웹 응용프로그램 보안 취약성 분석기 구현

소프트웨어무결점센터 Workshop

2010. 8. 25

한국항공대학교, 안 준 선

Outline

- 소개
- 관련 연구
  - Input Validation Vulnerability
- 연구 내용
  - Abstract Domain for Input Validation
  - Implementation of Vulnerability Analyzer
- 기존 연구
- 결론 & 향후 연구

소개

- 웹 응용프로그램 보안 취약성 분석기 구현
  - 입력언어 : PHP
  - 대상 보안 취약성 : Improper Input Validation
    - SQL 삽입
    - Cross Site Scripting(XSS)
    - PHP 파일 삽입
    - OS 명령어 삽입
      ...
  - practical false positives/false negatives

부적절한 입력값 검증

- 위험한 외부의 입력값을 적절한 검사 없이 내부의 보안에 민감한 연산에 사용
  - SQL 삽입: SQL 쿼리 생성
  - Cross Site Scripting(XSS): 동적 웹페이지 생성
  - PHP 파일 삽입: 파일 삽입 경로 생성에 사용
  - OS 명령어 삽입: 외부 명령어 생성에 사용
- 예 :SQL 삽입

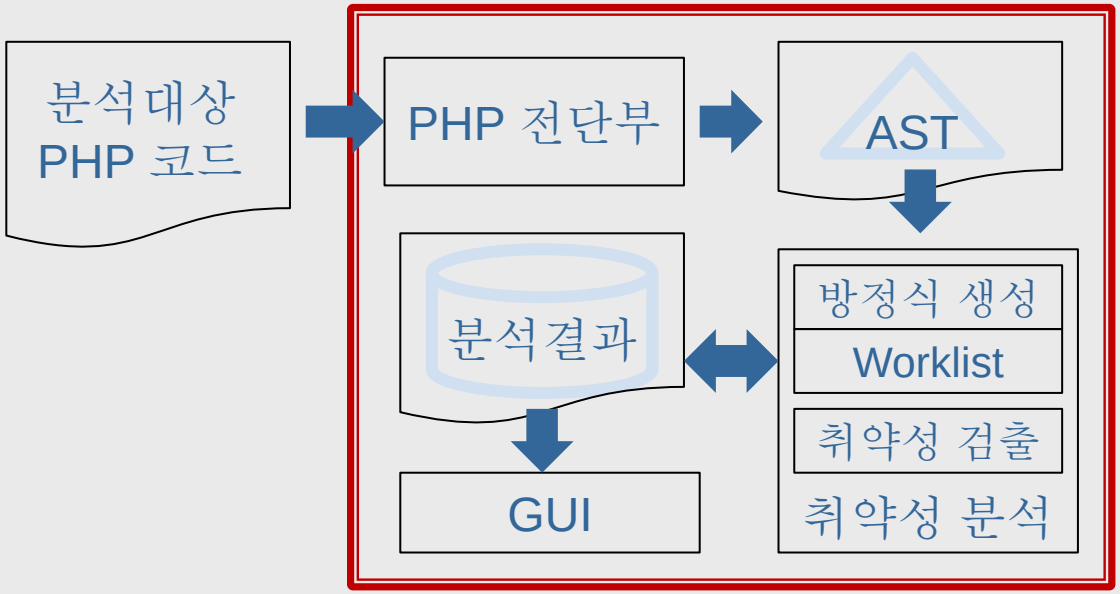
```
$id = $_Request('name');
mysql_query("SELECT MessageID,Subject FROM".
            "messages WHERE MessageID='$id'");
```

```
= name ' OR 1=1;
```

```
SELECT MessageID,Subject FROM messages WHERE
MessageID = ''; DROP TABLE('messages');
```

웹 응용 프로그램 보안 취약성 분석기

- 특징
  - 요약 해석 기반 분석
  - Context non-sensitive 함수간/file간 분석 사용
  - 전체 구조



PHP 언어 고려사항

- 문자열 자료값의 사용
  - Variable Variables

```
$x = “b”;
if (…) $x = “a”;
$$x = 1;  // $a = 1 or $b = 1;
```

  - Array Indexing

```
$x = ‘x’;
if (…) $x = ‘1’
$y = array($x=>’a’, ’b’);  // $y: (‘x’->’a’, 1->’b’) or
                           //      (1->’a’,2->’b’)
```

