Security Testing of Web Applications: Issues and Challenges

Arunima Jaiswal
Asst. Professor,
Amity University, Noida, India

Gaurav Raj
PhD Scholar, Punjab Technical University, Punjab, India

Dheerendra Singh, Ph.D
Professor & HOD
SUSCET, Tangori, Punjab

ABSTRACT

Due to the increasing complexity of web systems, security testing has become indispensable and critical activity of web application development life cycle. Security testing aims to maintain the confidentiality of the data, to check against any information leakage and to maintain the functionality as intended. It checks whether the security requirements are fulfilled by the web applications when they are subjected to malicious input data. Due to the rising explosion in the security vulnerabilities, there occurs a need to understand its unique challenges and issues which will eventually serve as a useful input for the security testing tool developers and test managers for their relative projects.

Keywords

Web applications, Security testing, Vulnerabilities

1. INTRODUCTION

In Recent years, we have witnessed rapid diffusion of internet which produces significant demand of web applications with strict security requirements. Due to which there is an increase in the number of vulnerabilities in web applications which can be exploited by attackers so as to gain unauthorized access to the web sites and web applications. Modern Web systems are really complex, distributed and heterogeneous, multilingual and multimedia, interactive and responsive, ever evolving, and rapidly changed [2].

Web domain is pervasive and dynamic in nature which makes it more prone to malevolent actions like security breaches, threats, virus attacks etc. In the light of diversification of the web applications, security becomes a critical issue and is related to the quality of the web application. So we can say that security becomes an elusive goal.

Thus security testing phase can be concatenated to the development phase for increasing the trustworthiness of the web applications. Goal of security testing is to detect those defects that could be exploited to conduct attacks [20]. Security testing helps to emulate and expose vulnerabilities like cross-site scripting, SQL injection, buffer overflow, file inclusion, URL injection, cookie modification. Due to the enormous increase in the web application vulnerabilities, there are various threats and challenges being faced which can cause a severe setback to the integrity, confidentiality and security of the web applications. So in order to devise any effective methodology or techniques for web security testing, we should first understand its unique challenges and issues. The goal of the paper is to discuss about various issues and challenges related to the security testing of web applications together with the tools which are used to perform security testing of web applications.

1.1 Organization of the paper

Rest of the paper is organized as follows. First we present the Literature Survey. Then discuss about the Review Process which is followed. Then focus on the various Issues and Challenges faced by Security Testing of web applications. Next briefly discuss about the Review Results, Current Trends and Future Directions. Finally we discuss about the Conclusions Followed by References.

2. LITERATURE SURVEY

There has been a lot of research in the field of security testing of web applications.

2.1 Studies carried out in Literature Survey

Garcia (1998) [30] discusses the use of performance measures such as probability of detection for sensors, barrier delay times, and response force time results in overall assessment of security effectiveness. This measure helps relate the risk at a facility to threats, targets, consequences of loss, and probability of attack.

Dima Alden et al. (1999) [28] discusses about the use of cryptographic module validation programs for increasing and maintaining the security of web applications. For example an application may use cryptographic module to generate passwords etc. Also it speaks of about the use of COTS components as they may cause serious threats to the security aspect of the application and thus they become another reason to endorse open testing.

Lyu R. Michael et al. (2000) [25] mentions about the use of firewalls as a method of protecting the network sites against external attacks and intrusion. It also discusses about four basic components in building a firewall like policy, advanced authentication, packet filtering, and application gateway.

Curphey Mark et al. (2006) [26] discusses about the web security vulnerabilities framework and various tools like source code analyzer, black box scanners, database scanners, binary analysis tools, runtime analysis tool, configuration analysis tool, proxies tools.

Choi Cheol et al. (2006) [5] mentions about parameter manipulation, cookie manipulation, modifying or hijacking a user’s session.

Wang Linzhang et al. (2007) [17] focuses on threat model driven approach for security testing. They identify threat as a condition that enables attacker to violate the security policy. Threats are behaviors that an attacker may pose to the system and violate security properties such as authentication, authorization, confidentiality and privacy.

Fonseca Jose et al. (2008) [14] focuses on the root cause of most security attacks are the vulnerabilities created by the software faults, and most critical web vulnerabilities are SQL injection and cross site scripting.

