RESEARCH ARTICLE OPEN ACCESS

An Efficient Review And Comparative Study Of Public Testing Techniques With A 3-Tier Security Model As Concerns Various Parameters

Asst.Prof. Ami S. Desai, Dr. Raviraj Vaghela, Dr. Sanjay Buch
Ph.D. Scholar of RK University, Rajkot[1]
Assistant Professor of Computer Engineering, RK University, Rajkot[2]
Prof. IT & CE Dept., Chhotubhai Gopalbhai Patel Institute of Technology, UTU, Bardoli[3]
India

ABSTRACT

Public methodologies, model, and tools for fusion testing focuses mainly on a high level and technical description of the testing process. Unfortunately, there is no mechanism focused fundamentally and overall on the management of these tests. It often results in a situation when the tests are badly planned, managed by multiple-stakeholders, differ from languages/environment and the vulnerabilities found are messily remediated. The goal of this article is to present a new security testing model called 3-Tier security model which is focused mainly on fundamentally and overall testing of multistakeholder websites. Development of this methodology was based on the comparative analysis of current methodologies, model, and tools on the base of different parameters.

Keywords :-Vulnerabilities, Multi stakeholders,cybercrime

I. INTRODUCTION

The use of web technology is considered to be a bonus in today's era, any age group is surely busy using the technology as we all are reliant on it. They are used to complete various tasks in our lives. Web technology is implemented in almost all the sectors and sections our lives, let it be business, communication, virtual relationships, purchasing, agriculture, banking[2], to keep check, control, and harness over natural forces, transportation; no matter which industry we deal in technology is used in a certain manner.

Technology itself is impartial, helpful or harmful; we make the selection between many alternatives to use from the service providers that deliver the facilities to exchange ideas, information, videos, pictures, and graphics using multistakeholder websites[3]. It also allows easy sharing and distribution of existing content to others so that professional work can be shared through networks.

There are certain issues regarding online swindle, better known as fraud occurs with people like hacking, phishing, theft, stalking, malware attack, child soliciting and abusing etc[7]. It is happened because of improper testing of websites which are used by users. To resolve the hacking and cybercrime problem proper testing of each and every end of the website is needed. This gap analysis identifies using public tools used by IT companies for testing and make secure multi and single stakeholder websites[4]. For searching, the gap of testing problem analysis, survey and literature reviews of related research papers are done.

