Global Scientific JOURNALS

GSJ: Volume 9, Issue 2, February 2021, Online: ISSN 2320-9186
www.globalscientificjournal.com

SECURITY ASSET CLASSIFICATION

Muhammad Bilal Shahzad, Sadeeq Jan, Sana Khattak, Omer Bin Tauqeer, Mohammad

Department of Computer Science & Information Technology, Univerity of Engineering & Techology Peshawar, Pakistan
Email: bilalshahzad188@gmail.com, sadeeqjan@yahoo.com, khattaksana6@gmail.com, omerbintauqeer@gmail.com, mohammadnh93@gmail.com

KeyWords
Security; Assets; Classifications; web-based systems; Information Technology; Hacking; Protection.

ABSTRACT

Attacks on the web-based systems have been increased significantly over the last decade. Organizations needs to protect their systems from such attacks. However, for large organizations, it becomes challenging to decide which systems needs how much protection. In this paper, we aim to develop a technique that can classify web-based assets for security. This technique is called asset classification. For asset classification we designed a questionnaire that covers several areas related to security, e.g., user access etc. We evaluated our technique on several websites and found it very efficient in classifying assets.

INTRODUCTION

Attacks on web-based systems have increased significantly over the last few years. A total of 32% increase have been observed in the number of hacked websites in 2016 compared to 2015. In March 2016, Google announced that **more than 50 million websites** worldwide was infected or malicious while this number was 17 million in March 2015 [1]. Similarly, the number of new Web application vulnerabilities published **in 2017 was 212% greater than the number disclosed in 2016** [1]**.** In 2018, **Google has sent over 45 million notifications** to registered website owners through Search Console, alerting them about possible problems with their websites that could affect their appearance in a search. Therefore, there is a dire need to take appropriate security measures to counter such attacks.

In today's world of cyber war, there is high risks to web based systems. In Pakistan, our enemies are always looking for damaging our online assets. Days after the terror attack in Pulwama, several Pakistani websites were reportedly hacked by "Team I Crew", which claimed to be an Indian hacker group [2].

Security testing is one of important part of any software development. To assess the security of any web-based system, assets should be classified on the basis of CIA (Confidentiality, Integrity, Availability). When data is Confidential, it should be protected from disclosure to unauthorized people. Integrity refers to the protection against unauthorized modification while availability ensures uninterrupted communication between clients (users) and web servers[3].

LITERATURE REVIEW

Due to increase in website application security issues, security testing is becoming important and critical activity of web application development. Purpose of security testing is to provide the confidentiality of the data, to check about the data leakage and maintain the functionality as intended [4]. It checks whether the security requirements are fulfilled by the web applications when they are subject to malicious input data [5]. 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 [6].

The existing approaches for mitigating threats to Web applications can be divided into client-side and server-side solutions. An application-level firewall offering protection in case of suspected *cross-site scripting* (XSS) attacks that attempt to steal a user's credentials [7]. Server-side solutions have the advantage of being able to discover a larger range of vulnerabilities, and the benefit of a security flaw fixed by the service provider is instantly propagated to all its clients. These server-side techniques can be further classified into dynamic and static approaches [8]. Dynamic tools and Perl's taint mode try to detect attacks while executing the audited program, whereas static analyzers scan the Web application's source code for vulnerabilities [9].

The Web platform is a complex ecosystem composed of a large number of components and technologies, including HTTP protocol, web server and server-side application development technologies (e.g., PHP, ASP), web browser and client-side technologies (e.g., JavaScript, Flash). Also, hackers in recent years are increasingly targeting web applications, since most networks are closely monitored through Intrusion Detection Systems (IDS) and firewalls [10].

Therefore, the web application layer needs to be secured from unauthorized users by building across the software development lifecycle security mechanism [6]. The effectiveness of the testing process may significantly depend on the tools use to support the process. Testing tools usually automate some of the tasks required by the process, such as test case generation, test case execution and evaluation of the test case result. Several testing tools support the production of useful testing documentation and provide a configuration and management of it [10].

