정보보호 R&D 데이터 첼런지

SSG(Sejong Security Group)

팀원 : 최광준, 조승현, 진호용, 나윤종, 이광진

INDEX

SSG-AEG

1. 개요

2. SSG-AEG

3. 예선 결과

4. 본선 결과

5. 평가

SSG-AEG

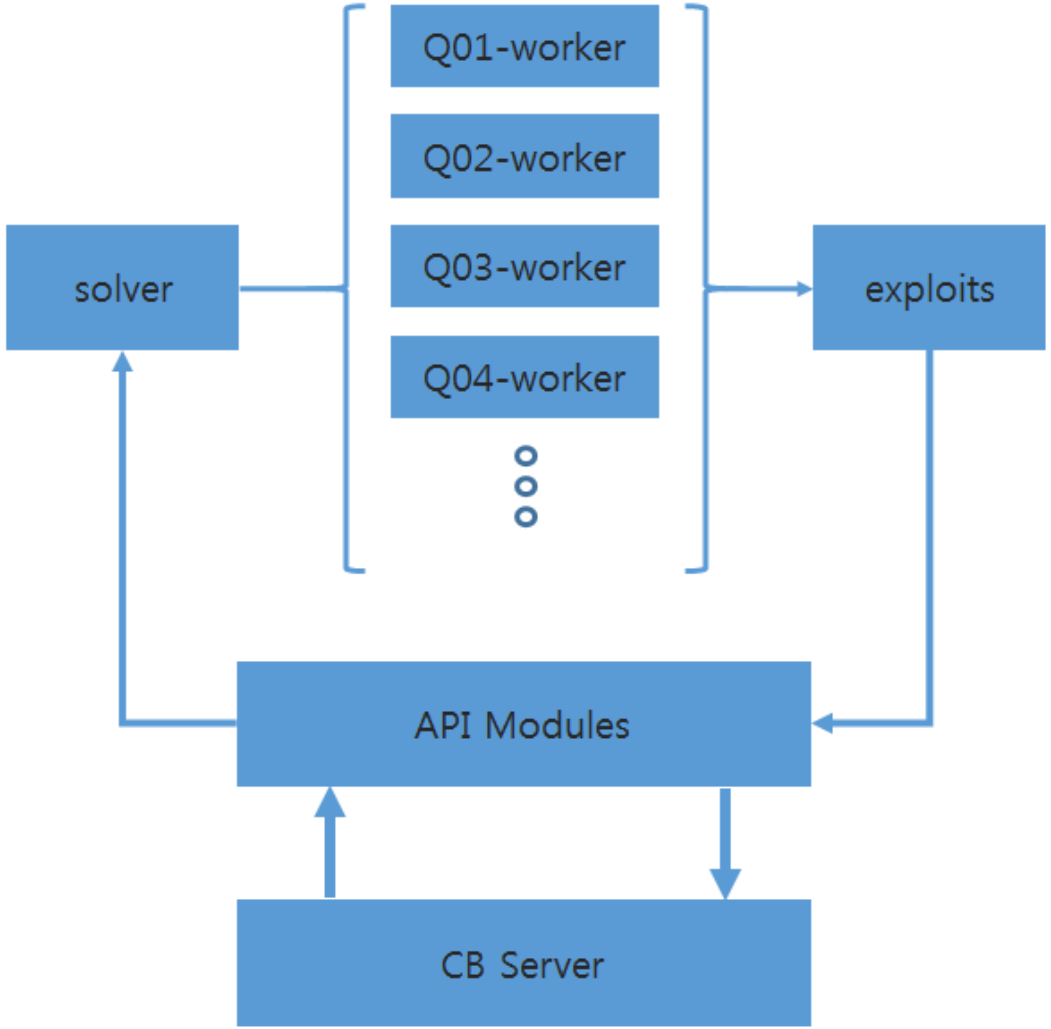
...

개요

- Machine명 : SSG-AEG
- 사용 언어 : Python
- 사용 모듈 : pwntools, ltrace, strace 등
- 핵심 기술 : Fuzzing

