Solution required for enhancing security testing for multi-stake holder on the bases of protection and suggestion mechanism

Asst.Prof. Ami S. Desai[1], Dr. Sanjay Buch[2]
PhD Scholar of RK University,Rajkot[1]
Prof. IT & CE Dept., Chhotubhai Gopalbhai Patel Institute of Technology, UTU, Bardoli[2]

ABSTRACT-

Online websites provide the wide range of facility for communication, Banking, Financial services and Insurance etc. These facilities provide transactions large volumes of data done every day on air. The sensitive and confidential nature of the data user host makes them the target of hackers. Facility for integration of website needs higher security testing. Protection of data from threats and malicious attacks is imperative to avoid loss of reputation and financial loss. To resolve security problem enhancement of Security testing and proper analysis is needed. It will minimize the risk of security and make sure for confidentiality, integrity, and availability of customer's transactions data. In this paper, we describe the customized framework for Security Testing for integrated websites with the comparative analysis of various testing methodology, model, and tool. Also provide the idea, design and explain a phase based security testing model, which provide vulnerabilities scanning and suggestions for the secure phase to multi-stake holder's website.

***Keywords*- Integrated websites, SET, SOA, Threats, Vulnerabilities, Multi stake holders**

I. INTRODUCTION

The Social networking is been now an integral part of our lives. People using the social networking websites are here to stay; thus bringing ghastly effects too. People need to be educated as to understand the proper and safe usage of sites, which certainly relates to privacy and security. If personal data is shared, and it becomes corrupted, it not only calls for fears on social networks but on our real-life persona as well. It's a huge challenge to provide knowledge regarding protecting identity online. The user needs to be imparted with knowledge. They tend to be growing comfort with, social platform providers, they generate revenue and lack the standards of the policies [10].

Maximum use of websites for share and convey of files, images, video clips, and text and personal details. Hacker aware about users weakness so these type of users are targeted via variety of malicious ways. They may because of privacy issues, identity theft, social networks spam, social networks malware, cyberstalking, hacking, identity theft, physical threats[6] and so on. it is briefly describes as bellow.

- Hacking and identity theft[3][8] is a type of common crime use forget access and misuse of user's personal device and personal identity[11] respectively using their permissions and awareness for money transfer. [7][14]
- Break copyrights laws by downloading music, movies, games, and software is a theft. Also get profit from use cracked software, company's logo, domain name and the idea of good name websites for misguiding people is also considered a crime.[7][6]
- Online harassment wherein the victim is subjected to a bombardment of mailing and online messages.[5] using cyberstalking.[7]
- Malicious software use for gain access and damage client devices by hackers. It will generate the pop-up and ask to download, as soon as downloading starts they start damaging victim's network and system.
- Children also not safe they targeted through chat rooms for the purpose of child pornography. Many hackers have been spending a lot of time to monitoring chat rooms frequented by children.

Websites or web services developed and testing using the different type of software processing model and different software processing model. Software testing methodologies are white box testing, black box testing and gray box testing.[1] Those public testing methodologies are basically check source code, input and output, path etc at developer level only. There are some process models such as waterfall, spiral, prototype, webE, V model etc. Those processing models have checking facility in testing phase. After web hosting, some web automated tools are provided in SOA for performance, load and security testing like Soap, Apache, Jmeter, SSL, Acunetix, SQL injector, Curl, Jconsole, Jprofiler, Jira, Bugzilla, Mantic, Redmine, SET etc. [15].

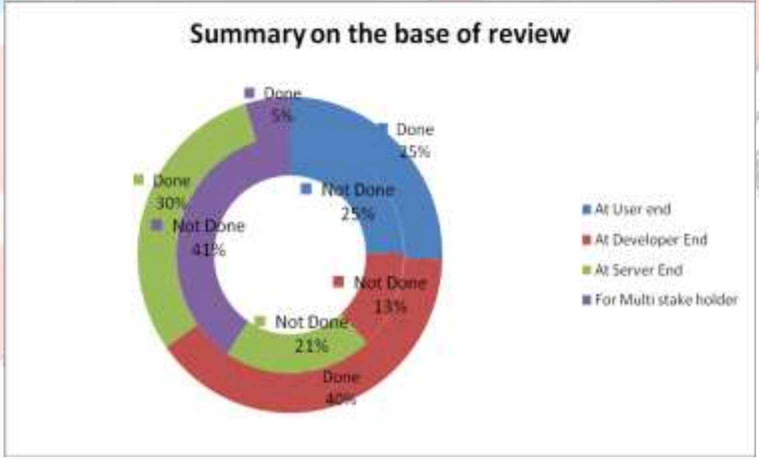
II. FINDINGS

Web services or websites are chained and depended on each other. They also divide into multi-stakeholders with different languages and platform. Online shopping, insurance provider company, online home loan provider's company etc. are the best example of multi shake holder organization.

