International Journal of Innovative Trends In Engineering
Issue 110, Volume 74, Number 02, February 2022
e-ISSN: 2395-2946

Review Article

A Review of Vulnerable Script Code in Web Application

Meena Deshbhratar[1], Prof. Anurag Shrivastav[2]

[1]*M.Tech. Scholar, Department of Computer Science & Engineering NIIST, Bhopal, INDIA*
[2]*Research Guide, Department of Computer Science & Engineering NIIST, Bhopal, INDIA*

ABSTRACT

Network security is becoming a more important concern in people's everyday life. Since people cannot live without the Internet, it is important to have a good and safe environment for networking. It's become more important when an internet user increases day by day. Cross site scripting (XSS) does, however, attack millions of websites. It is also use XSS to include cruel scripting code into apps and then return it to the customer side. If users are using the web browser to visit the injecting place of the cruel script code, it is directly run on the customer machine. The key words of XSS are generally found in the JavaScript browser or on the server element to filter cruel code. Conversely it is complex to collect all keywords in the detecting-record in order to avoid XSS attack. Nevertheless, it is possible to create various forms of cruel scripting. It is also sensible for more people to work on XSS and find more ways to avoid XSS attacks. In this paper reviewed the defending techniques for a variety of types of attacks in web applications. Also have found which methods give better performance.

KEYWORDS

Network Security, Web Application, Attack, cross-site scripting (XSS), Classification, Extreme Learning Machine (ELM).

1. INTRODUCTION

World Wide Web (www) has turn into an unstoppable part of world and web-surfing is a significant activity for the users who have done online purchases and activity. In the last decade, the internet has seen a huge growth of the exchange of data by many means, regardless of their distance or location, by volume, nature and channel. The internet has become in exacting the core channel by which global businesses operate and are extremely successful in traditional marketing strategies. Nearly every organization today continues to expand beyond its borders; therefore, almost every human endeavor and creation takes on a critical role in the network worldwide. Web apps are one of the best ways to accomplish this vital online presence. Web applications are web technology computer programs for performing tasks on the Internet. Thus, the arrival of web applications and other smart devices such as smart phones, tablets and other mobile devices has changed the medium of communication and the exchange of information among platforms. With well-known and all-round existence of these internet applications, app developers are enforced to think again their growth strategies and determining their security issues to

avoid targeting hackers and web assailants who are decision inadequate coding practices on the internet daily to appropriate responsive information and achieve the often, with the number of web applications rising, there are vulnerabilities and a major point of discussion in various development and defense forums for web applications. Web applications usually allow sensitive customer data (such as personal details, credit card numbers and information from social security groups) to be collected, analyses, stored and distributed immediately and repeatedly [1].

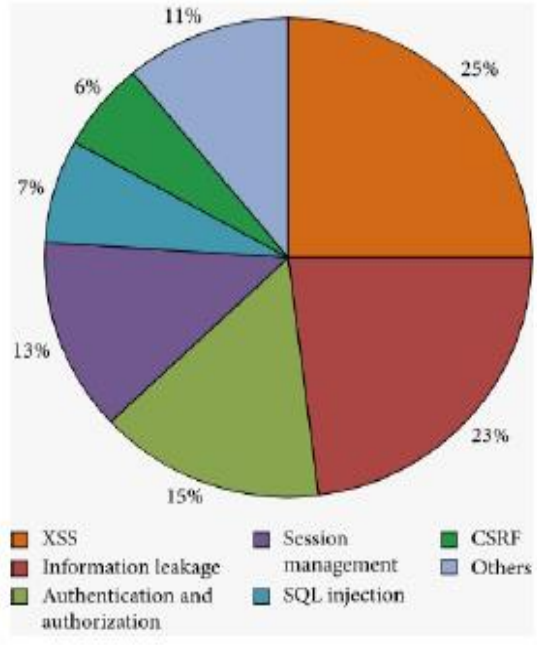


Figure 1.1 Centric Application Vulnerability Trend

Cross-site scripting is called cruel code addition in insecure web applications to trick users and redirect them to un-trusted websites (XSS)[1]. XSS can also arise when no failing is in the servers and database engine and is probably one of the most common web applications currently exposed which is shown in Figure 1.