Libya government websites are also susceptible to cyber-attacks. Currently no effort to assess the security level of the websites. This is probably due to lack of security experts in Libya, or lack of security awareness among the government agencies. This situation is not good for Internet security. Due to a lack of security assessment toward Libya government agencies in current literature [11].

Research the performance testing and performance improvement strategy in web application, a test generator can typically simulate user's behavior running tens to hundreds of Web client software[12]. Virtual users and Web servers communicate directly without having to use the Web-browser (such as IE or Firefox). In the performance tests, the running and testing number of the virtual users can be set in the generator. If more virtual users need to be simulated, it can be connected with multiple load generator, and centralized control, thereby generating a flow close to the limit. In addition, delay time can also be set between the acts of two tests.

One of the antecedents of person-organization identification is attractiveness, or the "favorableness of feeling" of the organization [13]. Retailers that are able to provide consumers with a positive, exciting, and memorable experience while they are shopping tend to be more successful than retailers that do not focus on providing such experiences.

The state of Saxony is providing a portal for all citizens to be informed on what aide they can receive from the state. The users need only to identify their life situation, then the system will inform them of what benefits they are entitled to, what offices are responsible, how to get there and what forms they have to fill out. Server also provides the forms for them to download and

submit [14-18]. This is a very important service in a region where 22% of the work force is unemployed and 17% of the people are receiving some kind of welfare.

Web services are widely used nowadays. Users can construct application system at a high speed to implement their functions by integrating the existing services [19] [20] [21].

METHODOLOGY

We have worked on a data set of more than 100 websites which are classified in multiple departments e.g., Finance. We have two method for classification of website's asset which are:

1. Manual Method
2. Automatic Method

APPROACH

In Automatic Method we design an automatic tool which can do all process of our manual work. First of all, we select keywords for all related questions which users can face. For each question there are several keywords.

ARCHITECTURE OF THE TOOL

The purpose of designing tool is to work it automatically just insert URL of website it give the output instantly. It is time saving and any un-professional user can use it easily. It is designed with the help of Java, first we write code which has access websites and then write another code which pick the keywords from source code then match with the existing keywords of database. If keywords are matched then its follow our question TURE otherwise FALSE.

5.3 COMPONENTS OF TOOL

Components of tool are consist of:

a) Questionnaire
b) Keywords
c) Websites/Source code

Conclusion

In this paper, we have designed a technique for asset classification of web sites for security requiremnts. The technique takes into account several types of information, e.g., user information, access rights. We evaluated our proposed technique on a huge dataset consisting of more than 100 websites. We have also developed an automated system for this process of asset classification.

In future work, the framework can be enhanced with the help of Natural Language Processing and Machine Learning technique to achieve full automation of classifying web based systems based on our proposed technique.

References

[1] "webarx," [Online]. Available: https://www.webarxsecurity.com/5-reasons-website-security-important-2018/. [Accessed 25 10 2019].

[2] "Times of india," [Online]. Available: https://timesofindia.indiatimes.com. [Accessed 09 09 2019].

[3] "DAWN," [Online]. Available: https://www.dawn.com/news/1302501. [Accessed 15 10 2019].

[4] S. Rafique, M. Humayun, Z. Gul, A. Abbas and H. Javed, "Systematic Review of Web Application Security Vulnerabilities Detection Methods," *Journal of Computer and Communications,* vol. 3, p. 28, 2015.

[5] A. Jaiswal, G. Raj and D. Singh, "Security Testing of Web Applications: Issues and Challenges," *International Journal of Computer Applications,* vol. 88, 1 2014.

[6] G. A. Di Lucca, A. R. Fasolino, F. Faralli and U. De Carlini, "Testing web applications," in *International Conference on Software Maintenance, 2002. Proceedings.*, 2002.

[7] N. Jovanovic, C. Kruegel and E. Kirda, "Pixy: A static analysis tool for detecting web application vulnerabilities," in *2006 IEEE Symposium on Security and Privacy (S&P'06)*, 2006.

