Tainted object propagation analysis for PHP 5 based on Pixy

Diploma thesis

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

Bonn, December 19, 2012

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

Contents

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

Bibliography

[ADL+06] David Aponovich, Lachlan Donald, Nick Langmaid, Matthew Magain, Ian Muir, and Kevin Yank. *The State of Web Development 2006/2007*. Sitepoint, 2006.

[AFH06] Werner Altmann, René Fritz, and Daniel Hinderink. *TYPO3 Enterprise Content Management*. Open Source Press, 2nd edition, 2006.

[Aho86] Aho, Alfred V. and Sethi, Ravi and Ullman, Jeffrey D. *Compilers: principles, techniques, and tools*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1986.

[AKD+08] Shay Artzi, Adam Kiezun, Julian Dolby, Frank Tip, Danny Dig, Amit Paradkar, and Michael D. Ernst. Finding Bugs In Dynamic Web Applications. In *ISSTA '08: Proceedings of the 2008 international symposium on Software testing and analysis*, pages 261–272, New York, NY, USA, 2008. ACM.

[Anl02] Chris Anley. Advanced SQL Injection In SQL Server Applications. `http://www.ngssoftware.com/papers/advanced_sql_injection.pdf` (retrieved 2010-01-26), 2002.

[apa10] apache.org incident report for 04/09/2010. `https://blogs.apache.org/infra/entry/apache_org_04_09_2010` (retrieved 2010-04-15), 2010.

[APM+07] Nathaniel Ayewah, William Pugh, J. David Morgenthaler, John Penix, and YuQian Zhou. Evaluating Static Analysis Defect Warnings On Production Software. In *PASTE '07: Proceedings of the 7th ACM SIGPLAN-SIGSOFT workshop on Program analysis for software tools and engineering*, pages 1–8, New York, NY, USA, 2007. ACM.

[aut10] Autoloading Classes. `http://de.php.net/manual/en/language.oop5.autoload.php` (retrieved 2010-04-15), 2010.

[Bec03] Kent Beck. *Test-Driven Development by Example*. Pearson Education/Addison-Wesley, Boston, 2003.

[Ber05] Sebastian Bergmann. *Professionelle Softwareentwicklung mit PHP 5*. dpunkt, Heidelberg, 2005.

[Ber08] Sebastian Bergmann. Phpunit. `http://www.phpunit.de/` (retrieved 2008-09-18), 2008.

[BKK07] Paul E. Black, Michael Kass, and Michael Koo. Source Code Security Analysis Tool Functional Specification Version 1.0. `http://samate.nist.gov/docs/source_code_security_analysis_tool_spec_01_29_07.pdf` (retrieved 2010-01-26), 2007.

[Bv06] Magiel Bruntink and Arie van Deursen. An empirical study into class testability. *Journal of Systems and Software*, 79(9):1219–1232, sep 2006.

[CER00] CERT. CERT Advisory CA-2000-02: Malicious HTML Tags Embedded in Client Web Requests. `http://www.cert.org/advisories/CA-2000-02.html` retrieved on 2009-11-17, 2000.

[cod08] Armorize CodeSecure. `http://www.armorize.com/pdfs/resources/codesecure.pdf` (retrieved 2010-02-16), 2008.

[Cop06] King Cope. Writeup about source code auditing: How to to break code by reading it. `http://www.milw0rm.com/papers/124` (retrieved 2009-12-03), 2006.

[cov09] Coverity Scan Open Source Report. `http://scan.coverity.com/report/Coverity_White_Paper-Scan_Open_Source_Report_2009.pdf` (retrieved 2009-10-30), 2009.

[CS05] Christoph Csallner and Yannis Smaragdakis. Check 'n' crash: combining static checking and testing. In *ICSE '05: Proceedings of the 27th international conference on Software engineering*, pages 422–431, New York, NY, USA, 2005. ACM.

[CW07] Brian Chess and Jacob West. *Secure Programming with Static Analysis*. Pearson Education, Boston, 2007.

[cwe07] About CWE. `http://cwe.mitre.org/about/` (retrieved 2012-11-19), 2007.

[cwe11] 2011 CWE/SANS Top 25 Most Dangerous Software Errors. `http://cwe.mitre.org/top25/` (retrieved 2012-11-19), 2011.

[cwe12a] CWE-2000: Comprehensive CWE Dictionary. `http://cwe.mitre.org/data/lists/2000.html` (retrieved 2012-11-20), 2012.

