ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

A Critical Review on Detecting Cross-Site Scripting Vulnerability

Ankita Shrivastava[1], Anil Rao[2]

M.Tech (Information Technology), Institute of Engineering & Technology, Alwar, Rajasthan Technical University, Kota Raj, India[1]

Assistant Professor, Institute of Engineering &Technology, Alwar, Rajasthan Technical University, Kota Raj, India[2]

ABSTRACT: The world relies on internet today. We can analyze it in several ways , if you consider the example of money transfer then there are several ways of transferring the money using world wide web, Social Sites and communities like Facebook, Twitter and LinkedIn, mail services etc. and all these services are rely on web browsers. Then the communication is provided by different protocols via web browsers. So security breaches and attacker can attack in the communication media for taking the advantage of misguiding or data hacking. Our paper main aim is to study different cross site scripting detection techniques and analyzes the loop holes so that in future the loops can be fulfilled for the better security.

KEYWORDS: Cross site scripting, Security breach, server and client communication, web browsers

1. INTRODUCTION

The client server environment can be better set by Tomcat apache server and it is used with Java Netbeans and the pages are designed through JSP [1]. The communication can be provided by using servlet in java. But the servlet code is cryptic so that JSP codes are embedded for this purpose.

The most of the attack can be possible in the trend of browser communication. SQL Injection attacks are also possible in this scenario because the malicious data can be added through the Query by the unauthorized users.
For Example we can consider a form in the below manner:

```
<form action="User Entry">
        <input type="text" name="user" value=""/>
        <input type="submit" value="Submit"/>
 </form>
```

Then it all depend on the select query that how we will apply on that to retrieve the better contents. Content sniffing attacks are also possible where content stealing or misleading will be added in the client side. Another type of vulnerabilities is cross-site scripting (XSS) attack [3, 4]. In this the attacker breaches the original policy or protocol applied form the origin. So this type of attack vulnerability provides more bad effects as the sensitivity of data increases or decreases. XSS is used to allow attackers to execute script in the victim's browser, which can hijack user sessions, deface web sites, insert hostile content, and conduct phishing attacks. Any scripting language supported by the victim□s browser can also be a potential target for this attack. Web based applications are accessed using Web based communication protocols and use Web browsers as graphical user interface. The most dangerous threat is alteration of the data in text, pdf files and images contents which is called content sniffing attack[5][6][7]. In this type of attach the data will be received by the client but the data is not correct or updated by the attacker.

To customize back plasticity in the HTML song and to digest round-trip delays, browsers offered the choice to encompass program pandect into the HTML permit depart is present and flawless on the catch by an interpreter integrated into the

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

browser [8]. Java Script code may not be mixed up with Java Server Pages (JSP); JSP code is executed at the server side and not at the client browser [9][10]. The Java Applets is an option purchaser combine technology cruise allows the download and conduct of Java applications to and at the client machine. The java Applets average does quite a distance right away manipulate the browser or HTML document [11].

The remaining of this paper is organized as follows. The related work in section 2. In section 3 we discuss about problem domain. In section 4 we discuss the analysis. The conclusions and future directions are given in Section 5. Finally references are given.

II. RELATED WORK

In 2010, Zubair M. Fadlullah et al. [12] to combat against attacks on encrypted protocols; they propose an anomaly-based detection system by using strategically distributed monitoring stubs (MSs). They have categorized various attacks against cryptographic protocols. The MSs, by sniffing the encrypted traffic, extract features for detecting these attacks and construct normal usage behavior profiles. Upon detecting suspicious activities due to the deviations from these normal profiles, the MSs notify the victim servers, which may then take necessary actions. In addition to detecting attacks, the MSs can also trace back the originating network of the attack. They call their unique approach DTRAB since it focuses on both Detection and TRAceBack in the MS level. The effectiveness of their proposed detection and traceback methods are verified through extensive simulations and Internet datasets.

In 2011, Misganaw Tadesse Gebre et al. [13] proposed a server-side ingress filter that aims to protect vulnerable browsers which may treat non-HTML files as HTML files. Their filter examines user uploaded files against a set of potentially dangerous HTML elements (a set of regular expressions). The results of their experiment show that the proposed automata-based scheme is highly efficient and more accurate than existing signature-based approach.

