  - Using static analysis, fuzz testing, etc. …
- Encourage defense, not just offense
  - Tie together security with reliability: Bugs are bad, whether they are exploitable or not
  - Elevate real concerns: performance and feature-fullness
- Provide direct feedback to contestants
  - The contest penalizes a lack of security: “feel” the mistake!

SCORING

- Build-it team
  - Gains points for good performance
  - Gains points for implementing optional features
  - *Loses* points for (unique) bugs found by breakers
    - More points for exploits
    - Fixing bugs helps show that multiple test cases might be tickling the same bug, thus reducing the penalty for those test cases
- Break-it team
  - Gains points for unique bugs found (scaled by how many other teams found the same bug)
    - Note that they are given access to submission source code
- Judges determine the 1st and 2nd place teams for both categories after round 3 (four prizes total)

PLATFORM

- Submissions must run in a Linux VM that we will provide
  - We unpack their submission in a defined directory and then run tests etc. within the VM
- Several benefits
  - VM is isolated from other software, limiting its negative effects on ours and others' software
  - Run-time environment is clearly defined (in advance), yet affords plenty of flexibility

DATA

- Teams must use a git repository, and share access to it with us
  - So we can see their process and intermediate checkins
- Teams must answer (brief) popup surveys during each phase
  - What are you working on? What problems are you dealing with? Who is doing what?
- And, of course, tests and final submissions available

For companies:
Sponsorship Opportunities

GET INVOLVED: SPONSORSHIP

- Three sponsorship levels
  - $2500 = Gold
  - $1500 = Silver
  - $750 = Bronze

- Benefits:
  - Shows your commitment to securing (not just breaking) systems
    - Logos, names noted prominently in contest materials (based on sponsorship levels)
  - Access to motivated, security-conscious students; we are aiming for 300-400 participants drawn from top CS schools
    - Gold and Silver: access to provided participant resumes, contact info
    - Gold: an event with participants co-located with the Cyber Maryland conference, and first access to resumes

GET INVOLVED: PARTICIPATION

- Provide personnel/input to help out
  - Human judges to resolve disputes
  - Professional “break-it” team
  - Designers of contest programming tasks
  - Other possibilities too (let us know)
- Company participants will be noted prominently on contest materials
  - Again: show your commitment to both sides of the security equation: breaking **and** building

JOIN US!

- Help us shift our nation's security mindset
  - Don't just reward those who can find flaws like the Heartbleed bug,
  - Reward those who build systems without such flaws in the first place!
- Your sponsorship and participation can make the contest a success
  - And gain you access to the best and brightest security-oriented minds
- See also our sponsorship document