[cwe12b] CWE: Organizations Participating. `http://cwe.mitre.org/compatible/organizations.html` (retrieved 2012-11-19), 2012.

[Dul08a] Dmitry Dulepov. Re: Call for suggestions: Unit tests for the 4.x core. `http://lists.netfielders.de/pipermail/typo3-project-4-3/2008-July/000162.html` (retrieved 2008-09-18), jul 2008.

[Dul08b] Dmitry Dulepov. *TYPO3 Extension Development*. Packt Publishing, Birmingham, 2008.

[EL08] Alexander Ebner and Patrick Lobacher. Inside TYPO3: Ein Blick in das Innere des CMS, Teil 2. *T3N*, pages 130–132, 2008.

[fac12] Facebook Developers: Access Tokens and Types. `https://developers.facebook.com/docs/concepts/login/access-tokens-and-types/` (retrieved 2012-11-21), 2012.

[Fea05] Michael C. Feathers. *Working Effectively With Legacy Code*. Pearson Education/Prentice Hall, Upper Saddle River, 2005.

[flo07] FLOW3: Development Principles. `http://flow3.typo3.org/about/principles/` (retrieved 2008-09-18), 2007.

[Fow00] Martin Fowler. *Refactoring: Improving the Design of Existing Code*. Addison-Wesley, Upper Saddle River, 2000.

[GKJ09] Arjun Guha, Shriram Krishnamurthi, and Trevor Jim. Using static analysis for ajax intrusion detection. In *WWW '09: Proceedings of the 18th international conference on World wide web*, pages 561–570, New York, NY, USA, 2009. ACM.

[GYF06] Emmanuel Geay, Eran Yahav, and Stephen Fink. Continuous code-quality assurance with safe. In *PEPM '06: Proceedings of the 2006 ACM SIGPLAN symposium on Partial evaluation and semantics-based program manipulation*, pages 145–149, New York, NY, USA, 2006. ACM.

[HHLT03] Yao-Wen Huang, Shih-Kun Huang, Tsung-Po Lin, and Chung-Hung Tsai. Web application security assessment by fault injection and behavior monitoring. In *WWW '03: Proceedings of the 12th international conference on World Wide Web*, pages 148–159, New York, NY, USA, 2003. ACM.

[HL02] Michael Howard and David E. Leblanc. *Writing Secure Code*. Microsoft Press, Redmond, WA, USA, 2002.

[HM04] Greg Hoglund and Gary McGraw. *Exploiting Software: How to Break Code.* Pearson Higher Education, 2004.

[HO05a] William G. J. Halfond and Alessandro Orso. Combining static analysis and runtime monitoring to counter sql-injection attacks. In *WODA '05: Proceedings of the third international workshop on Dynamic analysis*, pages 1–7, New York, NY, USA, 2005. ACM.

[HO05b] William G. J. Halfond and Alessandro Orso. Combining static analysis and runtime monitoring to counter sql-injection attacks. In *WODA '05: Proceedings of the third international workshop on Dynamic analysis*, pages 1–7, New York, NY, USA, 2005. ACM.

[HOM06] William G. J. Halfond, Alessandro Orso, and Panagiotis Manolios. Using positive tainting and syntax-aware evaluation to counter sql injection attacks. In *SIGSOFT '06/FSE-14: Proceedings of the 14th ACM SIGSOFT international symposium on Foundations of software engineering*, pages 175–185, New York, NY, USA, 2006. ACM.

[HP04] David Hovemeyer and William Pugh. Finding Bugs is Easy. *SIGPLAN Not.*, 39(12):92–106, 2004.

[HTL+05] Yao-Wen Huang, Chung-Hung Tsai, Tsung-Po Lin, Shih-Kun Huang, D. T. Lee, and Sy-Yen Kuo. A testing framework for web application security assessment. *Comput. Netw.*, 48(5):739–761, 2005.

[HTLK04] Yao-Wen Huang, Chung-Hung Tsai, D. T. Lee, and Sy-Yen Kuo. Non-detrimental web application security scanning. In *ISSRE '04: Proceedings of the 15th International Symposium on Software Reliability Engineering*, pages 219–230, Washington, DC, USA, 2004. IEEE Computer Society.

[Hug02] Fiona Hughes. PHP: most popular server-side Web scripting technology. `http://lwn.net/Articles/1433/` (retrieved 2010-01-26), 2002.