Hassan Doaa et al. (2008) [22] discusses about the broken access control vulnerability which exploits the fragility of the access control and is able to fetch the sensitive and confidential information.

Turpe Sven et al. (2008) [6] mentions about various issues like path traversal, command injection, cross site scripting, content spoofing, SQL injection, LDAP injection.

Noiumkar Preecha et al. (2008) [29] discusses about session hijacking, sidejacking, cookie cloning and sniffing cookies.

Mendes Naaliel et al. (2008) [24] focuses on the issues and vulnerabilities which are caused due to mis-configurations or by absence of any intrusion detection mechanism or firewalls. Also they mention about the threats which may occur due to the usage of the off the shelf components.

Saleh Kassem et al. (2008) [21] discuss about the comprehensive modeling of security requirements and introduces the security requirements behavior model to obtain secure and trustworthy web services and applications.

Fonseca Jose et al. (2008) [14] focuses on the root cause of most security attacks are the vulnerabilities created by the software faults, and most critical web vulnerabilities are SQL injection and cross site scripting.

Haixia Yang (2009) [7] discusses about the SQL injection vulnerability which occurs in the presentation layer (user layer) of web application.

Bau Jason et al. (2010) [8] discusses about the Cross Channel Scripting vulnerability which allows an attacker to inject malicious code into the web server which will thus manipulate the client or a server browser.

Salva Sebastien et al. (2010) [9] mentions about the vulnerabilities which are related to the security testing of web applications like xml injection, authentication, authorization.

Zhang Lijiu et al. (2010) [19] discusses about the issues like cross site request forgery, cross site scripting, malicious file execution and SQLi injection related to the web application security testing.

Terri Oda et al. (2011) [23] discusses about the web security issues like script injection, content injection, information leakage, cross site request forgery and Clickjacking.

Avancini Andrea et al. (2011) [1] mentions about the content injection, file injection and cross site scripting attack.

Choudhary Suryakant et al. (2012) [13] focuses on the crawling as essential for security testing of web applications. Crawling is automatic explorations of web application.

Andrea Avancini (2012) [15] discusses about a research plan to address problems of potentially attackable code. Also it speaks of cross site scripting vulnerabilities in which missing input validation can be exploited by attackers to inject malicious code into the application.

Avancini Andrea et al. (2012) [10] mentions about the issues like cross site scripting vulnerabilities, missing or inadequate validation of input data, disclosure of any sensitive information or hijacking of user session.

Andrea Avancini et al. (2012) [18] discusses about cross site scripting and SQLi vulnerabilities involved with many of the web applications build in java.

Buchler Matthias et al. (2012) [11] mentions about the most critical issue related with the security testing of web applications i.e. cross site scripting attack.

2.2 Summary of Literature Survey

Table 1. Author wise addressed issues in their papers

Author Name	**Issue addressed**
Mary Lynn Garcia [30]	probability of attack
Dima Alden et al. [28]	use of COTS components, use of cryptographic module validation programs
Michael R. Lyu et al. [25]	the use of firewalls as a method of protecting the network sites against external attacks and intrusion
Mark Curphey et al. [26]	discusses about the web security vulnerabilities framework and various tools
Choel Choi et al. [5]	parameter manipulation, cookie manipulation, modifying or hijacking a user’s session
Linzhang Wang et al. [17]	focuses on threat model driven approach for security testing. They identify threat as a condition that enables attacker to violate the security policy
Hassan Doaa et al. [22]	broken access control vulnerability
Sven Turpe et al. [6]	path traversal, command injection, cross site scripting, content spoofing, SQL injection, ldap injection, xpath injection
Preecha Noiumkar et al. [29]	session hijacking, sidejacking, cookie cloning and sniffing cookies
Naaliel Mendes et al. [24]	absence of any intrusion detection mechanism or firewalls, usage of the off the shelf components, mis-configuration
Fonseca Jose et al. [14]	focus on the most critical web vulnerabilities are SQL injection and cross site scripting.
Kassem Saleh et al. [21]	introduces the security requirements behavior model to obtain secure and trustworthy web services and applications
Yang Haixia [7]	SQL injection vulnerability
Jason Bau et al. [8]	Cross Channel Scripting vulnerability
Sebastien Salva et al. [9]	xml injection, authentication, authorization