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 information or data passed within different platform with languages. So, testing of multi-stakeholder web services becomes too difficult.

According to the review of more than 50 research paper different methods, algorithms and mechanism are available for testing and vulnerability scanning. There are 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. There are used for prevention, identification, and verification of cyber vulnerabilities.[10]

Using those tools, algorithm, methodology, 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. As per 50 research paper's available mechanism, tools, technology check vulnerabilities at different levels. According to graph analysis 25%,40%,30%,5% vulnerabilities checked at the user end, developer end, server end, and multi-stakeholder level respectively. Whereas 25%, 13%, 21%,41% does not check at the user end, developer end, server end, and multi-stakeholder level respectively.[15]



Graph 1: Level of testing

The conclusion is maximum checking at developer level and server level is done but it needs to enhance at the user end and multi-stakeholder end. The proposed model provides the level of testing, prevention, and suggestions.

III. THREE TIER MODEL

The Model is working in three steps. Input data, checking and log generate are main three stages.

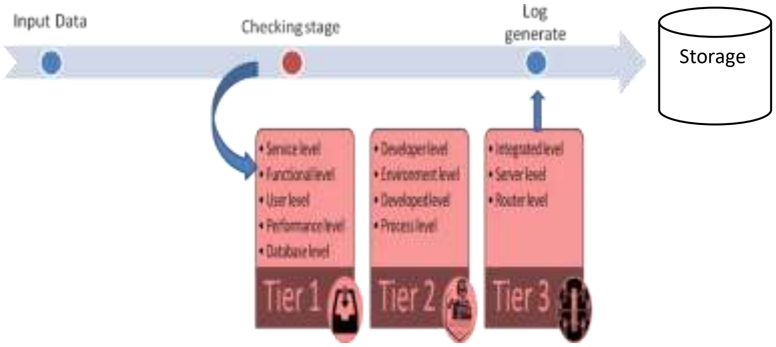


Figure 2 Three Tier Model

In first stage user, developer or other feed the data for testing entered data is valid or not, correct or not, complete or not. For example, a user entered his/her password for checking given password is strong enough or not. The developer needs to check all the code for vulnerability scanning. In any validation criteria missing at the user end, developer end and server end. It will be affected by the whole website as well as other websites. Thus all data will be entered in the model in the first stage.

In the second stage it is very important for testing, in this stage code testing, path testing, logic testing, condition testing, controls testing, validation testing, performance testing, database testing, integration testing, process testing, environmental testing, system testing covered at all levels. It divides into three tiers.

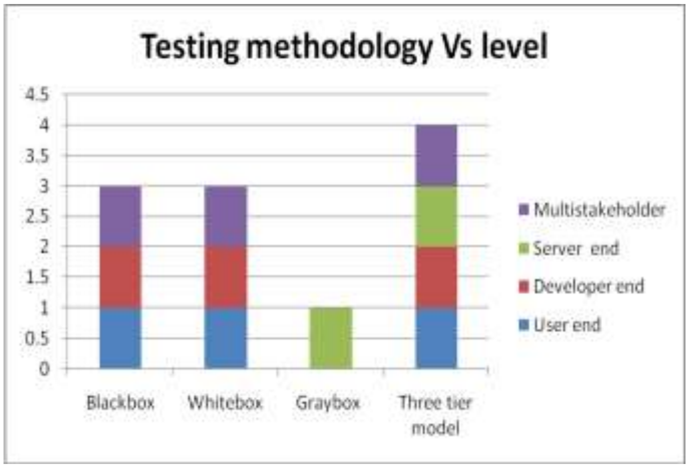
Tier 1 provides testing at the user level, which provides user end checking for scanning all protection mechanisms or functions used in source code or not. Here user may be developer or client. The user provides their personal and account information shared on websites. Developer provides their websites source code. In both condition, testing is necessary for security check thus database, performance, functional, input data testing, service related testing is checked in tier-1.