HTML types, cookies, secret fields and get and post parameters are all input source exploited by attackers. Three parties the intruder and the customer are part of the ordinary procedure. In information security testing [2, 4], the majority of methods cantered on preventing XSS attacks in web applications. There have been few research activities on its detection [5, 6].

The rest of paper is organized as follows: In section II we review the work-related web security. In section IV we describe the proposed framework for system. Section V gives expected result of the framework and finally sections VI conclude this paper.

2. LITERATURE SURVEY

With the rapid growth of internet, Web applications and products increasingly targeted by attackers using malware as they are easier to infect than conventional network and computers system. This is due to several reasons [2] such as presence of legacy devices with no security updates, low priority given to security within the development cycle, weak login credentials, etc. This research aims to find an effective solution to security issues faced by the network environment of Internet. This research will be used to develop a security defending system that can detect complex and changeable attacks, and can intelligently cope with sudden intrusions. Many researchers previously work on the security system using extreme machine learning algorithms.

Navdeep Kaur and Parminder Kaur [7] give a detailed study on input validation vulnerabilities in different web applications that are in real time environment. The authors provide a complete study on cross site scripting attacks in input validation with type of methods to eliminate the situation. According to their study, the problem can be disinfectant during the life cycle phase itself. Hence, vulnerability can be eliminated at larger cost.

Isatou Hydara et al [8] make a detailed study on state of art in cross site scripts with a systematic literature review. Different types of applications are intended for the study by the authors that concentrates on how and where the scripting vulnerabilities or attacks taken place. From their review results dynamic query generation avoids the scripting attacks more rather than static dimensions. Scripting attacks cannot be mitigating with the aid of single solution. The nonexistence of vulnerabilities will foil attacks from happening and keep wealth.

Steven Van Acker et.al [9] discusses on automatic discovery of scripting in web applications with a system names" Flashover". It is a combined structure of both static and dynamic code analysis with no forged positives in the query. The outcome shows that important numbers of high valued web applications are vulnerable to cross site scripting attacks, can be eliminated by using the flash over methodology.

Arputharaj Kannan [11] A self-aware message analysis and validation algorithm was given for detecting and providing from various scripting attacks in the real web applications. It receives request and supply responses together with specific query for input validation. A filtering policy is applied for the purpose of validating the user input query.

Chavan B, have explain in [15] the classification of the attacks and value that can change website, its data and its users. These vulnerabilities are classified with respect to the phase of the growth life cycle in which they happen [15].

Author [17] has presented research view of cross site scripting (XSS) molest and its obstacle in web applications. They have verified various types of XSS attacks and also the easing techniques for it. It has been famous that preventing XSS attack is very complicated task and shield techniques also desired to be simplified.

The Author [19] namely Duff, N. have presented in their study to the Cross Site Scripting attacks. Current security methods are discussed, which shows that a web developer should adopt secure programming practices in order to develop a safe web application.

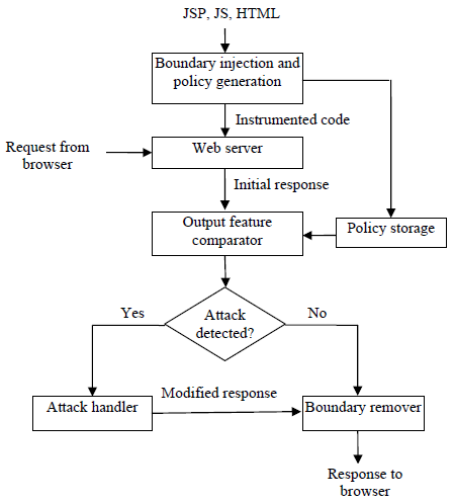
3. THEORY OF XSS

In a typical XSS attack the hacker infects a legitimate web page with his malicious client-side script. When a user visits this web page the script is downloaded to his browser and executed. There are many slight variations to this theme, however all XSS attacks follow this pattern.