Lijiu Zhang et al. [19]	cross site request forgery, cross site scripting, malicious file execution and SQLi injection
Terri Oda et al. [23]	Discusses about the web security issues like script injection, content injection, information leakage, cross site request forgery, clickjacking.
Andrea Avancini et al. [1]	content injection, file injection and cross site scripting attack
Suryakant Choudhary et al. [13]	focuses on the crawling as essential for security testing of web applications
Andrea Avancini [15]	cross site scripting vulnerabilities
Avancini Andrea et al. [10]	cross site scripting vulnerabilities, missing or inadequate validation of input data, disclosure of any sensitive information or hijacking of user session
Avancini Andrea et al. [18]	cross site scripting and SQLi vulnerabilities
Matthias Buchler et al. [11]	cross site scripting attack

3. REVIEW PROCESS

3.1 Planning

3.1.1 Identification of the need for a review:

This review has been conducted so as to gain knowledge about the issues and challenges related to the security testing of web applications. It has got indispensable relevance as it will provide us with the knowledge and update our information regarding enhancement of security of the web applications.

3.1.2 Specifying the research question:

Ques. 1: What are the vulnerabilities related to security of web testing?

Ques. 2: What are the challenges faced by web security testing?

Ques. 3: What are the possible issues related with security aspect of web testing?

Ques. 4: Does the challenges faced identify the risk associated with the secure web testing?

Ques. 5: Does the outcomes relate to factors of importance to practitioners?

Ques. 6: Is automated testing helpful for security testing of web applications?

Ques. 7: What role do agile techniques can play in terms of web application security testing?

3.2 Conducting the review

3.2.1 Selection of primary studies

Security is an important aspect of quality. Due to increasing heterogeneity and complexity of the web, testing of web applications for security remains an elusive task. Security testing of web applications undermines various attacks like SQL injection, content injection, cookie manipulation etc. Also it highlights various other threats and vulnerabilities which may result in security breaches and may hinder the privacy of the application leading to the lack of trustworthiness of the web services.

3.2.2 Criteria for study selection

A criterion for the study selection process was to include all those papers which provide us with relevant information about the security testing of web applications. There are various issues and challenges related with secure web testing. Many tools have been investigated for enhancing the security of web applications. Threats and risks are often associated with web security testing.

3.2.3 Selection of primary studies

For the survey, papers were collected from multiple sources including IEEE, Springer, Elsevier, ACM, etc. Apart from this, various articles, publications etc were also included during analysis. Also it includes the study of various tools which are used for security testing of web applications. It excludes study of various frameworks and method which are used for performing web security testing.

4. ISSUES AND CHALLENGES

Security is one of the crucial aspects of quality of any software or any application. Security testing of web applications attempts to figure out various vulnerabilities, attacks, threats, viruses etc related to the respective application. Security testing should attempt to consider as many as potential attacks as possible. So we attempt to identify various issues and challenges related to the security testing of web application. They are as follows:

4.1 Issues related to security testing of web applications

i. *Authentication* [9]: this involves confirming the identity of an entity/person claiming that it is a trusted one.

ii. *Authorization* [9]: it is a process where a requester is allowed to perform an authorized action or to receive a service.

iii. *Cross site scripting* [1, 6, 10-11, 14-15, 18-19]: it is a critical attack where an attacker might inject any malicious code in to the web page and these malicious code/scripts can access confidential information, or may even rewrite the content of any html page etc.

iv. *SQLi* [6, 7, 14, 18-19]: it is an attack where any malicious script/code is inserted into an instance of SQL server/database for execution which eventually will try to fetch any database information.

v. *Cross site request forgery* [19, 23]: it is a vulnerability which includes exploitation of a website by transmitting unauthorized commands from a user that a website trusts. Thus it exploits the trust of a website which it has on its user browser.

vi. *Xml injection* [9]: it is an attack where an attacker tries to inject xml code with aim of modifying the xml structure thus violating the integrity of the application.

