https://doi.org/10.48009/1_iis_2010_142-153

WEB APPLICATION SECURITY TESTING: AN INDUSTRY PERSPECTIVE ON HOW ITS EDUCATION IS PERCEIVED

John J. Scarpino, Robert Morris University, scarpino@rmu.edu

ABSTRACT

This paper exposes the growing importance of Web Application Security Testing (WAST) in industry and why adequate training on such systems must be included in Information Technology (IT) and Information Systems (IS) curricula at higher education institutions. Hardly any academic research studies have approached whether or not the competence of industry professionals in the field of Web software security testing is affected by the type of education they received while at college or university. Therefore, this paper will provide meaningful data that may be used by higher education institutions in the United States to further develop their IT programs.

Since many higher education institutions do not offer training on Web application security as a part of their IT programs, it is important to understand the expectations of the industry from those who are most familiar with it. The study will give insight to the Web application security-related knowledge of 18 Senior Software Quality Analysts. Nine of the subjects work at a Fortune 500 Financial Institution and another nine participate in an open collaborative software quality testing Web site called "UTest.com." Research will reveal the method of training through which they obtained their knowledge and if they believe that colleges and universities are well-equipped to provide Web application and security training. This study posits that software security testing is a discipline that should be included in all college and university IT curricula. It will hopefully serve as a blueprint for future software testing, software security testing and Web application security testing courses at institutions of higher learning across the country.

Keywords: Software Test Automation (STA), Application Security Testing (AST), Software Security Testing (SST), Web Application Security Testing (WAST), Software Security Testing Tools (SSTT).

INTRODUCTION

There is a pressing need for security software testing (SST) to be integrated into the curricula at colleges and universities in the United States. As the World Wide Web continues to evolve and become more complicated, so do the threats to all levels of Web application security. Higher education institutions must stay abreast of such trends and accommodate what will soon be an increased demand for a workforce that is knowledgeable in Web and software security. A research report from Jobfox, entitled "Top 20 Most Recession-Proof Professions," stated that *Testing / Quality Assurance* was the 12th most recession-proof position in 2008.[1] And the market for software testing services is growing. By the year 2013, it is estimated to reach a potential $56 billion, with an average annual compound growth rate (CAGR) of 9.5%.[2] The outlook for the future of security software testing is promising. Danny Allan, Director of IBM Watchfire's Web site Application Security Testing (WAST) tool, reported that 90% of the company's security budget was being spent on network security, while only 10% was allocated toward Web application security. Nevertheless, 75% of all attacks on the company were directed toward Web applications.[3] The need for well-educated Web security testers will continue to grow and remain one of the leading IT professions, despite the recent dip in the U.S. economy – but WAST should not be confused with "Secure Programming." Secure Programming teachings have been a part of higher education curricula as a means to ensure quality program development during the software development lifecycle. Indeed, there seems to be no set precedent for conducting a training course on WAST.

Software security testing ensures that software is protected from the threat of attack either by manual testing or through the use of modern software security testing tools (SSTT). Basic network security practices try to either prevent unauthorized access to a network resource or intercept content of a network message before a malicious system has the chance to do any

damage.[4] Still, the Internet's easy accessibility has given rise to a whole host of new Web security threats. Firewalls and intrusion-detection systems do not protect Web applications[5] from Cross-Site Scripting (XSS) and SQL Injection (SQLI) – the two systems that most frequently attack Web applications[6] – and Buffer Overflow. Closing access to an HTTP port is of course not a viable option because Web applications must remain accessible to the Internet. Furthermore, encrypting the contents of a network message (e.g., SSL) provides no protection from a hacker who overrides a Web account by XSS, or steals a password through another method called Session Hijacking, or forces a Web application to disclose sensitive information using SQLI.[7]

