ROSAEC center
Research On Software Analysis for Error-free Computing
소프트웨어 무결점 연구센터 NRF ERC

HANYANG UNIVERSITY 한양 1939

PLASSE RESEARCH

보안취약점 탐지도구 평가를 위한 기준 지표 자료집 구축

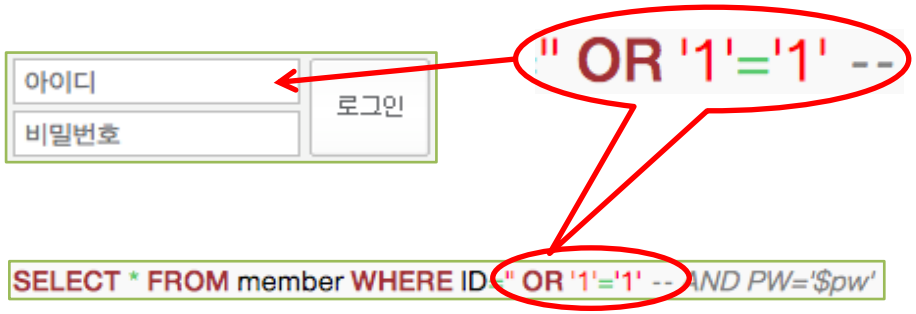
2014.07.29

한양대학교
프로그래밍언어연구실
오정욱

목차

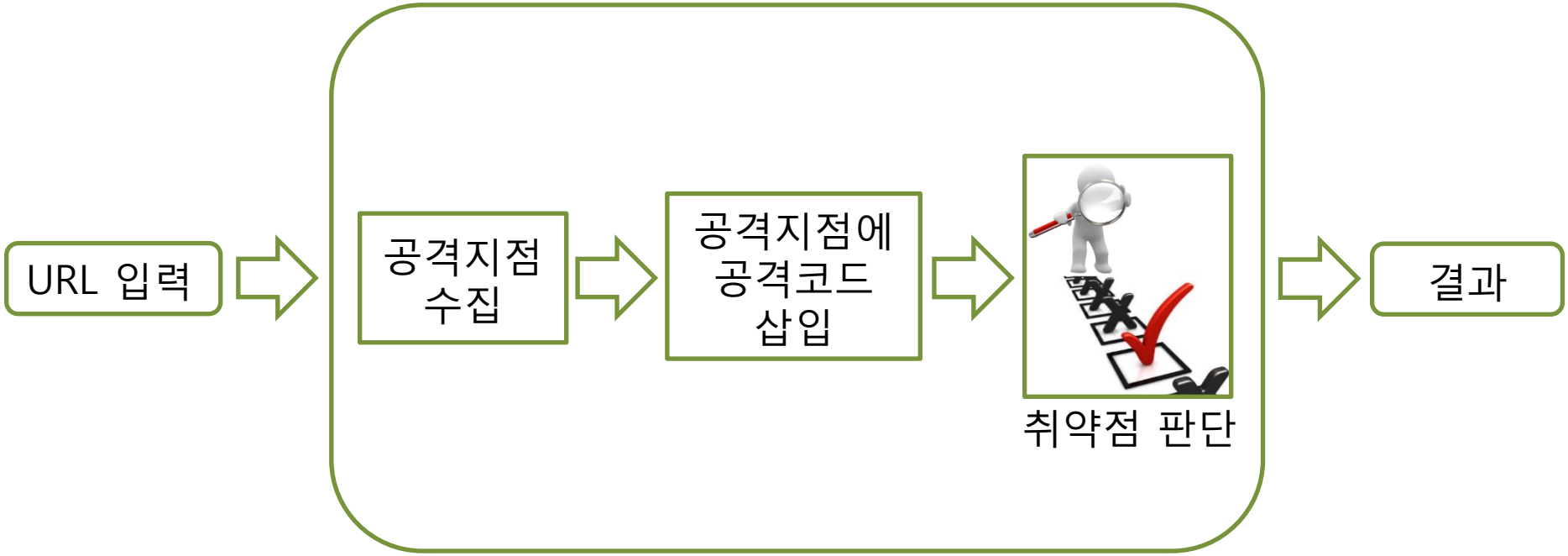
- 보안취약점 탐지도구란?
- 연구 목표
- 계획
- 예상 결과

보안취약점이란?



