Accepted Manuscript

A survey of detection methods for XSS attacks

Upasana Sarmah, D.K. Bhattacharyya, J.K. Kalita

PII: S1084-8045(18)30204-2

DOI: 10.1016/j.jnca.2018.06.004

Reference: YJNCA 2154

To appear in: *Journal of Network and Computer Applications*

Received Date: 5 February 2018

Revised Date: 26 April 2018

Accepted Date: 4 June 2018

Please cite this article as: Sarmah, U., Bhattacharyya, D.K., Kalita, J.K., A survey of detection methods for XSS attacks, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2018.06.004.

A Survey of Detection Methods for XSS Attacks

Upasana Sarmah[a], D.K. Bhattacharyya[a,*], J.K. Kalita[b]

[a]*Department of Computer Science and Engineering, Tezpur University, Napaam, Tezpur-784028, Assam, India*
[b]*Department of Computer Science, University of Colorado, Colorado Springs, CO 80918, USA*

Abstract

Cross-site scripting attack (abbreviated as XSS) is an unremitting problem for the Web applications since the early 2000s. It is a code injection attack on the client-side where an attacker injects malicious payload into a vulnerable Web application. The attacker is often successful in eventually executing the malicious code in an innocent user's browser without the user's knowledge. With an XSS attack, an attacker can perform malicious activities such as cookie stealing, session hijacking, redirection to other malicious sites, downloading of unwanted software and spreading of malware. The primary categories of XSS attacks are: non-persistent and persistent XSS attacks. **This survey focuses on studying comprehensively, the detection methods available in the literature for XSS attacks. The detection methods discussed in this study are classified according to their deployment sites and further sub-classified according to the analysis mechanism they employ. Along with discussing the pros and cons of each method, this survey also presents a list of tools that support detection of XSS attacks. We also discuss in detail three preconditions that has to be met in order to successfully launch an XSS attack. One of the prime objective of this survey is to identify a list of issues and open research challenges. This survey can be used as a foundational reading manual by anyone wishing to understand, assess, establish or design a detection mechanism to counter XSS attack.**

Keywords: XSS, vulnerabilities, attack, detection, prevention, tools, attack vectors, CSPs

1. Introduction

The Web is an essential part of our individual everyday lives as well as societal activities as a whole. With advancements in technology, even the most complex applications are being increasingly delivered over the Web. However, with the proliferation of services being provided, there arise crucial questions. How secure is the Web? How secure are we when we access a resource on the Web? Answers to such questions have a single pointed focus - Security at all levels of interaction on the Web [1].
With monumental advances in Cloud Computing data security is one of the main aspects to maintain the privacy, confidentiality, integrity and authority of the users. Issues such as Selective opening security and malleability are significantly related to Cloud Computing security [2]. Moreover, it becomes utterly difficult to uphold security due to the problem of Data Deduplication [3] and more so, when the users enjoy different privileges to access the data stored in such platforms. Aiming to find a solution to such problems, the authors in [4] propose a hybrid cloud architecture. With a similar intention to find security related problems and issues in Cloud Computing the authors in [5] discuss and emphasize the counter measures to deal with the problems. Some important research articles related to Cloud Computing

*Corresponding author
Email addresses: upatink@tezu.ernet.in (Upasana Sarmah), dkb@tezu.ernet.in (D.K. Bhattacharyya), jkalita@uccs.edu (J.K. Kalita)