MATTER: International Journal of Science and Technology
ISSN 2454-5880

Dougesha Chady, 2019

Volume 5 Issue 2, pp. 229-238

Date of Publication: 19th October 2019

DOI- https://dx.doi.org/10.20319/mijst.2019.52.229238

This paper can be cited as: Chady, D., (2019). A Short Study on the Current Status of Web Applications Security in Africa and Across the World. MATTER: International Journal of Science and Technology, 5(2), 229-238.

A SHORT STUDY ON THE CURRENT STATUS OF WEB APPLICATIONS SECURITY IN AFRICA AND ACROSS THE WORLD

Dougesha Chady
Northampton University, in Association with Amity Global Business School, Mauritius
Yeshv24@gmail.com

Abstract

This new digitalized era is bringing lots of advantages in the world of business today as many processes are being automated through web applications to ease the fast paced work life of people making things more rapidly and efficiently. However, due to some weaknesses in the configuration and development of web applications, it becomes easy for hackers to identify and exploit loopholes found in web applications. For that reason, it becomes vital to emphasize on the importance of web security. Therefore, a qualitative research methodology is used to investigate on the topic. To elaborate, the aim of this paper is to identify the common causes of data theft that occurred during the last few years, especially regarding the outbreak that happened in South Africa. Finally, few researches and development done in the area of security like SQl injection, Cross site scripting and others were examined.

Keywords

Web Applications, Web Security, Data Theft

1. Introduction

Web applications have replaced the traditional Desktop application, and are proven to be more efficient in use (Kiruthika et al., 2016). Similarly, it is important to enforce security in web applications to gain the trust of users and also to enhance the quality and value of these applications (Chen et al., 2006). Moreover, applications are vulnerable to cyber-attacks as they are connected to computer networks (Uskov, 2013). It has been investigated that attackers are able to exploit web applications because of insufficient validation in the three tier web architecture. (Piyushkumar et al., 2014), (Piyushkumar et al., 2015), (Park & Park, 2008) and (Khairkar et al., 2014). According to the "Web Application Security consortium", approximately 49% of applications have been assessed to high risk loopholes making them vulnerable to security breach (T. W. A. S. Consortium, 2014). The rest of the paper will identify the causes of web application vulnerabilities, recent web security breach and ways to prevent web attacks.

2. Causes of Web Application Vulnerabilities and Issues

Simon McCullough (2019) highlights that attacks related to web applications lead serious issues such as loss of confidential data and intellectual property for both companies and consumers. The most common security vulnerabilities that exist include:

- Cross-site scripting (XXS); Denial of service; Structured Query Language Injection, these vulnerabilities creates flaws in web applications (Cenzic, 2009). XXS and Structured Query Language Injection allow an attacker to enter untrusted data so as to break the web application (Scholte et al., 2013). Attackers tend to send malicious links at client side, and when a user clicks onto those links, confidential information of users can be exposed, this is an example of XXS attack (Malviya & Saurav, 2014) and (Frenz & Yoon,2012). In comparison to SQL injection, where intruders have the ability to corrupt the entire database (Livshits & Lam, 2005) & (Tajpour & Massrum, 2010).
- Secondly, "Directory traversal vulnerability", happens when software applications are not built with proper filter to prevent a user to enter directory operators in order to retrieve unauthorized data from database (Li et al., 2013).
- Next, it has been studied that hackers input malicious code to sever, such that the server is unable to differentiate between correct and incorrect codes (Malviya & Saurav, 2013).

- Also, it was analyzed that flaws found in source codes itself brings security attacks in web applications (Viega & McGraw, 2001). In some cases, attackers normally track and direct keyboard activities to server in order to perform illicit acts (Mehta & Jamwal, 2015).
- Similarly, according to a recently published article in March 2019 (Seals, 2019), Citrix can probably become victim of a cybercrime invasion known as password spraying attack that targets single sign on and cloud based applications.
- On the other hand, a loophole that allowed an unauthorized access to execute malicious commands on Cisco's "Web-based management interface" was identified. Target devices for this attack included: "Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W Wireless-N VPN Router". To rectify this issue, a new software update was released (Cisco, 2019).