SSG-AEG

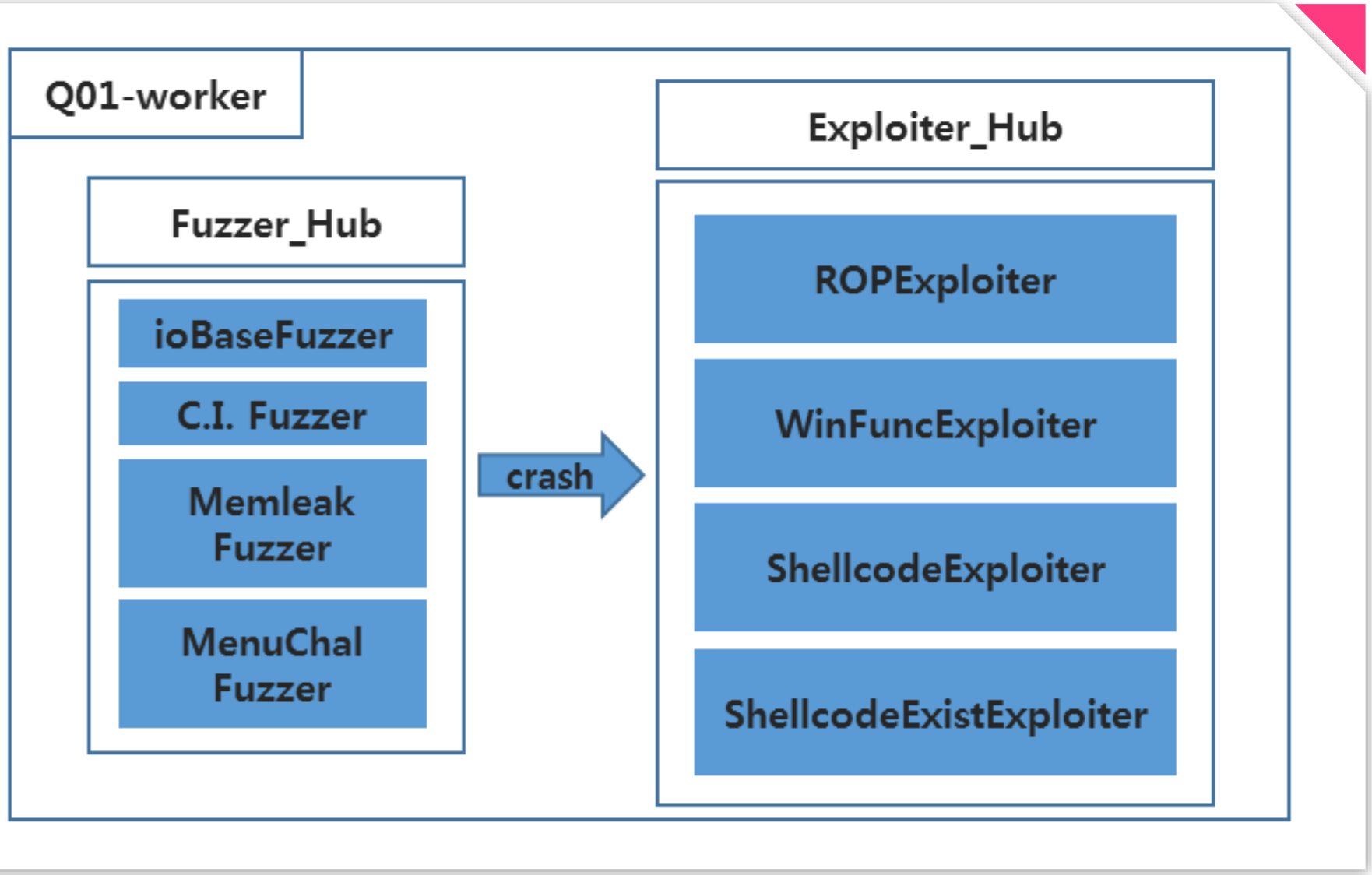
SSG-AEG



SSG-AEG

SSG-AEG

...



ioBaseFuzzer

- 기본적인 input type 기반 Fuzzer
- Ltrace 를 사용하여 input의 type(숫자, 문자열)을 탐지
- 무작위의 input을 생성하여 fuzzing

C.I. Fuzzer

- Command Injection 탐지 Fuzzer
- Ltrace 를 사용하여 input의 type(숫자, 문자열)을 탐지
- Flag를 출력하는 command가 포함되어 있는 문자열을 무작위로 입력
  - Ex : aaaaaaaa;tail fla*;aaaaaa
- 출력된 데이터에 로컬에서 생성한 flag 문자열이 있을 경우 탐지

MemLeakFuzzer

- Memory Leak 탐지 Fuzzer
- 프로그램에서 flag 파일을 fopen할 경우, 해당 경로를 인식하여 flag 파일 생성
- Ltrace 를 사용하여 input의 type(숫자, 문자열)을 탐지
- 무작위의 input을 생성하여 fuzzing
- 출력된 데이터에 로컬에서 생성한 flag 문자열이 있을 경우 탐지

MenuChalFuzzer

- Menu Challenge 문제 전용 Fuzzer
- 처음 출력된 문자열을 기반으로 메뉴 탐지
- Ltrace 를 사용하여 각 메뉴의 input type(숫자, 문자열) 및 size 탐지
- 무작위의 input을 생성하여 fuzzing

ROPExploiter

- Crash가 발생 했을 때, strace를 사용하여 eip가 조작되는 데이터의 offet 탐지
- 문제 파일에서 write, read 함수를 사용할 경우, 예선 때 사용된 libc offset 기반으로 자동으로 rop payload 작성

SSG-AEG

...

WinFuncExploiter

- Crash가 발생 했을 때, strace를 사용하여 eip가 조작되는 데이터의 offet 탐지
- 문제에 있는 main 및 다른 기본적인 함수를 제외한 함수들로 eip 조작

SSG-AEG

...

ShellcodeExploiter

- Crash가 발생 했을 때, strace를 사용하여 eip가 조작되는 데이터의 offet 탐지
- 메모리에 쉘코드를 적재하고 해당 주소로 eip 변조

ShellcodeExistExploiter

- Crash가 발생 했을 때, strace를 사용하여 eip가 조작되는 데이터의 offet 탐지
- 문제 파일에 shellcode라는 이름의 변수가 존재할 경우, 해당 주소로 eip 조작

SSG-AEG

...

예선 결과

- 총 문제 수 : 45 문제
- Crash 발생 : 39 문제
- Exploit : 14문제
- Memory Corruption, Memory Leak 등 다수 탐지

SSG-AEG

...

본선 결과

- 총 문제 수 : 40 문제
- Crash 발생 : 12 문제
- Exploit : 7 문제
  - 1 라운드 : Crash 3, Exploit 2
  - 2 라운드 : Crash 2, Exploit 1
  - 3 라운드 : Crash 7, Exploit 4
- Memory Corruption 다수 탐지

SSG-AEG

...

성능 비교

- 오픈소스 취약점 탐지 도구 Zeratool과 비교
  - 75배 빠른 속도(예선 1차 2번 문제 기준)
  - 3배 높은 crash 탐지율(예선 문제 기준)

SSG-AEG

...

Future Work

- Symbolic Execution 적용
- 취약점 탐지 정밀화(Input 패턴 확인 등)
- 코드 간결화