Review Article

ACCENTS Transactions on Information Security, Vol 4(15)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2019.414001

Computation analysis and review based on cross-site scripting attack

Manish Agrawal[1*], Kailash Patidar[2], Rishi Kushwah[3] and Sudesh Chouhan[3]
M.Tech Scholar, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[1]
Professor and HOD, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[2]
Assistant Professor, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[3]

Abstract
In cross site scripting (XSS) attacks malicious scripts are inserted in the web files for accessing the information or degrade the performance of the website. Now day's hackers are prominently using the scripts for malfunction scripting. In this paper a study has been presented for the prevention and detection of XSS attacks. This study provides a detail exploration of the methods used for detection, their impact and problem identification. It provides a systematic review for the exploration of the good methods in the direction of better detection of XSS attacks. Based on the analysis some future suggestions have been suggested.

Keywords
XSS, SQL injection attack, attack detection, PHP, J2EE, JSP.

1.Introduction
The security directions in different arena are increasing and the security standards have been increased in several aspects. But the vulnerabilities are also increasing with different style. In terms of web application cross-site scripting (XSS) attack is the most common attack type [1−5]. In different application JavaScript and PHP framework have been used. The client-side code has generally embedded in HTML pages. The complexity and the security increase parallel in the way that it allow the vulnerabilities also. It follows the different mechanism to adopt and prevent the vulnerabilities in different possible way. XSS are a security issue that occurs in web applications. Different customers with different intensions can achieve SQL Injection strike in the unmistakable course in the web world [6−9]. The disobedient and most skillfully threating strike is SQL Injection alteration. In this Modify the hawkish supporting completions the affirmation, by sincere register with segments, for the course of action for of permit in-help and to execute self-self-assured code [10].

*Author for correspondence

As to four frameworks and estimation are proposed in [11, 12], yet there is need of progress in the said field. The main objective of this paper is to computationally analysis and review based on cross-site scripting attack.

2.Literature review
In 2018, Madhusudhan and Shashidhara [15] discussed about cross channel scripting (XCS). They have suggested this as the dangerous web application vulnerability. They have suggested that it is performed through network protocols. It is the variant of XSS. They have analyzed and discussed XCS attack in detail prospective.

In 2018, Kaur et al. [16] suggested an offline and online based model for the malicious XSS attack detection on in online social network. They have tested their approach on five online social network for the XSS attack. Their result shows the little false positives and promising attack vulnerability detection.

In 2018, Bukhari et al. [17] discussed the malicious functions. They have suggested XSS as the client-side code injection attack. They have focused on type

1 or “nonpersistent cross-site scripting”. With non-determined cross-site scripting, malevolent code or content is inserted in a web demand, and after that in part or totally reverberated (or "reflected") by the web server without encoding or approval in the web reaction. The noxious code or content is then executed in the customer's web program which could prompt a few negative results. All together for this sort of cross-site scripting to be effective, a malevolent client must force a client into clicking a connection that triggers the non-tenacious cross-site scripting attack.

In 2018, Marashdih et al. [18] discussed web applications based on data and conducting service. They have suggested the PHP for the common framework for the web applications. Now a day’s security concern is the major issue. They have suggested that XSS vulnerability is common in PHP framework. They have suggested that because of the several applications and tools the security is now increase but there are several vulnerabilities remain s unfelt. They have discussed the PHP aspects their popularity variants with the applications.

In 2018, Algaith et al. [19] discussed the use of Static Analysis Tools (SATs) for the vulnerability. They have suggested that the use of several tools may be helpful in increasing the detection capabilities. But they have suggested that it may increase the false alarms number. So they have discussed the combination of SATs for the better suitability. They have analyzed the results based on five diverse SATs to find two types of vulnerabilities these are SQL Injections (SQLi) and XS. For this they have considerd132 plugins of the WordPress content management system (CMS). Based on their approach they have suggested empirically supported guidance based on SAT tools to achieve the low false positive rates.