[HYH+04a] Yao-Wen Huang, Fang Yu, Christian Hang, Chung-Hung Tsai, D. T. Lee, and Sy-Yen Kuo. Verifying web applications using bounded model checking. In *DSN '04: Proceedings of the 2004 International Conference on Dependable Systems and Networks*, page 199, Washington, DC, USA, 2004. IEEE Computer Society.

[HYH+04b] Yao-Wen Huang, Fang Yu, Christian Hang, Chung-Hung Tsai, Der-Tsai Lee, and Sy-Yen Kuo. Securing Web Application Code by Static Analysis and Runtime Protection. In *WWW '04: Proceedings of the 13th interna-*

tional conference on World Wide Web, pages 40–52, New York, NY, USA, 2004. ACM.

[JCS07] Ciera Jaspan, I-Chin Chen, and Anoop Sharma. Understanding the Value of Program Analysis Tools. In *OOPSLA '07: Companion to the 22nd ACM SIGPLAN conference on Object-oriented programming systems and applications companion*, pages 963–970, New York, NY, USA, 2007. ACM.

[JKK06a] Nenad Jovanovic, Christopher Kruegel, and Engin Kirda. Pixy: A Static Analysis Tool for Detecting Web Application Vulnerabilities (Short Paper). In *SP '06: Proceedings of the 2006 IEEE Symposium on Security and Privacy*, pages 258–263, Washington, DC, USA, 2006. IEEE Computer Society.

[JKK06b] Nenad Jovanovic, Christopher Kruegel, and Engin Kirda. Pixy: A Static Analysis Tool for Detecting Web Application Vulnerabilities (Technical Report). `http://www.seclab.tuwien.ac.at/papers/pixy_techreport.pdf` (retrieved 2009-12-03), 2006.

[JKK06c] Nenad Jovanovic, Christopher Kruegel, and Engin Kirda. Precise Alias Analysis for Static Detection of Web Application Vulnerabilities. In *PLAS '06: Proceedings of the 2006 workshop on Programming languages and analysis for security*, pages 27–36, New York, NY, USA, 2006. ACM.

[JKK07] Nenad Jovanovic, Christopher Kruegel, and Engin Kirda. Pixy: XSS and SQLI Scanner for PHP Programs. `http://pixybox.seclab.tuwien.ac.at/pixy/` (retrieved 2010-01-12), 2007.

[Jov05] Nenad Jovanovic. Lattice Tutorial. `http://www.iseclab.org/people/enji/infosys/lattice_tutorial.pdf` (retrieved 2010-01-12), 2005.

[Jov06] Nenad Jovanovic. PhpParser. `http://www.seclab.tuwien.ac.at/people/enji/infosys/PhpParser.html` (retrieved 2010-01-12), 2006.

[Jov07] Nenad Jovanovic. Web Application Security (PhD Thesis). `http://www.seclab.tuwien.ac.at/papers/phdthesis-nenad.pdf` (retrieved 2010-01-13), 2007.

[Kac08] Erich Kachel. Analyse und Maßnahmen gegen Sicherheitsschwachstellen bei der Implementierung von Webanwendungen in PHP/MySQL. `http://www.erich-kachel.de/wp-content/uploads/2008/08/sicherheitsschwachstellen_phpmysql_analyse_2408_01.pdf` (retrieved 2010-01-26), 2008.

[KE08] Christopher Kunz and Stefan Esser. *PHP-Sicherheit*. dpunkt, Heidelberg, 3rd edition, 2008.

[Ker05] Joshua Kerievsky. *Refactoring to Patterns*. Pearson Education/Addison-Wesley, Boston, 2005.

[KKKJ06] Stefan Kals, Engin Kirda, Christopher Kruegel, and Nenad Jovanovic. SecuBat: A Web Vulnerability Scanner. In *WWW '06: Proceedings of the 15th international conference on World Wide Web*, pages 247–256, New York, NY, USA, 2006. ACM.

[KLB05] Kristoffer Kvam, Rodin Lie, and Daniel Bakkelund. Legacy System Exorcism by Pareto's Principle. *OOPSLA '05: Companion to the 20th annual ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications*, pages 250–256, 2005.

[Kle08a] Oliver Klee. Adding Unit Tests to Legacy TYPO3 4.x extensions. *Proceedings of the T3CON08*, pages 15–22, oct 2008.

