International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Proposal: Web attacks and Webmaster's Education Co-Relation

***Roopesh Reddy Sadashiva Reddy* [a]*,Hima Bindu Sadashiva Reddy* [b]**

[a]*cse dept PDIT Hospet India roopeshreddy.s@gmail.com*
[b]*Atria Institute of Technology, Bangalore 560024, India*

DOI: https://doi.org/10.55248/gengpi.2022.3.7.42

ABSTRACT

There is a lot of research done so far. Each of the studies provides detailed information about theWeb attacks that occurred, and the precautions taken and implemented. However, we still find that the Web attacksexisteven all the solutions, research and security policy are provided. None of the studies explain why this problem persists even after multiple solutions have been suggested. There is no evidence as to why a permanent solution has not been discovered so far. At least one solution so that similar attacks do not repeat. Take for example the antivirus we use on our PC, it's very simple to understand. If we do not use this antivirus, our PC will be attacked by deadly viruses that can damage our computer. This is why anyone who owns a PC should definitely have anti-virus software installed. Similarly, developing software to resist Web attacks will be a very good solution to solve the problem of Webattacks. Development of this particular software was only possible after the discovery of possible attacks related to script attacks on multiple Websites. To find the gap, the proposed study should be done according to the details mentioned in the methodology section. Both dependent and independent variable as Web attacks and Web master has been proposed. Hypothesis for this proposal is defined based on these variables.

Keywords:Web master,Web applications, Webattacks, Webattack

1. Introduction

The online applications a user access are vulnerable to Web (Web) attacks. These attacks occur whilesubscribingto knowledge-based articles, interaction on social networking sites, etc. [1]. Since user interaction is a mandatory and frequent activity, all activities performed to require dynamic Web application interaction [1]. yes. Web applications are vulnerable to Web (Web) attacks if user input is not properly enabled [1]. Web attacks are causing a companion to the nursing trade panic we have a tendency for internet applications. Even if as many security scans as possible, along with development, quality assurance, user acceptance testers, and IT security personnel, are performed at intervals at very different levels in the industry. These attacks are still occurring. Where can I not see a possible fixed solution?

Despite what precautions are taken, are hackers still allowed to attack online applications? Various factors that trigger attacks Is it specific to your industry or programming language, for example? Around 2010, when an Web attack occurred on a security company's Web application (the company name was intentionally kept secret and it is one of the five companies with the highest security standards). Identifying the problem and getting an online application accessible from anywhere in the world was a nightmare for the company's IT professionals. Things didn't stop there. The team made these attacks almost terribly frequent (every three months for almost three years) [17]. Severity is a business support Web application that displays YouTube videos and animated GIF images and distorts the first Web page. Approximately 80% of Web applications across the World Wide Internet are vulnerable to Webattacks [4]. This attacks is considered a serious and pervasive security threat by Global Internet Security [2, 4]. This makes it easy for hackers to access your sensitive information.

Researchers argue that the root cause of these attacks is migration of multiple Web applications due to developer inexperience. Even if multiple solutions are needed for Web attacks, none are tracked and used efficiently [2]. According to the MITER Common Weakness Enumeration Institute's list of the 25 most dangerous packet errors, Web ranks as ideal [2]. A recent result on the top Open Internet Application Security Project (OWASP) attacks, Web Attacks, was ranked second [2]. There is an analytical study proposing new solutions for developers and directors through the

* *Corresponding author..*
E-mail address: roopeshreddy.s@gmail.com

implementation of security policies and certificates [3]. The introduction of security-related policies and certificates can be a strategy to facilitate seamless integration with popular Web applications by delegating SSL titles and secure shortcuts [3]. However, the main concern is having a genuine and dedicated staff (developers and administrators).

Very useful guidelines provide the basis for overcoming at least these heavyweight attacks. help. The results from this survey provide a complete picture of the extent to which teams that build and maintain Web applications perceive the devastating impact of Webattacks. This study aims to propose a method for identifying gaps in building Web applications that are free from Web attacks. Also consider the various measures taken to avoid Web attacks. Finally, suggest new solutions/notes and find a permanent solution.

