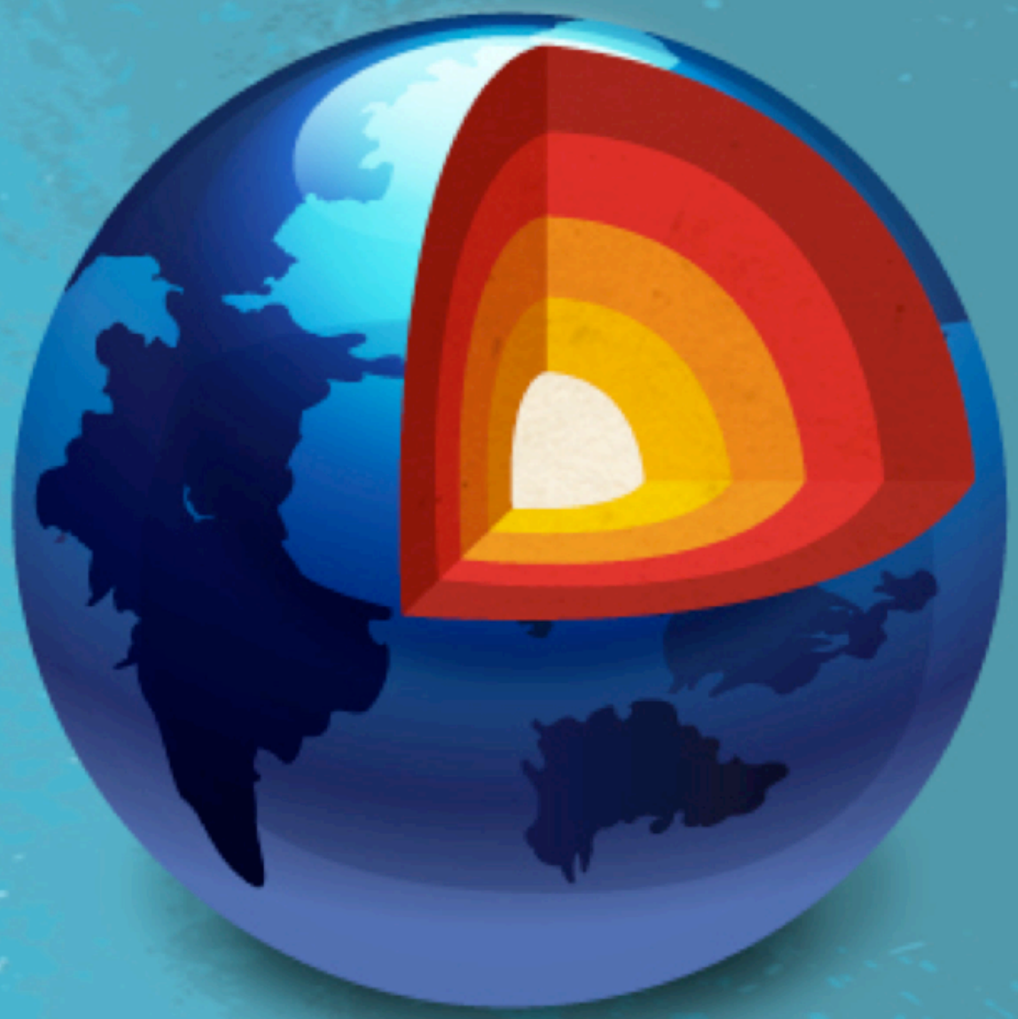
mozilla

REAL WORLD SECURITY

Security in an Open Source Project

Who is in the MOZILLA COMMUNITY?



- **CORE CONTRIBUTOR** *(hundreds)*
- **ACTIVE CONTRIBUTOR** *(thousands)*
- **CASUAL CONTRIBUTOR** *(hundreds of thousands)*
- **SUPPORTER** *(millions)*
- **USER** *(hundreds of millions)*

Find out where you fit in: wiki.mozilla.org/community

MOZILLA SECURITY

- Security Engineering Team
- Security Assurance Team
- Security Champions

SECURITY ENGINEERING

- “Builders”
- Team focused on security & privacy features
- Design & Implement new features and fix broken stuff

SECURITY ASSURANCE

- Security Assurance
  - Two Teams
    - Application Security - “Breakers”
    - Operations Security - “Defenders”