Tier 2 provides developer environment and administration side protection mechanism checking. Developer provides secure environment using updated operating system, antivirus, open port checking, and avoid use of adobe, extra security checking for website, use encryption functionality before passing information between browsers, use proper validation for protection of administrator's data. After completion of first and second tier integration testing, server level checking, router checking and log and summarize reports will be generated in tier 3.

The third stage is the last step of the model which provide suggestion and prevention messages which is stored in the database and which will be thus useful for providing the secure environment.

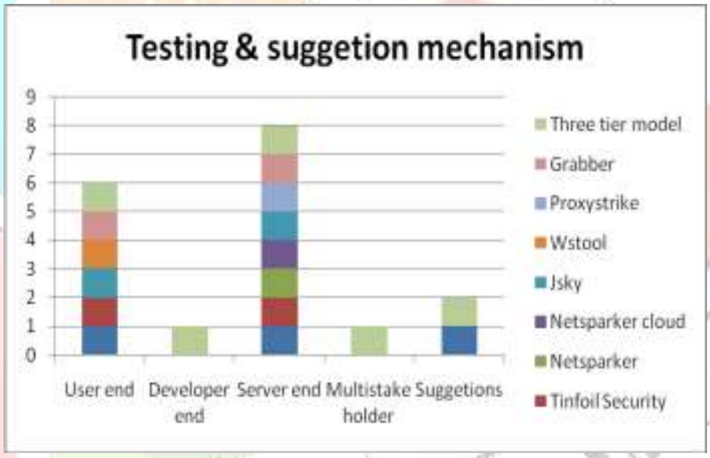
IV. COMPARATIVE ANALYSIS

According to sections-I, there is some public testing methodology which scanning and testing vulnerability at the different level of websites and web services. Comparison with three-tier security testing model displays in Graph III. Which clearly specify that three-tier security model provides the testing level at the user end, developer end, server end and multi-stakeholder.



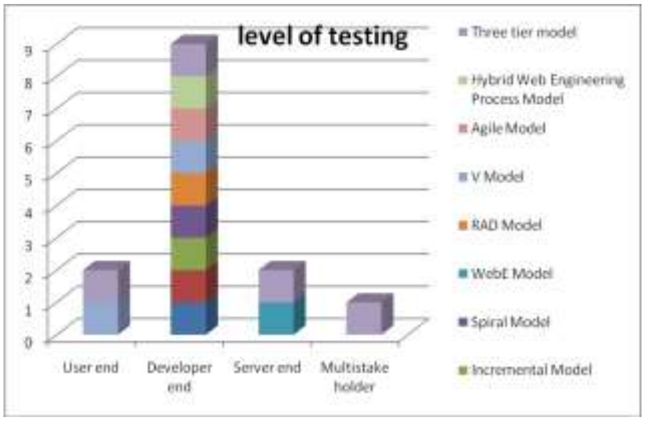
Graph 3. Testing methodology at different end

According to the review mentioned in Section-II of research papers, some tools, algorithms and technologies are identified which provides checking mechanisms at different levels. As per three-tier model, provides testing, suggestion, and prevention mechanism in three stages.



Graph 4. Testing & suggestion parameter for testing tools

Public process model methodology provides only testing facility. It does not provide suggestion and prevention mechanism. Comparison on based on testing display in graph V. There is nine public process model which mention in section-I are maximum work at developer end. Three tier model check at the user end, developer end, server end and multi-stakeholder.



Graph 5. Testing machanism at different levels

There are many tools available in current IT industry which provide testing mechanism maximum at developer end and server end only with large costing.

V. CONCLUSION

In this paper, we analyzed various process model, testing methodology, testing tools, algorithms etc for finding various loopholes in online transactions and communications. Also, specify various threats and crime occurs on the web scanning and preventing though three-tier security model. As per different graphs, reviews paper, survey summarized that lack of process model and methodology security challenges increase day by day. As per analysis need of Software testing model for Developer end, Client end, Server end and multi-stakeholder. In future require enhancing security checking mechanism practically implementation for providing the secure environment to the user, developer and server end.

VI. ACKNOWLEDGEMENT

I am grateful 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, *In*ternational 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