In 2018, Chen et al. [20] discussed about the root cause of XSS attack. As it is difficult to identify the correct JavaScript code and the JavaScript code injected by attackers by the JavaScript engine. They have discussed about the moving target defense (MTD). It is a novel technique to defeat attacks by frequently changing the system configuration. This paper portrays the structure and actualize of a XSS resistance technique dependent on MTD innovation. This strategy adds an irregular credit to each risky component in web application to recognize the javascript code in web application and the JavaScript code infused by aggressors and utilizations a security check capacity to confirm the irregular quality, if there is no arbitrary characteristic or the irregular property value is not correct in a HTML. Their results show that the method can effectively prevent XSS attacks.

In 2018, Ruohonen [21] discussed and examines software vulnerabilities in common Python packages used particularly for web development. Their dataset is basically on the base of PyPI package repository and the so-called Safety DB used to track vulnerabilities in selected packages within the repository. Their result suggest that the vulnerabilities in general is modestly severe and XSS type.

3.Gap analysis

The following gaps have been identified based on the study and analysis of the above literature.

1) Different hybrid combination of standard encryption and decryption techniques are missing to prevent the attacks.
2) Scripts missing the tokenization partitioning mechanism.
3) The alpha numeric combination is missing for checking the attack mechanism.
4) The combination of different data type is missing, maximum supports text based attack detection mechanism.
5) Efficient mechanism which can detect it in timely manner is also missing.

4.Findings

The methodological findings are shown in table 1. It shows the methodological advantages, the combination used with their impacts and gap findings.

Table 1 Comparative analysis

S.No	Reference	Approach	Results	Gaps
1	[22]	Cross Site Scripting: Detection	They have highlighted the security and vulnerability issues in web application specifically in regards to XSS.	They have suggested that the future work should include the expulsion phase of the infeasible ways from the control stream to identify all XSS vulnerability from the source code.

S.No	Reference	Approach	Results	Gaps
2	[23]	Countering Cross-Site Scripting	The most common vulnerability is XSS and one of the open web application security project (OWASP) best ten web-dangers. XSS happens when an electronic application permits untrusted data be acknowledged and sent back to a program. Additionally they can execute scripts inside a program that can mutilate sites, divert clients to vindictive substance and commandeer programs. One purpose behind this issue was the absence of engineers understanding the reasons for XSS. They have tended to the reasons for XSS and countermeasures to resistance against these dangers.	Practical implications are missing.
3	[24]	Defending against web vulnerabilities and cross-site scripting	Security analysts can address these shortcomings from two alternate points of view. They have to look past current methods by consolidating more compelling info approval and sterilization highlights. In time, advancement devices will fuse security structures, for example, ESAPI that actualize best in class innovation. They have highlighted concentrate on program check point of view, how analysts must incorporate program examination, design acknowledgment, concolic testing, information mining, and AI calculations to tackle distinctive programming building issues and to upgrade the adequacy of weakness location.	They have suggested that in future it can be used as the integrate program analysis, pattern recognition, concolic testing, data mining, and AI algorithms would be used rigorously to solve different software engineering problems to improve the effectiveness of vulnerability detection. They can likewise enhance the exactness of current techniques by picking up assault code designs from outside specialists.
4	[25]	Identifying cross-site scripting attacks based on URL analysis	They have presented an approach to recognize Cross-Site Scripting assaults in light of URL examination. The essential supposition of our technique is that the URL contains a section that can create a legitimate JavaScript punctuation tree. To start with, we extricate the parameters of the URL to deliver a substantial JavaScript sentence structure tree and weight its parsing profundity. On the off chance that its profundity surpasses a client characterized edge, the URL is viewed as suspicious. Second, to the special case URLs, a moment level of resistance is framed by breaking down its structure. The trial comes about exhibit that our approach can adequately recognize the vast majority of the noxious URLs from the kind ones.	How many pages are considered and considering all the pages may be time consuming.
5	[26]	Tracing out cross site scripting vulnerabilities	At the point when weakness is hindered, the assailant follows out an alternate component to adventure it.	Prevention mechanisms are missing.

