

# 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

|           |  |           |
|-----------|--|-----------|
| <b>1</b>  | <b>Introduction</b>  | <b>5</b>  |
| 1.1       | Motivation . . . . .   | 5         |
| 1.2       | Research problems and approach . . . . .                             | 5         |
| <b>2</b>  | <b>PHP</b>   | <b>7</b>  |
| 2.1       | Challenges in static analysis for PHP . . . . .                      | 7         |
| <b>3</b>  | <b>Vulnerabilities in PHP web applications</b>                       | <b>9</b>  |
| <b>4</b>  | <b>Static analysis</b>   | <b>11</b> |
| <b>5</b>  | <b>Review of existing static PHP vulnerability scanners</b>          | <b>13</b> |
| <b>6</b>  | <b>Pixy</b>  | <b>15</b> |
| <b>7</b>  | <b>PHP 5.4</b>   | <b>17</b> |
| <b>8</b>  | <b>Alias analysis for the new default pass-by-reference in PHP 5</b> | <b>19</b> |
| <b>9</b>  | <b>Implementation details and problems encountered</b>               | <b>21</b> |
| <b>10</b> | <b>Experimental evaluation of the modified version of Pixy</b>       | <b>23</b> |
| <b>11</b> | <b>Discussion</b>  | <b>25</b> |
| 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