
# OWASP Zed Attack Proxy (ZAP) 제대로 사용하기

NSR
정계옥

# Who am I?

- 이름 : 정 계 옥 (Jung Gyeok, 丁桂玉)
- 별명 : 훅크선장
- 나이 : 0x2B
- 직업 : 정부출연 연구기관 연구원
- 경력 : 리눅스 개발자 및 모의침투 테스터 (Penetration Tester)
  - BackTrack & Kali Linux 비공식 한글판 DVD 제작자
- 취미 : 리눅스, 임베디드 기기, RC비행기 등
- 연락처 : hook7346@gmail.com
- 블로그 : http://hook.tistory.com
- 페이스북 : https://www.facebook.com/gyeok.jung

# Agenda

- Zed Attack Proxy(ZAP) 소개
- ZAP의 기능별 설명
- ZAP과 Burp Suite Pro와 비교
- ZAP 사용법 시연

# What is ZAP?

- 사용하기 쉬운, 웹 애플리케이션 취약점 발견을 위한 통합된 모의침투 도구

# Some of ZAP's functionality

- Intercepting Proxy
- Traditional and AJAX spiders
- Automated scanner
- Passive scanner
- Forced browsing
- Fuzzer
- Dynamic SSL certificates
- Smartcard and Client Digital Certificates support
- Web sockets support
- Support for a wide range of scripting languages
- Plug-n-Hack support
- Authentication and session support
- Powerful REST based API
- Automatic updating option
- Integrated and growing marketplace of add-ons

# Some of ZAP's features

- Open source
- Cross platform (it even runs on a Raspberry Pi!)
- Easy to install (just requires java 1.7)
- Completely free (no paid for 'Pro' version)
- Ease of use a priority
- Comprehensive help pages
- Fully internationalized
- Translated into over 20 languages
- Community based, with involvement actively encouraged
- Under active development by an international team of volunteers
- ZAP is a fork of the well regarded Paros Proxy.

# Intercepting Proxy

- Achilles
  - 로컬 웹 프락시의 원조
  - 매우 직관적인 인터페이스와 단순한 기능
- Burp Suite & **Burp Suite Pro**
  - Free 버전과 **상용 Pro 버전**으로 구분되며, **scanner/intruder**/sequencer/comparer 등 다양한 기능
- Paros Proxy
  - 무료 로컬 웹 프락시의 대명사로, ZAP의 원조 (2013년이후 개발 중지)
- WebScarab
  - OWASP의 예전 로컬 웹 프락시 프로젝트(HTTP 프로토콜 분석)
- Fiddler 2
  - .NET 기반의 윈도우즈용 무료 HTTP 프로토콜 분석기
- Charles proxy
  - 또 하나의 저렴한? 유료 웹 디버깅 프락시

# ZAP's Attack Function

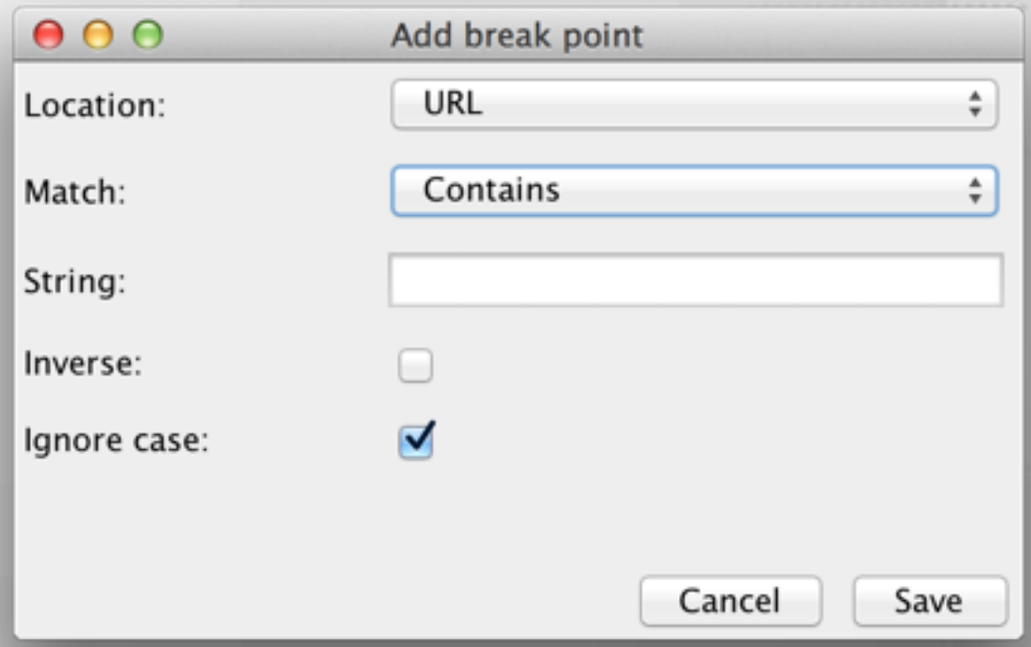
- Intercepting Proxy
  - SSL support
  - Web Socket 지원(HTML5 대응)
- 4개의 Mode
  - Safe / Protected / Standard / Attack
- Spider
  - Force Browsing
- Scanner
  - Active & Passive Scan
- Fuzzer
- Decode/Encode/Hash