vii. *Malicious file execution* [19]: web applications are often vulnerable to malicious file execution and it usually occurs the code execution occurs from a non trusted source.

viii. *Cookie cloning* [29]: where an attacker after cloning the user/browser cookies tries to change the user files or data or may even harm the injected code.

ix. *Xpath injection* [6]: it occurs when ever a website uses the information provided by the user so as to construct an xml query for xml data.

x. *Content spoofing* [6]: is an attack where an attacker tries to masquerades another program or user by falsifying the content/data.

xi. *Cookie sniffing* [29]: is a session hijacking vulnerability with the aim of intercepting the unencrypted cookies from web applications.

xii. *Cookie manipulation* [5]: here an attacker tries to manipulate or change the content of the cookies and thus can cause any harm to the data or he may even change the data.

xiii. *Sidejacking* [29]: is a hacking vulnerability where an attacker tries to capture all the cookies and may even get access to the user mailboxes etc.

xiv. *Broken access control* [22]: exploits the fragility in the access control mechanism of the web applications in order to fetch relevant and sensitive information.

xv. *Missing or inadequate validation of input data* [1, 10]: due to some missing or inadequate validation of input data, attacker may provide data having the scripts etc which when injected into a web page may lead to the disclosure of the sensitive information.

xvi. *Information or sensitive data disclosure* [10, 23]: security breaches may lead to the disclosure of any confidential or sensitive data from any web application.

xvii. *Social vulnerability (hacking), session hijacking* [4, 5, 10, 29]: is a popular hijacking mechanism where an attacker gains unauthorized access to the information.

xviii. *Mis-configuration* [24]: in appropriate or inadequate configuration of the web application may even lead to the security breaches.

xix. *Absence of secure network infrastructure* [24]: absence of any intrusion detection or protection system or failover systems etc may even lead to violation of the security breaches.

xx. *Off the shelf components* [24, 28]: these components are purchased from third party vendors so there occurs a suspicion about their security aspect.

xxi. *Firewall intrusion detection system* [1, 24, 25]: a firewall builds a secured wall between the outside/external network and the internal network which is kept to be trusted.

xxii. *Path traversal* [6]: is vulnerability where malicious un-trusted input causes non desirable changes to the path.

xxiii. *Command injection* [6]: is the injection of any input value which is usually embedded into the command to be executed.

xxiv. *Parameter manipulation* [5]: it is similar to XSS where an invader inserts malicious code/script into the web application.

xxv. *LDAP injection* [6]: it is similar to SQL and Xpath injection where queries are being targeted to LDAP server.

xxvi. *Bad code or fault in implementation* [2]: improper coding or fault in the implementation of the web application may even lead to the violation of the security of the web application.

xxvii. *Clickjacking* [23]: it is an attack where a user’s click may be hijacked so that the user would be directed to some other link which may contain some malicious code.

xxviii. *Content injection* [1, 23]: it is vulnerability where an attacker loads some static content that may be some false content into the web page.

xxix. *File injection* [1]: it refers to the inclusion of any unintended file and is a typical vulnerability often found in web applications. Example: remote file inclusion.

4.2 Challenges faced by security testing of web applications

One of the concerns of security testing of web applications is the development of automated tools for testing the security of web applications [3]. Increase in the usage of Rich Internet Applications (RIAs) also poses a challenge for security testing of web application. This is due to the fact that the crawling techniques which are used for exploration of the web applications used for earlier web applications do not fulfill the requirements for RIAs [3]. RIAs being more users friendly and responsive due to the usage of AJAX technologies. Another challenge could be the usage of unintended invalid inputs which may result in security attacks [1]. And these security breaches may lead to extensive damage to the integrity of the data. While working the mutants, one should be sincere enough to incorporate them as injecting && (and) instead of || (or) or any such other modification may lead to fault injection which could result in a security vulnerability as vulnerabilities do not take semantics into consideration [1]. This may even pose a challenge to the security testing of any such web application. Usage of insecure cryptographic storage may even pose a challenge to the web application security testing [1]. Security testing of web applications may face repudiation attacks where any receiver is not able to prove that the data received came from a specific sender or from any other unintended source [1]. Also the web development languages which we use may lack in enforcing the security policy which may even violate the integrity and confidentiality of the web application [11]. This may even pose a security threat. At times it is also possible that an invader is able to launder more information than intended, in such a case again this may lead to the set back to the integrity of the data which could be another challenge for a security tester.