- SQL Injection의 간단한 예
  - 항상 참이 되어 로그인이 됨

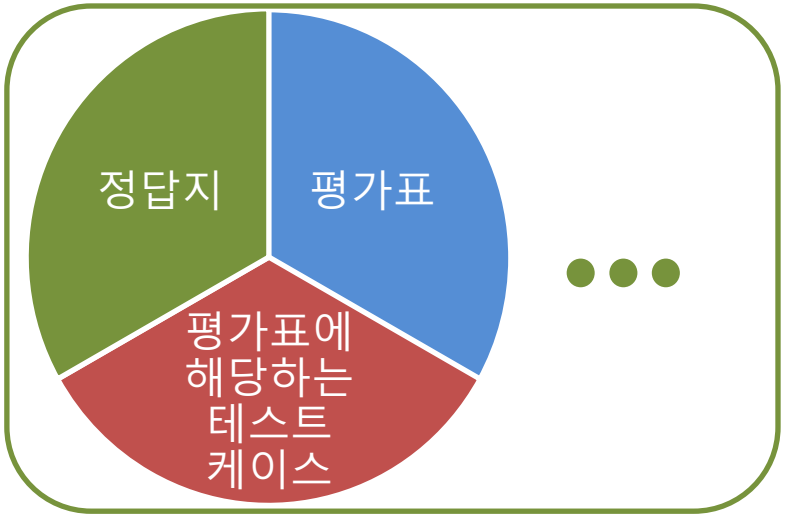
보안취약점 탐지도구란?



