Projects – code review

PA193 – Secure coding

Petr Švenda
Faculty of Informatics, Masaryk University, Brno, CZ

CROCS
Centre for Research on
Cryptography and Security

PROJECT: CODE REVIEW 14TH DECEMBER

Project – code review part

- Analyze and attack parser of assigned group
  - Assigned mapping in previous slides
  - The code is available in target GitHub repository
- Review the code both manually and with tools
  - Comment on code quality and good/bad programming patterns
- Try to attack the code
  - i.e. find problematic inputs => crash, exception, memory leak, DOS, invalid accepted input…
- Use techniques and tools you learned!

Project – code review part (cont.)

- If you need more info, contact target team members
  - Write down log of your interactions with target team
- Open GitHub issues in target repository
  - (repository of team you are reviewing project for)
  - for every separate issue you will find + description
- Write 2-3 pages A4 report from code review
  - What tests did you performed (automated tests, manual review)
  - What did you focus on
  - What did you find out, how serious are the problems
- Prepare presentation for the last seminar Dec 14

Present results (Finding summary)

- Location of the vulnerability
- Vulnerability class
- Vulnerability description
- Prerequisites (for exploiting vulnerability)
- Business impact (on assets)
- Remediation (how to fix)
- Risk
- Severity
- Probability

Finding summary - example

Problem identification: DSA-1571-1 openssl
Severity: critical
Risk: high - directly exploitable by external attacker
Problem description: crypto/rand/md_rand.c:276 & 473 – The random number generator in Debian's openssl package is predictable. This is caused by an incorrect Debian-specific change to the openssl package. One of the sources of a randomness based on usage of uninitialized buffer *buff* is removed.
Remediation: revert back to usage of uninitialized buffer *buff*

Code review submission

- Join the seminar group as usual
- Presentations: 10-15 minutes per team
  - By all team members
- Prepare PPT or PDF slides
- Upload to IS vault ‘Project: Phase2 (review)’
  - 2-3 pages A4 from code review
  - Presentation slides

PROJECT: BUG FIXING
DUE: 20TH JANUARY 2018 24:00

Project – bug fixing part

- Attend presentation of code review for your project
- Read report provided by code review team
- Analyze open GitHub issues
- Fix bugs, commit changes, close issues properly
  - Use git commit to close issue
- Create bugfix(s) for problem(s) found (pull request)
- Notify me (svenda@fi.muni.cz) when all your issues are fixed
  - 20th January 2017 at latest