2. Review of Literature

The White Hat Security Company publishes an annual detailed statistical report on Websecurity [5, 13, 14]. See the latest statistical reports for 2013, 2014 and 2015. Web was number one in 2013 and 2014 in 2015. Ranking dropped to 3rd place. This is a good sign that the industry is taking Webattacks very seriously [5, 13, 14]. In 2013 and 2014, programming languages such as Java, Perl, and PHP were the top three languages responsible for Web attacks [5, 13, 14].

According to the 2015 statistical report, the healthcare industry has been hit the most with this Web attacks. However, reports from 2013 and 2014 indicated that the gaming industry was the most targeted [16].

The xHunter tool is specifically designed to identify Website URLs vulnerable to Web attacks. This tool helps Web application owners take precautions [6]. One research study proposed a defense mechanism to avoid Web attacks. Giant companies such as HSBC, Google search engines, Facebook, and Vodafone have encountered these attacks.Primarily because of unvalidated user input. [7] The algorithm was implemented by modifying a popular Firefox Web browser to track sensitive information during aWeb attack. All of these tests were performed in a test environment and even attempted to prevent information leaks. [8]

The only concern about implementing thealgorithm is that there is no evidence or citation that it is implemented in the state of a real-time Web application or author. However, the Firefox Company has agreed to accept that solution. HTML and JavaScript form the main backbone for causing Web attacks [9]. There are many HTML and JavaScript tags a hacker can come up with to attack his Web application [10]. Web attacks are easy to execute but hard to prevent and track, so a detailed step-by-step approach to avoiding them is suggested, keeping in mind that the user experience is not compromised. [11]. Sensitive information flow detections are tracked based on the type of Web attack. Types of Web attacks include reflected Web attacks, stored Web attacks, and DOM-based Web attacks [11]. The solution proposed in this study is excellent, platform-independent [11].

The developers blamed for the attacks pointed out that coding standards and guidelines were not followed. Is the single development phase involved in the software development lifecycle? Why are other phases of the software development lifecycle such as design phase, code review phase, quality testing phase and user acceptance testing phase not taken into account? Why is there no evidence as to why development errors are not detected before the Web application is live?

On another note, the statistical report provides very useful information about very serious attacks. However, it doesn't state why the Webattacks ranked third in 2015 compared to 2013 and 2014. All the research studies do mention about the web attacks identified. However, none mention the education background the web masters have to solve these web attacks. Hence it is necessary to study the correlation between web attacks and web master to understand success of the web attacks solutions.

3. Methodology

The case studies will be used in the design of this qualitative study. For this case study, users will be provided with open-ended survey questions. Participants will be developers, and web masters. Sampling: Select high-impact areas based on the programming language. Conduct an investigation by gathering information from the department that encountered this attacks. The first category (50participants) includes gathering information from industry departments that have been hit by Web. The second category (50 participants) includes gathering information from the Ministry of Industry without Web attacks to date.

The survey is conducted online and will last no more than ten to fifteen minutes [18]. Personal information collected will be kept confidential. Each department head will be personally contacted to obtain contact information for team members. A certain time frame will be given for all employees to submit survey responses. Reminders will be sent to managers and employees to complete the survey [19]. Anyone who has not submitted a survey will be contacted and invited to complete the survey. Explain to them the severity of the Webattacks issue. Approximately six months will be spent on data collection.

Here are some of the questionnaires planned for the survey [20]. From the design phase, the planning phase will include a discussion of what security measures were taken? [21]. In terms of development, what standards are followed for security measures, in a detailed security analysis report performed immediately after the development phase? [22]. Performed security analysis for QA testing, user acceptance testing, post-production deployment? The reason why this attack (Web app worked) was not determined before it worked. Is this a new HTML content, please provide full details about HTML insert tag? Are any bugs reported during any phase of the software development lifecycle? Or is it considered a false positive, provide a reason for it? Has a full patch been made for the reported bugs or has it not been implemented for Web related attacks? Is it due to broken framework, design or user experience? Please provide a full detailed list of all HTML and JavaScript injection attacks? What tools have been used so far to scan for Webattacks? Are Web analysis tools free? Indicate the different security policies your team follows for Web application development. What are the different security certificates installed in your Web application? What is the highest level of education the developer or web master has?