# Mode 선택

- Safe Mode
  - 공격 행위가 허용되지 않는, 보기(read)만 가능
- Protected Mode
  - 일정범위(Scope)를 넘어서지 않는 공격 행위 가능
- Standard Mode
  - 공격 행위도 허용되는 일반적인 상태
- Attack Mode (ver 2.4.0부터 도입)
  - 사용자의 개입없이도 공격 행위가 자동으로 수행

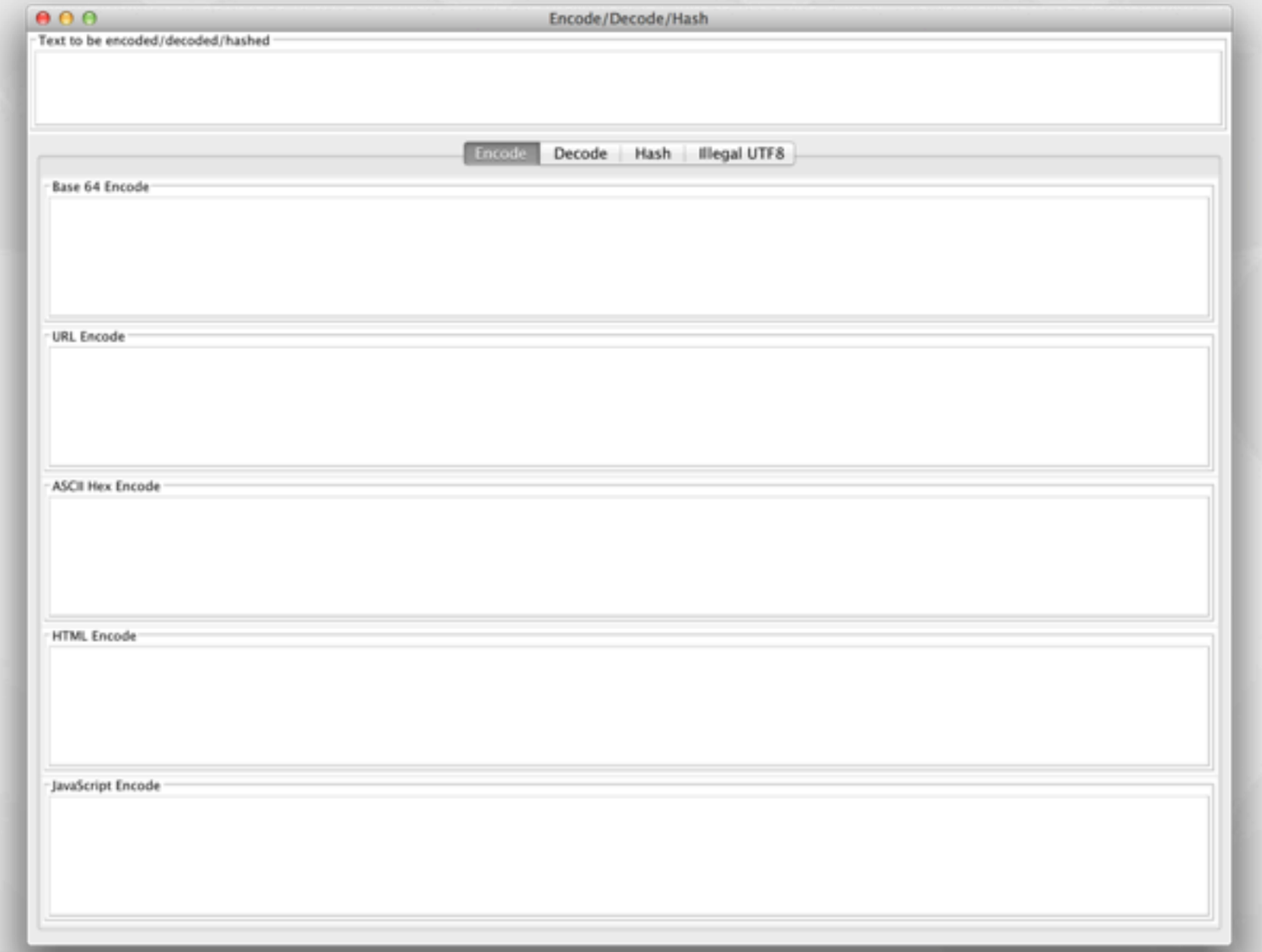
# 브레이크 포인트 (Break Point) : 중단점

- 사용자가 원하는 곳에서 멈추기
  - URL
  - HTTP Request (Header & Body)
  - HTTP Response (Header & Body)
- 정확한 문자열 또는 정규표현식 사용
  - 반대조건 적용
  - 대소문자 구분 무시