An attacker makes changes to web pages, attacker must first break the security of the web server and be able to upload and modify files on that server. Unfortunately, an XSS attack is much easier than that. Internet applications today are not static HTML pages. They are dynamic and filled with ever changing content. Modern web pages pull data from many different sources.

4. PROPOSED FRAMEWORK

The framework for the proposed work is explored. In this framework web-based security defending technique are proposed.



In this research work propose a safe browser plug-in with its integral support for JavaScript explanation. This proposed work implemented the interpreter to distinguish the client-side JavaScript base attacks so that the browser will not perform the insecure statements thereby defending the user protection from receiving compromised. The proposed protected browser will be able to identify a variety of JavaScript based attacks and will not let them perform on client region. The interpreter will restrain signatures of most of the eminent attacks, and it will spend regular expressions for finding the presence of any malicious JavaScript code in the recent webpage.

5. EXPECTED RESULT

The Extreme Learning Machine (ELM) is implemented by using MATLAB. Here the ELM is used to classify the malicious web page. There are two algorithms are used for classification such as Basic-ELM and ELM-Kernel finally the result is compared based on the four criteria like Training Time, Testing Time, Training Accuracy and Testing Accuracy.

6. CONCLUSION

This paper surveyed the attack detection techniques in brief and various methods algorithms are used in security system are discussed. In this work proposed the attack detection framework which is useful for the network security purpose in the web application. Extreme Learning Machine (ELM) is gives better performance in various parameters.

REFERENCES

[1]. NavdeepKaur and ParminderKaur," Input Validation Vulnerabilities in Web Applications", in Journal of Software Engineering, Vol 8, Issue 3, 2014, pp:116 – 126. https://scialert.net/abstract/?doi=jse.2014.116.126

[2]. IsatouHydara, Abu Bakar Md. Sultan, HazuraZulzalil, and NoviaAdmodisastro, "Current state of research on cross-site scripting (XSS) – A systematic literature review", in Information and Software Technology, Vol. 58, 2015, pp: 170–186. https://www.infona.pl/resource/bwmeta1.element.elsevier-60e13622-2c41-3dc5-87a6-28f04fa537c6

[3]. Steven Van Acker, Nick Nikiforakis, LievenDesmet, WouterJoosen, Frank Piessens, "FlashOver: Automated Discovery of Cross-site Scripting Vulnerabilities in Rich Internet Applications", in ASIACCS '12, May 2–4, 2012, Seoul,Korea. https://www.securitee.org/files/flashover_asiaccs2012.pdf

[4]. Juillerat,N., Enforcing Code Security in Database Web Applications using Libraries and Object Models, LCSD 2007,Canada, ACM 1-58113-000-0/00/004. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.214.7279&rep=rep1&type=pdf

[5]. Shalini, S. and Usha S., Prevention of Cross-Site Scripting attacks (XSS) on Web Applications in the Client Side, International Journal of Computer Science Issues, Volume 8, Issue4, No.1, 2011. https://www.ijcsi.org/papers/IJCSI-8-4-1-650-654.pdf

[6]. Weinberger, J. , Saxena, P. , Akhawe, D., Finifer,M., Shin,R. and Song,D., A Systemmatic Analysis of XSS Sanitization in Web Application Frameworks,ESORICS 2011 http://webblaze.cs.berkeley.edu/papers/empirical-webfwks.pdf

[7]. Lomte, R.M and Bhura, S.A., Survey of different Web Application Attacks & Its Preventive Measures, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 14, Issue 5. ISSN: 2278-8727 https://www.iosrjournals.org/iosr-jce/papers/Vol14-issue5/D01454651.pdf

