2014-12-04 Developers Forum

How to Join

- By Browser
  - https://www.uberconference.com/openmrs

- By telephone
  - US telephone number: +1 201.479.2627

Agenda

- Quickly review previous meeting minutes (5 min)
- Web Application Security w/ Sherif Koussa CEO of SecurifyLabs
- Review next meeting agenda

Minutes

View at notes.openmrs.org

Developers Forum 2014-12-04

Attendees

- Sherif Koussa
- Burke
- Rafa
- Wyclif
- Ryan
- Michael D.
- Daniel
- Karl
- Tammy
- Willa
- Serghei Luchianov
- Jim Hinson
- Paul
- Mike S.
- Ada

Agenda/Notes

Security Challenges for open source projects
- Attackers can easily research the code for their attack
- Community Awareness – i.e., raising awareness among contributors & users
• Contributors
  • Some may be more aware than others
• Users
  • Where does responsibility of developer end & consumer's responsibility start?
    • For example, OpenMRS assumes the physical box is protected, all unnecessary ports closed, only SSH and TLS access to the box
• Ineffective Security Models

OpenSAMM <http://www.opensamm.org/> "Software Assurance Maturity Model"
  • A good way to look at software security from a bird's eye view
  • Can be scaled to need
  • Tries to help organizations form a strategy for software security that is tailored to need
  • Helps answers the common questions:
    • Where do we start?
    • What is the root cause of our security problems?
• Separates software development into 4 functions:
  • Governance – leadership, road map
  • Construction – development
  • Verification – validation, testing
  • Deployment – delivering software & support
• There are three security practices that goes into the 4 functions. (Sums up to 12)
• How would SAMM apply to OpenMRS?
  • Governance
    • Regional Privacy Regulations
    • Security Awareness – Toughest challenge among open source community.
    • Community Education
    • User Education
  • Construction
    • Regional Security Requirements
    • Global/Regional Threat
    • Secure Coding
  • Verification
    • Security Testing
    • Security Code Reviews
    • Baseline Security Assessment
    • Vulnerability Management
  • Deployment
    • Incident Response
    • Developer Guide
    • User Guide

Good Examples
  • phpBB
They have a lot of CVEs prior to 2009, then they dropped dramatically (CVE=Common Vulnerabilities and Exposures, see <https://cve.mitre.org/>)

In 2009, phpBB went into a rewrite for software and got external help from security company to do an audit.
  - They fixed the issues discovered by the review
  - They created a guideline for secure coding for developers (best practices and for code review)

Typo3
  - Has list of types of security threats (http://docs.typo3.org/typo3cms/SecurityGuide/TypesOfThreats/Index.html)

NodeJS
  - Has a security project

Tiki Wiki
  - Crowdfunded an effort to provide "baseline security testing" and the maintained it with check lists for devs & code review

Moving Forward (*'s indicate level of urgency; *** = most urgent)

  - Governance
    - Strategy and Metrics **
    - Education Strategy *
  - Construction
    - Security Design Reviews *** (best way to minimize attacks)
      - Developer’s Guide **
  - Verification
    - Baseline Security Testing ***
  - Deployment
    - User’s Guide **
    - Incident Response ***
    - Vulnerability Management **

Questions

  - How often should Baseline Security Assessments be done?
    - Every major release (i.e., once every 10 years...)
    - Also depends on how strictly code reviews are maintained
    - Not all assessments are equal (e.g., some vulnerabilities need to be assessed by someone with experience/expertise)

  - Is it sufficient to have a list of security-related concerns for code review? Or should we have code reviews focused specifically on security concerns?
    - Smaller, easier goals are better. Security-focused reviews might be hard to maintain.
    - Formalize security in existing code reviews by having a few key steps (e.g., top 5) that are expected in a code review

  - Are there any good tools to automate security issue detection (e.g., like Sonarqube)?
    - Static code analysis tools are helpful, but there are high ratio of false positives
      - Either invest a lot of time configuring the tool to avoid false positives OR focus on the topmost security threats

  - How should we handle security concerns that are reported?
  - Are there best practices in other FOSS projects that we can use as a base for our response process?
  - CVE, what else?
  - Typo3 has a good process

  - Is focusing on anonymous attacks (with assumptions of protected box & SSL) a reasonable approach?
    - reasonable
Action Items

- Create a "Security Guide" module like our "Style Guide" module to teach devs about common security issues and provide best practice examples
- Look at our previous security audit & get another security audit
- Ensure "Style Guide" and basic module template (examples provided from the community) are using best practices for security
- Ensure that implementers guide has "chapter" on security that not only describes the assumptions/expectations/responsibilities of setting up a system, but also outlines the potential consequences if a step is not taken (e.g., what's the risk if I don't use SSL? what if I don't change my encryption key?)
- Make sure that sonarqube address topmost concerns
- Schedule a future call to discuss specific action items

Sorry for the intrusion - how do i see the power point - <Jim Hinson>  
http://connect.iu.edu/omrsdf  
connect.openmrs.org, join Developers Forum. If you are connected to uberconference, be sure to click the speaker in Adobe Connect to turn it off to avoid creating feedback loop... better yet, mute yourself first. :-)  

TODOs

jiraissues: com.atlassian.confluence.extra.jira.exception.JiraIssueMacroException: com.atlassian.confluence.macro.MacroExecutionException: Jira project doesn't exist or you don't have permission to view it.

Create a TODO: http://go.openmrs.org/todo

Transcripts

- Audio recording of the call: Listen online or download (available after the meeting)