3. Web Security Breach in Africa and Across the World

A study that was conducted by the Ponemon Institute, states that the cost of data loss increased from "$6.65 million in 2008 to $6.75 million in 2009" (Sherry, 2010). It was reported that on Friday 12 May 2017, approximately 57,000 software applications connected to a network was victim of a cybercrime attack referred as "WannaCry Ransomware" that was disturbed to around 100,000 countries service companies including universities and hospitals (Khaitan, 2017). In 2018, an IBM server referred as the "InfoSphere Information Server", was vulnerable to allow unauthorized users to perform cross site scripting attacks to gain sensitive information, and a new version as released to resolve this problem (IBM, 2018). Then again, in 2018, about 2,216 data breaches and "53,000 cyber security incidents" were reported in 34 countries (Press, 2019).

It was reported that African countries like Nigeria, Uganda and Kenya are facing problems due to cybercrime (Matu, 2019). Based on the findings of a research in (Croock, 2016). The concept "Bring Your Own Device (BYOD)" which is in emergence in South Africa can become one of the main causes of data theft. More importantly, Troy Hunt, an information security researcher investigated that that around 3000 files containing usernames and password of 60 million people was hacked and those information were retrieved mainly from a list of south African Websites (Vermeulen, 2018) and (Fihlani, 2017). Data gained from this attack was published by one amongst the company involved in "traffic fines online payments" in South Africa. Subsequently, this incident caused other risks as well, for instance, the password retrieved could be used to decipher other accounts as well. Conversely, the founder of website “haveibeenpwned” enabled users to check whether or not they have become victim of this act or not (SAAL, 2018). Furthermore, the root cause of the issue was investigated and it was found that the website was configured with “lax security” that authorized anyone with little technical knowledge to exploit database records (Fraser, 2017).. In the same way, approximately 50 million active users information was leaked from the well-known social media website Facebook due to a vulnerability that was related to one of its existing features (Simon, 2018).

A survey below published by Cert Mauritius state that around 31% hacking incidents ,22% of online harassment and 15% of Identity theft arose as illustrated on the graph below:

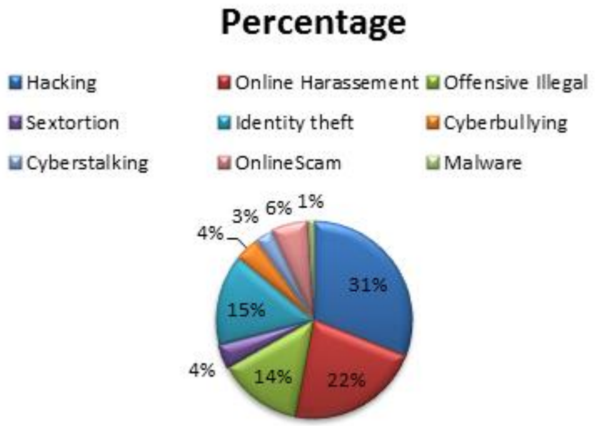

Figure 1: *Survey from cert Mauritius (Jan 2019)*

4. Preventing Web Security Attacks

It has been remarked that many researches are being undertaken to avoid and mitigate risk associated with vulnerabilities in web applications (Balzarotti et al., 2008), (Jovanovic et al., 2006), (Livshits et al., 2005) and (Wassermann & Su., 2007). For instance, Output Sanitization can be used as a method to prevent Cross-site scripting and Structured Query Language Injection, as it refines data that is inputted prior being processed in building the application (Robertson & Vigna, 2009), (Samuel & Saxena, 2011) and (Weinberger et al., 2011). Also, a study was conducted to improve the PHP interpreter to identify loopholes that lead to SQL injection (Pietraszek & Berghe, 2005). On the other hand, “an open source static tool named Pixy” was built to prevent Cross-site scripting (Jovanovic et al., 2006). Then again, a method has been designed to prevent Cross-site scripting attacks by utilizing the “Dynamic Cookies Rewriting Technique” (Putthacharoen & Bunyatnoparat, 2011).