Cross-Site Scripting and Buffer Overflows not only attack Web applications but also affect the server itself.[8] [9] [10] [11] The former infiltrates a targeted Web server with malicious code and redirects users to another server laden with virus-tainted JavaScript or VBScript Code.[12] [13] The latter often uses HTML pages, forms and tags to carry out application injection attacks;[14] the introduction of SQL query statements translates data into HTML, thereby making a variety of server-side programming languages (e.g., Java, ASP, dot-Net) indecipherable.[13] Another problem is Session Hijacking, which bypasses authentication by forging or stealing session identification or session cookies (e.g., session fixation or insufficient session expiration).[15] [6] Conversely, Path Transversal attacks insert code into the response URL (e.g., "..\") in an attempt to access directories outside the Web server's root or to command the application to behave sporadically.[16]

The inadequacy of current Web application security continues to threaten the privacy of corporate networks and personal computers, yet many higher education institutions do not offer training on Web application security as a part of their IT degree programs. The research outlined in this paper gives insight to the Web application security-related knowledge of 18 senior-level Software Quality Analysts in order to develop best practices through which IT education at U.S. colleges and universities may be managed.

It is important to understand the needs and expectations of the IT industry from those who are most familiar with it. This paper examines the following three questions: How much or little do software quality testers in industry value WAST? Where do the software quality testers who work in industry accomplish their WAST training? From where / what institution(s) do professional software quality testers think WAST training should be obtained? Nine of the 18 Software Quality Analysts who are profiled in this study work at a Fortune 500 Financial Institution that has several dozen departments, but with few employees who are solely dedicated to software testing. Many of the individuals from this company have a "Business Analyst" or "Developer" title, and also hold software testing responsibilities. An additional nine IT professionals participate in an open-collaborative software quality testing Web site called "UTest.com," which is quite the opposite of the Financial Institution. UTest.com employs expert software testers who conduct remote testing on various software applications for companies such as Google and Apple. These individuals receive compensation based on the severity of defect(s) they find.

This study posits that, due to the increasingly detrimental effect that poorly-tested software and Web applications have on the IT industry, software and Web application security testing is a discipline that should be included in all college, university and technical school IT curricula. The research in this paper will provide significant data on how the role of higher education is perceived by some of the industry's foremost expert Web application software testing professionals. It will reveal the method of training through which they obtained their knowledge and if they believe that colleges and universities are well-equipped to provide Web application and security training. Moreover, it is also hoped that this study imparts urgency upon the fact that future IT curricula must be able to meet the inevitable demand for the next generation Web application security testing workforce, and serves as a framework for the development of such courses and degrees.

ESCALATING WEB APPLICATION SECURITY THREATS

The Sarbanes-Oxley Act (SOX) of 2002,[17] the Health Insurance and Portability Act (HIPPA) of 1996[18] and the Financial Services Modernization Act of 1999 [19] [20] [21] all mandate conformity across a wide range of security requirements

designed to protect user identity and access to personal information. However, even this strict governmental regulation has not been enough to stem the growth and severity of threats to Web application security.[22] According to the 2002 CSI/FBI Computer Crime and Security Survey,[23] viruses and laptop theft were among some of the most frequently reported crimes, and there were no FBI Security Incident Categories in this survey that directly reflected Web application security. It wasn't until two years later in 2004 that the CSI/FBI Computer Crime and Security Survey started measuring the effect of Web application security attacks and reported an alarming increase in the crime. Further evidence supporting the CSI/FBI's claim came in 2005 with a survey conducted by the Federal Trade Commission which reported 8.3 million victims of Identity Theft that year.[22]

Web application security threats continued to skyrocket all the way through the end of the first decade in the 21st Century. In fact, by 2008 the CSI/FBI study reported that 11% of 517 respondents experienced a "successful" Web application security attack, with many claiming that the actual design of the applications may have been to blame for allowing the threat to infiltrate their computer.[23] IBM Internet Security Systems found almost 50% more infected Web pages in the last three months of 2008 than it did in all of 2007. A headline news article in the March, 17, 2009, issue of USA Today indicated that SQL injection attacks on Web sites had reached an estimated 450,000 per day.[24]

WEB APPLICATION SECURITY TRAINING

The economic impact of defective software is significant. In the U.S, it is estimated that software testing accounts for a little less than 1% of the national gross domestic product. With such a large part of the U.S. economy depending upon the software testing industry should consumers be convinced that domestically-produced software and computers are vigilantly developed and protected from future security threats?[25] Along the same lines, should educators at higher educational institutions be confident that they are educating students on how to detect security issues within software?