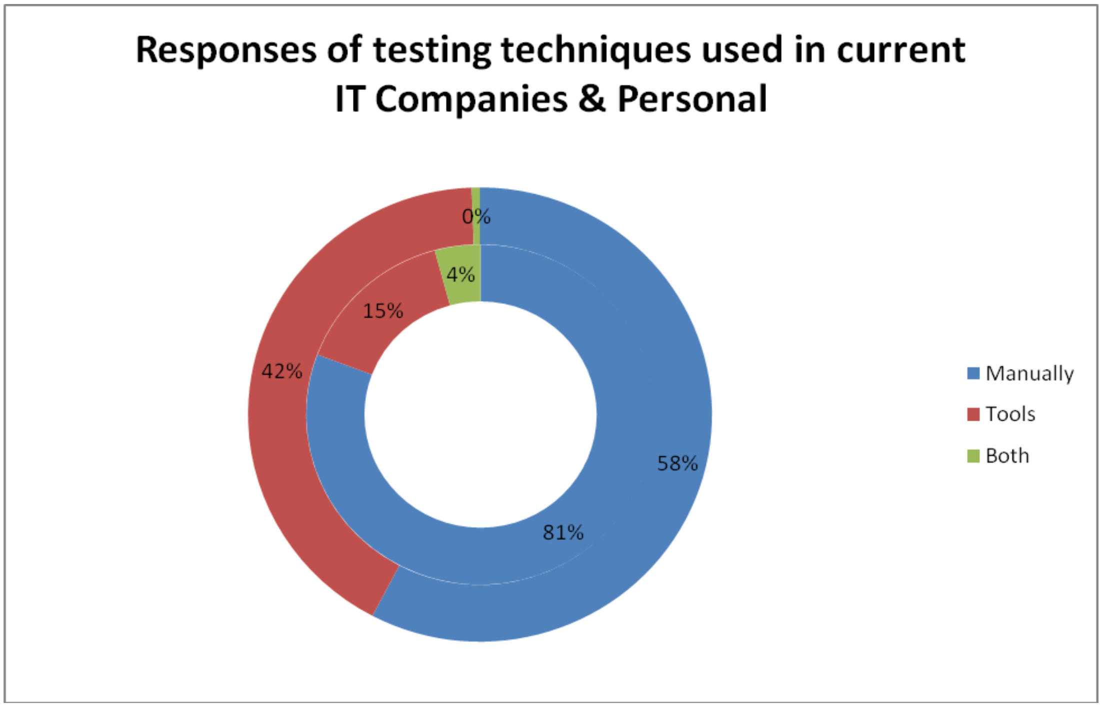
II. FINDINGS

Finding as per survey outcomes of 100 samples.

As stated in collecting 100 responses, 26 companies have been visited and the individual survey has been taken. These Companies are engaged in the development of websites or web services. Individual surveys are taken from those who are working as a software developer, programmer, tester or team leader etc in IT company.

In keeping with 100 samples result, 69.5% testing work is done manually using the testing methodology like white box, black box or gray box testing[1] and 28.5% testing is done using various tools, whereas 2% of them perform testing manually as well as using tools[5]. It is more elaborate percentage wise individually with companies and personal responses

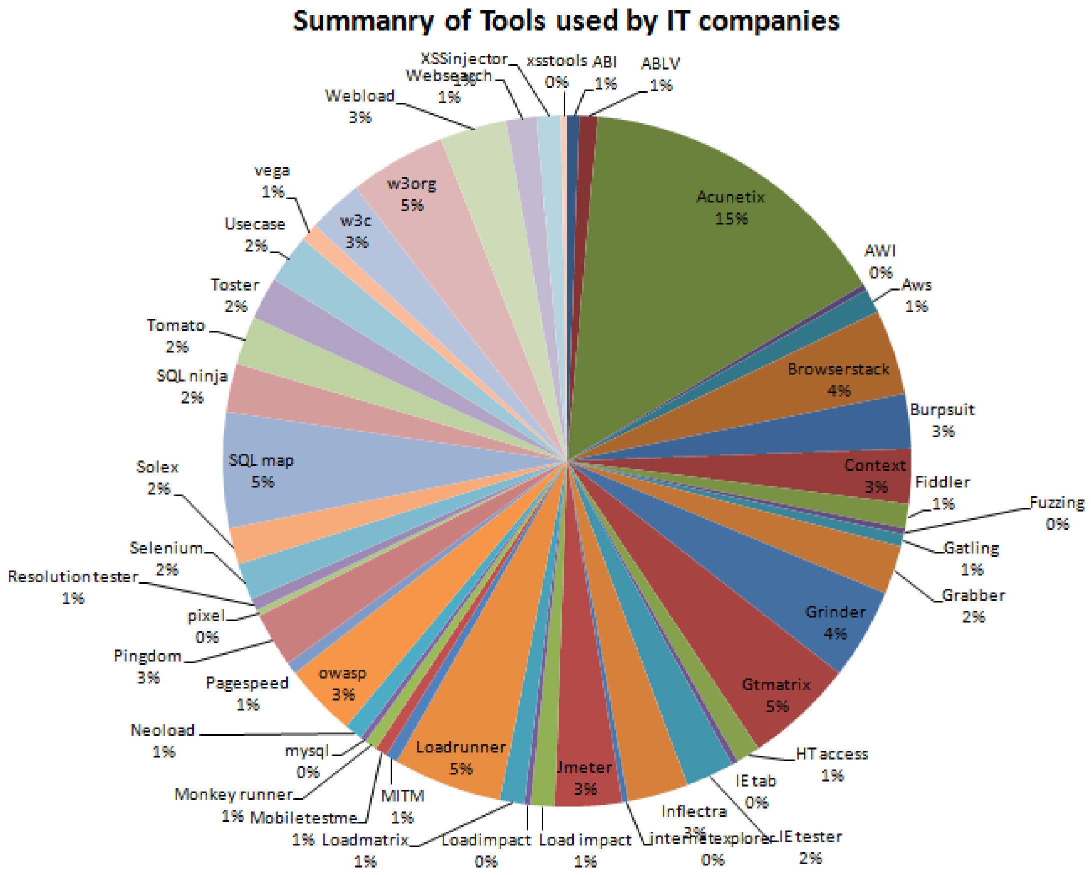
Although the survey result states that maximum testing is done manually, but still tools and technologies are requiring or rather lacking. It may be lacking proper testing is not done using currently available testing tools.