5. REVIEW RESULTS AND FUTURE TRENDS

5.1 Review Results

Ques. 1: **What are the vulnerabilities related to security web testing?**

Ans. 1: Various vulnerabilities related to the security testing of web applications are SQL injection, content injection, file injection, XML injection, LDAP injection, XPATH injection, cookie manipulation, cookie sniffing, cross site request forgery, cross site scripting, session hijacking, authentication, information disclosure, Clickjacking etc.

Ques. 2: **What are the challenges faced by security web testing?**

Ans. 2: Various challenges being faced by security web testing include the development of automated tools for web security testing, usage of RIAs web applications, usage of insecure cryptographic storage. Security tester should defend itself against variety of unspecified attacks like repudiation attacks etc. For a security tester, any trapdoor may become a potential damage to the application.

Ques. 3: **Does it identify the risk associated with the secure web testing?**

Ans. 3: It does helps in identifying the risk associated with the security testing of web applications. Risk may be associated with the design phase, development phase, deployment phase, maintenance phase and testing may be used to identify those risks indulged in the web application. It helps us to investigate about the fragility and weaknesses in the web application by exploiting against the vulnerabilities, threats associated with the web application. As we know, in SQL injection, an invader is able to alter the SQL queries and thus can gain unauthorized access to the backend. So the risk associated with it may be that the attacker is able to gain access to the data for which he is not authorized for.

Ques. 4: **What are the possible issues related with security aspect of web testing?**

Ans. 4: Broken or weak passwords, buffer overflows, hidden field manipulation, insecure use of cryptography, cookie sniffing, server mis-configurations, weak session management , sensitive data disclosure, parameter manipulation, social hacking, inadequate validation of input etc are other possible issue related to the security aspect of web testing.

Ques. 5: **Is automated testing helpful for security testing of web applications?**

Ans. 5: Development of automated tools had been always a concern for testing of web applications for security. It is harder to build automated tools for security testing of web applications than for testing of the functionality of the web application. The challenges faced by the automated tools for web security testing is that they have to keep up with the ever evolving and changing technologies (like RIAs) and adequately integrating into the existing development workflows.

Ques. 6: **What role do agile techniques can play in terms of web application security testing?**

Ans. 6: Agile methods like extreme programming and scrum etc are being used in variety of projects which assist them in delivering high quality applications in terms of security. Due to the enormous increase in the complexity of the web applications, there is a growing pervasive need for usage of agile techniques to build the secured web applications.

Ques. 7: **Does the outcomes relate to factors of importance to practitioners?**

Ans. 7: We believe that focusing on various issues and challenges related to the security testing of web applications will yield substantial significant dividends in identifying various risk, vulnerabilities, attacks, threats, viruses etc associated with the security testing of web based applications which can thus be avoided while building web application. Also it would be helpful in guiding a security tester to model the test application skillfully and designing the apt test strategy.

5.2 Current Trends and Future Direction

Increase in the security breaches has made security testing as an indispensable part of web application development life cycle. Security testing of web based applications helps to emulate and expose possible vulnerabilities and threats associated with the web application. It also checks whether the application fulfills all the requirements of security when exposed to any malicious input data. The technology is growing at a faster pace so testers have recognized the need for identifying the comprehensive testing capabilities to adapt themselves to the dynamic and heterogeneous nature of web domain. The paper discusses about various issues and challenges related to the current scenario of security testing of web based applications. It also articulates that testing is dependent on the implementation technologies so future testing techniques should keep track of all the issues while developing meticulous test design and test strategies for the same and also to adapt themselves to the dynamic pervasive nature of web. This finding remarks that there is an effective need to generate an efficient test environment for conducting security testing of web applications which may even arises new issues while testing.

6. CONCLUSIONS

In this paper, we have attempted to identify various issues and challenges faced by security testing of web based applications. A security tester thus should keep track of all the issues while conducting testing of web application for security. Also the information would be helpful for designing and modeling the effective test strategy and the test application. While performing security testing, a tester should also incorporate implementation related information and issues while testing which may be helpful in eradicating various vulnerabilities related to the security testing of web applications.

