

**Software Security**

**Fuzzing project**

# Fuzzing group project

- Form a team with 4 students
- Choose an **open-source C(++)** application that can take **input from the command line** in some **complex file/input format**
  - For instance, any graphics library for image manipulation
  - Check on <http://lcamtuf.coredump.cx> if it has already been fuzzed with afl; if so, you will have to test old release
  - Check that the build process is not too complex given your C/C++ experience
- Try out **fuzzing tools** – **afl/afl++**, **zuff**, **HongFuzz**, ... - to look for security vulnerabilities (esp. memory corruption)
  - with/without **instrumentation** - **ASan**, **MSan**, **UBSan**, **valgrind**,... for additional checks on memory safety
  - Optional variations: 1) investigate bugs; 2) check against known CVEs, 3) introduce bugs; 4) test older releases; 5) try different settings or seed inputs; 6) try other fuzzing tools; ...

# afl trophy list <https://lcamtuf.coredump.cx/afl/>

|                                                                                                                                                                  |                                                                                                                                                                           |                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| IJG jpeg <a href="#">1</a>                                                                                                                                       | libjpeg-turbo <a href="#">1</a> <a href="#">2</a>                                                                                                                         | libpng <a href="#">1</a>                                                                                                              |
| libtiff <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> <a href="#">5</a>                                                                | mozjpeg <a href="#">1</a>                                                                                                                                                 | PHP <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> <a href="#">5</a>                                         |
| Mozilla Firefox <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a>                                                                          | Internet Explorer <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a>                                                                                 | Apple Safari <a href="#">1</a>                                                                                                        |
| Adobe Flash / PCRE <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a>                                                                       | sqlite <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> ...                                                                                        | OpenSSL <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> <a href="#">5</a> <a href="#">6</a> <a href="#">7</a> |
| LibreOffice <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a>                                                                              | poppler <a href="#">1</a>                                                                                                                                                 | freetype <a href="#">1</a> <a href="#">2</a>                                                                                          |
| GnuTLS <a href="#">1</a>                                                                                                                                         | GnuPG <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a>                                                                                             | OpenSSH <a href="#">1</a> <a href="#">2</a> <a href="#">3</a>                                                                         |
| PuTTY <a href="#">1</a> <a href="#">2</a>                                                                                                                        | ntpd <a href="#">1</a> <a href="#">2</a>                                                                                                                                  | nginx <a href="#">1</a> <a href="#">2</a> <a href="#">3</a>                                                                           |
| bash (post-Shellshock) <a href="#">1</a> <a href="#">2</a>                                                                                                       | tcpdump <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> <a href="#">5</a> <a href="#">6</a> <a href="#">7</a> <a href="#">8</a> <a href="#">9</a> | JavaScriptCore <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a>                                                |
| pdfium <a href="#">1</a> <a href="#">2</a>                                                                                                                       | ffmpeg <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> <a href="#">5</a>                                                                          | libmatroska <a href="#">1</a>                                                                                                         |
| BIND <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> ...                                                                                                   | QEMU <a href="#">1</a> <a href="#">2</a>                                                                                                                                  | lcms <a href="#">1</a>                                                                                                                |
| Oracle BerkeleyDB <a href="#">1</a> <a href="#">2</a>                                                                                                            | Android / libstagefright <a href="#">1</a> <a href="#">2</a>                                                                                                              | iOS / ImageIO <a href="#">1</a>                                                                                                       |
| FLAC audio library <a href="#">1</a> <a href="#">2</a>                                                                                                           | libsndfile <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a>                                                                                        | less / lesspipe <a href="#">1</a> <a href="#">2</a> <a href="#">3</a>                                                                 |
| strings (+ related tools) <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> <a href="#">5</a> <a href="#">6</a> <a href="#">7</a>          | file <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a>                                                                                              | dpkg <a href="#">1</a> <a href="#">2</a>                                                                                              |
| Info-Zip unzip <a href="#">1</a> <a href="#">2</a>                                                                                                               | libtasn1 <a href="#">1</a> <a href="#">2</a> ...                                                                                                                          | OpenBSD pfctl <a href="#">1</a>                                                                                                       |
| NetBSD bpf <a href="#">1</a>                                                                                                                                     | man & mandoc <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> <a href="#">5</a> ...                                                                | IDA Pro [reported by authors]                                                                                                         |
| clang / llvm <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> <a href="#">5</a> <a href="#">6</a> <a href="#">7</a> <a href="#">8</a> ... | nasm <a href="#">1</a> <a href="#">2</a>                                                                                                                                  | ctags <a href="#">1</a>                                                                                                               |
| mutt <a href="#">1</a>                                                                                                                                           | procmail <a href="#">1</a>                                                                                                                                                | fontconfig <a href="#">1</a>                                                                                                          |
| pdksh <a href="#">1</a> <a href="#">2</a>                                                                                                                        | Qt <a href="#">1</a> <a href="#">2</a> ...                                                                                                                                | wavpack <a href="#">1</a>                                                                                                             |
| redis / lua-cmsgpack <a href="#">1</a>                                                                                                                           | taglib <a href="#">1</a> <a href="#">2</a> <a href="#">3</a>                                                                                                              | privoxy <a href="#">1</a> <a href="#">2</a> <a href="#">3</a>                                                                         |
| perl <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> <a href="#">5</a> <a href="#">6</a> <a href="#">7</a> ...                           | libxmp                                                                                                                                                                    | radare2 <a href="#">1</a> <a href="#">2</a>                                                                                           |
| SleuthKit <a href="#">1</a>                                                                                                                                      | fwknop [reported by author]                                                                                                                                               | X.Org <a href="#">1</a> <a href="#">2</a>                                                                                             |
| exifprobe <a href="#">1</a>                                                                                                                                      | jhead [?]                                                                                                                                                                 | capnproto <a href="#">1</a>                                                                                                           |
| Xerces-C <a href="#">1</a> <a href="#">2</a> <a href="#">3</a>                                                                                                   | metacam <a href="#">1</a>                                                                                                                                                 | djvulibre <a href="#">1</a>                                                                                                           |

# Fuzzing group project

1. Coming week: pick an application and hand in Brightspace assignment with application & its input format
  - If needed, next week we can discuss suitability & feasibility
2. For the rest of Oct & Nov: spend 4hrs per week to see how far you get & collect results in some report
  - Good to pick one day to work and/or sync on this with your groups
3. We will discuss & compare experiences at the end
  - And maybe along the way

For the fuzzing you can use your university Azure account, Google cloud - and you own computer, of course.

More important than using the maximal processing power is using the same processing power for experiments to compare tools & options.

# Picking project

- Must be an **open-source** project written in **C or C++**
- Ideal project has
  - complex input format
  - process single inputs, one at a time - so no protocols
  - simple build process
  - is not too mature, so it has not been thoroughly fuzzed before
- If the application has a GUI, fuzzer will have to by-pass the GUI
- Look for evidence of fuzzing in the code repository
- Steer clear of FFmpeg and ImageMagick