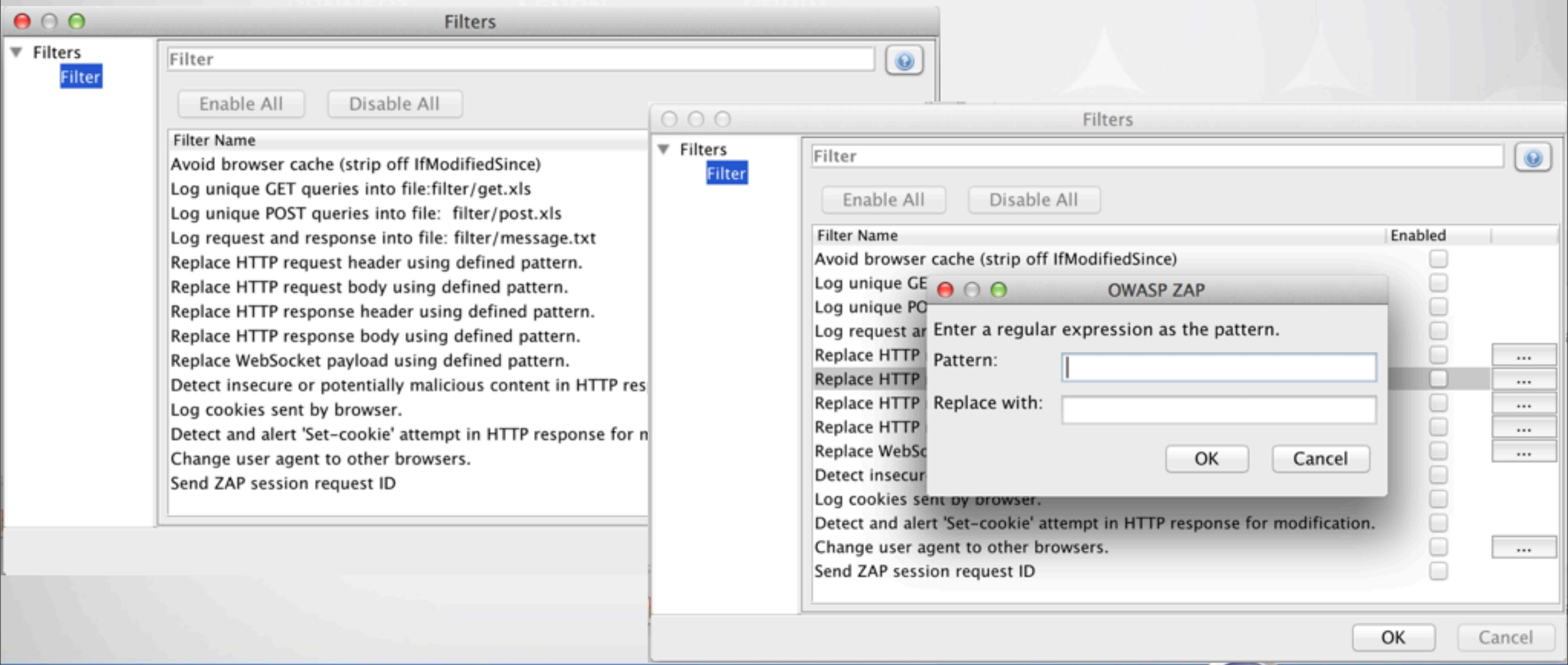
# Encode/Decode/Hash

- URL 또는 데이터 내의 문자열 인코딩 및 디코딩 가능



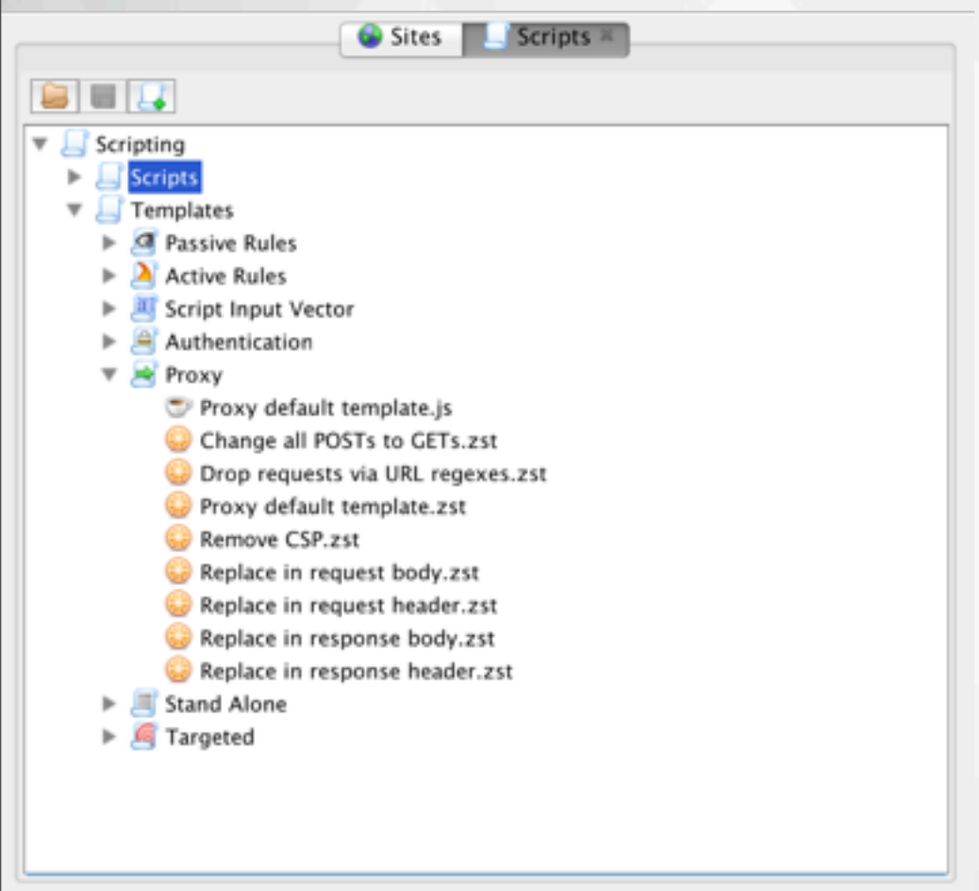