A company called “White Source” encouraged developers to opt for open source modules and elements to keep them updated on the latest upgrades and reports about security. Likewise, in the future, artificial intelligence will be used as a mechanism to counteract data theft that occurs due to human errors using virtual assistants to input complex commands and configure systems (Lang, 2018).

It is important that organizations conduct penetration testing on systems to mitigate risks associated with web attacks,. The three phases of Penetration testing is explained in by Zaher et al., (2018): Firstly, Test preparation that identifies the objectives and duration of the tests; Secondly, Test Implementation that includes the collection of information to perform analysis and examination of existing vulnerabilities (Gupta,2014). Consequently, the second phase comprises of two steps namely the identification and reduction of vulnerabilities before releasing a new version of the application (Ami & Hasan, 2012). Finally, Test analysis is done based on the results gained throughout the penetration testing process and presented in the form of a report.

5. Recommendation & Conclusion

Most Organizations rely on web applications in order to conduct their daily activities. Hence, it is essential to ensure that data is kept in a safely manner in web applications to avoid problems that can lead to loss of money and reputation for companies. This research covers analysis done by experts to look for solution to minimize data breaches by proposing innovative ideas for developers to implement while developing web applications. Similarly, proposal to mitigate data theft can include the need for employers to train staffs to use and operate systems wisely to eliminate breaches that occur due to human negligence. Also, proper risk and vulnerability assessment is required to be able to forecast and prevent issues in the future. In short, users need to abide and follow a proper information security policy to mitigate cybercrime.

References

Ami.P and Hasan.A(2012)."Seven Phrase Penetration Testing Model," International Journal of Computer Applications, vol. 59, no.5, p. ISSN: 0975 – 8887. https://doi.org/10.5120/9543-3991

Balzarotti D., Cova M., Felmetsger V., Jovanovic.N, Kirda.E, Krugel.C, and Vigna.G Saner (2008).composing static and ¨dynamic analysis to validate sanitization in web applications. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA. https://doi.org/10.1109/SP.2008.22

Cisco (2019). Cisco RV110W, RV130W, and RV215W Routers Management Interface Remote Command Execution Vulnerability. [online] Available at: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190227-rmi-cmd-ex.

Cert-Mu (2019). Computer Security Incident Response Team of Mauritius -Home. [online] Cert-mu.govmu.org. Available at: http://cert-mu.govmu.org/English/Pages/default.aspx.

Croock, G. (2016). *An Africa Perspective: Cyber Threats, Security and Data Protection*. [online] Bdo.co.za. Available at: https://www.bdo.co.za/en-za/insights/2016/cyber/an-africa-perspective-cyber-threats-security-and-data-protection.

Cenzic (2009).“Web application security trends report Q3-Q4, 2008”, available at: www.cenzic. com/downloads/Cenzic_AppSecTrends_Q3-Q4-2008.pdf.

Chen, S., Choo, C. and Chow, R. (2006).“Internet security: a novel role/object-based access controlfor digital libraries”, Journal of Organizational Computing and Electronic Commerce, Vol. 16 No. 2, pp. 87-103. https://doi.org/10.1207/s15327744joce1602_1

Frenz. C. M., Yoon. J. P. (2012).“XSSmon: A Perl Based IDS for the Detection of Potential XSS Attacks”,Systems, Applications and Technology Conference (LISAT), IEEE Long Island. https://doi.org/10.1109/LISAT.2012.6223107

Fihlani, P. (2017). *Millions caught in SA's 'worst data breach'*. [online] BBC News. Available at: https://www.bbc.com/news/world-africa-41696703.

Fraser, A. (2017). *Revealed: the real source of SA's massive data breach - TechCentral*. [online] TechCentral. Available at: https://techcentral.co.za/revealed-real-source-sas-massive-data-breach/77626.

Itnewsafrica.com. (2019). F5 releases first annual Application Protection Report |IT News Africa – Up to date technology news, IT news, Digital news, Telecom news, Mobile news, Gadgets news, Analysis and Reports | Africa's Technology News Leader. [online] Available at: https://www.itnewsafrica.com/2018/12/f5-releases-first-annual-application-protection-report.

