致　谢　南开大学机器智能研究所的老师同学对本文的写作提供了帮助，各位审阅论文专家提出了宝贵意见，在此一并致谢！

参考文献

[1] Chen Ya-Long, Jiang Guo-Hua. Based on FSM Web application research on test case generation. Electronic Science and Technology, 2013, 26(4): 17-21(in Chinese)
(陈亚龙，江国华. 基于 FSM 的 Web 应用测试用例生成研究. 电子科技，2013，26(4)：17-21)

[2] Wang Yu-Ding, Yang Jia-Hai, Xu Cong, et al. Survey on access control technologies for cloud computing. Journal of Software, 2015, 26(5): 1129-1150(in Chinese)
(王于丁，杨家海，徐聪等. 云计算访问控制技术研究综述. 软件学报，2015，26(5)：1129-1150)

[3] Erik R, Axiomatics A B. OASIS Extensible Access Control Markup Language (XACML). Versions 3.0. Boston, USA: OASIS Open, 2013

[4] Butler B, Jennings B, Botvich D. XACML policy performance evaluation using a flexible load testing framework//Proceedings of the 17th ACM Conference on Computer and Communications Security. Chicago, USA, 2010: 978-980

[5] Liu A X, Chen F, Hwang J H. Designing fast and scalable XACML policy evaluation engines. IEEE Transactions on Computers, 2011, 60(12): 1802-1817

[6] Wang Ya-Zhe, Feng Deng-Guo, Zhang Li-Wu, Zhang Min. XACML policy evaluation engine based on multi-level optimization technology. Journal of Software, 2011, 22(2): 323-338(in Chinese)
(王雅哲，冯登国，张立武，张敏. 基于多层次优化技术的 XACML 策略评估引擎. 软件学报，2011，22(2)：323-338)

[7] Niu De-Hua, Ma Jian-Feng, Ma Zhuo, et al. HPEngine: high performance XACML policy evaluation engine based on statistical analysis. Journal on Communications, 2014, 35(8): 206-215(in Chinese)
(牛德华，马建峰，马卓等. 基于统计分析优化的高性能 XACML 策略评估引擎. 通信学报，2014，35(8)：206-215)

[8] Sun F, Xu L, Su Z. Static detection of access control vulnerabilities in web applications//Proceedings of the 20th USENIX Conference on Security. San Francisco, USA, 2011

[9] Bisht P, Hinrichs T, Skrupsky N, et al. NoTamper: Automatic blackbox detection of parameter tampering opportunities in web applications//Proceedings of the 17th ACM Conference on Computer and Communications Security. Chicago, USA, 2010: 607-618

[10] Payet P, Doupé A, Kruegel C, et al. EARs in the wild: Large-scale analysis of Runution after redirect vulnerabilities //Proceedings of the 28th Annual ACM Symposium on Applied Computing. Coimbra, Portugal, 2013: 1792-1799.12

[11] Doupé A, Boe B, Kruegel C, et al. Fear the EAR: Discovering and mitigating Runution after redirect vulnerabilities// Proceedings of the 18th ACM Conference on Computer and Communications Security. Chicago, USA, 2011: 251-262

[12] Dalton M, Kozyrakis C, Zeldovich N. Nemesis: Preventing authentication & access control vulnerabilities in web applications //Proceedings of the 18th Conference on USENIX Security Symposium. Montreal, Canada, 2009: 267-282

[13] Son S, McKinley K S, Shmatikov V. Rolecast: Finding missing security checks when you do not know what checks are. ACM SIGPLAN Notices, 2011, 46(10): 1069-1084

[14] Son S, McKinley K S, Shmatikov V. Fix Me Up: Repairing access-control bugs in web applications//Proceedings of the Network and Distributed System Security Symposium. San Diego, USA, 2013: 712-727

[15] Monshizadeh M, Naldurg P, Venkatakrishnan V N. MACE: Detecting privilege escalation vulnerabilities in web applications //Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. Scottsdale, USA, 2014: 690-701

[16] Muthukumaran D, O'Keeffe D, Priebe C, et al. FlowWatcher: Defending against data disclosure vulnerabilities in web applications//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. Denver, USA, 2015: 603-615

[17] Li Xiaowei, Xue Yuan. BLOCK: A black-box approach for detection of state violation attacks towards web applications //Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC). Orlando, USA, 2011: 247-256

[18] Li Xiaowei, Yan Wei, Xue Yuan. SENTINEL: Securing database from logic flaws in web applications//Proceedings of the 2nd ACM Conference on Data and Application Security and Privacy. San Antonio, USA, 2012: 25-36

[19] Li Xiaowei, Xue Yuan. LogicScope: Automatic discovery of logic vulnerabilities within web applications//Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security. Hangzhou, China, 2013: 481-486

[20] Han Dao-Jun, Gao Jie, Zhai Hao-Liang, Li Lei. Research development of access control model. Computer Science, 2010, 37(11): 29-33(in Chinese)
(韩道军，高洁，翟浩良，李磊. 访问控制模型研究进展. 计算机科学，2010，37(11)：29-33)

[21] Wonohoesodo R, Tari Z. A role based access control for Web services//Proceedings of the 2004 IEEE International Conference on Services Computing (SCC 2004). Shanghai, China, 2004: 49-56

WEN Shuo, born in 1987, Ph. D. His research interests include software engineering and software security.

XU Jing, born in 1967, professor, Ph. D. supervisor. Her research interests include software engineering and software security.

YUAN Li-Ying, born in 1990, M. S. candidate. Her research interests include software analysis and software security.

LI Xiao-Hong, born in 1990, M. S. candidate. Her research interests include software analysis and software security.

XU Si-Han, born in 1991, Ph. D. candidate. Her research interests include software engineering and software testing.

SI Guan-Nan, born in 1981, assistant professor. His research interests include software engineering and software evaluating technology.

Background

Web applications have become more and more popular for achieving information over the Internet. However, access control vulnerability can expose sensitive data of web applications although most of web applications implement access control mechanisms which restrict the data access privileges of different roles and users. When a web application has access control vulnerabilities, attackers can bypass the intended security mechanism and access unauthorized data. To protect the sensitive information, the testing of web applications should be effective and efficient. Test case generation is one of the key issues during the whole testing phase. Nevertheless, existing test case generation approaches have limits and high redundant while providing certain coverage. In this paper, we present a novel test case generation approach for discovering access control vulnerabilities in web applications. From the collected Samples, we identify the set of rules which are allowed for each role or user and conclude the access control policy. Based on the inferred policy, our method can generate reduced and effective test cases. A prototype system ACV-Scanner is also implemented for evaluation over a set of web applications. The experiment results demonstrate that our method can effectively decrease the test cases, reduce the false negative and improve the efficiency while exploiting different categories of access control vulnerabilities.

This work is supported by the Tianjin Science and Technology Committee (No. 12JCZDJC20800), the National Key Technology R&D Program (No. 2013BAH01B05) and the National Natural Science Foundation of China (Grant No. 61402264).

Our research group has focused on the research of software security testing for many years and applied 3 Issued Software Patents and 6 software copyrights. The members of our group have participated in 2 National Natural Science Foundation projects, 1 National Key Technology R&D Program, and 3 Tianjin Science and Technology Committee projects.

Our group has published more than 30 papers toward software security testing area. Most papers written in Chinese are published in famous Chinese journals, including: Science China, Chinese Journal of Computers, Journal of Computer Research and Development, High Technology Letters. The papers written in English are also published in important international conferences, including: COMPSAC 2012, 2013, 2015, HPCC 2013, ICECCS 2014.