These questionnaires will help us learn how industries free from Web attacks have implemented security measures related to Webattacks. Additionally, we will learn how industries with reported Web attacks have failed to maintain security standards. This will give us insight into how hackers come up with new techniques and insert code every time. The survey or data collection is done through a Website [23]. The submitted data will be stored in the MongDB database. Once the data is collected, an SQL query will be used to generate a report based on certain criteria.

Limitations are accuracy of user-supplied information is the first limitation identified. Within an industry, the same employee may not work for that team for a longer period of time. If proper documentation is not kept about these attacks, new employees to the team may not be able to provide accurate information to this investigation. The availability of key participants is another limitation. For example, a participant is the main person involved in resolving the web attack and is on sick leave.

Two variables identified in this research areWeb master's education and Web attack. The independent variable is Webmaster education. The dependent variable is frequency? Severity? Of Web attack. Education independent variable signifies the educational background of the Webmasters which can range from high school, diploma, bachelor degree, master degree.

Hypothesis proposed for this study is:

H1: Web attacks occurred rarely if Webmasters are Masters degree holders

H2: Web attacks occurred frequently if Webmasters are high school pass out

4. Summary

Each study provides detailed information about the web attack that occurred, the precautions taken and implemented. However, we still find that the attacksexist behind all the solutions, research and security policy provided. None of the authors explain why this problem persists even after multiple solutions have been suggested. There is no evidence as to why a permanent solution has not been discovered so far. At least one solution so that similar attacks do not repeat. Similarly, developing software to resist Web attacks will be a very good solution to solve the problem of Webattacks. A web masters education is important to help resolve issue effectively. It is necessary to find the relationship of theweb master and the web attacks to avoid further vulnerabilities. To find the gap, the proposed study should be done according to the details mentioned in the methodology section.

REFERENCES

[1] Hydara, I, Bakar Md Sultan, A, Zulzalil, H, Admodisastro, N (2014). Current state of research on Web (XSS) – A systematic literature review. Department of Software Engineering and Information System, 170 –186, 10.1016/j.infsof.2014.07.010

[2] Venkat Narayana Rao, T, Tejaswini, V, Preethi, K (2012) DEFENDING AGAINST WebATTACKS AND Web, Journal of Global Research in Computer Science, Volume 3, No. 5, 60 – 64

[3] Garcia-alfaro, J, Navarro-Arribas2, G. (2007). Prevention of Web Attacks on Current Web Applications. In Meersman, R.O.B.E.R.T. & Tari, Z.A.H.I.R (Eds), On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS (pp. 1770-1784).

[4] Dr. Shanmugam1, J, Dr. Ponnavaikko2, M (2008) Web-Latest developments and solutions: A survey, Int. J. Open Problems Compt. Math., Vol. 1, No. 2, 102 - 121

[5] Whitehatseccom. (2013). Whitehatseccom. Retrieved 14 December, 2015, from https://www.whitehatsec.com/assets/WPstatsReport_052013.pdf

[6] Athanasopoulos, E , Krithinakis, E, Markatos, E, (2010) Hunting Web Attacks in the Network, Institute of Computer Science Foundation for Research and Technology, 1-8

[7] Amit Singh, A, Sathappan, S (2014) A Survey on WebWeb-attack and Defense Mechanisms, International Journal of Advanced Research in Computer Science and Software Engineering Research Paper ,Volume 4, Issue 3 , 1160 – 1164

[8] Vogt, P, Nentwich, F, Jovanovic, N, Kirda, E, Kruegel, C and Vigna, G (2007) Web Prevention with Dynamic Data Tainting and Static Analysis, Secure Systems Lab Technical University Vienna, 1-12

[9] NSA, September 2011 Protect Against Web (Web) Attacks , Information Assurance Mission as National Security Agency, 1-2

[10] Kaur, G (2014) Study of Web Attacks and Their Countermeasures, International Journal of Computer Applications Technology and Research, Volume 3, Issue 10, 604 – 609.