S.No	Reference	Approach	Results	Gaps
			XSS assault is likewise a misuse of one of the vulnerabilities existing in the web applications. They have highlighted the weakness in capacities and ascribe of present day scripts to complete cross site scripting assault and recommends preventive measures.	
6	[27]	Detection and Prevention of Cross Site Scripting Attacks	They have suggested that 80% of the web applications are defenceless against security dangers, as in light of the study directed by OWASP. This is every now and again found inside pages with dynamic substance and it carryout distinctive vindictive operations like capturing client sessions, destroys sites, divert the client to malevolent destinations, secret key robbery and so on. In first stage, client given URL is separated and tried for defencelessness utilizing concolic testing approach.	They have suggested that in the future attack estimation of all individual processes to set the threshold value dynamically may be analysed. This System can be enhanced by making utilization of the client contribution with more information which are to be recently created with the cheat sheet. One inadequacy of the present framework is that occasionally permits the infused inquiry in which are absent in the database. This can be enhanced by including the refreshed cheat sheet information in the approval part with powerfully in future.
7	[28]	Cross-site scripting attacks procedure and prevention strategies	Cross-site scripting assaults and barrier has been the site of assault and guard is a critical issue. As per the present comprehension of the tumult on the crosssite scripting, breaks down the causes and damage cross-website scripting assaults arrangement of assaults XXS finish handle XSS assaults made a complete examination, and afterward for the web program incorporates Mobility there are cross-webpage scripting channel laxity given from normal clients peruse the web and web application designers two the resistance. Cross-site scripting attacks effective strategy.	Practical implementations are missing.
8	[29]	Study of cross-site scripting attacks and their countermeasures	The assailants may take profit of these vulnerabilities and can abuse the information in the database. Think about demonstrates that over 80% of the web applications are powerless against XSS assaults. XSS is one of the lethal assaults and it has been honed over the most extreme number of understood web crawlers and social destinations. XSS assaults, its sorts and distinctive strategies utilized to oppose these assaults with their relating constraints.	Practical implementations are missing.
9	[30]	Approach for cross-site scripting detection and removal based on genetic algorithms	They proposed to explore an approach based on genetic algorithms that will have the capacity to distinguish and expel cross-site scripting vulnerabilities from the source code before an application is conveyed.	Different combinations of algorithm can be applied to check the effectiveness of the approach.
10	[31]	Cross-site scripting	In XSS assault, the aggressor runs	Practical implementations are

S.No	Reference	Approach	Results	Gaps
		attack in Android apps	noxious code in the WebView part of casualties Smartphone. Along these lines, WebView is a fundamental segment in both Android and iOS telephones. It empowers the application to show the substance of online assets on telephone. So They have examined the XSS assault, break down their fundamental causes and concentrate on potential arrangements	missing.

5.Conclusion and future suggestions

This paper explores the possibility of different aspects of detection and prevention of XSS attacks. It provides an explanatory approach for the elaboration of the previous related works. It highlighted the methods used, approach, results and the gaps in the previous literature. Based on the previous work it is suggested that there is a need of a framework which can efficiently handle the detection as soon as it is scripted and better prevention mechanism will apply for preventing it by the hybridization of standard encryption techniques.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Shahriar H, Zulkernine M. S2XS2: a server side approach to automatically detect XSS attacks. In international conference on dependable, autonomic and secure computing 2011 (pp. 7-14). IEEE.

[2] Conteh NY, Schmick PJ. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research. 2016; 6(23):31-8.

[3] Manimaran A, Durairaj M. The conjectural framework for detecting DDoS attack using enhanced entropy based threshold technique (EEB-TT) in cloud environment. International Journal of Advanced Computer Research. 2016; 6(27):230-7.

[4] Gupta S. Secure and automated communication in client and server environment. International Journal of Advanced Computer Research. 2013; 3(4):263-71.

[5] Shrivastava A, Choudhary S, Kumar A. XSS vulnerability assessment and prevention in web application. In international conference on next generation computing technologies 2016 (pp. 850-3). IEEE.

[6] Shar LK, Tan HB. Defending against cross-site scripting attacks. Computer. 2011; 45(3):55-62.

[7] Dubey A, Gupta R, Chandel GS. An efficient partition technique to reduce the attack detection time with web based text and PDF files. International Journal of Advanced Computer Research. 2013; 3(1):9.

[8] Kiani M, Clark A, Mohay G. Evaluation of anomaly based character distribution models in the detection of SQL injection attacks. In international conference on availability, reliability and security 2008 (pp. 47-55). IEEE.

[9] Shukla N. Data mining based result analysis of document fraud detection. International Journal of Advanced Technology and Engineering Exploration (IJATEE). 2014; 1(1):21-5.