  - String Conversion

```
$x = “12bac”+3;  // $x == 15
```

PHP 언어 고려사항

- Reference Assignments

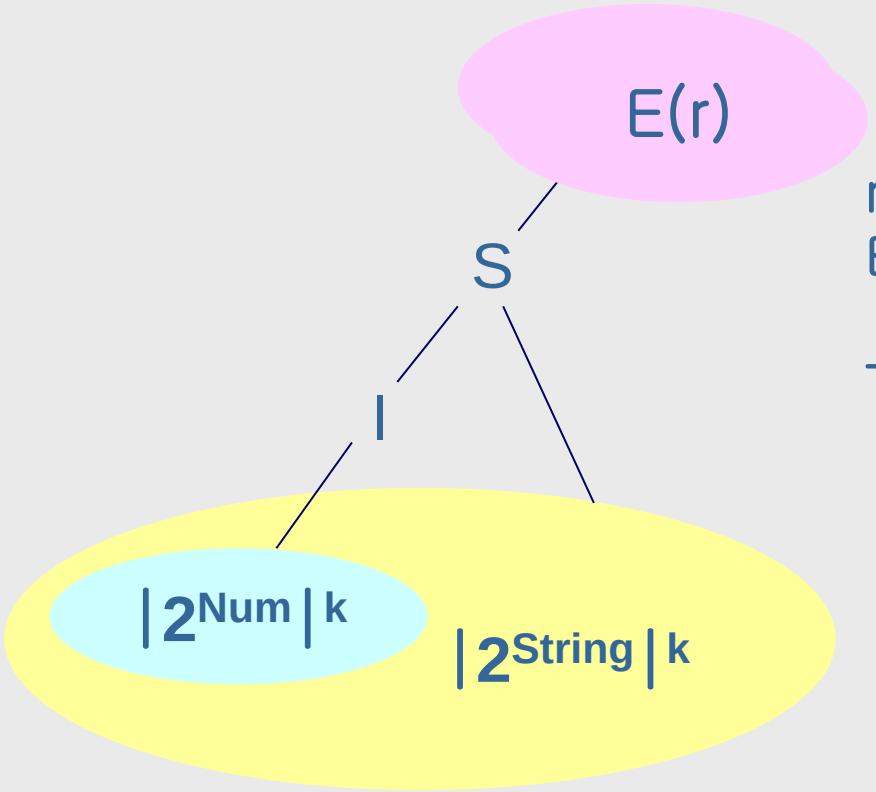
```
$x = array(11,12,13);
$x[0] =& x[1];
$y =& $x[1];
$y = 0;     // $y == $x[0] == $x[1] == 0
```

- Copy on Assignments

```
$x = array(11,12,13);
$y = array(21,22,23);
$z = array($x, $y);
$x[0] = 1;        // $x :  (0,12,13)
                  // $z : ((11,12,13), (21,22,23))
```

요약 공간

- 요약공간: 외부의 위험 문자열의 제거를 추적



r ∈ Regexp
E(r) ∪E(r') = E(r&r')

Top Value : E(#)

요약 공간

- 함수 정의 예: preg_replace(pat, rep, sub)

preg_replace(r,s,E(r')) =

E(c_1|...| c_n) where s="" and c_i's are single character in L(r'| r)

E(r|r') if s cannot be a substring of any s'∈L(r'|r) and r and r' cannot produce a substring of s

E(r) if s cannot be a substring of any s'∈L(r) and r cannot produce a substring of s

E(r') if s cannot be a substring of any s'∈L(r') and r' cannot produce a substring of s

E(#) otherwise

ex) preg_replace("<!", "", E(ab|x)) = E(x)

preg_replace("bc*", "de", E(d|ef)) = E(bc*)

