NEED TO ENHANCEMENT OF PUBLIC TESTING APPROACH FOR VULNERABILITY SCANNING & SECURITY TESTING FOR MULTI-STAKEHOLDER

Asst.Prof. Ami S. Desai[1], Dr. Raviraj Vaghela[2], Dr. Sanjay Buch[3]
PhD 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]

ABSTRACT- The use of the Internet has become second daily habits of millions of people. Due to that habits security of people's information is a most challenging aspect of the internet. Organizations, Government, Social or Individual every person are facing security risks. The use of the internet brings new and dangerous risks day to day. This is due to increasing attempts from unauthorized third parties to compromise private information for their own benefit – the whole wide area of cybercrime. Cause of improper and incomplete development of website security development or testing, hackers can easily take benefit. Generally, all websites are managed by multi-stakeholder. Thus it is tuff to prevent and test multi-stakeholder websites. This paper provides the comparative analysis of various testing methodologies, models, and tools on the base of testing and comparative analysis with current testing mechanisms. Provide the idea or highlights of a phase based security testing model, which provide vulnerabilities scanning for the secure phase to multi-stake holder's website.

Keywords- SET, SOA, Threats, Vulnerabilities, Multi stake holders

I. INTRODUCTION

Today is a world of e-transaction, cashless transaction, and e-communication. People share their thoughts, ideas, messages, even account information via the internet. The Internet provides a user-friendly and fastest platform for communication. This platform provides through websites which may be the single stakeholder or multi-stakeholders. We have awareness about single stakeholder websites and its security testing. But nowadays websites are managed by multi-stakeholder With the increased use of social media websites, more and many opportunities have opened up to seal the identity and perpetrate fraud online and resulting in cybercrime. The issues include privacy issues, identity theft, social networks spam, social networks malware, and physical threats[6] They tend to be growing comfort with, social platform providers, they generate revenue and lack the standards of the policies[10]. Hacking, theft, phishing, cyberstalking, identity theft, Child soliciting and Abuse, pornography, encryption, SQL injection, XSS etc are common words as well as the attack on internet world.

In general, most of the website developers are testing their websites using white box testing, black box testing and gray box testing for protection.[1] After web hosting, some web automated tools are provided in SOA for performance, load and security testing like Soap, Apache JMeter, Acunetix, SQL injector, Curl, Jconsole, Jprofiler, Jira, Bugzilla, Mantic, Redmine, SET, SSL etc. [15]. Developers use process model during the development of software website or system according to requirement. In some public process model like waterfall model, prototype model, incremental model V model, webE model, Spiral model, has tested as a phase. There are some loopholes or lacking so security testing does not work properly. As per research reviews and survey some outcomes will mention in next section.

II. FINDINGS

In general web services or websites implemented and working in chain manner. In chain manner, multiple organizations or stakeholders are depended on each other. That stakeholder may or may not be followed in the same environment, operating system, languages, framework, library functions or API. This kind of environment is very difficult to test. So they are dependent on other tester company for testing.

For example in the online payment system, information pass through five stakeholders like consumer, card issuing bank, card network, Acquiring bank, Merchant. Thought out this process five multi-stakeholder may follow different platform, language, environment, API. Thus users information or data passed on the different platform with languages. So, testing of multi-stakeholder web services becomes too difficult.

