이미지뷰어 소프트웨어 버그헌팅

1/19 준비

91913232/김우종

목차
버그헌팅 준비

- 버그헌팅이란 무엇일까?
- 버그헌팅의 준비물
  - Target
  - Fuzzer
  - Debugger
- 그 외
  - 2주동안 뭐함?
  - H4C 웹 세미나 후기

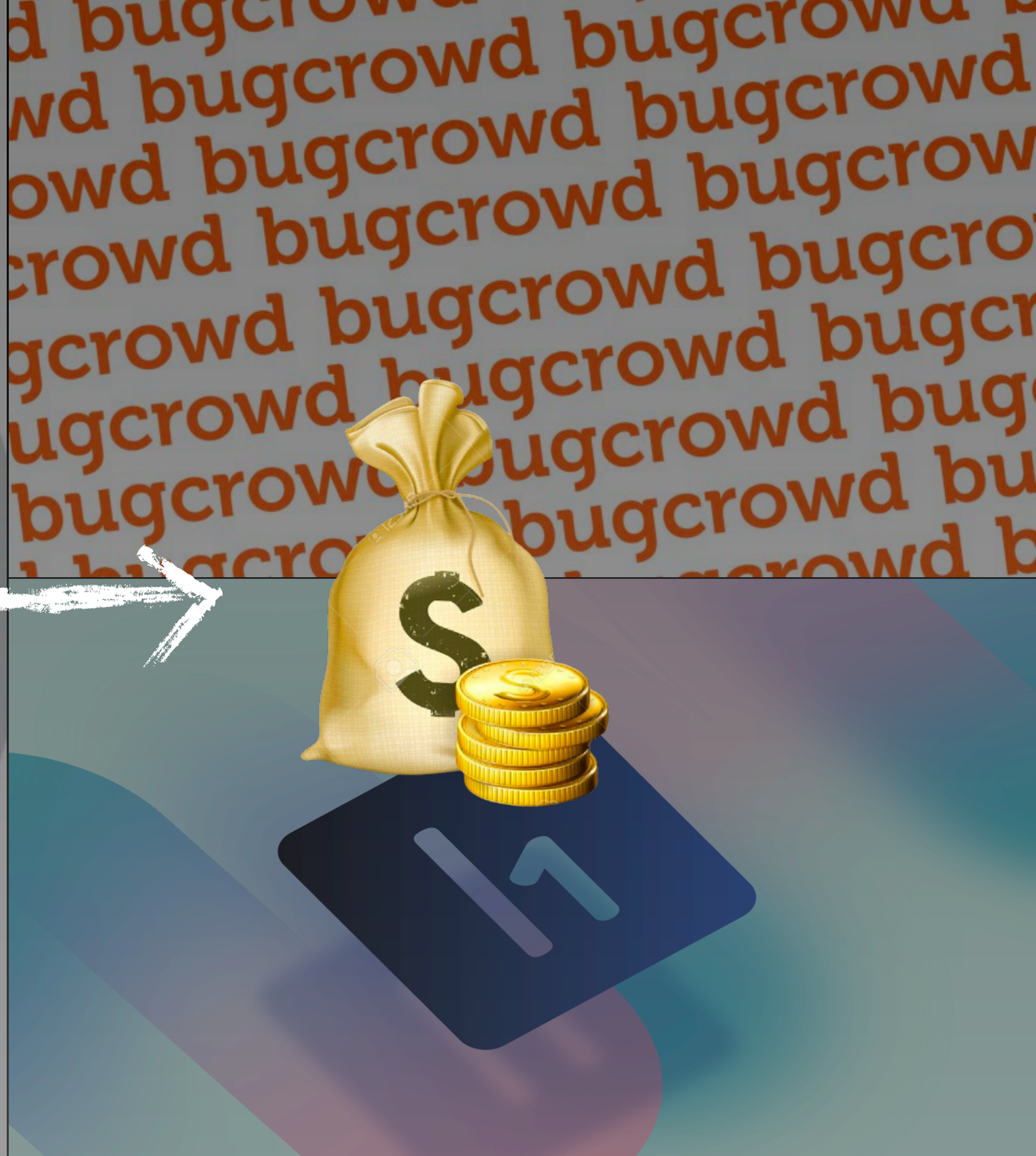
버그헌팅이란 무엇일까?

버그헌팅이란 무엇일까?

벌레? 사냥?

- 버그헌팅이란?
  - 서비스의 버그를 찾고 제보하여 수익금을 얻는 행위
  - 버그란?
    - 프로그램 실행과정에서 발생하는 오류


Korea Internet & Security Agency
한국인터넷진흥원


bugcrowd

버그헌팅 준비물

버그 헌팅 준비물

벌레 찾을 준비!