요약 공간

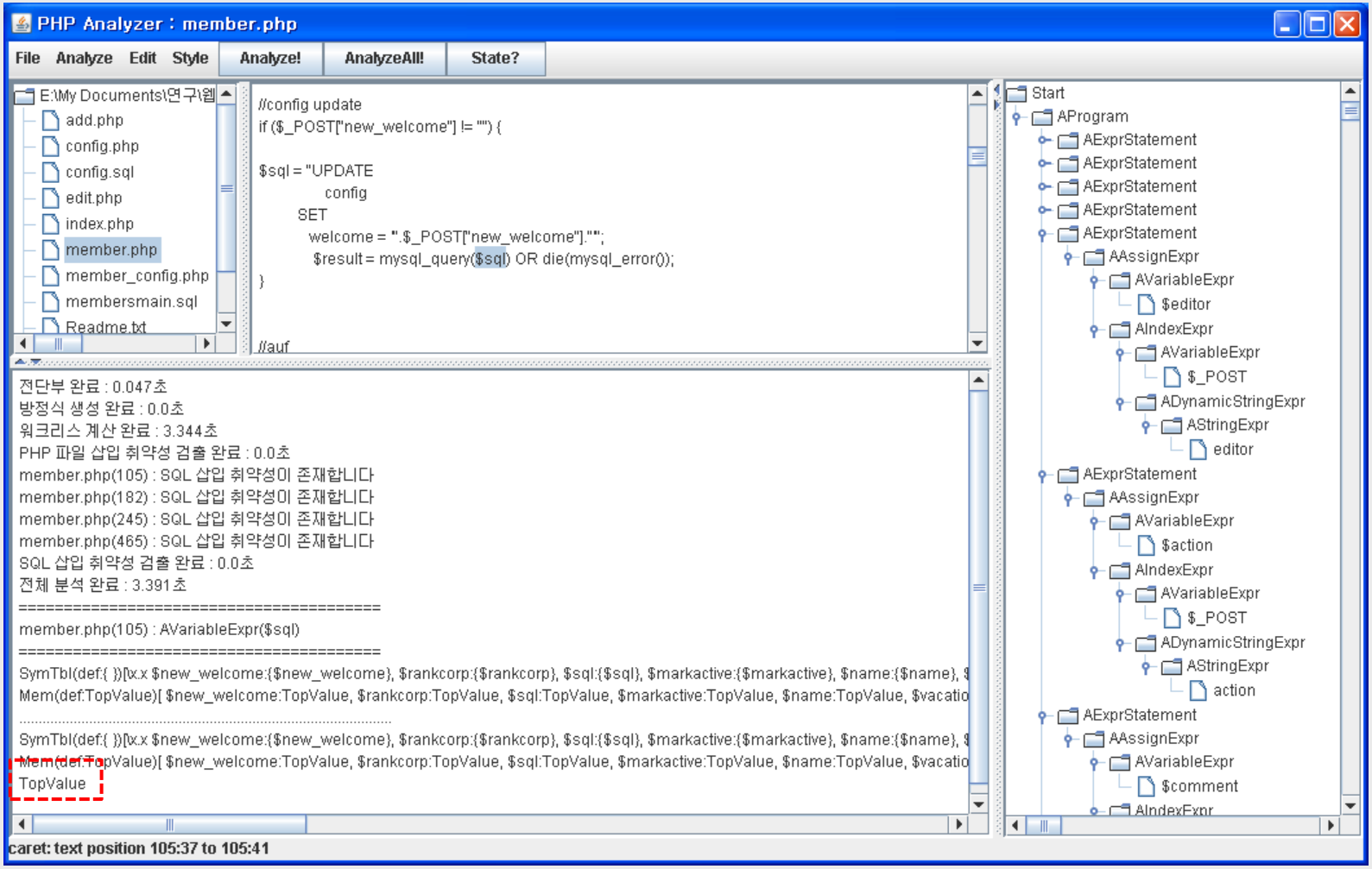
- 메모리 상태
  - State : SymbolTable * Memory
  - SymbolTable : (Loc -> Addr)*Addr
  - Memory : (Addr -> Value)*Value
  - Value := E(r) | S | I | {s1, ..., sk} | ArrayValue