IT industry trends present an enormous opportunity for U.S. colleges, universities and technical schools to create cutting-edge programs that increase enrollment and mold a well-educated IT workforce for the future. In fact, many software quality assurance and security problems could be avoided with the proper planning and right kind of education. Software is most likely to fail when quality assurance training is given only to the quality assurance staff and not members of the project management team, if it is not consistently updated throughout the project development lifecycle, and if the team members are not receptive to the style or method of training given.[26] Web application and software security testing skills can be learned in a formal classroom setting or through an internship, or even by shadowing an IT professional, or by unconventional methods such as self-help books and studying in a group setting with others who are interested in learning the same information.[26] Schools currently do little to expose their students to much of anything outside of traditional engineering and computer science, yet it is imperative that higher education meets industry demand by promoting software security. These institutions should offer courses that not only focus on software testing, but also security engineering, design principles and guidelines, implementation risks, design flaws and analysis techniques.[27] The curricula must drive the most promising students to concentrate on a specific testing field in which they can excel.

Although the need for Web and software security testers has gone widely unnoticed at U.S. institutions for higher learning, national and international IT organizations are stepping up to address it head-on. In 2000, the U.S. National Institute of Standards and Technology (NIST) announced an accreditation of four National Information Assurance Partnerships (NIAP) for IT security testing, in alliance with the Common Criteria Testing Laboratories (CCTL). This accreditation allows this body to perform assessments of commercial off-the-shelf (COTS) products aligned with the Common Criteria for Information Technology Security Evaluation (ISO/IEC15408). The NIST accreditation is now acknowledged by 12 other countries.[28] This was followed in 2004 by the establishment of a single, universal standard for software testing education by the British Computer Society of Information Systems Examinations Board (ISEB) and the International Software Testing Qualification Board (ISTQB).[29]

There is clearly a gap between the perception of the IT industry at U.S. colleges, universities and technical schools, and the reality of what that industry truly needs to thrive.

RESEARCH APPROACH

A quantitative, 12-question survey was distributed to Software Quality Analyst professionals who work at a Fortune 500 Financial Institution and software testers at UTest.com. Seven of these questions were Yes / No answers, three were multiple choice, three questions required the respondent to rank their choices by matter of importance, and one question required a personalized answer from the respondent.

The survey was first distributed to the Fortune 500 Financial Institution in the beginning of June 2009. After 30 days of data collection, the survey was "closed." Only nine of the 18 Software Quality Analysts from the Fortune 500 Financial Institution returned the survey with their responses, thereby defining the sample size also needed from UTest.com. The survey was sent to UTest.com via SurveyMonkey.com in July 2009 and "closed" as soon as the nine-respondent threshold was reached, bringing the total number of respondents to 18.

A quantitative analysis was then performed by separately compiling the data collected from the nine respondents of each organization and then comparing the sum of data for each organization. The analysis illustrated how many respondents answered each question; how many respondents skipped each question; the total number of responses for each question; the response percentage rate; and the respondent's answer to each question. For the questions that required the respondent to rank their choices, the analysis revealed the total number of respondents in each organization that ranked each item and the average rating for each item.

Survey Questions and Design

Question 1

Question: Please fill in the following information: Occupation / Position Held / Department.

Answer: Open-ended

Question 2

Question: How many years of software quality assurance experience do you have?

Answer Choices: None / 1 – 5 years / 6 – 10 years /10+ years

Question 3

Question: Do you think that Web application security testing is important (i.e., testing for security threats, SQL injection, cross-site scripting etc.)?

