『**개발 계획서**』

**Web Fuzzer**

한강모, 손우정, 장재원, 한승훈

**2020.07.26**

**목차**

1. **개요**
2. **구조**
3. **시드 파일의 구성**
4. **웹 방화벽 우회**
5. **공격 방법**

5.1 XSS(Cross Site Scripting) 공격

5.2 SQLi(SQL Injection) 공격

5.3 Directory Traversal 공격

**1. 개요**

1) 목적: Web Fuzzer

2) 언어: Python 3

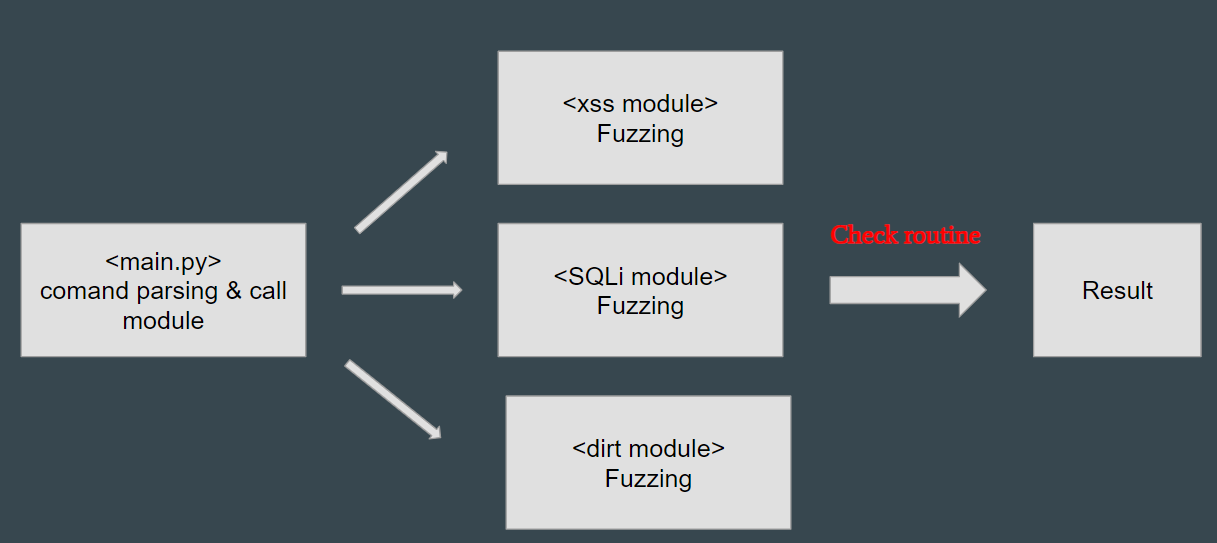
3) OS 환경: Python 기반 Windows/Linux 계열 크로스 플랫폼 동작 가능

4) 개발 환경: JetBrains PyCharm Community Edition 2018.3.2

5) 인터프리터 : Python 3.6 인터프리터

6) 네트워크 환경: IPv4, HTTP

**2. 구조**



main.py를 기준으로 XSS, SQLi, Dirt 모듈을 나누어서 Fuzzing 후 공격 성공여부를 검증하는 방식으로 설계하였다.

**3. 시드 파일의 구성**

Web Fuzzer에서 시드 파일이란, 웹 해킹에서 사용할 수 있는 XSS, SQLi, Directory Traversal 등과 같은 여러 공격 벡터들이 사용할 수 있는 쿼리 또는 문자열을 모아놓고, Fuzzer가 활용하기 쉽게 구성해 놓은 파일 또는 그 묶음들을 말한다.

좋은 퍼징 결과를 이끌어 내기 위해서 Fuzzer를 잘 구성하는 것도 중요하지만, Fuzzer가 활용할 수 있는 시드 파일을 잘 구성하는 것도 중요하다.

* 구성 시드 파일
  + XSS(Cross Site Scripting) 공격 Seed File
  + SQLi(SQL Injection) 공격 Seed File
  + Directory Traversal 공격 Seed File

**4. 웹 방화벽 우회**

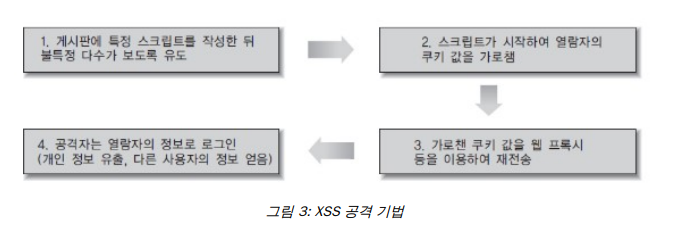
대부분의 웹 서비스는 **웹 해킹 공격시도를 WAF와 키워드 검증 로직으로 무력화** 한다. 따라서 공격이 가능한 경우에도 이러한 Inline 방어 기법들에 의해 공격을 실패하는 경우가 많다.

따라서 본 개발자들은 WAF 및 검증로직을 우회하는 방법에 대해 연구하여 구현한다. 또한 이를 **Seed File에 자동 적용하여 WAF를 우회할 수 있는 Seed File을 자동 생성할 수 있는 모듈을 개발**한다.

* 우회 기법 조사
  + 주석 처리 기법
  + 대소문자 교체 기법
  + 키워드 대체 기법
  + 문자 인코딩 기법
  + BOF 공격 기법

**5. 공격 방법**

5.1 XSS(Cross Site Scripting) 공격

XSS는 다른 사용자의 정보를 추출하기 위해 사용되는 공격 기법이다.  
간단히 예를 들면 게시판이나 검색 부분, 즉 사용자의 입력을 받아들이는 부분에 스크립트 코드를 필터링하지 않음으로써 공격자가 스크립트 코드를 실행할 수 있게 되는 것이다.

[그림 3]은 실제 XSS 취약점을 이용하여 다른 사용자의 쿠키 값을 훔쳐 그 사용자로 로그인하는 과정을 순차적으로 표현한 것이다.

5.2 SQLi(SQL Injection) 공격

SQL Injection은 웹페이지를 통해 입력된 파라미터 값을 이용하여 쿼리를 재구성 하는 방법이다. 많은 웹 페이지들이 사용자나 프로그램이 생성한 파라미터 값을 이용해 쿼리를 만들고 실행하는데, 이때 정 상적인 값이 아닌 파라미터 값이 입력될 때 비정상적인 쿼리가 실행되며, 따라서 원하지 않는 결과가 나 올 수 있다.

5.3 Directory Traversal 공격

directory traversal 또는 path traversal은 서버 시스템의 중요 정보를 악의적인 쿼리를 통해 접근해서 다운로드 하는 것이다. 현재 beebox에서는 중요 정보를 접근하는 쿼리가 성공하면, 화면에 그 정보를 렌더링해주는 형식으로 되어있다. directory traversal은 ../../../../etc/passwd와 같은 형식으로 ../../ 가 반드시 들어가고, ~~~/ 로 끝내고 리스폰스에서 index of 문자열이 존재하는지를 체[크하는 방식으로 directory listing도 수행할 수 있다.