IBM (2018). IBM Security Bulletin: IBM InfoSphere Information Server is vulnerable to a Cross-Frame scripting issue (CVE-2018-1432) - United States. [online] Www-01.ibm.com. Available at: http://www-01.ibm.com/support/docview.wss?uid=swg22014911.

Jovanovic.N, Kruegel.C, and Kirda.E (2006). Pixy: A Static Analysis Tool for Detecting Web Application Vulnerabilities (Short Paper). In Proceedings of the 2006 IEEE Symposium on Security and Privacy, pages 258–263, Oakland, CA, USA, IEEE Computer Society https://doi.org/10.1109/SP.2006.29

K.,. K. K. Ankita Gupta(2014), "Vulnerability Assessment and Penetration Testing," International Journal of Engineering Trends and Technology-, vol. 4, no. 3.

Khaitan, R. (2017). The 10 Countries Suffering Most The WannaCry Malware Attack. [online] Frontera. Available at: https://frontera.net/news/global-macro/1-the-10-countries-most-affected-by-the-wannacry-malware-attack. https://doi.org/10.25089/MERI/2017/v10/i2/151167

Khairkar.D, Deepak D Kshirsagar, Sandeep Kumar(2013), "Ontology for Detection of Web Attacks", International Conference on Communication Systems and Network Technologies. https://doi.org/10.1109/CSNT.2013.131

Kiruthika, J., Khaddaj, S., Greenhill, D. and Francik, J. (2016). User Experience design in web applications. IEEE International Conference on Computational Science and Engineering, 978-1-5090-3593-9/16(10.1109), p.642. https://doi.org/10.1109/CSE-EUC-DCABES.2016.253

Livshits. V. B. and Lam. M. S..(2005).Finding Security Errors in Java Programs with Static Analysis. In Proceedings of the 14th USENIX Security Symposium, pages 271–286.

Lang, L. (2018). *Five Trends That Will Shape IT In 2019*. [online] Forbes.com. Available at: https://www.forbes.com/sites/theyec/2018/11/28/five-trends-that-will-shape-it-in-2019/#41102d73f399.

Li, L., Dong, Q., Zhu, L. and Liu, D. (2013). The Appilication of Fuzzing in Web software security vulnerabilities Test. 2013 International Conference on Information Technology and Applications, 978-1-4799-2876-7/13, p.130. https://doi.org/10.1109/ITA.2013.36

Matu, P. (2019). Companies In Africa Can't Afford To Turn A Blind Eye To Cyber Security. [online] Forbes.com. Available at:

https://www.forbes.com/sites/riskmap/2017/07/11/companies-in-africa-cant-afford-to-turn-a-blind-eye-to-cyber-security.

Mehta T. S. and Jamwal. S. (2015).“Model to prevent websites from xss vulnerabilities,” IJCSIT) International Journal of Computer Science and Information Technologies, vol. 6, no. 2, pp. 1059–1067.

Malviya V. K., Saurav.S (2013).“On Security Issues in Web Applications through Cross Site Scripting (XSS)”,20th Asia-Pacific Software Engineering Conference. https://doi.org/10.1109/APSEC.2013.85

Pietraszek.T, Berghe.C.V (2005). Defending Against Injection Attacks through Context Sensitive String Evaluation. In: Proc. Recent Advances in Intrusion Detection. 8th International Symposium. Seattle: 124-145. https://doi.org/10.1007/11663812_7

Putthacharoen.R, Bunyatnoparat.P, (2011).Protecting Cookies from Cross Site Script Attacks Using Dynamic Cookies Rewriting Technique. “Method for Detecting Cross-Site Scripting Attacks".

Press, g. (2019). 60 Cybersecurity Predictions For 2019. [online] Forbes.com. Available at: https://www.forbes.com/sites/gilpress/2018/12/03/60-cybersecurity-predictions-for-2019/#63f0c7e04352.

Piyushkumar A. Sonewar, Nalini A. Mhetre(2014)."A Survey of Intrusion Detection System for Web Application", International Journal of Engineering Research and Technology Vol. 1 (02), ISSN 2278 –0181.