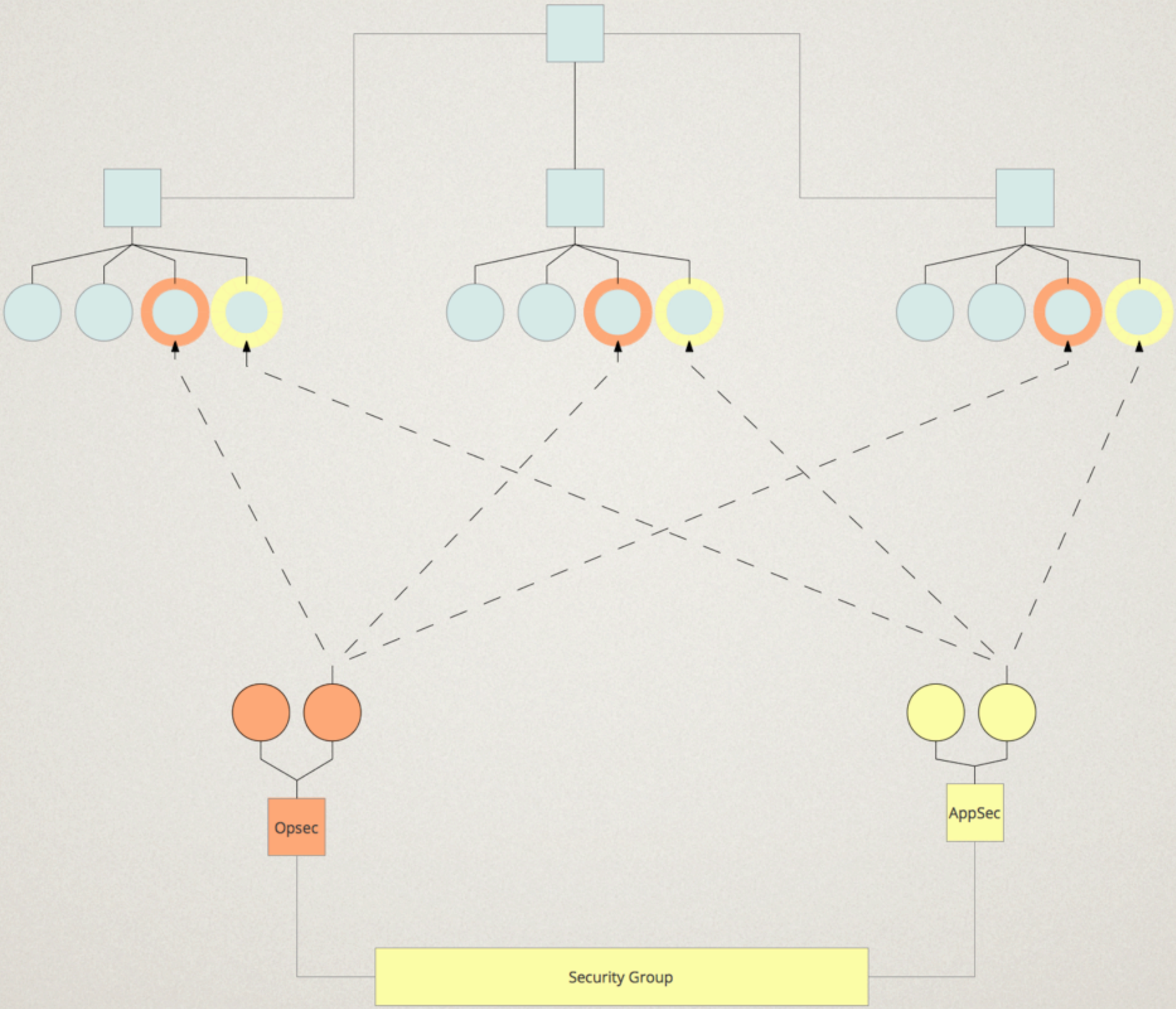
OPERATIONS SECURITY

- Traditional Network & Host Security
  - Network Security Monitoring
  - Hardening, Infrastructure Testing
  - Server & Network Security
  - Operating System Security

APPLICATION SECURITY

- Web & Platform Security
  - Security for all Mozilla hosted services and sites
  - Security for all products Mozilla ships
  - Code review, pen testing, vendor security
  - Security architecture & risk assessment

Engagement Model



SECURITY CHAMPIONS

- Everyone Else!
  - Contributors interested in security
  - Security Mentors
    - SMEs in areas that help out
  - Security Champions
    - Project team members who “own” security

mozilla

BUG BOUNTY PROGRAM

Break Stuff, Make Money!