[Kle08b] Oliver Klee. Call for suggestions: Unit tests for the 4.x core. `http://lists.netfielders.de/pipermail/typo3-project-4-3/2008-July/000161.html` (retrieved 2008-09-18), jul 2008.

[Kra09] Marcus Krause. TYPO3 Association 2nd Quarterly Report 2009. `http://secure.t3sec.info/blog/post/2009/08/18/typo3-association-2nd-quaterly-report-2009/` (retrieved 2010-02-17), 2009.

[Kra10] Marcus Krause. Preannouncements - no general use for TYPO3 advisories. `http://buzz.typo3.org/teams/security/article/preannouncements-no-general-use-for-typo3-advisories/` (retrieved 2010-03-22), 2010.

[L+06] Kai Laborenz et al. *TYPO3 4.0 – Das Handbuch für Entwickler*. Galileo Press, Bonn, 2nd edition, 2006.

[LC08] Benjamin Livshits and Weidong Cui. Spectator: detection and containment of javascript worms. In *ATC'08: USENIX 2008 Annual Technical Conference on Annual Technical Conference*, pages 335–348, Berkeley, CA, USA, 2008. USENIX Association.

[Lem05a] Robert Lemke. Grünes Gefühl mit TYPO3. *T3N*, pages 37–38, 2005.

[Lem05b] Robert Lemke. Refactoring and Unit Testing with TYPO3. *Proceedings of the TYCON3*, sep 2005.

[LFMT04] G. A. Di Lucca, A. R. Fasolino, M. Mastoianni, and P. Tramontana. Identifying cross site scripting vulnerabilities in web applications. In *WSE '04: Proceedings of the Web Site Evolution, Sixth IEEE International Workshop*, pages 71–80, Washington, DC, USA, 2004. IEEE Computer Society.

[Lig08] Kasper Ligaard. phpunit typo3 extension. `http://forge.typo3.org/projects/show/extension-phpunit` (retrieved 2008-09-18), 2008.

[Lin02] Johannes Link. *Unit Tests mit Java*. dpunkt, Heidelberg, 2002.

[LL05] V. Benjamin Livshits and Monica S. Lam. Finding Security Vulnerabilities in Java Applications with Static Analysis. In *SSYM'05: Proceedings of the 14th conference on USENIX Security Symposium*, pages 18–18, Berkeley, CA, USA, 2005. USENIX Association.

[LM08] Yin Liu and Ana Milanova. Static analysis for inference of explicit information flow. In *PASTE '08: Proceedings of the 8th ACM SIGPLAN-SIGSOFT workshop on Program analysis for software tools and engineering*, pages 50–56, New York, NY, USA, 2008. ACM.

[LMLW08] Monica S. Lam, Michael Martin, Benjamin Livshits, and John Whaley. Securing web applications with static and dynamic information flow tracking. In *PEPM '08: Proceedings of the 2008 ACM SIGPLAN symposium on Partial evaluation and semantics-based program manipulation*, pages 3–12, New York, NY, USA, 2008. ACM.

[LR92] William Landi and Barbara G. Ryder. A safe approximate algorithm for interprocedural aliasing. *SIGPLAN Not.*, 27(7):235–248, 1992.

[Mal07] Stanislav Malyshev. Securing PHP—Approaches to Web Applications Security. In *Web 2.0 Security & Privacy 2007 (Workshop)*, 2007.

[Mes07] Gerard Meszaros. *xUnit Test Patterns*. Pearson Education/Addison-Wesley, Boston, 2007.

[MLA07] Ettore Merlo, Dominic Letarte, and Giuliano Antoniol. Automated protection of PHP applications against SQL injection attacks. In *CSMR '07: Proceedings of the 11th European Conference on Software Maintenance and Reengineering*, pages 191–202, Washington, DC, USA, 2007. IEEE Computer Society.

[Mor09] Morrison, Jason. Open-Redirect-URLs: Wird eure Website von Spammern ausgenutzt? `http://googlewebmastercentral-de.blogspot.de/2009/02/open-redirect-urls-wird-eure-website.html` (retrieved 2012-11-21), 2009.

[MS09] Ofer Maor and Amichai Shulman. Blindfolded SQL Injection. `http://www.imperva.com/docs/Blindfolded_SQL_Injection.pdf` (retrieved 2010-01-26), 2009.

[Nat09a] National Institute of Standards and Technology. CWE-200: Information Exposure. `http://cwe.mitre.org/data/definitions/200.html` (retrieved 2010-01-26), 2009.