# 필터 : 실시간 치환

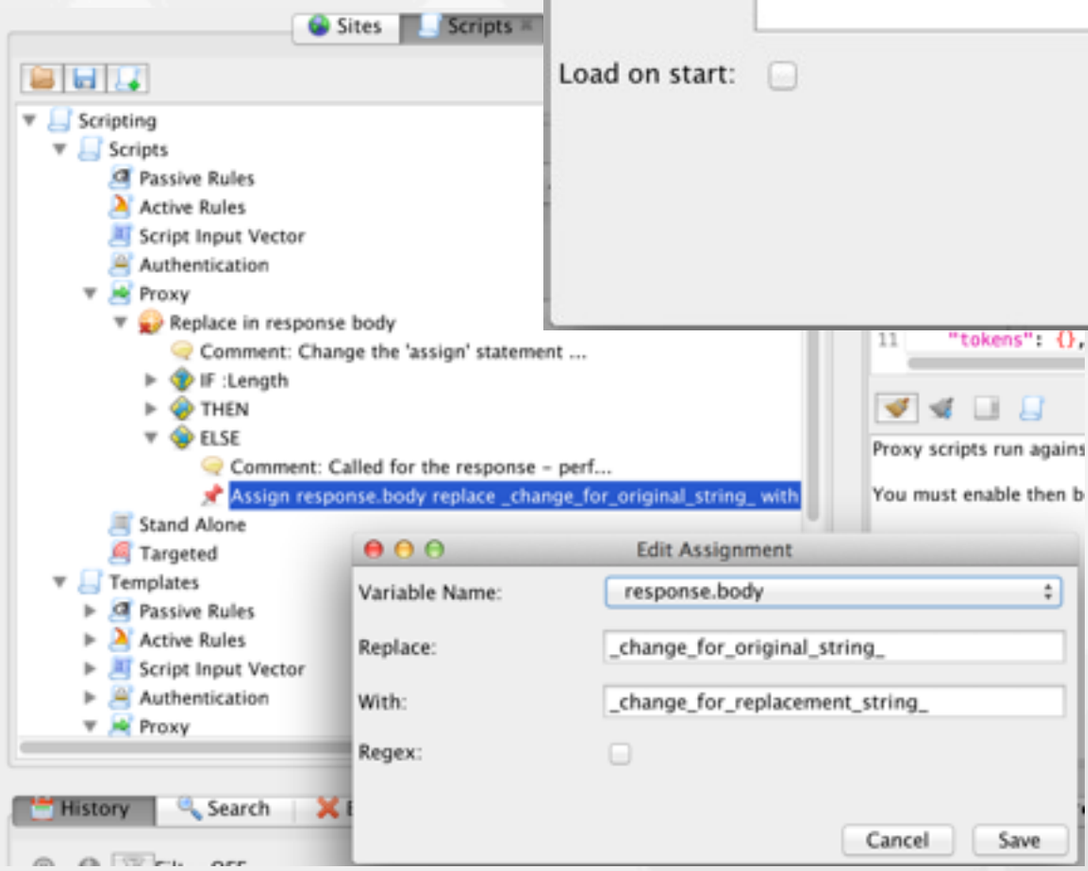
- 정규표현식으로 특정 패턴을 실시간 치환
- 부분별로 딱 하나만 정의 가능 **(향후 스크립트 기능으로 대체 예정)**