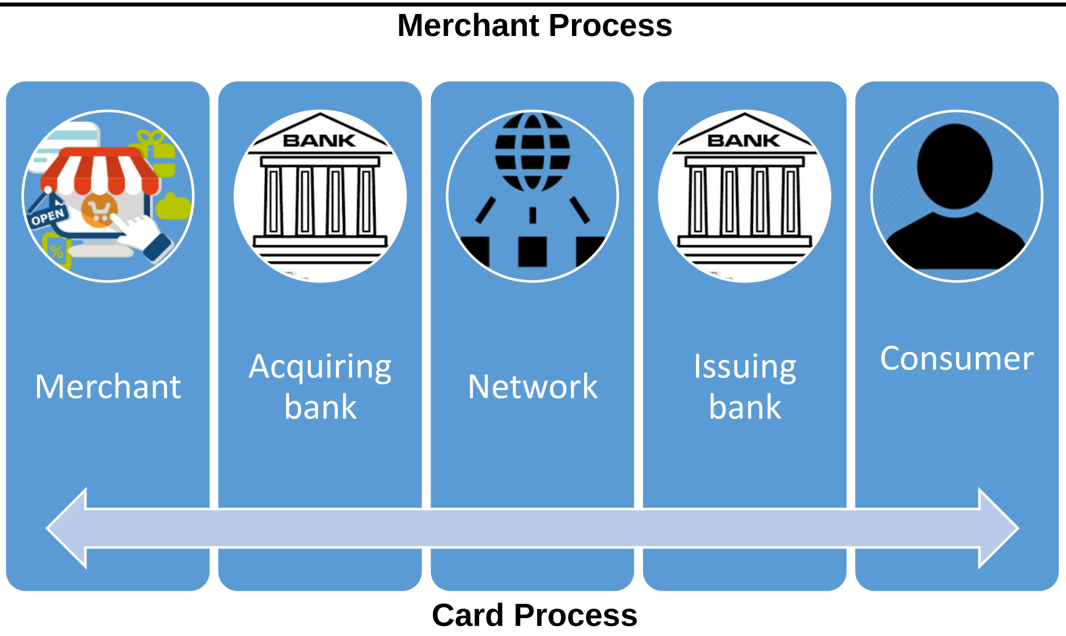

Figure 1 Payment chain

II. LACKING IN CURRENT TESTING METHOD, PROCESS MODEL OR TESTING TOOLS

Process model

The Website, web services and software are developing on the base of software engineering process model. Selection of process model is depending upon user's requirement. Some public models are waterfall model, spiral model, incremental model, prototype model, WebE etc which selected based on customer requirements. In these process models, testing is a phase.

Limitations of public process model[17]

Waterfall model Tester role will be involved in testing phase only. Development of requirement given by the client should be clear before we start the next phase of testing because in waterfall model the development phase should be freeze before we start the testing phase. Further changes will not be considered.

The prototype model has limitations such as every phase is an iterative, trial-and-error process that takes place between the developers and the users. Often unaware of the effort needed to add error-checking and security features which a prototype may not have.

Another interesting facet of iterative development is that activities across increments can overlap. It is not usually the case that one increment completes entirely before the next one begins is a limitation of the Incremental model.

Spiral model testing group needs to be able to handle the requirements of non-formal and formal standard testing requirements at different stages of the lifecycle

There is unauthorized posting of new product information erroneous or poorly tested functionality that frustrates visitors to a website. Security holes that expose internal company systems, and other economically unpleasant or even disastrous consequences checks during webE model.

RAD is not appropriate when technical risks are high. This occurs when a new application makes heavy use of new technology or when the new software requires a high degree of interoperability with existing computer programs.

V model developer and tester works parallel so it is rigid and the least flexible. This Model does not provide a clear path for problems found during testing phases. V Model should be followed for the small project where requirements are clear and easy to understand at the beginning of development. V Model should be followed for the project where very less probability to make the changes in the middle of testing or development phase which are unplanned.

Agile model work on the large project, then it becomes difficult to development and testing. In agile model, for customer satisfaction software need frequently change and update.

Hybrid web engineering process model has five levels developing in hybrid web engineering process model but there is no any specification for security testing.

Testing Methodology

All web site developers and software developers are testing their websites / customize software using white box testing, black box testing and gray box testing. White Box testers have access to the source code and are aware of the system and its architecture. A Black Box tester typically interacts with a system through a user interface by providing inputs and examining outputs without knowing where and how the inputs were operated upon. Gray Box tests are generated and are based on information such as state-based models or architecture diagrams of the target system.

Limitation of testing method

White box testing has limitation such as difficult to scale, difficult to maintain, cultural stress, highly intrusive. Black box testing fails for localized Testing, Inefficient Test Authoring, and Blind Coverage. Gray box testing has limitation for partial Code Coverage and Defect Identification.

In traditional system input and output is checked by unknown and fixed interface so it is the easiest task. But in the web services entire system works on three different interfaces, operating system, programming language and also dependent on the 3rd party for library API (application programming interface), online payment(bank), shipping (currier services) etc so it is difficult to test/examine.