[Nat09b] National Institute of Standards and Technology. CWE-22: Path Traversal. `http://cwe.mitre.org/data/definitions/22.html` (retrieved 2010-01-26), 2009.

[Nat09c] National Institute of Standards and Technology. CWE-352: Cross-Site Request Forgery (CSRF). `http://cwe.mitre.org/data/definitions/352.html` (retrieved 2010-01-26), 2009.

[Nat09d] National Institute of Standards and Technology. CWE-78: Improper Sanitization of Special Elements used in an OS Command (OS Command Injection). `http://cwe.mitre.org/data/definitions/78.html` (retrieved 2010-01-26), 2009.

[Nat09e] National Institute of Standards and Technology. CWE-79: Failure to Preserve Web Page Structure (Cross-site Scripting. `http://cwe.mitre.org/data/definitions/79.html` (retrieved 2010-01-26), 2009.

[Nat09f] National Institute of Standards and Technology. CWE-89: Improper Sanitization of Special Elements used in an SQL Command (SQL Injection). `http://cwe.mitre.org/data/definitions/89.html` (retrieved 2010-01-26), 2009.

[Nat09g] National Institute of Standards and Technology. CWE-94: Failure to Control Generation of Code (Code Injection). `http://cwe.mitre.org/data/definitions/94.html` (retrieved 2010-01-26), 2009.

[NMBW08] Nachiappan Nagappan, E. Maximilien, Thirumalesh Bhat, and Laurie Williams. Realizing quality improvement through test driven development: results and experiences of four industrial teams. *Empirical Software Engineering*, 13(3):289–302, June 2008.

[OGGB07] Vadim Okun, William F. Guthrie, Romain Gaucher, and Paul E. Black. Effect of Static Analysis Tools on Software Security: Preliminary Investigation. In *QoP '07: Proceedings of the 2007 ACM workshop on Quality of protection*, pages 1–5, New York, NY, USA, 2007. ACM.

[osv11] OSVDB: The Open Source Vulnerability Database. `http://osvdb.org/` (retrieved 2011-01-10), 2011.

[OWA12] OWASP. Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet. `https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet` (retrieved 2012-11-21), 2012.

[PCA09] Massimiliano Di Penta, Luigi Cerulo, and Lerina Aversano. The life and death of statically detected vulnerabilities: An empirical study. *Inf. Softw. Technol.*, 51(10):1469–1484, 2009.

[PCFY07] M. Pistoia, S. Chandra, S. J. Fink, and E. Yahav. A survey of static analysis methods for identifying security vulnerabilities in software systems. *IBM Syst. J.*, 46(2):265–288, 2007.

[php07a] About PHP-front: Static analysis for PHP. `http://www.program-transformation.org/PHP/PhpFront` (retrieved 2010-02-16), 2007.

[php07b] PHP-SAT.org: Static analysis for PHP. `http://www.program-transformation.org/PHP/` (retrieved 2010-02-16), 2007.

[php12] PHP Manual: header(). `http://php.net/manual/de/function.header.php` (retrieved 2012-11-20), 2012.

[RAF04] Nick Rutar, Christian B. Almazan, and Jeffrey S. Foster. A Comparison of Bug Finding Tools for Java. In *ISSRE '04: Proceedings of the 15th International Symposium on Software Reliability Engineering*, pages 245–256, Washington, DC, USA, 2004. IEEE Computer Society.

[RBS07] Dagfinn Reiersøl, Marcus Baker, and Chris Shiflett. *PHP in Action*. Manning, Greenwich, 2007.

[Rim08a] Mario Rimann. Green Bar Feeling bei TYPO3-Extensions. *T3N*, pages 96–97, 2008.

[Rim08b] Mario Rimann. Makelloser Code durch effizientes Testen. *T3N*, pages 65–66, 2008.

[Rin11] Georg Ringer. TYPO3 4.5 – CSRF-Schutz. `http://typo3blogger.de/typo3-4-5-csrf-schutz/` (retrieved 2012-11-21), 2011.

[Son06] Dug Song. Static Code Analysis Using Google Code Search. `http://asert.arbornetworks.com/2006/10/static-code-analysis-using-google-code-search/` (retrieved 2009-12-03), 2006.

[str08] Stratego/XT. `http://strategoxt.org/Stratego/WebHome` (retrieved 2010-02-16), 2008.

[SW06] Zhendong Su and Gary Wassermann. The essence of command injection attacks in web applications. In *POPL '06: Conference record of the 33rd ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 372–382, New York, NY, USA, 2006. ACM.