Answer Choices: Yes / No

Question 4

Question: Do you conduct Web application security testing as a part of your job?

Answer Choices: Yes / No

Question 5

Question: Have you ever taken a training course on Web application security testing that did not use testing tools?

Answer Choices: Yes / No

Question 5.1

Question: If you answered "yes" to Question 5, where did you take this course?

Answer Choices: College Instruction / Private Training / Company Training / Web Site

Question 6

Question: Have you ever taken a training course on Web application security testing that did use testing tools?

Answer Choices: Yes / No

Question 6.1

Question: If you answered "yes" to Question 6, where did you take this course?

Answer Choices: College Instruction / Private Training / Company training / Web Site

Question 7

Question: Do you think training on Web application security testing should not be based on the use of testing tools?

Answer Choices: Yes / No.

Question: 8

Question: Please rank the following training venues based on where you think Web application security testing should first be introduced. (1 = your first choice, 4 = your last choice)

Answer Choices: University or College / Private Training / Company Training / Web Site

Question 9

Question: Do you believe that educational opportunities are readily available for someone to learn Web application security testing without the use of testing tools?

Answer Choices: Yes / No

Question 10

Question: Please rank the following training venues based on where you believe educational opportunities are most readily available for someone to learn Web application security testing, without the use of testing tools (1 = your first choice, 4 = your last choice)

Answer Choices: University or College / Private Training / Company Training / Web Site

Question 11

Question: Do you believe that educational opportunities are readily available for someone to learn Web application security testing with the use of testing tools?

Answer Choices: Yes / No

Question 12

Question: Please rank the following training venues based on where you believe educational opportunities are most readily available for someone to learn Web application security testing with the use of tools (1 = your first choice, 4 = your last choice)

Answer Choices: University or College / Private Training / Company Training / Web Site

RESULTS

Question 1: Please fill in the following information: Occupation / Position Held / Department.

Answer	**Fortune 500 Financial Institution**	**UTest.com**
Software Tester	4	9
Business Analyst	4	0
Software Engineer	1	0
TOTAL	**9**	**9**

Question 2: How many years of software quality assurance experience do you have?

Fortune 500 Financial Institution			UTest.com		
Answer Choices	**Response % Rate**	**No. of Responses**	**Answer Choices**	**Response % Rate**	**No. of Responses**
None	0.0%	0	None	0.0%	0
1 – 5 years	11.1%	1	1 – 5 years	77.8%	7
6 – 10 years	33.3%	3	6 – 10 years	11.1%	1
10+ years	55.6%	5	10+ years	11.1%	1
answered question		**9**	***answered question***		**9**
skipped question		**0**	***skipped question***		**0**

Question 3: Do you think that Web application security testing is important (i.e., testing for security threats, SQL injection, cross-site scripting etc.)?

Fortune 500 Financial Institution			UTest.com		
Answer Choices	**Response % Rate**	**No. of Responses**	**Answer Choices**	**Response % Rate**	**No. of Responses**
Yes	100.0%	9	Yes	100.0%	9
No	0.0%	0	No	0.0%	0
answered question		**9**	***answered question***		**9**
skipped question		**0**	***skipped question***		**0**

Question 4: Do you conduct Web application security testing as a part of your job?

Fortune 500 Financial Institution			UTest.com		
Answer Options	**Response % Rate**	**No. of Responses**	**Answer Options**	**Response % Rate**	**No. of Responses**
Yes	22.2%	2	Yes	77.8%	7
No	77.8%	7	No	22.2%	2
answered question		**9**	***answered question***		**9**
skipped question		**0**	***skipped question***		**0**

Question 5: Have you ever taken a training course on Web application security testing that did not use testing tools?

Fortune 500 Financial Institution			UTest.com		
Answer Choices	**Response % Rate**	**No. of Responses**	**Answer Choices**	**Response % Rate**	**No. of Responses**
Yes	11.1%	1	Yes	11.1%	1
No	88.9%	8	No	88.9%	8
answered question		**9**	***answered question***		**9**
skipped question		**0**	***skipped question***		**0**

Question 5.1: If you answered "yes" to Question 5, where did you take this course?