- 버그 헌팅 준비물
  - Target
  - Fuzzer
  - Debugger

Target

어떤 종류의 벌레를 잡지?

- 버그헌팅이란 서비스의 버그를 찾고 제보하여 수익금을 얻는 행위이다.
- 수많은 타겟들 중 버그헌팅을 진행할 서비스(타겟)을 잡자.

Target

어떤 종류의 벌레를 잡지?

- 버그헌팅이란 서비스의 버그를 찾고 제보하여 수익금을 얻는 행위이다.
- 수많은 타겟들 중 버그헌팅을 진행할 서비스(타겟)을 잡자.

Fuzzer

벌레를 어떻게 찾아야 하지..?

- Fuzzing이란?
  - 프로그램이 가지고 있는 잠재적인 취약점을 식별하기 위해 사용되는 기술
  - 두가지 대표적인 방식의 퍼징
    - Dumb Fuzzing
      - 테스트 케이스를 만들기 위해 타겟 프로그램에 대한 이해가 없어도 됨
    - Smart Fuzzing
      - 타겟 프로그램 입력에 대한 구조를 미리 파악하여 테스트 케이스 생성

Fuzzer

벌레를 어떻게 찾아야 하지..?

- Fuzzing이란?
  - 프로그램이 가지고 있는 잠재적인 취약점을 식별하기 위해 사용되는 기술
  - 두가지 대표적인 방식의 퍼징

Dumb fuzzing
Bff Fuzzer

Smart fuzzing
Peach Fuzzer

Fuzzer

어떻게 찾아야 하지..?

- Fuzzing이란?
  - 프로그램이 가지고 있는 잠재적인 취약점을 식별하기 위해 사용되는 기술
  - 두가지 대표적인 방식의 퍼징

Dumb fuzzing
Bff Fuzzer

Smart fuzzing
Peach Fuzzer

Debugger
벌레를 자세히 들여다 보자!

- 디버거?
  - 다른 대상 프로그램을 테스트하고 디버그하는데 사용되는 프로그램
  - 디버거의 종류
    - 사용자 수준 디버거
      - OllyDebugger, Immunity Debugger, IDA Pro
    - 커널 수준 디버거
      - WinDBG, SoftICE, Syser

Debugger
벌레를 자세히 들여다 보자!

- 디버거?
  - 다른 대상 프로그램을 테스트하고 디버그하는데 사용되는 프로그램
  - 디버거의 종류
    - 사용자 수준 디버거
      - OllyDebugger, Immunity Debugger, IDA Pro
    - 커널 수준 디버거
      - WinDBG, SoftICE, Syser

      디버거는 그냥 마음에 드는거 사용

그 외

2주 동안 한것들...?

그 외

2주동안 삽질....

- Bff fuzzer - python2.7 서비스 종료 및 python3과 충돌 ——;; pip 안먹음 등등…
- Crash 분석 - 각잡고 한 3개? 정도… 개당 한 3일씩 버린것 같음…. 크래시 하나 날아갈때마다 내 시간도 같이 버려지는 느낌이 듬… 난 왜 아직도 뭐 하나 유의미 하게 한 것이 없는가…
- 아 ㅋㅋ 지금 Keynote보면 아시겠지만 Macbook Air M1 옴
  - 근데 도커도 안됨 (linux x86_64 elf 파일이 안돌아감 이걸로 포너블 못함 ㅠ)
  - 안드로이드 공부하려고 안드로이드 스튜디오 깔았더니 M1호환 안되서 Rosetta2로 에뮬 돌리는데 안드로이드 스튜디오 안드로이드 에뮬 지원 X
  - 아직은 사지 마셈 ㅋㅋ (하지만 난 후회 안함 감성이 그만큼 커버침 뭣보다 2.5키로 돌덩이 안들고 다녀도 되서 맘에 듦)

그 외

H4C 웹세미나 후기

- Section
  1. 머신러닝과 보안 위협, 그리고 수학
  2. Network Hacking is too fun!
  3. 자알 도라거이 도어적 학호암
  4. About-Real Time Protection
  5. RF-Drone Replay Attack
  6. Excel 4.0 매크로 악성코드 진화 방법

그 외

H4C 웹세미나 결론

- 열시미 하자….
- 그리고 비대면 웹 세미나 같은걸로도 적당히 머리 깨져볼 수 있다….
- 그래도 오프라인 해킹캠프 충격에 비할바는 안되긴 함…
- 해킹캠프를 한번도 안가봤는데 뭔가 공부에 있어서 자극이 필요하다 싶으면 이번 온라인 해킹캠프도 괜춘헐듯…?

Q&A

질문있으십니까...?