02.TechNote

Error rendering macro 'html'

Notify your Confluence administrator that "Bob Swift Atlassian Apps - HTML" requires a valid license. Reason:

VERSION_MISMATCH

Tool

- Debugger
  - PEDA
  - pwndbg
  - Pwndbg(scwuaptx)
  - qira
- Symbolic execution
  - angr
  - Triton
  - Ponce
- Exploit development library
  - PWNTOOLS

Analysis

- 01.Static program analysis
  - Clang Static Analyzer
- 02.Dynamic program analysis
  - ASAN - Address Sanitizer
  - Valgrind - Memcheck
- 03.Symbolic execution(feat. Concrete execution)
- 04.Concolic execution
- 05.Taint analysis
  - IR(Intermediate Representation)
- 06.DBI(Dynamic Binary Instrumentation)
  - PIN
  - Valgrind
  - Dyninst
  - DynamoRIO

Fuzzing

- Domato
- Boofuzz
- radamsa
- Honggfuzz
- AFL - American fuzzy lop
- libFuzzer
- Wadi

Error rendering macro 'html'

Notify your Confluence administrator that "Bob Swift Atlassian Apps - HTML" requires a valid license. Reason:

VERSION_MISMATCH

Protection Tech

- 01.NX Bit(MS : DEP)
- 02.ASLR
- 03.Canaries
- 04.RELRO
  - Lazy binding(Feat. Now binding)
- 05.PIC
  - 01.Static Library
  - 02.Shared Library
- 06.PIE

Exploit tech

- 01.Shellcode
  - 01.The basics technic of Shellcode
  - 02.Create a shellcode that executes "/bin/sh"
  - 03.Bind Shellcode
  - 04.Reverse Shellcode
  - 05.Pwntools Shellcode (Shellcraft)
- 02.Return to Shellcode
- 03.RTL(Return to libc)
  - 01.RTL(Return to Libc) - x86
  - 02.RTL(Return to Libc) - x64
- 04.Frame faking(Fake ebp)
- 05.Frame Pointer Overwrite
  - 01.Frame Pointer Overwrite(One-byte Overflow) - x86
  - 02.Frame Pointer Overwrite(One-byte Overflow) - x64
- 06.ROP(Return Oriented Programming)
  - 01.ROP(Return Oriented Programming)- x86
  - 02.ROP(Return Oriented Programming)- x64
  - 03.ROP(Return Oriented Programming) - mmap, mprotect
- 07.SROP(Sigreturn-oriented programming)
  - 01.SROP(Sigreturn-oriented programming) - x86
  - 02.SROP(Sigreturn-oriented programming) - x64
- 08.BROP(Blind Return Oriented Programming)
- 09.Race condition
- 10.One-gadgets(feat. PLT/GOT overwrite)
- 11.Heap Spray
- 12.Heap Feng Shui
- 13.JOP(Jump-Oriented Programming)
- 14.Return-to-csu(__libc_csu_init)
  - 01.Return-to-csu (feat. JIT ROP) - x64
  - 02.Return-to-csu(feat. Return-to-vuln, Just-In-Time Code Reuse) - x64
- 15.Return-to-dl-resolve
  - 01.Return-to-dl-resolve - x86
  - 02.Return-to-dl-resolve - x64(feat.Return-to-csu)
- 16.Stack pivot

Heap Exploit tech

- 01.Malloc - glibc(ptmalloc2)
  - 01.Malloc - glibc (ptmalloc2)[English]
  - 01.Malloc - glibc (ptmalloc2)[Korean]
- 02.Heap Exploitation
  - Double free
    - Double free [English]
    - Double free [Korean]
  - first-fit(Use-After-Free)
    - first-fit(Use-After-Free) [English]
    - first-fit(Use-After-Free) [Korean]
  - unsorted bin attack
    - unsorted bin attack[English]
    - unsorted bin attack[Korean]
  - Overlapping chunks
    - Overlapping chunks[English]
    - Overlapping chunks[Korean]
  - Poison null byte
    - Poison null byte [English]
    - Poison null byte [Korean]
  - Unsafe unlink
    - Unsafe unlink [English]
    - Unsafe unlink [Korean]
  - The House of Force
    - The House of Force[English]
    - The House of Force[Korean]
  - The House of Spirit
    - The House of Spirit[English]
    - The House of Spirit[Korean]
  - The House of Lore
    - The House of Lore[English]
    - The House of Lore[Korean]
  - House of einherjar
    - House of einherjar [English]
    - House of einherjar [Korean]
  - House of Orange
    - House of Orange[English]
    - House of Orange[Korean]

Error rendering macro 'html'

Notify your Confluence administrator that "Bob Swift Atlassian Apps - HTML" requires a valid license. Reason: VERSION_MISMATCH