Answer Choices	Response % Rate	No. of Responses	Answer Choices	Response % Rate	No. of Responses
College Instruction	0.0%	0	College Instruction	0.0%	0
Private training	0.0%	0	Private training	0.0%	0
Company training	100.0%	1	Company training	0.0%	0
The Web	0.0%	0	The Web	100.0%	1
answered question		**1**	***answered question***		**1**
skipped question		**8**	***skipped question***		**8**
Fortune 500 Financial Institution			**UTest.com**		

Question 6: Have you ever taken a training course on Web application security testing that did use testing tools?

Answer Choices	Response % Rate	No. of Reponses	Answer Choices	Response % Rate	No. of Reponses
Yes	22.2%	2	Yes	22.2%	2
No	77.8%	7	No	77.8%	7
answered question		**9**	***answered question***		**9**
skipped question		**0**	***skipped question***		**0**
Fortune 500 Financial Institution			**UTest.com**		

Question 6.1: If you answered "yes" to Question 6, where did you take this course?

Answer Options	Response Percent	Response Count	Answer Options	Response Percent	Response Count
College Instruction	0.0%	0	College Instruction	0.0%	0
Private Training	50.0%	1	Private Training	50.0%	1
Company Training	0.0%	0	Company Training	50.0%	1
The Web	50.0%	1	The Web	0.0%	0
answered question		**2**	***answered question***		**2**
skipped question		**7**	***skipped question***		**7**
Fortune 500 Financial Institution			**UTest.com**		

Question 7: Do you think training on Web application security testing should not be based on the use of testing tools?

Answer Choices	Response % Rate	No. of Responses	Answer Choices	Response % Rate	No. of Responses
Yes	0.0%	0	Yes	22.2%	2
No	100.0%	9	No	77.8%	7
answered question		**9**	***answered question***		**9**
skipped question		**0**	***skipped question***		**0**
Fortune 500 Financial Institution			**UTest.com**		

Question 8: Please rank the following training venues based on where you think Web application security testing should first be introduced. (1 = your first choice, 4 = your last choice)

Fortune 500 Financial Institution **UTest.com**

Answer Choices	1	2	3	4	Average Rating	No. of Responses	Answer Choices	1	2	3	4	Average Rating	No. of Responses
University or College	4	2	1	2	**2.11**	9	University or College	4	0	1	2	**2.14**	7
Private Training	0	2	2	4	**3.25**	8	Private Training	2	1	2	2	**2.57**	7
Company Training	1	5	2	1	**2.33**	9	Company Training	1	4	2	0	**2.14**	7
The Web	4	0	3	1	**2.13**	8	The Web	0	2	2	3	**3.14**	7
answered question						**9**	***answered question***						**7**
skipped question						**0**	***skipped question***						**2**

Question 9: Do you believe that educational opportunities are readily available for someone to learn Web application security testing without the use of testing tools?

Fortune 500 Financial Institution			UTest.com		
Answer Options	**Response Percent**	**Response Count**	**Answer Options**	**Response Percent**	**Response Count**
Yes	22.2%	2	Yes	50.0%	4
No	77.8%	7	No	50.0%	4
answered question		**9**	***answered question***		**8**
skipped question		**0**	***skipped question***		**1**

Question 10: Please rank the following training venues based on where you believe educational opportunities are most readily available for someone to learn Web application security testing, without the use of testing tools (1 = your first choice, 4 = your last choice)

Fortune 500 Financial Institution							UTest.com						
Answer Choices	**1**	**2**	**3**	**4**	**Average Rating**	**No. of Responses**	**Answer Choices**	**1**	**2**	**3**	**4**	**Average Rating**	**No. of Responses**
University or College	1	0	0	1	**2.50**	2	University or College	1	1	0	2	**2.75**	4
Private training	0	1	0	1	**3.00**	2	Private training	2	1	1	0	**1.75**	4
Company training	1	1	0	0	**1.50**	2	Company training	0	2	1	1	**2.75**	4
The Web	0	0	2	0	**3.00**	2	The Web	1	0	2	1	**2.75**	4
answered question						**2**	***answered question***						**4**
skipped question						**7**	***skipped question***						**5**

Question 11: Do you believe that educational opportunities are readily available for someone to learn Web application security testing with the use of testing tools?