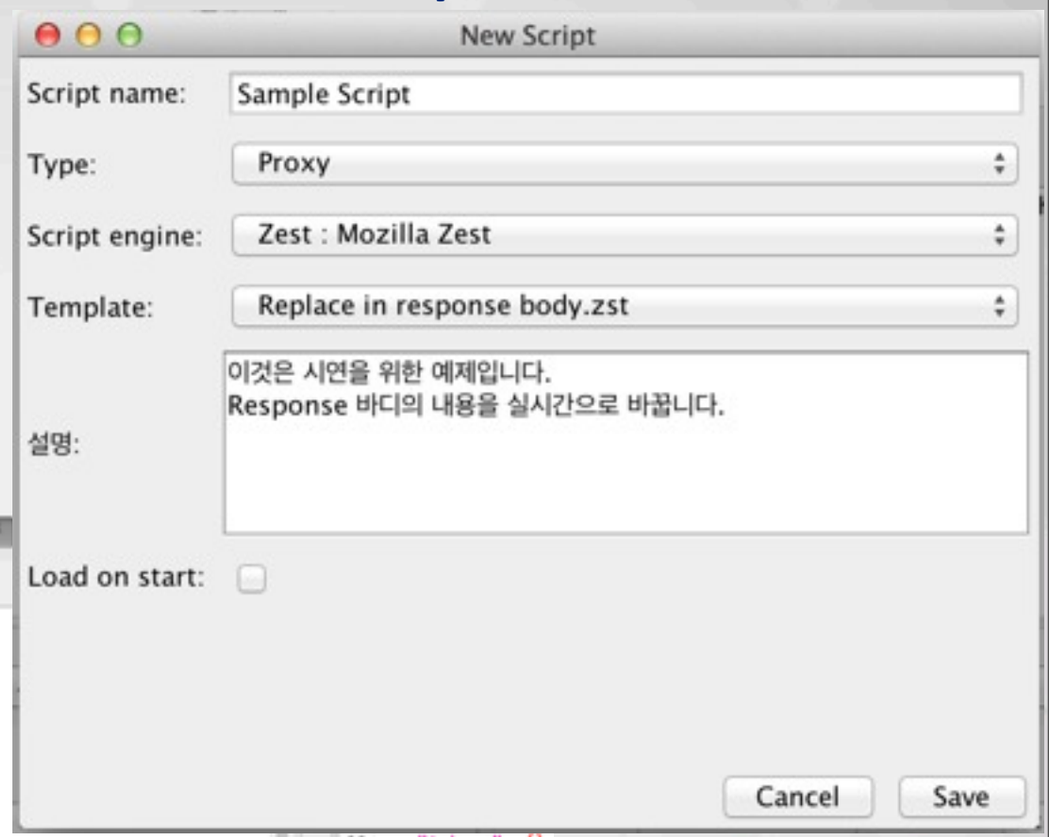


# Zest 스크립트 (실시간 치환 정의)

- Templates 에서 종류 선택 가능
- 오직 ELSE 구문에서만 처리