[11] SHALINI1, S, USHA2, S (2011) Prevention Of Web Attacks (Web) On Web Applications In The Client Side, International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, 650 - 654

[12] Practical Research: Planning and Design, P. D. Leedy & J. E. Ormrod, 11th (2015)

[13] Whitehatseccom. (2014). Whitehatseccom. Retrieved 14 December, 2015, from http://info.whitehatsec.com/rs/whitehatsecurity/images/statsreport2014-20140410.pdf

[14] Whitehatseccom. (2015). Whitehatseccom. Retrieved 14 December, 2015, from https://info.whitehatsec.com/rs/whitehatsecurity/images/2015-Stats-Report.pdf

[15] Rodriguez, K. M., Reddy, R. S., Barreiros, A. Q., & Zehtab, M. (2012, June). Optimizing Program Operations: Creating a Web-Based Application to Assign and Monitor Patient Outcomes, Educator Productivity and Service Reimbursement. In DIABETES (Vol. 61, pp. A631-A631). 1701 N BEAUREGARD ST, ALEXANDRIA, VA 22311-1717 USA: AMER DIABETES ASSOC.

[16] Kwon, D., Reddy, R., & Reis, I. M. (2021). ABCMETAapp: R shiny application for simulation-based estimation of mean and standard deviation for meta-analysis via approximate Bayesian computation. Research synthesis methods, 12(6), 842–848. https://doi.org/10.1002/jrsm.1505

[17] Reddy, H. B. S., Reddy, R. R. S., Jonnalagadda, R., Singh, P., & Gogineni, A. (2022). Usability Evaluation of an Unpopular Restaurant Recommender Web Application Zomato. Asian Journal of Research in Computer Science, 13(4), 12-33.

[18] Reddy, H. B. S., Reddy, R. R. S., Jonnalagadda, R., Singh, P., & Gogineni, A. (2022). Analysis of the Unexplored Security Issues Common to All Types of NoSQL Databases. Asian Journal of Research in Computer Science, 14(1), 1-12.

[19] Singh, P., Williams, K., Jonnalagadda, R., Gogineni, A., &; Reddy, R. R. (2022). International students: What’s missing and what matters. Open Journal of Social Sciences, 10(02),

[20] Jonnalagadda, R., Singh, P., Gogineni, A., Reddy, R. R., & Reddy, H. B. (2022). Developing, implementing and evaluating training for online graduate teaching assistants based on Addie Model. Asian Journal of Education and Social Studies, 1-10.

[21] Sarmiento, J. M., Gogineni, A., Bernstein, J. N., Lee, C., Lineen, E. B., Pust, G. D., & Byers, P. M. (2020).Alcohol/illicit substance use in fatal motorcycle crashes. Journal of surgical research, 256, 243-250.

[22] Brown, M. E., Rizzuto, T., & Singh, P. (2019). Strategic compatibility, collaboration and collective impact for community change. Leadership & Organization Development Journal.

[23] Sprague-Jones, J., Singh, P., Rousseau, M., Counts, J., & Firman, C. (2020). The Protective Factors Survey: Establishing validity and reliability of a self-report measure of protective factors against child maltreatment. Children and Youth Services Review, 111, 104868

[24] Reddy Sadashiva Reddy, R., Reis, I. M., & Kwon, D. (2020). ABCMETAapp: R Shiny Application for Simulation-based Estimation of Mean and Standard Deviation for Meta-analysis via Approximate Bayesian Computation (ABC). *arXiv e-prints*, arXiv-2004.