In 2011, Anton Barua et al. [7] developing a server side content sniffing attack detection mechanism based on content analysis using HTML and JavaScript parsers and simulation of browser behavior via mock download tests. They have implemented our approach in a tool that can be integrated in web applications written in various languages. In addition, they have developed a benchmark suite for the evaluation purpose that contains both benign and malicious files. They have evaluated their approach on three real world PHP programs suffering from content sniffing vulnerabilities. The evaluation results indicate that their approach can secure programs against content sniffing attacks by successfully preventing the uploading of malicious files.

In 2012, Takeshi Matsudat et al. [14] proposed a new detection algorithm against cross site scripting attacks by extracting an attack feature of cross site scripting attacks considering the appearance position and frequency of symbols. Their proposed algorithm learns the attack features from given attack samples. They prepared samples for learning and testing, to show the effectiveness of their proposed algorithm. As the result their proposed detection method was successfully detected attack test samples and normal test samples.

In 2012, Fokko Beekhof et al. [15] consider the problem of content identification and authentication based on digital content fingerprinting. They investigate the information theoretic performance under informed attacks. In the case of binary content fingerprinting, in a blind attack, a probe is produced at random independently from the fingerprints of the original contents. Contrarily, informed attacks assume that the attacker might have some information about the original content and is thus able to produce a counterfeit probe that is related to an authentic fingerprint corresponding to an original item, thus leading to an increased probability of false acceptance. They demonstrate the impact of the ability of an attacker to create counterfeit items whose fingerprints are related to fingerprints of authentic items, and consider the influence of the length of the fingerprint on the performance of finite length systems. Finally, the information-theoretic achieveble rate of content identification systems sustaining informed attacks is derived under asymptotic assumptions about the fingerprint length.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

In 2012, Dawei Wang et al. [16] suggest Payload-based approaches are effective to known DOS attacks but are unable to be deployed on high-speed networks. To address this issue, flow-based DOS detection schemes have been proposed for high-speed networks as an effective supplement of payload-based solutions. Author suggest that the existing flow-based solutions have serious limitations in detecting unknown attacks and efficiently identifying real attack flows buried in the background traffic. In addition, existing solutions also have difficulty to adapt to attack dynamics. To address these issues, they propose a flow-based DOS detection scheme based on Artificial Immune systems. They adopt a tree structure to store flow information such that we can effectively extract useful features from flow information for better detecting DoS attacks. They employ Neighborhood Negative Selection (NNS) as the detection algorithm to detect unknown DoS attacks, and identify attack flows from massive traffic. Because the strong tolerance of NNS, the proposed solution is able to quickly adapt attack dynamics.

In 2013, Nagarjun, P.M.D. et al. [17] propose variants of RTS/CTS attacks in wireless networks. We simulate the attacks behavior in ns2 simulation environment to demonstrate the attack feasibility as well as potential negative impact of these attacks on 802.11 based networks. They have created an application that has the capability to create test bed environment for the attacks, perform RTS/CTS attacks and generate suitable graphs to analyze the attack's behavior. They also briefly discuss possible ways of detecting and mitigating such Low rate DoS attacks in wireless networks.

In 2013, Animesh Dubey et al. [6] propose an efficient partition technique for web based files (jsp, html, php), text (word, text files) and PDF files. They are working in the direction of attack time detection. For this motivation they are considering mainly two factors first in the direction of minimizing the time, second in the direction of file support. For minimizing the time we use partitioning method. They also apply partitioning method on PDF files. There result comparison with the traditional technique shows the effectiveness of their approach.

In 2013, Seungoh Choi et al. [18] prove that Interest flooding attack can be applied for Denial of Service (Dos) in Content Centric Network (CCN) based on the simulation results which can affect quality of service. They expect that it contributes to give a security issue about potential threats of DoS in CCN.

In 2013, Michelle E Ruse et al. [19] propose a two-phase technique to detect XSS vulnerabilities and prevent XSS attacks. In the first phase, they translate the Web application to a language for which recently
developed concolic testing tools are available. Their translation also identifies input and output variables that are used to generate test cases for determining input/output dependencies in the application. Dependencies indicate vulnerabilities in the application that can be potentially exploited when the
application is deployed. In the second phase, based on the input/output dependencies determined in the first phase, they automatically instrument the application code by including monitors. The monitors check exploitation of vulnerabilities at runtime. In addition to being both as efficient and effective as the available XSS attack detection techniques, their two-phase method is also capable of identifying XSS vulnerabilities that occur due to (a) conditional copy (of inputs to outputs) and (b) construction of malicious string inputs from the concatenation of singularly benign inputs.