Testing Tools

During the development and after web hosting testing is managing different tools on the server end. Some web automated tools are provided in SOA for automation performance, load and security testing like Soap, Apache JMeter, Curl, SQL injector, console, Acunetix, JSky, Iscan, Jprofiler, Jira, Bugzilla, Mantic, Redmine, SET, SSL etc.

Limitation of testing tools

On the base of review and survey, vulnerability scanning done on developer end, due to this security testing is needed to enhance client and server end. Server level security scanning is very important because if any website is uploaded to the shared server it can be 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

The testing methodology, the process model or tools are lacking behind on various issues like multi-stakeholders websites. Thus a process model is required to overcome these security challenges at the user's end, developer's end and server's end which will be fulfilled in the proposed model.

III. PHASE BASED APPROACH

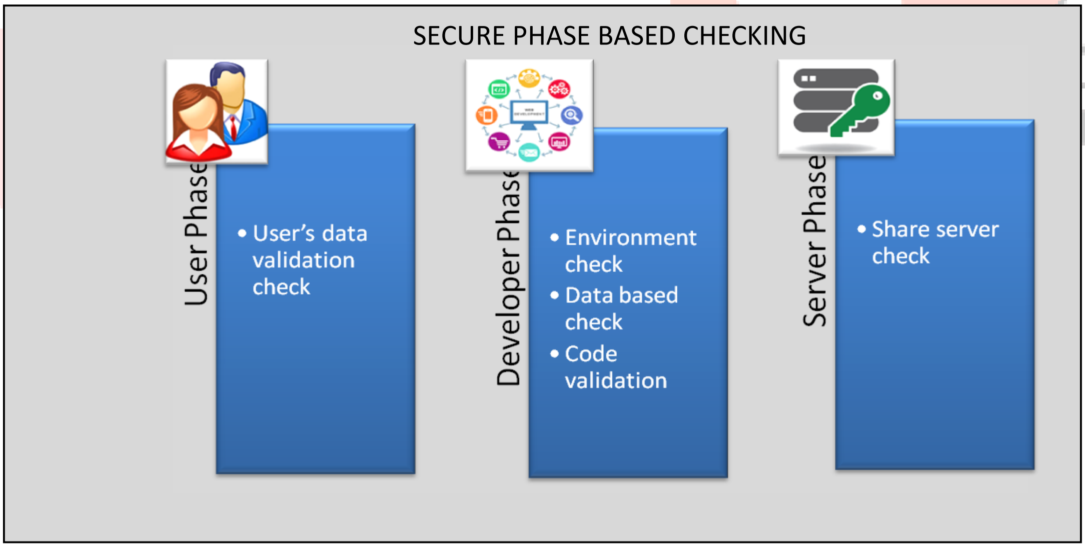

Figure 2 Phase based model

The following section provides the Phase-based model solution and its functionality. It is developed after comparative analysis of various reviewed testing models, testing methods, testing tools, testing approach or algorithm.

PHASE BASED MODEL

Figure 2. Display a security testing approach, which indicates by gray color. The approach provides a secure environment for users end, developer end, and server end. This approach provides secure transactions checking facility on the base of content checking algorithm. This approach divides mainly into three phases. User phase, developer phase, and server phase.

Used Phase provides checking or testing to secure user end. User end checking is important because lack of user end testing user can enter invalid data, script, backdoor or malicious code. Cause of lack of security user's data does not verify so invalid, wrong, incomplete, invalid formatted data will be inserted by user or hackers in the database. These wrong entered data will be affected by users personal data, developer end or also affected on the server end.

Developer phase checking is a very important feature of making secure web testing. In case of developer environment use of the non updated operating system, outdated virus scanning software, Adobe software, unsecured environments etc will affect on websites. Admin panel data should be needed highly secure code, encryptions, authentication is also a very important part of testing. Developer side validation of user input, display proper error messages and validation check is needed. So Developer end should be secured is necessary for secure multi-stake websites.