취약성의 검출

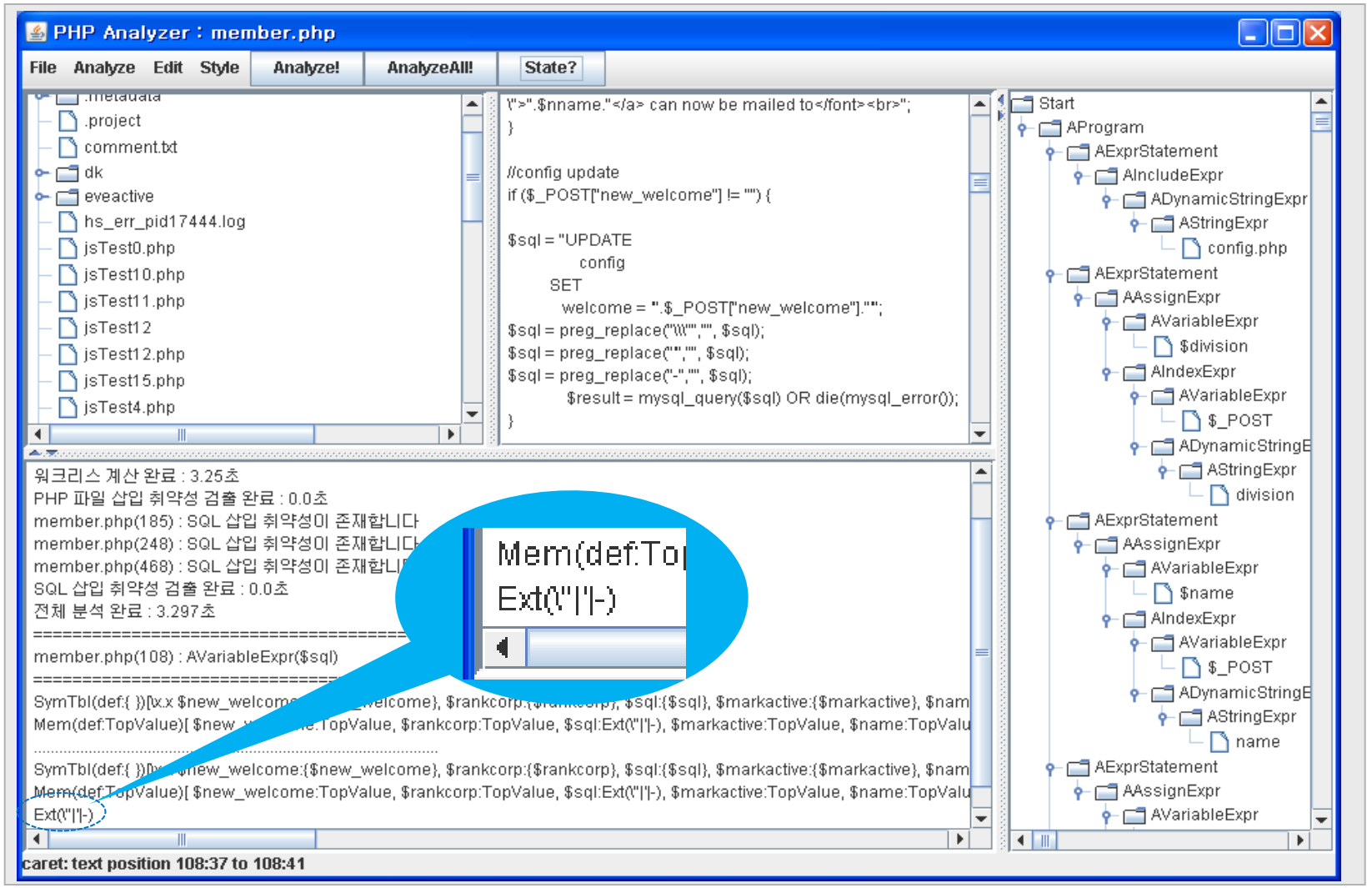
- 민감한 작업에 외부의 입력값 E(r)이 사용되고, r에 위험 문자열이 포함되지 않으면 취약한 것으로 판단
- 위험 문자열
  - SQL 삽입: ', ", --
  - Cross Site Scripting(XSS): &, <, >, “, ‘, /, …
  - PHP 파일 삽입: /, //, ₩, ₩₩, ., ..
  - OS 명령어 삽입: /, //, ₩, ₩₩, ., ..