Fortune 500 Financial Institution			UTest.com		
Answer Options	**Response Percent**	**Response Count**	**Answer Options**	**Response Percent**	**Response Count**
Yes	55.6%	5	Yes	42.9%	3
No	44.4%	4	No	57.1%	4
answered question		**9**	***answered question***		**7**
skipped question		**0**	***skipped question***		**2**

Question 12: Please rank the following training venues based on where you believe educational opportunities are most readily available for someone to learn Web application security testing with the use of tools (1 = your first choice, 4 = your last choice)

Fortune 500 Financial Institution

Answer Choices	1	2	3	4	Average Rating	No. of Responses
University or College	1	2	0	2	**2.60**	5
Private Training Company	2	0	1	2	**2.60**	5
Training Web Site	2	1	2	0	**2.00**	5
	0	2	2	1	**2.80**	5
answered question						**5**
skipped question						**4**

UTest.com

Answer Choices	1	2	3	4	Average Rating	No. of Responses
University or College	2	0	1	0	**1.67**	3
Private Training Company	0	2	1	0	**2.33**	3
Training Web Site	0	1	1	1	**3.00**	3
	1	0	0	2	**3.00**	3
answered question						**3**
skipped question						**6**

CONCLUSION

All 18 survey respondents believe that Web application security testing is important, even though five out of the nine individuals who work at the Fortune 500 Financial Institution did not hold a "Software Tester" title. Nonetheless, a total of only six industry professionals surveyed indicated that they participated in any kind of Web application or software security testing training at some point in their careers. Furthermore, none of these individuals received their training at a college or university setting. This information reinforces the theory that there is considerable opportunity for higher education institutions to increase their course offering and include classes on Web application security and software testing, thereby making their institution more attractive for prospective students and IT professionals who want to continue their education.

Two respondents (one from each organization) participated in a class on Web application security testing that *did not* use testing tools as a part of the training. The Software Quality Analyst from the Fortune 500 Financial Institution noted that he or she took this particular training course at the company, whereas the professional software tester from UTest.com received his or her training via the Web. Only four respondents (two from each organization) participated in training on Web application security testing that *did* use security testing tools. One of the Software Quality Analysts from the Fortune 500 Financial Institution and one of the professionals at UTest.com received private training. The other Software Quality Analyst from the Fortune 500 Financial Institution received his or training via the Web and the second UTest.com professional went through company training.

When asked if Web application security training should not include the use of testing tools, all nine of the Fortune 500 Financial Institution Software Quality Analysts answered "no," and seven respondents from UTest.com felt the same way. The overwhelming response of 16 individuals in favor of using testing tools during training could mean that IT professionals who have a practical, working knowledge of the tools used in industry are deemed more valuable than someone who doesn't have such experience.

Eight total respondents named "University or College" as their first choice of venue where Web application security testing should be introduced. With an average rating of 2.12 between responses from both the Fortune 500 Financial Institution and UTest.com, "University or College" ranked the highest overall. This information further emphasizes the wide gap between what is currently offered at higher education institutions and the reality of what is needed by the IT industry. An additional four respondents from the Fortune 500 Financial Institution indicated that their first choice for a training venue was "The Web." Ironically, none of the professionals at UTest.com mentioned "The Web" as an option for security testing, which may show that even though they work in an online environment, they might not feel that the Web offers the best kind of training.