BUG BOUNTIES

- Break Stuff
  - Find legitimate security issues in products, services & sites
- Get Money
  - Get money ($500-$3000 depending on risk)

BUG BOUNTIES

- How much?
  - > $600,000 since program started
- Who?
  - Many people, but a core set of consistent contributors
  - Youngest? 12

REAL WORLD BUGS

Real World Bugs

BUG #1 - XSS

- [One of the] Worst Offenders!
- ~600 bugs on file
- Allows execution of script supplied by an attacker

EXAMPLE

- litmus.mozilla.org
  - Test case management service
  - Conveniently provides a learning tool for XSS :/
- Stored XSS

```
"><""<img src="<img src=search"/
onerror=alert(document.cookie)//">@inva
lidemail.info
```

BUG #2 - CSRF

- State Management Bug

- ~200 on file

- Allows an attacker to leverage the browser to access an authenticated session

BUG #3 - SQLI

- Allows an attacker to run arbitrary queries
- Any SQLi allows complete compromise of the database
- Example: https://bugzilla.mozilla.org/show_bug.cgi?id=701920

NO DEMO!

- I don’t have a real world, working exploitable site that I have permission to use :(

```
@@ -229,8 +230,8 @@ def processCallers(caller, path=None, funcid=None):
    # Instead, let's first find the function that we're trying to find.
    cur = conn.cursor()
    if funcid is None:
-     cur.execute('SELECT * FROM functions WHERE fqualname %s' %
-       like_escape(caller))
+     cur.execute('SELECT * FROM functions WHERE fqualname LIKE ?', (
+       '%' + caller + '%'))
```

- Simple to fix, easy to exploit

BUG #4 - LOCATION SECURITY

- Firefox 16
- Simple regression
- Violation of same origin policy
- window.location could be accessed if a page loaded a resource dynamically

3 WAYS TO HELP OUT!

- Contributor
- Mentorships
- Internships

CONTRIBUTOR

- Help find security bugs!
  - Open one of our sites
  - Start testing
  - File bugs
- Help Fix Bugs
  - Find an open bug in Bugzilla
  - Ask for help on how to fix it!

MENTORSHIP

- https://wiki.mozilla.org/Security/Mentorship
- Formal Volunteer Contribution Program
  - 200+ hour project
  - Assigned a Mentor
  - Structured opportunity to learn and contribute
- Benefits
  - Still qualify for bounties
  - Get credit for solving a problem
  - Gain practical experience

INTERNSHIPS

mozilla
UNIVERSITY RECRUITING

ABOUT GET INVOLVED PROJECTS mozilla

Seen enough? apply now »

Spend your summer doing good.

At Mozilla, we love interns. Don't take our word for it, though. Check out what our interns themselves have to say about working for us.

Meet our Teams »

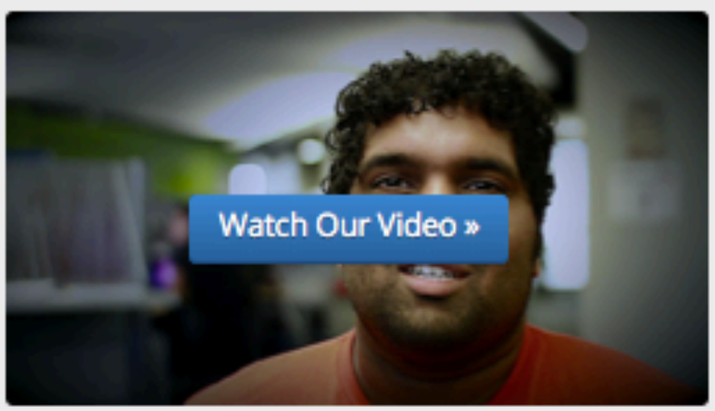
YouTube | Twitter | Facebook | IRC | Careers

Upcoming Events

Sep 11 CMU
Technical Opportunities Conference

Sep 11 Georgia Tech
Georgia Tech Career Fair

more...



PennApps Hackathon 2012

October 1, 2012

This past weekend, I had the privilege of attending the PennApps Hackathon at the University of Pennsylvania. This event was very dear to my heart, as I am an app developer in my day-to-day work. It was awesome to see so many students hacking on apps and building the "next big thing". Possibly the coolest [...]

read more »

QUESTIONS?

Yvan Boily
yboily@mozilla.com
@ygjb

Want to learn more?
OWASP, InfoSecBC, BSidesVancouver