IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Automating Bug Bounty: A Modern Approach For Discovering Vulnerabilities

Ashutosh R Mishra , Sachin Jain
Department of Computer Science
Parul University, Vadodara

Abstract

Bug bounty is the process of discovering vulnerabilities. Due to the advancement in technology, the Internet is gaining billions of new users every year[6]. The Internet is accessed via Browser to browse Web applications, which mainly serve static or dynamic web pages, whose main aim is to provide the information or services to the user. The Internet consists of billions of websites that are available with minimal security features or lack secure codes which invites hackers to exploit vulnerabilities present in websites and as result data breaches occur at the organizational level which in turn harms the organization's reputation and loses its trust with users. To prevent such attacks, Cybersecurity Researchers and developers spend a lot of time testing their web applications before deploying in the real world or on the Internet. Automating and developing such tools which are capable of detecting the vulnerabilities would be a great contribution to cybersecurity and as result, this would secure the organization from the Attackers and save ample amounts of time in the Testing phase. So, in this review paper, 5 such brief examples are presented, wherein the researchers have performed vulnerability assessment, penetration testing and along with this the researchers have proposed a method to automate the process of finding vulnerabilities.

I. INTRODUCTION

some bugs which can readily decrease time and increase the efficiency of the developers and organization.

II. LITERATURE SURVEY

Paper [1], is the earliest work on this domain and it focuses mainly on the three features for the classification.

1. Automating Process of Finding vulnerabilities in content management websites Especially in WordPress, zoomla , Drupal and etc.

2. Object Storage Misconfiguration

This states about the different misconfigurations in cloud-based services made by the user which make the instance vulnerable to exposing sensitive data present in the instance, The most widely used instance are Aws, and Azure

3. Source Code Review

It is a Process where the Developers leave some sensitive information publicly which quite often includes Database Credentials, Admin Username and Password, Where a normal user can use these credentials to takeover admin accounts Paper[2], work is purely presented on the Network Security and Penetration testing where an organization security researchers attempt to penetrate the internal networks and The broad view of the Internet has produced a remarkable growth of the demand for Web-enabled applications with more and more solid requirements of dependability, security, accessibility, inter-operability, and Due to market coercion and

very short time-to-market, the testing or examining of Web-based applications is often overlooked by developers, as They think this is too time- consuming process and it lacks a significant payoff. This deprecable practice affects negatively the standard of the applications and, therefore set off the need for cost-effective, efficient and testing approaches for authenticating and validating them The main objective of Paper is to automate the process of finding the vulnerabilities present in the web application, regards of any content management system or any frameworks used by the web application , Making an Internet a Safer place from black hat hackers, whose aim is to demolish the organization Name By making the Data breaches and selling it to the dark web, The study also needs a good proficiency level in penetration testing and cybersecurity, As this vulnerabilities can be reported in many forms whether directly contacting the organization vulnerability disclosure program or by using third-party services like Bugcrowd,

Hackerone, Integrity and many more. Performing the following Vulnerability assessment on web applications takes a long period of time, the main aim is to make a tool that can automate find the loopholes or vulnerabilities in their system and try to exploit up to the topmost access level

Different Types of tools were used for wireless penetration testing among the most used are EtherApe which is used to visualize the network, This helps the researchers to know the full map of the entire network. Even security tester tries to Reverse engineer the exploit to apply patches in the system once the penetration testing is finished, During the Testing phases, some problems were occurred like system failures and unresponsiveness which made an increase in testing time

Other tools which were also quite useful in Network Testing are Aircrack-ng, Metasploit, Zenmap, Armitage, Reaver, Nessus, As the test finished, Two things were concluded

1. There is a good tool to visualize the network, where the user can see the entire network as the web
2. Use of WPA/WPA2 PSK Security is necessary in wifi Security

Paper[3], Focuses on Outcomes of testing of a web application while Penetration testing the most of issues were discovered related to Authentication, Authorization, Cross-site scripting Cross-Site Request Forgery, XML Injection, While testing the author focused on OSWAP top 10 Vulnerabilities which made him clearer to work on the target. While building the web application, it is necessary to focus on different challenges and issues pertaining towards the security testing of the web application. By doing so, it will supply extraordinary dividends in identifying different kinds of risks, attacks, vulnerabilities, viruses, threats, etc pertaining to the security testing of web-based applications. By doing so, it can serve as a guide to a security tester for modeling the application of a test in an efficient way. The author came to the conclusion that an attempt was made for identify numerous problems and difficulties encountered while testing the security of web-based applications. Thus while conducting the security testing of applications which are web-based, a tester should be informed about all the issues and challenges pertaining to security. Along with this the information will be helpful in designing and modeling an efficient strategy of test and its application. The tester should also consolidate information related to the issues faced during the implementation which might be helpful in eradicating numerous vulnerabilities associated to the web applications while performing security testing.