The perception among IT industry professionals is that higher education institutions harbor the most versatility in the means to provide Web application security testing training, both with and without the use of testing tools. This is supported by their responses to Question 10 and Question 12. For venues that offer training on testing tools (Question 10), "University or College" ranked second (avg. 2.5) only to "Company Training" (avg. 1.5) by the Fortune 500 executives and "Private Training" (avg. 1.75) by the UTest.com software testers. The results of Question 12 show that "University or College" ranked first (avg. 1.65) among UTest.com software testers and second (avg. 2.6) by the Fortune 500 professionals, for venues that do not offer training on testing tools.

The results of this study illustrate that education on Web application security testing is valued by professionals in the IT industry, but there are few venues through which such education may be obtained. The differences among particular company and/or requirements may also dictate a different style of instruction. It may be up to the software professional to find the best place to receive Web application security training based on his or her unique situation. Software quality assurance testing, Web application and software security testing, and software performance testing are all separate practices that require professional, hands-on expertise to execute them properly. Besides specialized software testers like Web application software security testers, software business analysts and software change management positions are also in high demand. These positions often work with software testing, as shown in the Fortune 500 executives' answers to Question 1.

From an industry perspective, colleges and universities are thought of as the best overall venue to obtain Web application security testing, yet higher education institutions lack the resources necessary to meet industry demand. As it stands, simply using classic textbook instruction on how to find and report software bugs alone should not be the standard for software testing classes. Nor should programming development classes be taught merely how to program software without also educating students on how to test the security of those same software applications. Instructors who have actually worked in the software security testing field are ideal candidates to implement educational change on such a large scale. They are well-equipped with the information, tools and instructional materials needed to meet the industry demand that higher education institutions currently overlook.

REFERENCES

[1] Jobfox. (2008). *Jobfox Top 20 Most Recession-Proof Professions*. Retrieved January 1, 2010 from http://www.jobfox.com/Site/Employer/pdf/TopJobsJuly08.pdf

[2] Dinham, P. (2009, March 11). Global growth slowdown in software & systems testing services. *ITwire*. Retrieved January 10, 2010, from Web site: http://www.itwire.com/content/view/23757/598/

[3] Yeo, V. (2006, November 27). Hackers ride on Web app vulnerabilities. *ZDNet Asia*. Retrieved January 1, 2010, from http://www.zdnetasia.com/news/security/0,39044215,61969925,00.htm

[4] Laverty, J., & Scarpino, J. (2009). Web Application Security Instructional Paradigms and the IS Curriculum. *The International Association for Computer Information Systems*, VOL X, No. 1 pg. 87 – 94.

[5] MacDonald, N., & Weinschenk, J. (n.d.) Securing Networks and Desktops is Not Enough. [Video posted on Web site *Cenzic Software*. Retrieved January 1, 2010, from http://www.cenzic.com/resources/reg-required/videos/Gartner-on-Web-Application-Security/

[6] WASC Threat Classification Taxonomy Graphic. (2005). *Web Application Security Consortium.* Retrieved January 1, 2010, from http://cwe.mitre.org/documents/sources/WASCThreatClassificationTaxonomyGraphic.pdf

[7] Microsoft TechNet. (2000, February 2). Cross-*Site Scripting Security Exposure Executive Summary*.
Retrieved January 1, 2010, from http://technet.microsoft.com/en-us/library/cc750326.aspx

[8] Soler, M. (2007, January 2). Apache 1.3.37 htpasswd buffer overflow vulnerability. Message posted to
http://seclists.org/fulldisclosure/2007/Jan/0044.html

[9] Apache HTTP Server Project. (2006, July 27). Fixed in Apache httpd 1.3.37. Message posted to
://httpd.apache.org/security/vulnerabilities_13.html

[10] eEye Digital Security. (2001, June 18). *Microsoft Internet Information Services Remote Buffer Overflow*
(SYSTEM Level Access). Retrieved January 1, 2010, from http://research.eeye.com/html/advisories
/published/AD20010618.html

[11] CERT® Advisory CA-2003-09 Buffer Overflow in Core Microsoft Windows DLL. (2003, March 17)
Retrieved January 1, 2010, from Carnegie Mellon University, Software Engineering Institute Web
site*:* http://www.cert.org/advisories/CA-2003-09.html

[12] Rafail, J. (2001). Cross-Site Scripting Vulnerabilities. *Software Engineering Institute at Carnegie Mellon*
University. Retrieved January 1, 2010, from www.cert.org/archive/pdf/cross_site_scripting.pdf

[13] Gregg, M. (2006). "Certified Ethical Hacker." Que Publishing.