Piyushkumar A. Sonewar, Nalini A. Mhetre (2015).A Novel Approach for Detection of SQL Injection and Cross Site Scripting Attacks ", IEEE's International Conference on pervasive computing (ICPC).

Park Y J, J C Park (2008)."Web Application Intrusion Detection System for Input Validation Attack", Third International Conference on Convergence and Hybrid Information Technology. https://doi.org/10.1109/ICCIT.2008.338

Robertson.W and Vigna.G(2009).Static enforcement of web application integrity through strong typing. In Proceedings of the 18th USENIX Security Symposium, pages 283–298. USENIX Association.

Scholte, T., Robertson, W., Kirda, E. and Balzarotti, D. (2012). Preventing Input Validation Vulnerabilities in Web Applications through Automated Type Analysis. *IEEE 36th*

International Conference on Computer Software and Applications, 0730-3157, p.233. https://doi.org/10.1109/COMPSAC.2012.34

Sherry.D(2010).Web 2.0 Security Threats and How to Defend Against Them, https://searchsecurity.techtarget.com/magazineContent/Web-20-security-threats-and-how-to-defend-against-them.

SAAL, P. (2018). *Data leak exposes personal records of nearly 1 million South Africans*. [online] Available at: https://www.timeslive.co.za/news/sci-tech/2018-05-24-data-leak-exposes-personal-records-of-nearly-1-million-south-africans.

Samuel.M, Saxena. P and D. Song(2011). Context-sensitive autosanitization in web templating languages using type qualifiers. In Proceedings of the 18th ACM conference on Computer and communications security, CCS '11, pages 587–600, New York, NY, USA, ACM. https://doi.org/10.1145/2046707.2046775

Seals, T. (2019). Citrix Falls Prey to Password-Spraying Attack. [online] Threatpost.com. Available at: https://threatpost.com/citrix-password-spraying/142649.

Simon, M. (2018). Facebook account hack FAQ: What happened, how it affects you, and what you should do now. [online] PCWorld. Available at: https://www.pcworld.com/article/3310040/facebook-account-breach-faq.html.

Sukhoo.A,(2019).'A study on web security in a public organization in Mauritius'.Level 3, Mindspace Building, Bhumi Park, Cybercity, Ebene, Mauritius, 72201.

T. W. A. S. Consortium. (2014).Insufficient transport layer protection. [Online]. Available: http://projects.webappsec.org/w/page/13246927/FrontPage.

Tajpour A., Massrum M. (2010).“Comparison of SQL Injection Detection and Prevention Techniques”,2nd International Conforence on Education Technology and Computer (ICETC).

Uskov,A.(2013).Software and web Applications Security: State-of-the-Art Courseware and Learning Paradigm. IEEE global engineering Education Conference, 978-1-4673- 6110-1/13,p.608. https://doi.org/10.1109/EduCon.2013.6530168

Viega, J. and McGraw, G. (2001). Building Secure Software, How to Avoid Security Problems the Right Way, 1st ed., Addison-Wesley Professional Computing Series, New York, NY.

Vermeulen, J. (2018). *Huge data breach discovered with South African websites listed – Report*. [online] Mybroadband.co.za. Available at:

https://mybroadband.co.za/news/security/250443-huge-data-breach-discovered-with-south-african-websites-listed-report.html.

Wassermann.G and Su.Z (2007).Sound and Precise Analysis of Web Applications for Injection Vulnerabilities. In Proceedings of the ACM SIGPLAN 2007 Conference on Programming Language Design and Implementation, San Diego, CA, USA, ACM. https://doi.org/10.1145/1250734.1250739

Weinberger.J, Saxena.P, Akhawe.D, Finifter.M, Shin.R, and Song.D(2011). An Empirical Analysis of XSS Sanitization inWeb Application Frameworks. Technical report, UC Berkeley. https://doi.org/10.1007/978-3-642-23822-2_9

Zaher Al Shebli, H. and Beheshti, B. (2018). A Study on Penetration Testing Process and Tools. *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 17842208. https://doi.org/10.1109/LISAT.2018.8378035