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
DUE: 14TH DECEMBER 24:00

Seminar 10-12

Team A:
Surendra Sharma 459205@mail.muni.cz
Rajesh Mehta 459194@mail.muni.cz
T Ramu 459204@mail.muni.cz
Parser: PCAP FILES
https://github.com/surendra060/PCAP_TCP_PARSER/
Code reviews for: Team B

Team B:
Gonashvili, Mariami 459190@mail.muni.cz
Martin Bajanik 396204@mail.muni.cz
Milan Patnaik 459197@mail.muni.cz
Mayank Samadiay 459200@mail.muni.cz
Parser: TLSv1.0 – TLSv1.2 Record protocol + Handshake protocol
https://github.com/bayotop/tls-parser
Code reviews for: Team A

Seminar 14-16

Team C:
Maria Hatalova 410158
Matej Evin 422617
Simon Nespesny 422774
Parser: JSON parser
https://github.com/hhhj123/PA193-parser
Code reviews for: Team D

Team D:
Valentyn Kuznietsov, učo 448296
Peter Soóky učo 448291
Zuzana Matějková 442060
Parser: PDF ver. 1.3 parser
https://github.com/sookyp/PA193_parser
Code reviews for: Team E

Team E:
Fatjona Poda - 464247@mail.muni.cz
Michal Rajčan - 396338@mail.muni.cz
Marco Gasparini - 464395@mail.muni.cz
Parser: zip parser
https://github.com/xire-/SecureCodingParser
Code reviews for: Team C

Seminar 16-18

Team F:
Petr Veselý (454919)
Maruthi Gillela (459206)
Guruprasad Bidare Venkatesh (459196)
Parser: gif
https://github.com/lastfreenickname/GIFparser
Code reviews for: Team G

Team G:
Prashanth Reddy g uco 459207
Suresh Kumar Badddipudi UCO 459198
Svačina, Lukáš
Parser: PNG parser
https://github.com/sureshbaddipudi/PNG-Parser
Code reviews for: Team H

Seminar 16-18 (cont.)

Team H:
Ashwin Arvind Yakkundi 459202@mail.muni.cz
Rajesh Kumar hackme.rajesh@gmail.com
Ananya Chatterjee 459203@mail.muni.cz
Parser: TIFF 6.0 without compression
https://github.com/PA193/Parser-Project
Code reviews for: Team I

Team I:
Martin Sárkány 410016
Balaji Kommuru 459208
Mohammad Akhtar 459199
Parser: PCAP
https://github.com/balaji-kommuru/PCAP-PARSER
Code reviews for: Team F

Project – code review part

- Analyze and attack parser of assigned group
  - Assigned mapping in previous slides
  - The code is available in target GitHub repository
  - Presentations available in *PA193Parser_presentations.zip*
- 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 15

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 a randomly selected team member
- Prepare PPT or PDF slides
  - Upload into IS together with other files in advance
- Deadline Dec 14 by 24:00 to put files into the IS
  - “Parser - code review and presentation” vault
  - 2-3 pages A4 from code review
  - Presentation slides

PROJECT: BUG FIXING
DUE: 20TH JANUARY 2017 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