7. REFERENCES

[1] Security Testing of Web Applications: a Search Based Approach for Cross-Site Scripting Vulnerabilities, Andrea Avancini, Mariano Ceccato , 2011- 11th IEEE International Working Conference on Source Code Analysis and Manipulation.

[2] Special section on testing and security of Web systems Alessandro Marchetto. Published online: 14 October 2008 © Springer Verlag 2008

[3] Solving Some Modeling Challenges when Testing Rich Internet Applications for Security. Suryakant Choudhary1, Mustafa Emre Dincturk1, Gregor v. Bochmann1,3, Guy-Vincent Jourdan1,3 1EECS, University of Ottawa 3IBM Canada CAS Research. Iosif Viorel Onut, Paul Ionescu Research and Development, IBM. 2012 IEEE Fifth International Conference on Software Testing, Verification and Validation.

[4] Idea: Automatic Security Testing for Web Applications. Thanh-Binh Dao1 and Etsuya Shibayama2 1 Dept. of Mathematical and Computing Sciences, Tokyo Institute of Technology, 2-12-1 O-okayama Meguro Tokyo Japan 2 Information Technology Center, The University of Tokyo,2-11-16 Yayoi Bunkyo-ku Tokyo Japan F. Massacci, S.T. Redwine Jr., and N. Zannone (Eds.): ESSoS 2009, LNCS 5429, pp. 180–184, 2009. _c Springer-Verlag Berlin Heidelberg 2009.

[5] Automatic Test Approach of Web Application for Security (AutoInspect). Kyung Cheol Choi and Gun Ho Lee, Springer-Verlag Berlin Heidelberg 2006.

[6] SUPPORTING SECURITY TESTERS IN DISCOVERING INJECTION FLAWS. Sven T¨urpe, Andreas Poller, Jan Trukenm¨uller, J¨urgen Repp and Christian Bornmann, Fraunhofer-Institute for Secure Information Technology SIT, Rheinstrasse 75,64295 Darmstadt, Germany, 2008 IEEE,Testing: Academic & Industrial Conference - Practice and Research Techniques.

[7] A Database Security Testing Scheme of Web Application, Yang Haixia ,Business College of Shanxi University, Nan Zhihong, Scholl of Information Management,Shanxi University of Finance & Economics,china. Proceedings of 2009 4th International Conference on Computer Science & Education.

[8] State of the Art: Automated Black-Box Web Application Vulnerability Testing. Jason Bau, Elie Bursztein, Divij Gupta, John Mitchell, Stanford University 2010 IEEE Symposium on Security and Privacy.

[9] An Approach Dedicated for Web Service Security Testing, S´ebastien Salva, Patrice Laurencot and Issam Rabhi. 2010 Fifth International Conference on Software Engineering Advances.

[10] Security Testing of Web Applications: A Research Plan by Andrea Avancini,Fondazione Bruno Kessler, 2012 IEEE,ICSE 2012, Zurich, Switzerland , Doctoral Symposium.

[11] Semi-Automatic Security Testing of Web Applications from a Secure Model by Matthias Buchler,Johan Oudinet,Alexander Pretschner, Karlsruhe Institute of Technology, 2012 IEEE Sixth International Conference on Software Security and Reliability.

[12] Testing web applications. Giuseppe Antonio Di Lucca, Anna Rita Fasolino, Francesco Faralli, Ugo De Carlini. Italy. Proceedings of the International Conference on Software MAintenance 2002 IEEE.

[13] Solving some modeling challenges when testing rich internet applications for security Suryakant Choudhary, Mustafa Emre Dincturk, Gregor v. Bochmann, Guy Vincent Jourdan, Iosif Viorel Onut, Paul Ionescu. 2012 IEEE Fifth International Conference on Software Testing, Verification and Validation.

[14] Mapping software faults with web security vulnerabilities. Jose Fonseca and Marco Vieira. International conference on Dependable Systems & Networks : Anchorage, Alaska,june 2008 IEEE.