III. PROBLEM DOMAIN

After discussing several research works we can come with some problem area in the traditional approaches which are following:

1) We can adopt several encryption techniques like RSA, RC4 etc. for protecting the data when the data will be send to the client environment [20].
2) We can work in the direction of different JPEG images and Flash also.
3) Missing of automated identification of file upload procedures in web applications and auto response [21][22].
4) Position and frequency based testing with simple visualization tracking is also missing.
5) Association, partitioning and clustering techniques can be used for reducing the time in the case of file preparation [23].

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

6) Blocking facility can be provided if the data is altered by any unauthorized user. So that the other misleader functionalities will be prevented in the authorized area and auto correction from the server can be provided. It will provide a better attack prevention.
7) Hybrid encryption techniques are allowed as the file formats are different, so it will be better to allow different encryption techniques based on the file format.

Table 1: Problem Analysis

S.NO	SOURCE	TECHNIUE USED	ADVANTAGES	MISSING/SUGGESTIONS
1	[7]	Their approach intercepts a suspected file upload request at the server side, obtains the file to be uploaded, and applies our framework to conclude whether the file is safe to be uploaded or not. They uses javascript for server side programming. They have evaluated theirapproach on three real world PHP programs suffering from content sniffing Vulnerabilities.	Their results indicate that their approach can secure programs against content sniffing attacks by successfully preventing the uploading of malicious files.	1) Automated Integration. 2) Overhead Reduction 3) Suggest some other file formats.
2	[6]	They proposed an efficient partition technique for web based files (jsp, html, php), text (word, text files) and PDF files. They are working in the direction of attack time detection. For this motivation they are considering mainly two factors first in the direction of minimizing the time, second in the direction of file support.	1) File Load can be handled properly. 2) Reducing the attack detection Time. 3) Splitting of PDF Files.	1) Automated integration. 2) Image Files are not considered. 3) Content Positions are not considered after attack.
3	[14]	They Proposed the algorithm of cross site scripting attacks detection considering the appearance position and frequency of characters including in an input strings.	Content Positions and frequency are considered in the case of XSS attack.	But if the attack is only simple visualization of file then the attack is not detected.
4	[15]	They demonstrate the impact of the ability of an attacker to	Their information-theoretic achievable	

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

		create counterfeit items whose fingerprints are related to fingerprints of authentic items, and consider the influence of the length of the fingerprint on the performance of finite-length systems.	rate of content identification systems sustaining informed attacks is derived under asymptotic assumptions about the fingerprint length.	
5	[18]	They explained how to make DoS by Interest flooding attack in CCN. We then showed that Interest flooding attack can cause the effect of DoS since the attack makes quality of services sufficiently degraded by discarding legitimate Interest from normal user due to PIT full.	The results showed that Interest flooding attack cannot be Ignored not only for a security issue but also for guarantee of quality of service in CCN.	Prevention methodologies are discussed.
6	[19]	They have presented a method for identifying XSS vulnerability and detecting their exploitation. Their technique relies on smart translation of Web applications, deploying a unit testing engine to detect vulnerabilities, and applying code instrumentation to monitor attacks that exploit those vulnerabilities.	They have shown that their technique is efficient and can easily identify conditional copy vulnerability.	They suggest that their work can be extended to detect and prevent different types of injection attacks in Web applications written in other languages. The overall objective is to develop a generic framework that allows grammar-based automatic translation of Web applications written in any language into intermediate test-language, as well as automatic instrumentation of Web applications based on the results of testing the test-language.

IV. ANALYSIS

After analysis of several research paper. We come with some result analysis by the authors working in the same field. Based on the assumptions we strongly suggest strong standard encryption techniques like Blowfish, AES, RC4 and content mapping can also be provided side by side. The types of storage format can also be extended from the previous research.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

V. CONCLUSION AND FUTURE DIRECTION

The previously described technique allows detecting and preventing different attacks in the web environment with server and client side programming. But an attacker finds a gap to bypass the protection mechanism adopted by us. So our paper provides the possible insights in these directions. In this paper we want to discover the possible attack scenario and possible remedies. We also discuss the present's techniques. In future we can design a framework based on better encryption techniques with mapping classifier enable mechanism accepting different file formats.