Server phase is playing an important role in publishing or uploading websites. In any circumstances, server end is not safe, then uploaded websites on that server also affected. Hacker mainly targets server because of generally more than one websites share the same server for publishing. Any of that published website targeted by the hacker will easily get access to other websites. Some time proxy server, Cloning of websites, router setting, wifi setting also affect the security of server end.

This phased based model satisfied some of them lacking and provide the secure environment. Comparative analysis with other mechanism will be explained in next section.

IV. COMPARATIVE ANALYSIS

The following section provides table of comparative analysis of various reviewed testing models, testing methods, testing tools, testing approach or algorithm

According to reviewed research paper, different methods and mechanism such as SOA testing model, Validate response via SOA, Antiphishing, tunnel protection, domain testing, social network security mechanism, 2FA, AHP, NetIFC, binding method, encryption method, proxy based solution, HTTPI protocol, wireshark, networkminer, VAPT tool, ARP, RTT, Jmeter, XML encryption, WS addressing, t-method, w-method, malicious feedback checking, IP address restriction, MRSA cryptosystem, string matching algorithm, reverse session hijacking, XP agile model, STRIDE model, Gaia method, Cluster technique, hash functions, etc. are used for prevention, identification and verification of cyber vulnerabilities.[10]

Because of these, developer end vulnerability can be scanned. According to some research papers mentioned mechanism can be check about browser prevention, online payment system, online bank transaction, online threats, issues & risks, privacy and security issues, testing techniques, vulnerabilities type & lifecycle, SQL injection, XSS, XML, SOAP, Sniffing, performance & load testing, Cyber & DDOS attacks, mobile crime and so on are identified. In maximum cases mechanism will work any two ends checking from the user end, developer end, server end or multi-stakeholder.

According to 100 samples survey result, 69% testing work is done manually and 29% testing is done using various tools, whereas 2% of them perform testing manually as well as using tools and those IT companies currently tools used for various testing process like functional testing, requirement testing, validation testing, performance testing, resolution testing, SQL injection testing and so on. As per 100 samples, 90% responded that process model is required for security checking. Because any development is based on the process model. Thus security at development level is to make server level and user level security.Comparison table displays working feature of testing tools/algorithm/mechanism.

AUTHOR YEAR	MODEL / METHOD / ALGORITHM / TOOL	Vulnerability Scanning or testing level			
		User	Developer	Server	Multi stake holder
Alisherov and Sattarova, 2009	Penetration testing	✗	✓	✓	✗
Netmarcom Kishore, 2009	2FA	✓	✓	✗	✗
Ali *et al.*, 2011	PCI-based DMA	✗	✓	✓	✗
Ali *et al.*, 2011	MySQL injector	✗	✓	✓	✗
Costinela-Luminita, 2011	Moodle platform	✓	✗	✓	✗
Hattangadi, 2011	SOA testing model	✗	✓	✓	✓
Gao, Bai and Tsai, 2011	Cloud-based application testing	✗	✓	✓	✗
Xue, 2011	SQL injector	✗	✓	✗	✗

Costinela-Luminiţa and Nicoleta-Magdalena, 2012	Moodle	✓	✓	✓	✗
Darwish and Hassan, 2012	Ib-MRSA cryptosystem and one time Id	✓	✗	✓	✗
Hongbin, Fengyu and Tao, 2012	WS-Security	✗	✓	✓	✗
Mainka, Somorovsky and Schwenk, 2012	Penetration testing	✓	✓	✗	✗
Schieferdecker, Grossmann and Schneider, 2012	MBST	✗	✓	✗	✗
Shahazad, Khan and Chandra, 2012	communication tunnel	✓	✓	✗	✗
Aaron Marback et al. 2013	security testing approach	✓	✓	✗	✗
Choudhary, Aaseri and Roberts, 2013	HTTPI	✗	✗	✓	✗
Poonam *et al.*, 2013	UIO-method	✓	✗	✗	✗
Wang, Wang and Li, 2013	MD5 and SHA1	✓	✗	✗	✗
Cristescu, Stoica and Ciovică, 2014	OGSA	✗	✓	✗	✗
Lad, Prof and Baria, 2014	token machanism	✓	✗	✗	✗
Sultana, Sadiq and Ahmad, 2014	AHP	✗	✓	✗	✗
Chou, 2015	NetIFC	✓	✗	✗	✗
Hedin and Moradian, 2015	Gaia method	✗	✗	✗	✓
Karumanchi and Squicciarini, 2015	Proxy based solution	✗	✗	✓	✗
Saleh *et al.*, 2015	String matching algorithm	✗	✓	✗	✗
Tambaram, 2015	malicious feedback rating	✗	✓	✗	✗
Garg, Singla and Jangra, 2016	Hadoop	✗	✗	✓	✗
Karmore and Mahajan, 2016	ANN method	✓	✓	✗	✗
Garg, Singla and Jangra, 2016	Hadoop method	✗	✗	✓	✗