[15] Testing of Web Applications: A Research Plan. Andrea Avancini Fondazione Bruno Kessler, Trento, Italy. 978-1-4673-1067-3/12/$31.00c 2012 IEEE.

[16] Testing Security Policies for Web Applications. Wissam Mallouli, Gerardo Morales and Ana Cavalli GET/INT, 9 rue Charles Fourier, 91011 Evry Cedex, France. 2008 IEEE International Conference on Software Testing Verification and Validation Workshop (ICSTW'08) 978-0-7695-3388-9/08 $25.00 © 2008 IEEE.

[17] A Threat Model Driven Approach for Security Testing. Linzhang Wang, Department of Computer Science, Nanjing University, Eric Wong, Department of Computer Science, University of Texas at Dallas, Dianxiang Xu, Department of Computer Science, North Dakota State University. Third International Workshop on Software Engineering for Secure Systems (SESS'07). 2007 IEEE.

[18] Grammar Based Oracle for Security Testing of Web Applications by Andrea Avancini and Mariano Ceccato, Fondazione Bruno Kessler, Trento, Italy. 2012 IEEE,AST 2012, Zurich, Switzerland.

[19] D-WAV: A Web Application Vulnerabilities Detection Tool Using Characteristics of Web Forms. Lijiu Zhang, Qing Gu, Shushen Peng, Xiang Chen, Haigang Zhao, Daoxu Chen State Key Laboratory of Novel Software Technology, Department of Computer Science and Technology, Nanjing University. 2010 Fifth International Conference on Software Engineering Advances.

[20] Grammar Based Oracle for Security Testing of Web Applications Andrea Avancini and Mariano Ceccato, Fondazione Bruno Kessler Trento, Italy. 2012 IEEE.

[21] The Security Requirements Behavior Model for Trustworthy Software Kassem Saleh1 and Maryam Habil2. 1Kuwait University, Dept. of Information Science, 2American University of Sharjah, Dept. of Computer Science. 0-7695-3082-6/08 $25.00 © 2008 IEEE. 2008 International MCETECH conference on e-technologies.

[22] Challenges for Security Typed Web Scripting Languages Design. Doaa Hassan,National Telecomm.Institute, Sherif El- Kassas,American University in Cairo, Ibrahim Ziedan,Faculty of Engineering,Zagazig University. 2008 IEEE,The Fourth International Conference on Information Assurance and Security.

[23] Enhancing web page security with security style sheets Terri Oda and Anil Somayaji (2011) IEEE.

[24] Assessing and Comparing Security of Web Servers. Naaliel Mendes, Afonso Araújo Neto, João Durães, Marco Vieira, and Henrique Madeira CISUC, University of Coimbra. 2008 14th IEEE Pacific Rim International Symposium on Dependable Computing.

[25] Firewall Security: Policies, Testing and Performance Evaluation. Michael R. Lyu and Lorrien K. Y. Lau. Department of computer science and engineering. The Chinese University of Hong kong, Shatin, HK. 2000 IEEE.

[26] Web application security assessment tools- Mark Curphey and Rudolph Araujo 2006 IEEE security & privacy.

[27] Security Testing in Software Engineering Courses. Andy Ju An Wang. Department of Software Engineering. School of Computing and Software Engineering. Southern Polytechnic State University. 34th ASEE/IEEE Frontiers in Eductaion Conference. 2004 IEEE.

[28] Raising the bar on software testing - Alden Dima, John Wack, and Shukri Wakid (1999)IEEE.

[29] Top 10 Free Web-Mail Security Test Using Session Hijacking Preecha Noiumkar,Thawatchai Chomsiri,Mahasarakham University,Maha sarakham, Thailand. Third 2008 International Conference on Convergence and Hybrid Information Technology. Development of Security Engineering Curricula at US

Universities.Mary Lynn Garcia, Sandia National Laboratories.1998 IEEE.

[30] Automated Security Test Generation with Formal Threat Models Dianxiang Xu, Senior Member, IEEE, Manghui Tu, Michael Sanford, Lijo Thomas, Daniel Woodraska, and Weifeng Xu, Senior Member, IEEE. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 4, JULY/AUGUST 2012.