취약점 탐지기의 구성도

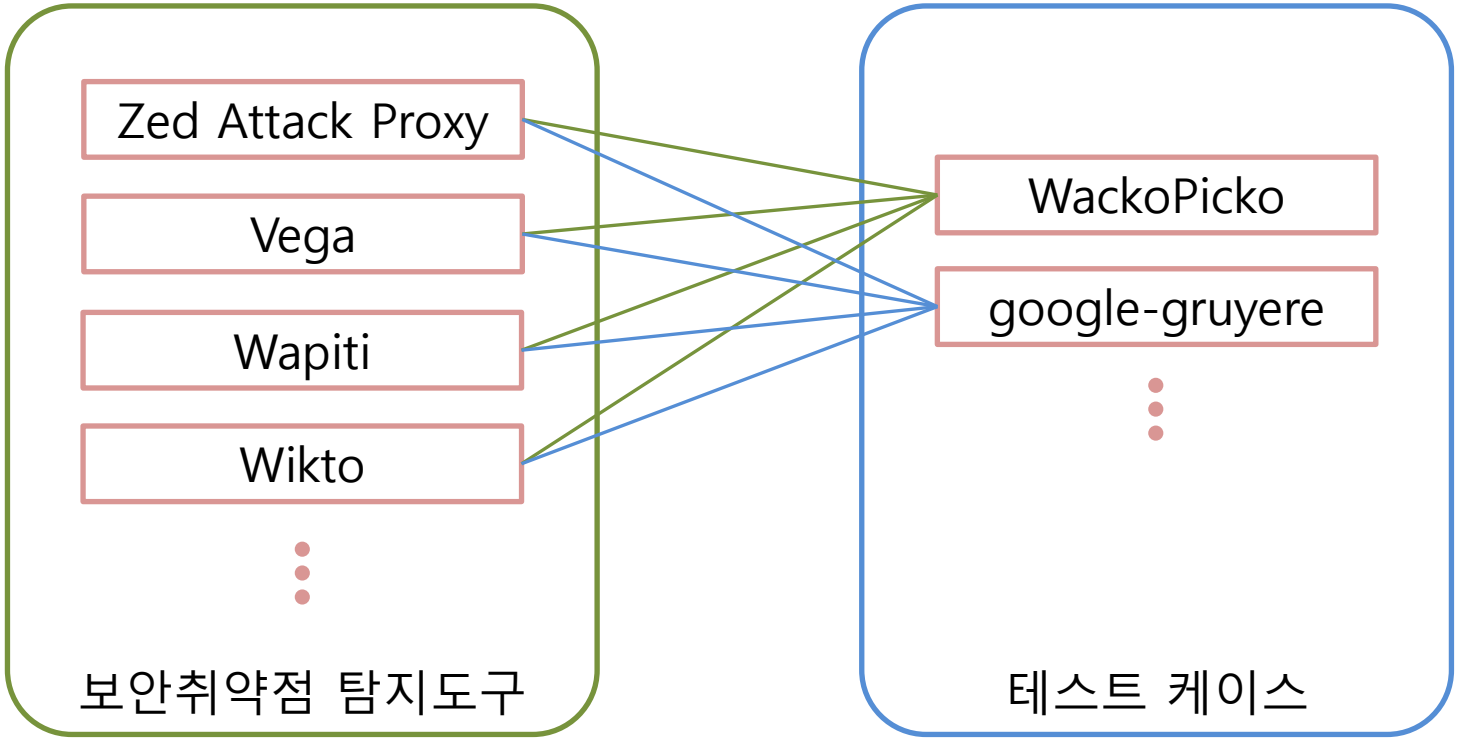
연구 목표

- 각각의 탐지도구가 검출할 수 있는 취약점은 서로 다름
- 탐지도구를 평가하는 정확한 기준이 없음
- 보안취약점 탐지도구의 평가를 위한 기준 지표 자료집을 구축하는 것이 목표



기준 지표 자료집

계획



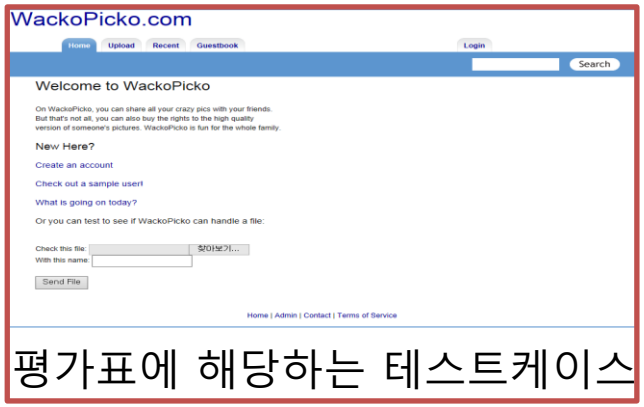
- OWASP에서 제공하는 보안취약점 탐지도구 목록을 기준으로 진행

- 취약점이 알려져 있는 테스트 케이스를 사용

예상 결과

번호	취약점	위치
1	Stored SQL injection	/users/register.php -> /users/similar.php
2	Reflected SQL injection	/users/login.php
3	SessionID vulnerability	/admin/login.php
4	Reflected XSS	/pictures/search.php?query=blah
5	Stored XSS	/guestbook.php
6	Directory Traversal	/pictures/upload.php
7	Multi-Step Sotred XSS	/pictures/view.php?picid=3
8	Forceful Browsing	/pictures/highquality.php?picid=3&key=hightquality
...	...	...

테스트 케이스의 정답지



평가표에 해당하는 테스트케이스

	Stored SQL injection	Reflected SQL injection	Stored XSS	Reflected XSS	...
Vega	o	o	o	o	...
ZAP	o	o	o	o	...
Wapiti	x	x	o	o	...
Wikto	x	o	o	x	
...	...	...	...	...	...

평가표

기준 지표 자료집

감사합니다