REFERENCES

[1] D. Flanagan. JavaScript: The Definitive Guide. December 2001. 4th Edition.
[2] ECMA-262, ECMAScript language specification, 1999.
[3] David Endler. The Evolution of Cross Site Scripting Attacks. Technical report, iDEFENSE Labs, 2002.
[4] CERT. Advisory CA-2000-02: malicious HTML tags embedded in client web requests.
[5] Syed Imran Ahmed Qadri, Prof. Kiran Pandey, "Tag Based Client Side Detection of Content Sniffing Attacks with File Encryption and File Splitter Technique", International Journal of Advanced Computer Research (IJACR), Volume-2, Number-3, Issue-5, September-2012.
[6] Animesh Dubey, Ravindra Gupta, Gajendra Singh Chandel," An Efficient Partition Technique to reduce the Attack Detection Time with Web based Text and PDF files", International Journal of Advanced Computer Research (IJACR),Volume-3 Number-1 Issue-9 March-2013.
[7] Anton Barua, Hossain Shahriar, and Mohammad Zulkernine, "Server Side Detection of Content Sniffing Attacks", 2011 22nd IEEE International Symposium on Software Reliability Engineering.
[8] Richard Sharp and David Scott," Abstracting Application Level Web Security," In Proceedings of the 11th ACM International World Wide Web Conference (WWW 2002), May 7-11, 2002.
[9] Peter wurzinger, Christian Platzer, Christian Ludl, and Christopher Kruegel,"SWAP:Mitigating XSS Attacks using a Reverse Proxy," In proceedings of the 2009 ICSE Workshop on Software Engineering for secure systems,pp.33-39,2009.
[10] Engin Kirda, Nenad Jovanovic, Christopher Kruegel and Giovanni Vigna,"Client-Side Cross-Site Scripting Protection," ScienceDirect Trans.computer and security ,pp.184-197,2009.
[11] Nao Ikemiya and Noriko Hanakawa, "A New Web Browser Including A Transferable Function to Ajax Codes", In Proceedings of 21st IEEE/ACM International Conference on Automated Software Engineering (ASE '06), Tokyo, Japan, pp. 351-352, September 2006.
[12] Zubair M. Fadlullah, Tarik Taleb,Athanasios V. Vasilakos, Mohsen Guizani and Nei Kato, "DTRAB: Combating Against Attacks on Encrypted Protocols Through Traffic-Feature Analysis", IEEE/ACM Transactions On Networking, Vol. 18, No. 4, August 2010.
[13] Misganaw Tadesse Gebre, Kyung-Suk Lhee and ManPyo Hong, "A Robust Defense against Content Sniffing XSS Attacks", IEEE 2010.
[14] Matsuda, T.; Koizumi, D.; Sonoda, M., "Cross site scripting attacks detection algorithm based on the appearance position of characters," Communications, Computers and Applications (MIC-CCA), 2012 Mosharaka International Conference on , vol., no., pp.65,70, 12-14 Oct. 2012.
[15] Fokko Beekhof, Sviatoslav Voloshynovskiy ,Farzad Farhadzadeh," Content Authentication and Identification under Informed Attacks", IEEE 2012.
[16] Dawei Wang; Longtao He; Yibo Xue; Yingfei Dong, "Exploiting Artificial Immune systems to detect unknown DoS attacks in real-time," Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on , vol.02, no., pp.646,650, Oct. 30 2012-Nov. 1 2012.
[17] Nagarjun, P.M.D.; Kumar, V.A.; Kumar, C.A.; Ravi, A., "Simulation and analysis of RTS/CTS DoS attack variants in 802.11 networks," Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on , vol., no., pp.258,263, 21-22 Feb. 2013
[18] Seungoh Choi, Kwangsoo Kim, Seongmin Kim, and Byeong-hee Roh," Threat of DoS by Interest Flooding Attack in Content-Centric Networking" IEEE 2013.
[19] Ruse, M.E.; Basu, S., "Detecting Cross-Site Scripting Vulnerability Using Concolic Testing," Information Technology: New Generations (ITNG), 2013 Tenth International Conference on , vol., no., pp.633,638, 15-17 April 2013.
[20] Ashutosh Kumar Dubey,Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava,"Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", CONSEG 2012.
[21] Bhupendra Singh Thakur, Sapna Chaudhary, Content Sniffing Attack Detection in Client and Server Side: A Survey, International Journal of Advanced Computer Research (IJACR), Volume-3 Number-2 Issue-10 June-2013.
[22] Saket Gupta," Secure and Automated Communication in Client and Server Environment", International Journal of Advanced Computer Research (IJACR) Volume-3 Number-4 Issue-13 December-2013.
[23] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Vipul Agarwal, Yogeshver Khandagre, "Knowledge Discovery with a Subset-Superset Approach for Mining Heterogeneous Data with Dynamic Support",Conseg-2012.