[8]. Chavan, S.B and Meshram,B.B., Classification of Web Application Vulnerabilities, International Journal of Engineering Science and Innovative Technology (IJESIT),Volume 2, issue 2, 2013. http://www.ijesit.com/Volume%202/Issue%202/IJESIT201302_35.pdf

[9]. Garg, A. and Singh, S., A Review on Web application Security Vulnerabilities, International Journal oF Advance Research in Computer Science and Software Engineering, Volume 3, Issue1, 2013. https://pdfcoffee.com/web-application-security-vulnerabilities-pdf-free.html

[10]. S.A. Gadhiya, K.H. Wandra, The Research Perspective:XSS Attack and Prevention of XSS Vulnerability in Web Application, International Journal of Engineering Development and Research, volume2, Issue 4. ISSN: 2321-9939. https://www.ijedr.org/viewfull.php?&p_id=IJEDR1404058

[11]. Singh, A. and Sthappan,S. , A survey on XSS web-attack and Defence Mechanisms, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 4, Issue 3, 2014. ISSN:2277 128X

[12]. Kaur G., Study of Cross-Site Scripting Attacks and their Countermeasures, International Journal of Computer Applications Technology and research, Volume 3, Issue 10, 2014. ISSN:2319-8656 https://ijcat.com/archives/volume3/volume3issue10.pdf

[13]. Mukesh Gupta, Mahesh Govil, Girdhari Singh. "Predicting Cross-Site Scripting (XSS) Security Vulnerabilities in Web Applications", Malviya National Institute of Technology, IJCSSE, 2015. https://ieeexplore.ieee.org/document/7219789/authors#authors

[14]. AnkitShrivastava, SantoshChoudhary, Ashish Kumar. "XSS Vulnerability Assessment and Prevention in Web Application", Manipal University Jaipur, INGCT, 2016. https://ieeexplore.ieee.org/abstract/document/7877529

[15]. Samer Attallah Mhana; Jamilah Binti Din; Rodziah Binti Atan "Automatic Generation of Content Security Policy to Mitigate Cross Site Scripting", Universiti Putra Malaysia Serdang, ICSITech, 2016. https://ieeexplore.ieee.org/document/7852656/metrics#metrics

[16]. Punam Thopate, PurvaBamm, SnehalKunjir. "Cross Site Scripting Attack Detection & Prevention System", IJARCET, Vol 3 Issue 11, 2014. http://ijarcet.org/wp-content/uploads/IJARCET-VOL-3-ISSUE-11-4035-4039.pdf

[17]. Mohit Dayal Ambedkar; Nanhay Singh Ambedkar; Ram Shringar Raw "A Comprehensive Inspection Of Cross Site Scripting Attack", Institute of Advanced Communication Technologies and Research, New Delhi, ICCCA, 2016. https://ieeexplore.ieee.org/document/7813770

[18]. http://www.acunetix.com/websitesecurity/cross-site-scripting/

[19]. "Program Slicing Stored XSS Bugs in Web Application", by Yi Wang, Zhoujun Li and Tao Guo, Beijing, China, IEEE, 2011. https://www.computer.org/csdl/proceedings-article/tase/2011/4506a191/12OmNyTfg7b

[20]. Matthew Van Gundy and Hao Chen, "Noncespaces: Using randomization to defeat cross-site scripting attacks", in

computers & security, Vol.31, 2012, pp: 612 – 628. https://dl.acm.org/doi/10.1016/j.cose.2011.12.004

[21]. Debasish Das, Utpal Sharma and D.K. Bhattacharyya, "Detection of Cross-Site Scripting Attack under Multiple Scenarios", in The British Computer Society 2013, Volume 58, Issue 4, April 2015 https://academic-oup com.eres.qnl.qa/comjnl/article/58/4/808/335989?login=true