* OWASP Prevention Cheat Sheet

실행화면


PHP Analyzer : member.php
File Analyze Edit Style Analyze! AnalyzeAll! State?
E:\My Documents\연구\웹
add.php
config.php
config.sql
edit.php
index.php
member.php
member_config.php
membersmain.sql
Readme.txt
//config update
if ($_POST["new_welcome"] != "") {
$sql = "UPDATE
config
SET
welcome = ".$_POST["new_welcome"]."";
$result = mysql_query($sql) OR die(mysql_error());
}
//auf
전단부 완료 : 0.047초
방정식 생성 완료 : 0.0초
워크리스 계산 완료 : 3.344초
PHP 파일 삽입 취약성 검출 완료 : 0.0초
member.php(105) : SQL 삽입 취약성이 존재합니다
member.php(182) : SQL 삽입 취약성이 존재합니다
member.php(245) : SQL 삽입 취약성이 존재합니다
member.php(465) : SQL 삽입 취약성이 존재합니다
SQL 삽입 취약성 검출 완료 : 0.0초
전체 분석 완료 : 3.391초
member.php(105) : AVariableExpr($sql)
TopValue
caret: text position 105:37 to 105:41
Start
AProgram
AExprStatement
AAssignExpr
AVariableExpr
$editor
AIndexExpr
$_POST
ADynamicStringExpr
AStringExpr
editor
$action
action
$comment

실행화면


PHP Analyzer : member.php
File Analyze Edit Style Analyze! AnalyzeAll! State?
.project
comment.txt
dk
eveactive
hs_err_pid17444.log
jsTest0.php
jsTest10.php
jsTest11.php
jsTest12
jsTest12.php
jsTest15.php
jsTest4.php
\">".$nname." can now be mailed to
";
}
//config update
if ($_POST["new_welcome"] != "") {
$sql = "UPDATE
config
SET
welcome = ".$_POST["new_welcome"]."";
$sql = preg_replace("\\\"","", $sql);
$sql = preg_replace("'","", $sql);
$sql = preg_replace("-","", $sql);
$result = mysql_query($sql) OR die(mysql_error());
}
워크리스 계산 완료 : 3.25초
PHP 파일 삽입 취약성 검출 완료 : 0.0초
member.php(185) : SQL 삽입 취약성이 존재합니다
member.php(248) : SQL 삽입 취약성이 존재합니다
member.php(468) : SQL 삽입 취약성이 존재합니
SQL 삽입 취약성 검출 완료 : 0.0초
전체 분석 완료 : 3.297초
member.php(108) : AVariableExpr($sql)
Mem(def:To
Ext(\"|'|-)
Start
AProgram
AExprStatement
AIncludeExpr
ADynamicStringExpr
AStringExpr
config.php
AExprStatement
AAssignExpr
AVariableExpr
$division
AIndexExpr
AVariableExpr
$_POST
ADynamicStringE
AStringExpr
division
AExprStatement
AAssignExpr
AVariableExpr
$name
AIndexExpr
AVariableExpr
$_POST
ADynamicStringE
AStringExpr
name
AExprStatement
AAssignExpr
AVariableExpr
caret: text position 108:37 to 108:41

True positives...

- SQL 삽입 취약성

프로그램	파일	라인수	검출 갯수	시간
EVE Activity Tracker(1.0)	Member.php	510	4	3.156
	User.php	136	1	0.032
	config_gedcom.php	132	2	0.417

- PHP 파일 삽입 취약성

프로그램	파일	라인수	검출 갯수	시간
PHPGEDVIEW -2.65	functions.php,	1856	1	0.843
	authentication_index.php	418	1	0.422
	config_gedcom.php	132	2	0.417
Mantis-1.0.0rc2	bug_sponsorship_list_view_inc.php	155	2	0.427
PhpDig-1.8.9-rc1	config.php	472	6	1.099

결론

- 향후 연구
  - File Inclusion

```
...
include($libpath.$command.".php");
...
```

  - Direct File Access
  - 성능 향상
    - memory state 최적화
    - copying on assignment
    - worklist algorithm
  - 언어 지원 확장
  - Domain 수정 (prefix, postfix)

결론

- 관련연구
  - Minamide, WWW '05
    - PHP 문자열 데이터 분석 (CFG 분석)
  - Z. Su and Wasserman, PLDI '07
    - SQL Injection 취약성 분석
  - Z. Su and Wasserman, ICSE '08
    - XSS 취약성 분석
  - Doh et al, SAS '09
    - Abstract Parsing