  - Zest Action : Print 만 추가 권장

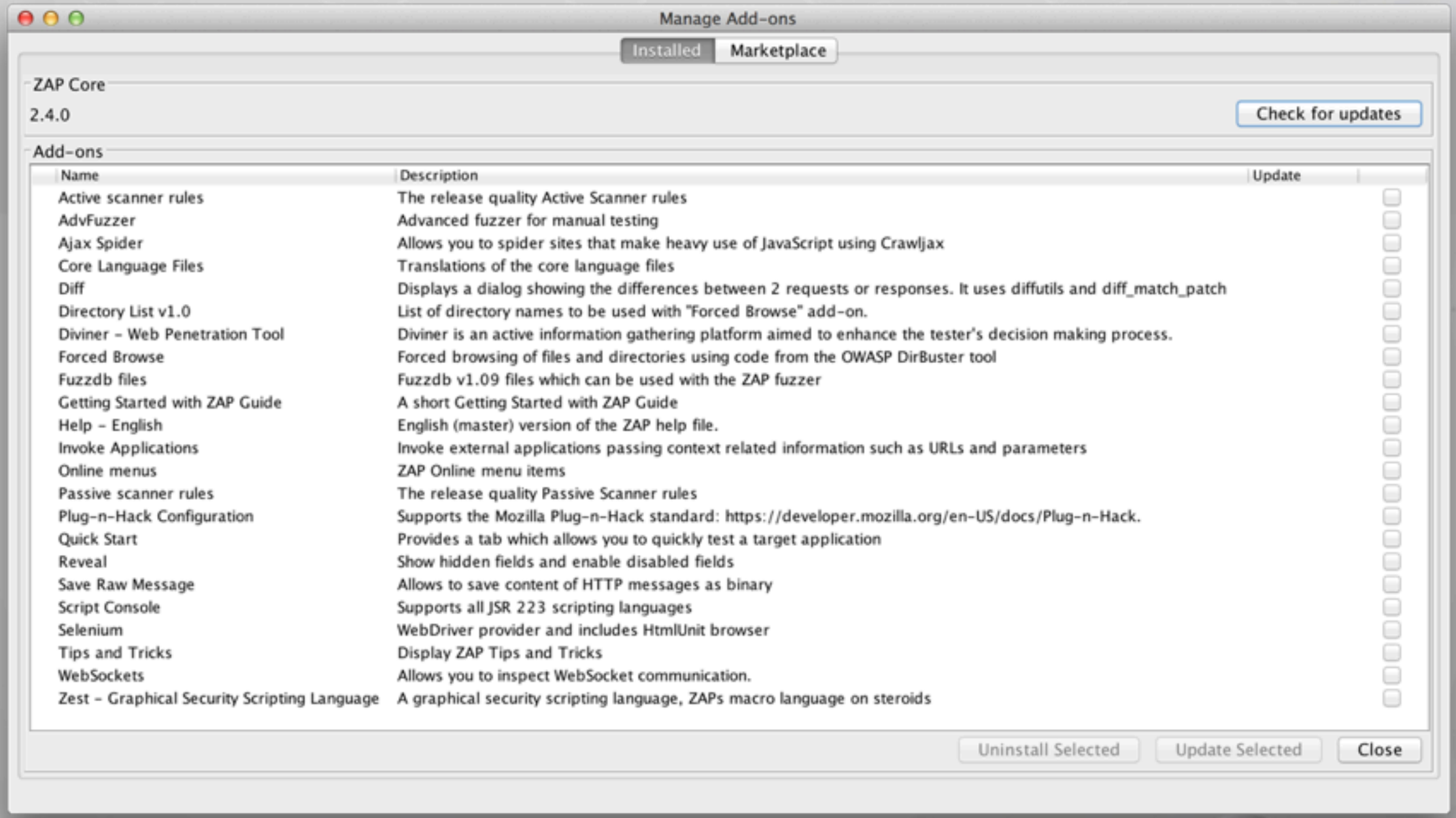


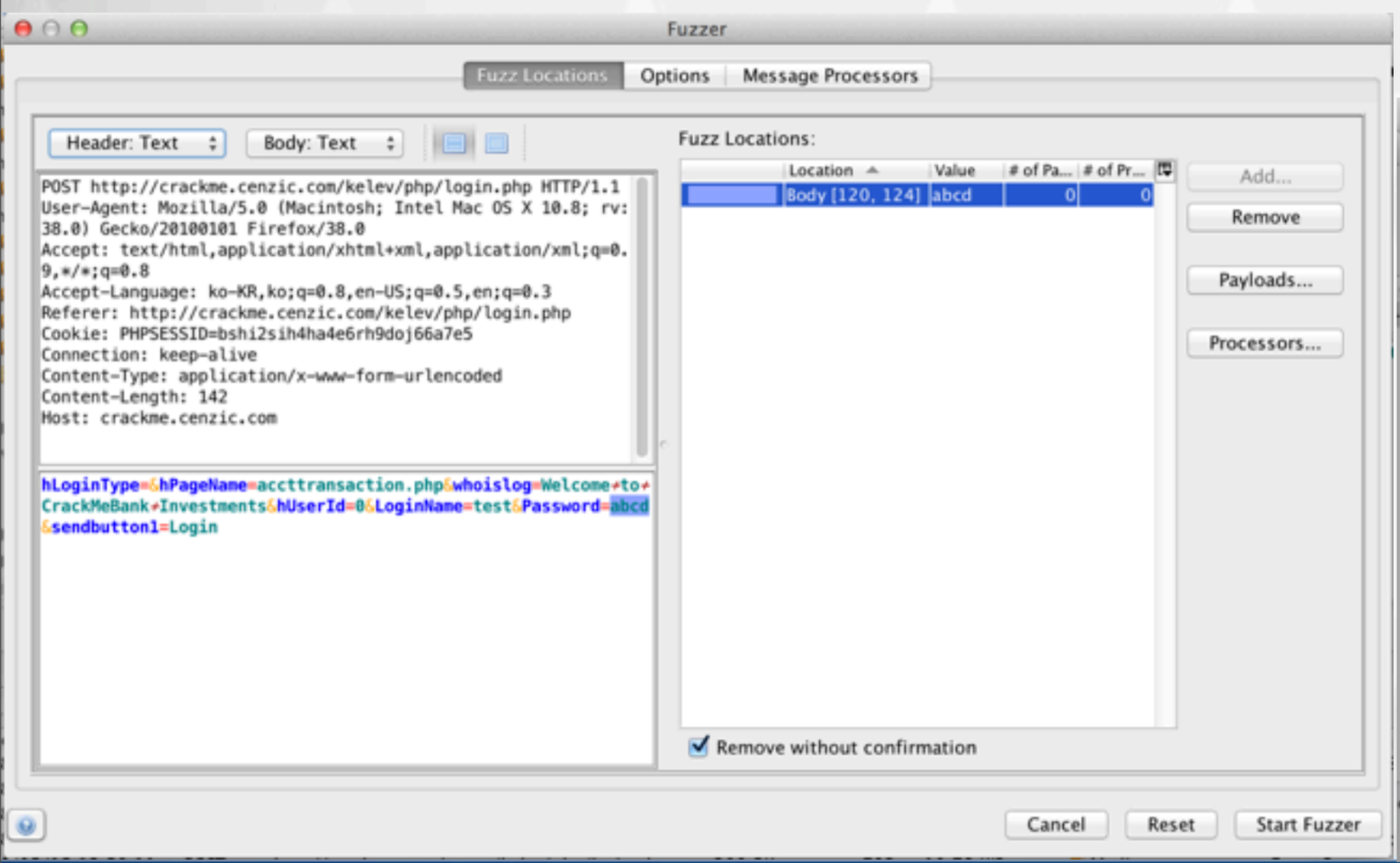
