Tainted object propagation analysis for PHP 5 based on Pixy

Diploma thesis

Oliver Klee
Bonner Str. 63, 53173 Bonn
pixy@oliverklee.de

Bonn, 16. Dezember 2012

Rheinische Friedrich-Wilhelms-Universität Bonn
Institut für Informatik III
Professor Dr. Armin B. Cremers

Inhaltsverzeichnis

1 Introduction **5**
1.1 Motivation 5
1.2 Research problems and approach 5

2 PHP **7**
2.1 Challenges in static analysis for PHP 7

3 Vulnerabilities in PHP web applications **9**

4 Static analysis **11**

5 Review of existing static PHP vulnerability scanners **13**

6 Pixy **15**

7 PHP 5.4 **17**

8 Alias analysis for the new default pass-by-reference in PHP 5 **19**

9 Implementation details and problems encountered **21**

10 Experimental evaluation of the modified version of Pixy **23**

11 Discussion **25**
11.1 Related work 25
11.2 Conclusions 25
11.3 Further work 25

1 Introduction

1.1 Motivation

1.2 Research problems and approach

2 PHP

2.1 Challenges in static analysis for PHP

3 Vulnerabilities in PHP web applications

4 Static analysis

5 Review of existing static PHP vulnerability scanners

6 Pixy

7 PHP 5.4

8 Alias analysis for the new default pass-by-reference in PHP 5

9 Implementation details and problems encountered

10 Experimental evaluation of the modified version of Pixy

11 Discussion

11.1 Related work

11.2 Conclusions

11.3 Further work

Literaturverzeichnis