[31] Testing Web-based applications: The state of the art and future trends. Giuseppe A. Di Lucca a, Anna Rita Fasolino. 0950-5849/$ - see front matter © 2006 Elsevier B.V.

[32] Structural Testing of Web Applications. Chien-Hung Liu David C. Kung Pei Hsia, Department of Computer Science and Engineering. Chih-Tung Hsu, Sun Microsystems, Inc. 0-7695-0807-3/0$01 0.00 0 2000 IEEE.

[33] Automated Web Application Testing Using Search Based Software Engineering. Nadia Alshahwan and Mark Harman CREST Centre, University College London. 978-1-4577-1639-3/11/$26.00 c 2011 IEEE.

[34] Agile Security Testing of Web-Based Systems via *HTTPUnit.* A. Tappenden, P. Beatty, J. Miller, *University of Alberta.* A. Geras, M. Smith, *University of Calgary.* Proceedings of the Agile Development Conference (ADC'05) 0-7695-2487-7/05 $20.00 © 2005 IEEE.

[35] Security Objectives within a Security Testing Case Study. Kaarina Karppinen, Reijo Savola, Mikko Rapeli, Esa Tikkala. Second International Conference on Availability, Reliability and Security (ARES'07). 0-7695-2775-2/07 $20.00 © 2007 IEEE.

[36] Security Testing: Turning Practice into Theory. Sven Türpe, *Fraunhofer Institute for Secure Information Technology SIT.* 2008 IEEE International Conference on Software Testing Verification and Validation Workshop (ICSTW'08) 978-0-7695-3388-9/08 $25.00 © 2008 IEEE.

[37] Automatic Testing of Program Security Vulnerabilities, Hossain Shahriar and Mohammad Zulkernine, School of Computing. 2009 33rd Annual IEEE International Computer Software and Applications Conference.

[38] A new solution for complex security testing, DongHu, Department ofTeaching Affairs. 2009 International Conference on Test and Measurement.

[39] Increasing Trustworthiness Through Security Testing Support. Jose Romero-Mariona; Hadar Ziv; Debra Richardson, University of California, Irvine; Donald Bren School of Information and Computer Sciences. IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust. 978-0-7695-4211-9/10 $26.00 © 2010 IEEE.

[40] Risk–Based Security Testing in Cloud Computing Environments, Philipp Zech, Institute of Computer Science ,University of Innsbruck, Innsbruck, Austria. 2011 Fourth IEEE International Conference on Software Testing, Verification and Validation.

[41] Model-checking Driven Security Testing of Web-based Applications. Alessandro Armando, Roberto Carbone ,DIST, University of Genova, Genova, Italy ; Luca Compagna,, Keqin Li, Giancarlo Pellegrino, SAP Research, Mougins, France. 978-0-7695-4050-4/10 $26.00 © 2010 IEEE.

[42] Experiences in Security Testing for Web-based Applications. Chengying Mao, School of Software,, Jiangxi University of Finance and Economics, 330013 Nanchang, P. R. China. ICIS 2009, November 24-26, 2009 Seoul, Korea. Copyright © 2009 ACM 978-1-60558-710-3/09/11... $10.00".

[43] Automated Security Testing of Web. Widget Interactions. Cor-Paul Bezemer, Ali Mesbah, and Arie van Deursen, Delft Univ. of Technology, The Netherlands. ESEC-FSE'09, August 23–28, 2009, Amsterdam, The Netherlands. Copyright 2009 ACM 978-1-60558-001-2/09/08 ...$5.00.

[44] Web Security Testing Approaches: Comparison Framework. Fakhredin T. Alssir, Moataz Ahmed, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia. Springer-Verlag Berlin Heidelberg 2012.

[45] Coverage Criteria for Automated Security Testing of Web Applications. Thanh Binh Dao, Dept of mathematical and computing sciences ,Tokyo ins. Of tech., Japan and Etsuya Shibayama, Information Technology Centre, the university of Tokyo, Japan. Springer-Verlag Berlin Heidelberg 2010.

[46] Web Security : Research Challenges and Open Issues. V. Geetha and Pranesh V. Kallapur, Dept of information technology, NITK, Karnataka, India. Springer-Verlag Berlin Heidelberg 2010.