# Add-ons

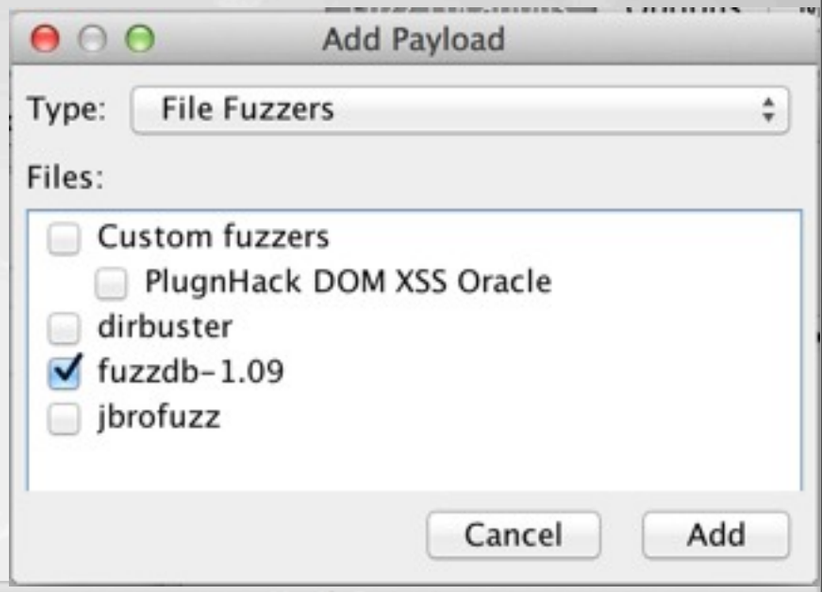
- Scanner, Fuzzer, Scripts & Manuals...

