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
16TH DECEMBER

Project – code review part

- Analyze and attack mnemonic phrase generator of the assigned group
- Review the code both manually and with tools
  - Comment on code quality and good/bad programming patterns
  - Try to use tools not used by the original team
- 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 lecture Dec 16

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

- Presentation will be for all groups at once instead of lecture on 16th December
- Presentations: 10 minutes per team + discussion
  - By all team members
  - Please keep the assigned time – we need to fit all groups into 2 hours
- Prepare PPT or PDF slides
- Upload to IS vault ‘Project: Phase2 (review)’
  - 2-3 pages A4 from code review
  - Presentation slides

Project – bug fixing part

- For the issues found, open it as GitHub issues
- Select at least one non-trivial issue found
- Fix the bug, reference the GitHub issue and create pull request
- Present the screenshot showing the pull request during your presentation