Graph 1: Responses of testing techniques used in current IT companies & Personal

According to the graph , as per companies responses they done 81% work manually testing and 15% using different tools whereas 4% responded that they can do testing manually as well as using tools.

Approximately more than 70 employees responded, from that 58% of employees done testing process manually and 42% using tools. Finally according to, IT companies and personal opinion , currently they used tools for the various testing process like functional testing, requirement testing, validation testing, performance testing, resolution testing, SQL injection testing and so on are categorized as bellowed.



Graph 2: Responses for tools used in current IT companies

According to the response of graph 2, maximum responded that 15% companies used acunetix. GTmatrix, Sql map, webload, grinder tools are used by companies 5%, 5%, 3%, and 4% respectively.

As stated in the survey, there are many tools available for functional testing, load testing, performance testing, resolution testing, SQL injection, security testing, XSS testing, web service testing, scanning/block open port, sniffing and traceroute. But still, there are several limitations of every tool that implies that it requires the enhancement of security checking mechanism.

The 3-tier security testing model resolves security testing problems. This model checks vulnerability at different ends, which provides user end security checking to prevent user's data at the time of online transactions. 3-tier security model checks security at developer end and makes sure the developer's environment is safe with a secure database and code before uploading any website. 3-tier also provide security suggestions and security checking after uploading website. Verification of 3-tier security model tested by many single stakeholders and multi-stakeholders IT companies for security testing of their websites. Based on those testing results from comparative analysis done between 3-tier security model with the current testing model, methodology, and tools. Some of them described in the next section. It is clear evidence of 3-tier security model give a concept to a resolved security problem.

III. COMPARATIVE ANALYSIS

Several tools name describe with their use in II section. The form that lists out tools trial versions of several tools like quttera, webinspector, sucuri, penetest-tools etc are available so it is selected to generating comparison reports with 3-tier security model. Testing is done and comparison generated on the base of commercial websites which are already uploaded. Some of the Comparison reports of various tools with a 3-tier security model put on view as bellow.

[A] Testing level parameter

Tools name	**Userend**	**Developerend**	**Serverend**	**Multistakeholder**
Quttera	1	1	0	0
Webinspector	0	1	1	0
Sucuri	1	1	1	0
pentest-tools	0	1	1	0
Siteguarding	1	1	0	0
Virustotal	0	1	0	0
Foregenix	0	1	1	0
Scanmyserver	0	1	1	0
QUALYS: ssllabs	1	1	1	0
Grabber	1	1	0	0
Acunetix	1	1	1	0
3-tier security model	1	1	1	1

Table 1 Testing level at different ends Vs Tools

Table-1 shows the comparison of 10 tools Vs 3-tier security model. It shows that the maximum 44% checking by public tools done on developer level than 22% and 30% at the user end and server end. and minimum checking is done on the multistakeholder website. Only 3-tier security checking provide security checking at the multistakeholder end whereas server end checking done minimum by public tools.

Due to this security testing is needed to enhance clients and server end. Server level security scanning is very important because if any website is uploaded to the shared server it can be the next target of the hackers. If the user end security testing is not properly performed, then his/her personal or account information can be misused by cyberpunk[6]

[B] Reporting & Suggestion parameter

The table below shows the comparison of public tools with 3-tier security model with other models with respect to suggestion Mechanism. The 3-tier security model not only gives the highest number of suggestions at each stage of software development but it also provides preventative functionality for secure website generation. It also provides the report of suggestions. For other models maximum at three stages the suggestions are provided but in 3-tier security model at all stages of software development, suggestions are provided along with the report.

