A Framework for Preserving the Privacy of Online Users Against XSS Worms on Online Social Network

Pooja Chaudhary, National Institute of Technology, Kurukshetra, Kurukshetra, Haryana, India
B. B. Gupta, National Institute of Technology, Kurukshetra, Kurukshetra, Haryana, India
Shashank Gupta, Birla Institute of Technology and Science, Pilani, India

ABSTRACT

This article presents a hybrid framework i.e. OXSSD (Online Social Network-Based XSS-Defender) that explores cross-site scripting (XSS) attack vectors at the vulnerable points in web applications of social networks. Initially, during training phase, it generates the views for each request and formulates the access control list (ACL) which encompasses all the privileges a view can have. It also ascertains all possible injection points for extracting malicious attack vectors. Secondly, during recognition phase, after action authentication XSS attack vectors are retrieved from the extracted injection points followed by the clustering of these attack vectors. Finally, it sanitizes the compressed clustered template in a context-aware manner. This context-aware sanitization ensures efficient and accurate alleviation of XSS attacks from the OSN-based web applications. The authors will evaluate the detection capability of OXSSD on a tested suite of real world OSN-based web applications (Humhub, Elgg, WordPress, Drupal and Joomla). The performance analysis revealed that OXSSD detects injection of illicit attack vectors with very low false positives, false negatives and acceptable performance overhead.

KEYWORDS

Access Control List (ACL), Cross-Site Scripting (XSS) Attack Vectors, Request Authentication, Session, XSS Cheat Sheet

1. INTRODUCTION

In the modern era of Web 2.0 technologies and HTML5-based web applications, Online Social Networking (OSN) is considered to be the most popular method for information sharing has drawn most of public attention. According to Nielson’s Social media report (Bilbao-Osorio, Dutta, & Lanvin, 2013), around 80% of active Internet users daily visit one of the OSN sites. OSN is a virtual place, where people create their own profile, find new friends and re-establish the lost connections based on the common attributes and behavior. The popular OSN utilized nowadays is Facebook with over more than 1 billion active users. Other famous OSNs are Google+ with more than 235 million active users; Twitter has over 200 million active users and LinkedIn with more than 160 million active users. However, as user share every type of information on OSN platform ranging from personal to professional and so on hence; such networks suffer from various categories of cyber-attacks. The most prominent attack found on OSN sites is the Cross Site Scripting (XSS) attack (Gupta & Gupta, 2014; Gupta & Sharma, 2012; Gupta et al., 2015). XSS attack has turned out to be a plague for the Online Social Network (OSN)-based web applications like Facebook, Twitter, and LinkedIn. It comes
under the umbrella of code injection vulnerability wherein adversary inserts illicit JavaScript code at the vulnerable points in the web application so that when benign user visits the web page script gets processed by the browser and XSS attack is successfully launched. The motto behind such attack is to steal the sensitive credentials of the active users by injecting the malicious JavaScript code in the form of some posts on such web applications (Gupta & Gupta, 2015).

XSS worm comes in three different flavors: 1) Reflected XSS (Gupta et al., 2015) in which attacker lures the victim to click on illicitly crafted URL which leads to the execution of reflected malicious script included in the response from the server; 2) Stored XSS (Gupta & Gupta, 2015) in which attacker permanently inserts malicious scripts into the server. After that, when web pages is loaded at browser then malicious scripts get executed and results into XSS attack; 3) DOM-based XSS attacks (Gupta & Gupta, 2015) occurred because client-side scripts dynamically alter the DOM structure of web page in order to run malicious scripts. Although, the key goal of all these four different categories of XSS worms is to steal the sensitive credentials such as transaction passwords, credit card numbers, etc. of the online user. Figure 1 highlights the simple scenario triggered for the initialization of the XSS attack.

However, the technique of exploitation of such worms is different on different platforms of OSN. Table 1 highlights the details of incidents of XSS attacks of OSN platforms.

**1.1. Related Work**

Input validation and sanitization is considered to be the first and foremost defensive measure for mitigating the effect of XSS worms from the platforms of web applications. In view of this, numerous XSS defensive methodologies have been proposed by the researchers to detect and alleviate the effect of XSS worms from the web application developed on diverse platforms. Livshits et al. (2013) proposed an automated technique of sanitizer placement by statically analyzing the stream of infected data in the program. Samuel et al. (2011) proposed a type-qualifier based method that can be utilized

---

**Figure 1. Simple XSS attack scenario**

![Simple XSS attack scenario](image-url)
Development and Evaluation of a Methodology for Developing Marketing Websites
Tomayess Issa, Martin West and Andrew Turk (2010). Integrating Usability Engineering for Designing the Web Experience: Methodologies and Principles (pp. 103-123).
www.igi-global.com/chapter/development-evaluation-methodology-developing-marketing/40495?camid=4v1a

Optimal Strategy in Queueing Systems in Emergency Department
www.igi-global.com/article/optimal-strategy-in-queueing-systems-in-emergency-department/193010?camid=4v1a