Abstract

Cross Site programming (XSS) is the script attack in web pages, and it is accounted as one of the most dangerous problems of web applications. The researchers of security have investigated on different problems and they have found that the XSS vulnerability exists in many of known websites. The vulnerability is applied when an attacker reaches to an authorized user's web explorer optionally and he/she might do cookie theft, develop destructive software, thieve the session and change the path of destruction. The validation of the user’s input is the first obstacle to protect the web applications against this vulnerability. The main aim of improving the security of web applications is improvement in the quality of user’s input validation. Unfortunately, the web application developers usually forget the user’s input validation and/or implement a weak validation. In this paper, it is attempted to present a pattern to validate the user’s input correctly in the web applications, and the obtained results are compared with the tools of scanning the existing vulnerability.

References
   Applications”, in: 7th International Workshop on Automation of Software Test (AST), no. line 13,
3. Common Vulnerabilities and Exposures (The Standard for Information Security
   Vulnerability Names) http://cwe.mitre.org/
4. D. Balzarotti et al., “Saner: Composing Static and Dynamic Analysis to Validate
5. H. Shahriar and M. Zulkernine, “MUTEC: Mutation-Based Testing of Cross Site Scripting,”
6. Isatou Hydara, Abu Bakar Md. Sultan, Current state of research on cross-site scripting
7. José Fonseca, Marco Vieira, Henrique Madeira, “Testing and comparing web vulnerability
   scanning tools for SQL injection and XSS attacks”, in: 13th IEEE International Symposium on
8. L.K. Shar, H.B.K. Tan, “Predicting common web application vulnerabilities from input
   Eng. – ASE, p. 310, 2012
9. M.S. Lam et al., “Securing Web Applications with Static and Dynamic Information Flow
   Manipulation (PEPM 08), ACM, pp. 3-12, 2008
10. N. Li et al., “Perturbation-Based User-Input-Validation Testing of Web Applications,” J.
    Systems and Software, Nov. 2010, pp. 2263-2274
11. Open Web Application Security Project, XSS (Cross-Site Scripting), Prevention Cheat
    Sheet, 2015; https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_
    Prevention_Cheat_Sheet.
    Services Input Validation Model”, in: IEEE Network Operations and Management Symposium
13. R. Komiya, I. Paik, M. Hisada, “Classification of malicious web code by machine
    learning”, in: 3rd International Conference on Awareness Science and Technology iCAST, pp.
15. White Hat Security Website Stats Report 2015,

Index Terms
Computer Science
Networks
Keywords

web vulnerabilities, input validation, XSS malware