[8] B. Chowdhury, M. Chowdhury and J. Abawajy, "Securing a smart anti-counterfeit web application," *Journal of networks,* vol. 9, pp. 2925-2933, 2014.

[9] D. Gupta, D. Singh, D. Kumar, U. Sharma and others, "Vulnerabilities and Security of Web Applications," in *2018 4th International Conference on Computing Communication and Automation (ICCCA)*, 2018.

[10] X. Li and Y. Xue, "A survey on web application security," *Nashville, TN USA,* 2011.

[11] A. A. Ali and M. Zamri Murah, "Security Assessment of Libyan Government Websites," *2018 Cyber Resilience Conference (CRC,* pp. 1-4, 2018.

[12] N. S. Aziz, A. Kamaludin, "Using pre-test to validate the Questionnaire for Website Usability (QWU," in *2015 4th International Conference on Software Engineering and Computer Systems (ICSECS,* 2015.

[13] K. Zhu, J. Fu, Y. Li, "Research the performance testing and performance improvement strategy in web application," *2010 2nd International Conference on Education Technology and Computer,* pp. V2-328-V2-332, 2010.

[14] Z. C. Lee and J. Yurchisin, "The Impact of Website Attractiveness, Consumer-Website Identification, and Website Trustworthiness," *2010 IEEE/ACIS 9th International Conference on Computer and Information Science,* pp. 301-306, 2010.

[15] P. McMinn, M. Shahbaz, and M. Stevenson, "Search-Based Test Input Generation for String Data Types Using the Results of Web Queries," *2012 IEEE Fifth International Conference on Software Testing, Verification and Validation,* pp. 141-150, 2012.

[16] H. M. Sneed, "Testing an e-government Web site," in *Seventh IEEE International Symposium on Web Site Evolution*, 2005.

[17] V. Stovanova, D. Petrova-Antonova and S. Ilieva, "Automation of Test Case Generation and Execution for Testing Web Service Orchestrations," in *2013 IEEE Seventh International Symposium on Service-Oriented System Engineering*, 2013.

[18] B. Vani, R. Deepalakshmi and S. Suriya, "Web based testing — An optimal solution to handle peak load," 2013.

[19] X.Y. Guo, Y.H. Chen, X.S. Qui and F. Tang, "Design and implementation of performance testing model for Web Services," *2010 2nd International Asia Conference on Informatics in Control, Automation and Robotics (CAR 2010,* pp. 353-356, 2010.

[20] Z. Yongjian, "Website Log Statistical Testing and Analysis," *2019 International Conference on Smart Grid and Electrical Automation (ICSGEA*, pp. 591-594, 2019.

[21] Y. Yu, N. Huang and Q. Luo, "OWL-S Based Interaction Testing of Web Service-Based System," *Third International Conference on Next Generation Web Services Practices (NWeSP'07,* pp. 31-34, 2007.

[22] N. Negara, E. Stroulia, "Automated Acceptance Testing of JavaScript Web Applications," *2012 19th Working Conference on Reverse Engineering,* pp. 318-322, 2012.

[23] C. Atkinson, F. Barth, D. Brenner and M. Schumacher, "Testing Web-Services Using Test Sheets," *2010 Fifth International Conference on Software Engineering Advances,* pp. 429-434, 2010.

[24] S. H. Shafin, L. Zhang and X. Xu, "Automated testing of Web Services system based on OWL-S," *2012 World Congress on Information and Communication Technologies,* pp. 1103-1108, 2012.

[25] E. Martin, S. Basu and T. Xie, "WebSob: A Tool for Robustness Testing of Web Services," *29th International Conference on Software Engineering (ICSE'07 Companion,* pp. 65-66, 2007.

[26] Y. Park, W. Jung, B. Lee and C. Wu, "Automatic Discovery of Web Services Based on Dynamic Black-Box Testing," *2009 33rd Annual IEEE International Computer Software and Applications Conference,* vol. 1, pp. 107-114, 2009.