Tools name	quttera	Webinspector	sucuri	pentest-tools	siteguarding	Virus total	Foregenix	Scanmyserver	QUALYS: ssllabs	Grabber	Acunetix	3-tier security model
Report	P	P	P	P	P	N	N	N	P	P	N	P
Suggestion	P	N	N	N	N	N	N	N	N	P	P	P

Table 2 Reporting & Suggestion mechanism at different ends Vs tools

[Provided – P, Not provided – N]

Table-2 shows the comparison of 10 tools Vs 3-tier security model. It shows that 67% provide report facility, in these reports highlights of the check, is displayed. They do not describe the suggestion mechanism to enhance security. As per that report 89% tools not provide suggestion mechanism by public tools. Whereas a 3-tier security model provides reporting and detail suggestion for enhancing security mechanism.

[C] Cost of Website Vulnerability Scanning

The table shows the comparison of the cost of Website Vulnerability Scanning of 3-tier security Model with other models. The cost of other tools ranges from $.249 to $9588. Some of the tool's cost change based on the size of website, environment, type of website and requirements. The 3-tier security model can be developed with no cost and 12 Audit features checking facility is provided. That features include user end, developer end, server end and multi-stakeholder end checking, reporting and suggestions also in no costing.

Tools name	Scanning Charge per year (in $)
Quttera	249
Webinspector	259.2
Sucuri	299.9
pentest-tools	950
Siteguarding	299.5
Virustotal	Not fix
Foregenix	Not fix
Scanmyserver	359.4
QUALYS: ssllabs	Not fix
Grabber	2064
Acunetix	120 to 9588
3-tier security model	No cost

Table 3 Public tools Vs 3-tier security model cost base parameter[6]

By means of comparison analysis A, B, and C, the testing methodology, the process model or tools are lacking behind on various issues like testing of multi-stakeholder websites. Thus a 3-tier security model is a way to overcome security challenges at the user's end, developer's end server's end, and multi-stakeholder end.

V. CONCLUSION

The 3-tier security model is responsible for the secure multi-stakeholder website based on service-oriented architectures. This model was designed for the management of secure transaction and communications. In any online business communications system, user's and developer's data and after uploading at server end security checking challenges are considered as an indicator of the security gaps which generate weakness in the system protection and are vulnerable to attacks. As per findings of survey and research papers, analysis a security model requires security testing for multi-stakeholder. Based on the comparative analysis and reports 3-tier security testing model is useful and fruitful for the multi-stakeholder website for a secure and safe mode to user and developer. Future work includes extending this approach to freely available for any type of websites practically.

ACKNOWLEDGMENT

I am grateful to Dr. Raviraj Vaghela, Professor of RK University, Rajkot for providing motivational support and guidance for methodology generation.
I thank Dr. Sanjay Buch, Prof. IT & CE Dept., Chhotubhai Gopalbhai Patel Institute of Technology, UTU, Bardoli for guidance on this subject that greatly improved the manuscript.

REFERENCES

[1] Acharya, Shivani, and Vidhi Pandya. "Bridge between Black Box and White Box – Gray Box Testing Technique." International Journal of Electronics and Computer Science Engineering 2: 175-184.

[2] Ajeet, Singh, Karan Singh, and Shahazad. "A Review: Secure Payment System for Electonic Transaction." IJARCSSE 2, no. 3, March 2012.

[3] Gunatilaka, Dolvara." A survey of privacy and security issues in social networks". http://www.cse.wustly.edu/~jain/cse571-11/ftp/social/index.html.

[4] Tan Phan, Jun Han, Garth Heward,Steve Versteeg. "Protecting Data in Multi-Stakeholder Web Service." no. 978-1-60558-799. ACM, April 2010.

[5] Ami Desai and Dr. Sanjay Buch." Prevention is better than Cure: Need of a Security Vulnerability Scanner Model to Overcome Security Testing Issues at Multi Stakeholder Based on Survey". International Journal of Innovations & Advancement in Computer Science. ISSN: 2347 – 8616 Volume-6, Issue-10, Oct.-2017.70-78

[6] Ami Desai and Dr. Sanjay Buch." Identification of Security Challenges and Security Issues in Social Oriented Architecture". No. ISSN: 2319 – 1058, *International Journal of Innovations in Engineering and Technology*, Volume 5 Issue 3 June 2015.:82-86.

[7] Ami Desai and Dr. Sanjay Buch." Security and fraud issues due to existing process model of software engineering and unawareness of online transaction and communication fraud".International Journal of advance research. ISSN: 2393-2835 Volume-4, Issue-4, April.- 2017.34-38