Paper[4] mainly addresses Web application Testing. In the current scenario, an abrupt distribution of the web has been observed which composed some crucial interest of web applications which required several security related requirements. Due to this, the web applications' vulnerabilities are increasing, which can be then further exploited by the intruders to amass unwarranted admittance to the web applications and the destinations. The present frameworks of the web are genuinely convoluted, dispersed and composite, multilingual with visual and audio, innate and receptive, steadily moving forward, with swift changes. Webspace is obligatory and ever changing in essence and due to this, it is prone to malicious exercises like security penetration, dangers, infection assaults and many more. With the constant increase in the number of applications based on web, security turns out to be a primary issue and it requires to be identified based on the nature of web application. So it can be understood that security is of prime importance. In order to expand the reliability of the web applications, the security testing stage can be connected to the improvement stage. The sole purpose of security testing is to recognize the deformities that could be exploited for leading invasion. Security testing aids with emulating and uncovering fragility like SQL infusion, cross-site prearranging, support flood, URL infusion, record incorporation and treat alteration. Due to the huge expansion in the web application vulnerabilities, various threats and challenges are being confronted which can pose a dangerous hazard to the respectability, privacy, and security of the web applications. So it is required to comprehend the exceptional difficulties and challenges before devising any system or procedures for web security testing. With this objective, the paper examines various challenges and difficulties identified with the security testing of web applications along with the equipment which are utilized for performing the above task.

Paper[5] hashes out the future trend about the web applications which states that the objective of security testing is to verify the effectiveness of the overall web system defense against undesired access of unauthorized users, as well as their capability to preserve system resources from improper use and to grant the access to authorized users to authorized services and resources, System vulnerabilities affecting the security may be an entrance to an attacker to get into companies internal network and exploit it further. Both the running environment and the application can be responsible for security failures, In the case of Web application heterogeneous implementation and execution technologies, together increases the possibility of accessing them from anywhere which may make Web applications more vulnerable than traditional ones, and may make security testing more difficult to be accomplished.

III. Conclusion

The reports discovered new vulnerabilities among them the most were Cloud misconfiguration which was running on different services like AWS , and azure which leaks out sensitive data of the users. According to the thesis discovering such misconfigured buckets can easily be identified via automation , and can easily be informed to the instance owner,the main challenge is to identify the owner of the following bucket which need a manual task, Several New Critical Vulnerabilities like Remote code execution, Cross-site scripting, Sql Injections, and many more were discussed which can be easily automated to find them out in order to protect the application from getting exploited , As a result it gave Developers new idea to learn new vulnerabilities in the web application and also reduced their burden in testing phase, Moreover, New ways to test the wireless devices were discovered so that an organization can perform penetration testing on their internal network to know the level of security they are using, automation would be a great move in the future Using such tools would provide a great support in upcoming years of cybersecurity making internet more secure and safe place to browse.

IV. References

[1] Ján Masarik & RNDr. Václav Matyáš [2019] Automating Bug Bounty:Master's Thesis

[2] Brandon F. Murphy & John F. Kennedy (2013).Network Penetration Testing and Research

[3] Jaiswal, Arunima & Raj, Gaurav & Singh, Dheerendra. (2014). Security Testing of Web Applications: Issues and Challenges. International Journal of Computer Applications. 88. 10.5120/15334-3667.

[4] Kumar, Sandeep & Mahajan, Renuka & Kumar, Naresh & Khatri, Sunil Kumar. (2017). A study on web application security anddetectingsecurityvulnerabilities.451-455. 10.1109/ICRITO.2017.8342469.

[5] Di Lucca, G iuseppe. (2005). Testing Web-based applications: the state of the art and future trends. Information & Software Technology - INFSOF. 48. 65- 69 Vol. 1. 10.1109/COMPSAC.2005.95.

[6] The Satatista Report 2021[Online] : *https://www.statista.com/statistics/617136/digital-population-worl dwide/*