[swa09] OWASP SWAAT Project. `http://www.owasp.org/index.php/Category:OWASP_SWAAT_Project` (retrieved 2009-10-30), 2009.

[TYPa] TYPO3 Association. What are extensions? `http://typo3.org/extensions/what-are-extensions/` (retrieved 2010-02-17).

[TYPb] TYPO3 Association. What are reviews? `http://typo3.org/extensions/what-are-reviews/` (retrieved 2010-02-17).

[VA06] Markus Völter and Jonathan Aldrich. Static code analysis. `http://www.se-radio.net/podcast/2007-06/episode-59-static-code-analysis` (retrieved 2008-09-09), 2006.

[Vaa03] Sami Vaaraniemi. The benefits of automated unit testing. `http://www.codeproject.com/KB/architecture/onunittesting.aspx` (retrieved 2008-09-09), November 2003.

[ver08] CodeSecure Verifier Source Code Analysis Scanner. `http://www.armorize.com/pdfs/resources/verifier.pdf` (retrieved 2010-02-16), 2008.

[W3T12a] W3Techs. Usage of server-side programming languages for websites. `http://w3techs.com/technologies/overview/programming_language/all` (retrieved 2012-11-16), 2012.

[W3T12b] W3Techs. Usage of server-side programming languages for websites. `http://w3techs.com/technologies/details/pl-php/all/all` (retrieved 2012-11-16), 2012.

[Wei12] Weiland, Jochen and Schams, Michael. TYPO3 Security Guide. `http://typo3.org/documentation/document-library/guides/doc_guide_security/current/` (retrieved 2012-11-21), 2012.

[WF08] Michael S. Ware and Christopher J. Fox. Securing Java Code: Heuristics and An Evaluation of Static Analysis Tools. In *SAW '08: Proceedings of the 2008 workshop on Static analysis*, pages 12–21, New York, NY, USA, 2008. ACM.

[WHKD00] Chenxi Wang, Jonathan Hill, John Knight, and Jack Davidson. Software Tamper Resistance: Obstructing Static Analysis of Programs. Technical report, Charlottesville, VA, USA, 2000.

[Wik08] Wikipedia. Regression testing. `http://en.wikipedia.org/wiki/Regression_testing` (retrieved 2008-09-09), 2008.

[Wil07] Dan Wilson. Is Eclipse Slow for you? `http://www.nodans.com/index.cfm/2007/4/15/Is-Eclipse-Slow-for-you` (retrieved 2010-02-17), 2007.

[WS07] Gary Wassermann and Zhendong Su. Sound and precise analysis of web applications for injection vulnerabilities. In *PLDI '07: Proceedings of the 2007 ACM SIGPLAN conference on Programming language design and implementation*, pages 32–41, New York, NY, USA, 2007. ACM.

[WS08] Gary Wassermann and Zhendong Su. Static detection of cross-site scripting vulnerabilities. In *ICSE '08: Proceedings of the 30th international conference on Software engineering*, pages 171–180, New York, NY, USA, 2008. ACM.

[XA06] Yichen Xie and Alex Aiken. Static detection of security vulnerabilities in scripting languages. In *USENIX-SS'06: Proceedings of the 15th conference on USENIX Security Symposium*, Berkeley, CA, USA, 2006. USENIX Association.

[yas09] Yasca—Yet Another Source Code Analyzer. `http://www.yasca.org/` (retrieved 2009-12-03), 2009.

[Yin03] Robert K. Yin. *Case Study Research: Design and Methods*, volume 5. Sage Publications, Thousand Oaks, 3rd edition, 2003.

[zen10] Tips to Manage Zend Studio 6.x and 7.x Performance Issues. `http://kb.zend.com/?View=entry&EntryID=307` (retrieved 2010-03-22), 2010.

[Zha10] Haiping Zhao. HipHop for PHP: Move Fast. `https://developers.`

`facebook.com/blog/post/2010/02/02/hiphop-for-php--move-fast/` (retrieved 2012-11-16), 2010.

[ZWN+06] Jiang Zheng, Laurie Williams, Nachiappan Nagappan, Will Snipes, John P. Hudepohl, and Mladen A. Vouk. On the Value of Static Analysis for Fault Detection in Software. *IEEE Trans. Softw. Eng.*, 32(4):240–253, 2006.

List of Figures

List of Tables