George and Sangeetha, 2016	parallelism multi core approach	✗	✓	✗	✗
George and Sangeetha, 2016	SSL and RSA encryption	✓	✓	✗	✗
Hiremath, Malle and Patil, 2016	Mobile crime detection	✗	✗	✗	✓
Macher *et al.*, 2016	STRIDE model	✗	✗	✓	✗

Table 1 Comparative Analysis of Various Reviewed Models/ Method /Algorithm

According to table 1, the testing methodology, the process model or tools are lacking behind on various issues like multi stakeholders websites. Thus a process model is required to overcome these security challenges at the user's end, developer's end and server's end which will be fulfilled in the proposed model.

V. CONCLUSION

The phased based approach is responsible for the secure multi-stakeholder website based on service-oriented architectures. This approach has designed for management of secure transaction. In any online business communications system, there is some user side, developer side and server side challenges are considered as an indicator of the security gaps which generate weakness in the system protection and are vulnerable to attacks. As per analysis need of Software testing model for Developer end, Client end, Server end and multi-stakeholder. About 70% reviewed that they do not have any software process model for security testing at Developer end, User end and Server end. Nearly 72.66% admitted that they do not have any software testing methodology for security testing at Developer end, User end and Server end. Future work includes extending this approach to develop Security testing/technology/tools for multi stakeholder's website/web services practically.

VI. ACKNOWLEDGEMENT

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.

VII. 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. Adam Kie˙zun, Philip J. Guo,Karthick Jayaraman,Michael D. Ernst. "Automatic Creation of SQL Injection and Cross-Site Scripting Attacks." Software Engineering, 2009. ICSE 2009. IEEE 31st International Conference (IEEE), May 2009: 199 - 209.

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

4. Asankav.wso2.com. "How to Efficiently Test Service Oriented Architecture." WSO2. 4 11, 2014.

5. Daniel Walnycky a, Ibrahim Baggili a, *, Andrew Marrington b, Jason Moore a,Frank Breitinger. "Network and device forensic analysis of Android social-messaging applications." (ELSEVER) 2015: 577-584.

6. Goela, Jai Narayan, and BM Mehtreb. "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology." ICRTC(science direct) (elsevier) 5.2015: 710-715.

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

8. Information resellers. the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate, United States: Government office, 2013.

9. Karumanchi, Sushama, and Anna Squicciarini. "A Large Scale Study of Web Service Vulnerabilities." Internet Services and Information Security 5, no. 1 (FEB 2015): 53-69.

10. Mary-Luz Sánchez-Gordóna, Lourdes Morenoa. "Toward an integration of Web accessibility into testing processes." Edited by Procedia Computer Science 27. 5th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-exclusion, DSAI 2013. ELSESIVER, 2014. 281 – 291.

11. Normalini, M.K., T. Ramayah. "Biometrics Technologies Implementation in Internet Banking Reduce Security Issues?" International Congress on Interdisciplinary Business and Social Science (ELSEVER), 2012: 365-369.

12. Patil, sheetal, and S D Joshi. "Identification of Performance Improving Factors for Web Application by Performance Testing." IJETAE 2, no. 8. Aug 2012: 433-436.

13. Pressman, Roger S. Software Engineering. Vol. 1. New york: McGraw-Hill, 2001.

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

15. Yunus, Mamoon. "Fundamentals of SOA Security Testing." Service Technology Magazine, Feb 2012: 1-6.

16. 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.

17. 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

18. 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