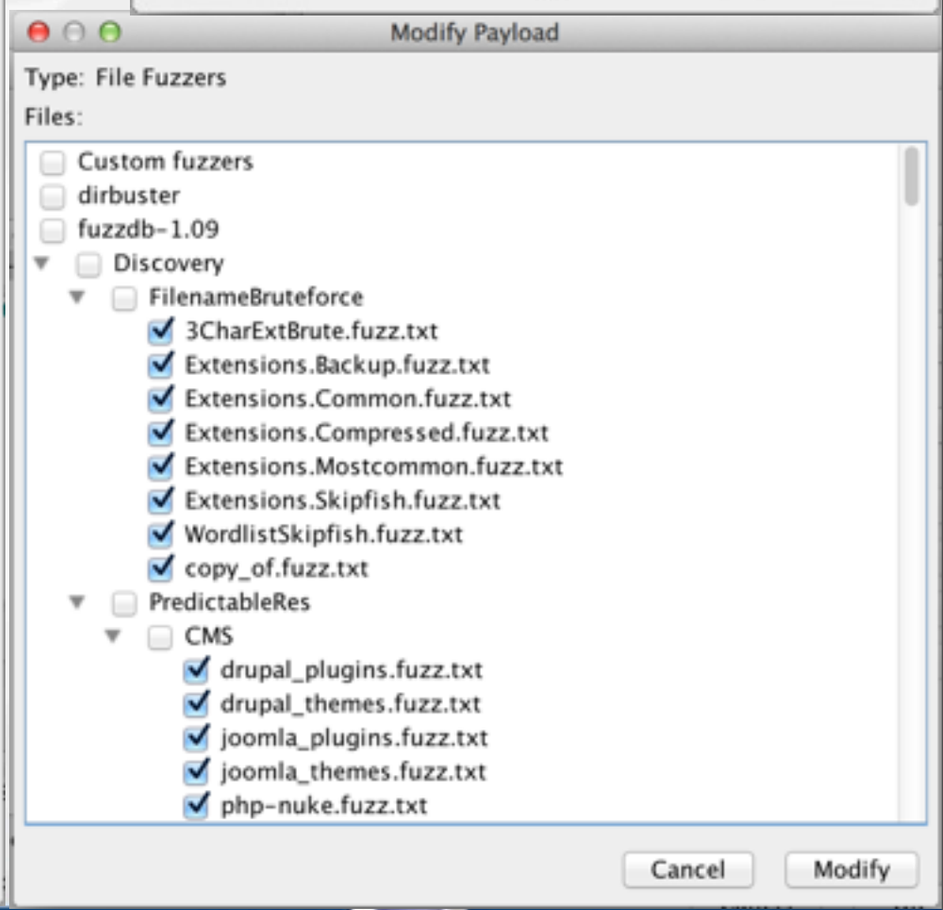


# 웹 퍼징 : fuzzdb 사용

- Payloads : 데이터의 종류
- Processors : 데이터의 처리 방법



# Better than Burp Suite [Pro]

- Active Scan & Passive Scan
  - 무료라고 보기에는 너무 훌륭한 기능
- Contexts
  - URL들의 묶음에 별도의 특성들을 부여 가능
- 확장성 및 유연성
  - Script 지원으로 자체 기능 개발 추가 가능(ECMA, Zest, Apple)
  - fuzzdb와 같은 오픈소스 프로젝트 결과물 사용 가능
  - *Burp Suite v1.5*부터 *Extender*라는 *API* 기반 확장 기능을 추가
- 엔터프라이즈 서비스 *(ZaaS : ZAP as a Service)*
  - 웹 인터페이스를 지원하는 서버 기반 서비스 예정

# ZaaS : ZAP as a Service

- 데스크탑 ZAP과 비교

| 종류 | Desktop ZAP | ZaaS |
|---|---|---|
| Database | Local HSQLDB | Enterprise (e.g MySQL) |
| Data Structure | DB and In memory | DB |
| Processes | One | Multiple |
| Deployment | Single machine | Distributed |
| Users | One | Multiple |
| Roles | One | Multiple |
| Access | Swing UI / API | Web UI / API |
| Application Lifetime | Hours | Five nines capability |
| License | Apache V2 | Apache V2 |

# Less than Burp Suite [Pro]

- Raw Packet 처리
  - ZAP은 표준 HTTP 프로토콜만을 처리 (apache's client library)
- Multi-positions Fuzzing
  - 동일 HTTP request 내에서 여러 곳(두 곳 이상)의 부분을 대상으로 순차적 또는 복합적인 퍼징 기능 필요 (Burp Suite의 intruder 고급 기능)
- Sequencer와 Comparer
  - 세션키 값과 같은 순차적인 값을 추척할 수 있는 기능
  - Request/Response 패킷 쌍을 대상으로 Word 또는 Byte 단위로 비교

# ZAP과 Burp Suite Pro 비교표

| ZAP | Burp Suite Pro | 비고 |
|---|---|---|
| Contexts | Target > Scope | Contexts는 속성 부여 가능한 개념 |
| Proxy | Proxy | |
| Spider | Spider | ZAP은 AJAX Spider도 보유 |
| Scanner | Scanner | ZAP은 Passive Scanner도 보유 |
| Fuzz | Intruder | Intruder는 Multi-position 퍼징 가능 |
| Resend | Repeater | |
| - | Sequencer | Fuzz 기능으로 가능할 듯 |
| Encode/Decode/Hash | Decoder | |
| - | Comparer | Raw 데이터 저장 후, 외부 도구 이용 |
| Add-ons | Extender | |
| Sessions | State | State는 단순한 상태 저장 개념 |
| Filter | Match and Replace | Filter 기능은 곧 없어짐, Zest Script로 대체 |
| Zest/ECMA Script | - | 사용자에게 확장기능 부여(오픈소스) |

# 시연

- Intercepting Proxy 설정
  - MS Windows 7 운영체제 환경에서
  - HTTPS MITM을 위한 인증서 export와 브라우저의 인증서 import
- HTTP Request & Response Intercept
  - 패킷 중간에서 잡아서 보기
- Brake point 추가
  - 중단점을 이용한, 패킷 중간에서 잡아서 보기
- Zest Script를 이용한 실시간 패킷 변조
  - Action : print를 통한 디버그 메시지 출력
- Fuzzdb를 사용한 웹 퍼징