[10] Qadri SI, Pandey K. Tag based client side detection of content sniffing attacks with file encryption and file splitter technique. International Journal of Advanced Computer Research. 2012; 2(3):215-21.

[11] Thakur BS, Chaudhary S. Content sniffing attack detection in client and server side: a survey. International Journal of Advanced Computer Research. 2013; 3(2):7-10.

[12] Valeur F, Mutz D, Vigna G. A learning-based approach to the detection of SQL attacks. In international conference on detection of intrusions and malware, and vulnerability assessment 2005 (pp. 123-140). Springer Berlin Heidelberg.

[13] Ezumalai R, Aghila G. Combinatorial approach for preventing SQL injection attacks. In international conference on advance computing 2009 (pp. 1212-7). IEEE.

[14] Junjin M. An approach for SQL injection vulnerability detection. In international conference on information technology: new generations 2009 (pp. 1411-4). IEEE.

[15] Madhusudhan R, Shashidhara. Cross channel scripting (XCS) attacks in web applications: detection and mitigation approaches. In cyber security in networking conference 2018 (pp. 1-3). IEEE.

[16] Kaur G, Pande B, Bhardwaj A, Bhagat G, Gupta S. Defense against HTML5 XSS attack vectors: a nested context-aware sanitization technique. In international conference on cloud computing, data science & engineering 2018 (pp. 442-6). IEEE.

[17] Bukhari SN, Dar MA, Iqbal U. Reducing attack surface corresponding to type 1 cross-site scripting attacks using secure development life cycle practices. In international conference on advances in electrical, electronics, information, communication and bio-informatics 2018 (pp. 1-4). IEEE.

[18] Marashdih AW, Zaaba ZF, Suwais K. Cross site scripting: investigations in PHP web application. In

international conference on promising electronic technologies 2018 (pp. 25-30). IEEE.

[19] Algaith A, Nunes P, Jose F, Gashi I, Vieira M. Finding SQL injection and cross site scripting vulnerabilities with diverse static analysis tools. In European dependable computing conference 2018 (pp. 57-64). IEEE.

[20] Chen P, Yu H, Zhao M, Wang J. Research and implementation of cross-site scripting defense method based on moving target defense technology. In international conference on systems and informatics 2018 (pp. 818-22). IEEE.

[21] Ruohonen J. An empirical analysis of vulnerabilities in python packages for web applications. In international workshop on empirical software engineering in practice 2018 (pp. 25-30). IEEE.

[22] Marashdih AW, Zaaba ZF. Cross Site Scripting: Detection Approaches in Web Application. International Journal of Advanced Computer Science & Applications. 2016; 1(7):155-60.

[23] Ray LL. Countering cross-site scripting in web-based applications. International Journal of Strategic Information Technology and Applications. 2015; 6(1):57-68.

[24] Rao TV. Defending against web vulnerabilities and cross-site scripting. Journal of Global Research in Computer Science. 2012; 3(5):61-4.

[25] Tang Z, Zheng N, Xu M. Identifying cross-site scripting attacks based on URL Analysis. International Journal of Engineering and Manufacturing. 2012; 2(5):52.

[26] Kour H, Sharma LS. Tracing out cross site scripting vulnerabilities in modern scripts. International Journal of Advanced Networking and Applications. 2016; 7(5):2862.

[27] Duraisamy A, Subramaniam M. Detection and prevention of cross site scripting attacks using concolic testing and pattern filtering approach in web application. Australian Journal of Basic and Applied Sciences. 2016; 10(18): 66-73.

[28] Wang X, Zhang W. Cross-site scripting attacks procedure and prevention strategies. In MATEC web of conferences 2016 (p. 03001). EDP Sciences.

[29] Kaur G. Study of cross-site scripting attacks and their countermeasures. International Journal of Computer Applications Technology and Research. 2014; 3(10):604-9.

[30] Hydara I, Sultan AB, Zulzalil H, Admodisastro N. An approach for cross-site scripting detection and removal based on genetic algorithms. In the international conference on software engineering advances 2014.

[31] Sedol S, Johari R. Survey of cross-site scripting attack in android apps. International Journal of Information & Computation Technology. 2014; 4(11):1079-84.