[14] McAlearney, A. (2004, July 29). Automated SQL Injection: What Your Enterprise Needs to Know.
Search Software Quality TechTarget. Retrieved January 1, 2010, from
http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci996075,00.html#

[15] Steel, C., Nagappan, R., & Lai. R. (2005). *Core Security Parameters: Best Practices and Strategies for*
J2EE, Web Services and Identity Management. Prentice Hall.

[16] (2006, August 28). Patch Transversal Attack. [Content posted on Web site *SPAMfighter.*] Retrieved
January 1, 2010, from http://www.spamfighter.com/News-6260-Path-Transversal-Attack.htm

[17] One Hundred Seventh Congress of the United States of America. (2002). *Sarbanes-Oxley Act of 2002.*
Retrieved January 1, 2010 from http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf

[18] DocuTeam LLC. (1997). *Executive Summary of HIPAA Provisions.* Retrieved January 2, 2010, from
http://www.thedocuteam.com/docs/hipaaprovisions.doc

[19] U.S. Federal Trade Commission. (1999). *Gramm-Leach-Bliley Act: Disclosure of Nonpublic Personal*
Information. [15 USC, Subchapter I, Sec. 6801-6809] Retrieved January 2, 2010, from Web site:
http://www.ftc.gov/privacy/glbact/glbsub1.htm

[20] U.S. Federal Trade Commission. (1999). *Gramm-Leach-Bliley Act: Fraudulent Access to Financial*
Information. [15 USC, Subchapter II, Sec. 6821-6827]. Retrieved January 2, 2010, from
http://www.ftc.gov/privacy/glbact/glbsub2.htm

[21] U.S. Senate Committee on Banking, Housing, and Urban Affairs. (1999). *Gramm-Leach-Bliley Act:*
Summary of Provisions. Retrieved January 1, 2010, from

http://banking.senate.gov/conf/grmleach.htm

[22] U.S. Federal Trade Commission. (2007, November 27). *FTC Releases Survey of Identity Theft in the U.S. Study Shows 8.3 Million Victims in 2005.* [Online press release]. Retrieved January 2, 2010, from http://www.ftc.gov/opa/2007/11/idtheft.shtm

[23] "2002 CSI/FBI Computer Crime and Security Survey. Computer Security Institute." Retrieved 1/2/2010 from Web site: wwww.gocsi.com

[24] Acohido, B. (2009, March 17). Website-infecting SQL injection attacks hit 450,000 a day. *USA Today.* Retrieved January 1, 2010, from http://www.usatoday.com/tech/news/2009-03-16-sql-attacks-cyber-security_N.htm

[25] Howles, T., & Daniels, S. (2003). Widespread effects of defects. *Quality Progress, 36*(8), 58-63.

[26] Zimmerman, L.V. (2001). "Plan for training to ensure software quality." *AACE International Transactions, 51*, 3.

[27] McGraw, G. (2003, March-April). From the Ground Up: The DIMACS Software Security Workshop. *IEEE Software & Security, 1*, 59-66.

[28] National Institute of Standards and Technology. (2000). NIST Announces Accreditation of Four NIAP Common Criteria Testing Laboratories (CCTLs) For IT Security Testing. *Journal of Research of the National Institute of Standards and Technology, 105*(5).

[29] (2004). International syllabus being developed for software-testing specialists. *Industrial and Commercial Training, 36*(4), 182.