Asian Journal of Information Technology 16 (2-5): 169-177, 2017
ISSN: 1682-3915

A Taxonomy Study of XSS Vulnerabilities

Nayeem Khan, Johari Abdullah and Adnan Shahid Khan
Faculty of Computer Science and Information Technology,
Universitiy Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia

Abstract: As the demand of using internet and our dependence on web application to perform our daily activities is increasing every day, protecting web application from getting attacked by cyber criminal's becomes imperative. The most common type of attack on web applications is XSS. XSS is considered as a major growing web security threat. XSS attacks are the scripts that are embedded in a web page and are executed at the victim's machine. The objective of this study is to perform a literature review on the studies conducted on prevention and detection of XSS vulnerability. Results suggest that research in this field is going on very actively but no study provided full solution to this problem. More focus should be given to hybrid techniques and techniques using probabilistic model for detection of XSS vulnerability.

Key words: Taxanomy study, cross site scripting, web security, web application vulnurability, threat, Malaysia

INTRODUCTION

Cross Site Scripting (XSS) has been around since 199's as one of the major security vulnerability. OWASP (Open Web Application Security Project) has ranked XSS on 2nd among top ten web security vulnerabilities affecting users through web applications. As reported by Web hacking incident database for 2013, XSS vulnerabilities accounted 43% of all reported vulnerabilities. Statistics clearly demand the need to prevent and detect such types of security vulnerability. XSS is a type of injection attack that allows an attacker to send malicious scripts to end-users through a web browser in order to achieve the purpose of attack by stealing victim's confidential data such as password, cookie, sessions, hijacking browser, redirecting users to malicious sites and take unauthorized actions without user's knowledge. The attacker can be an internal or external user or even an administrator that has the ability to send malicious code to the interpreter in the web browser or to the target server. OWSAP has categorized XSS vulnerabilities into three types reflected, stored and DOM based. Stored XSS occurs when malicious Java script is stored on the target server in database, guest book's message forum's, etc., the malicious scripts gets executed when the user visits the malicious site thereby passing the privileges of the user to the attacker which then takes illegitimate actions without user permission. In reflected XSS the attacker injects the malicious code into the server. The injected code is reflected back to attacker in the form of error message or search result which may include some or part of inputs provided to the server as a request. Then reflected XSS attacks are sent to target victim through email or links embedded on the web pages to steal the confidential or takes control over the victim's computer. Document Object Model (DOM) is another kind of XSS vulnerability which occurs due to the inappropriate handling of the objects in a web page. In DOM based XSS entire tainted data flow from source to sink takes place in the web browser. The source of XSS can be any HTML element or the web page's URL while any method with sensitive call which can cause malicious code to be executed is the sink (Klein, 2005). The purpose of the taxonomy study is to show the current scenario of the research on XSS and to highlight the area where more research needs to done.

MATERIALS AND METHODS

The research questions which were addresses in this study (Fig. 1) are as:

- Q1: How much research has been done towards detection and prevention of XSS since its existence?
- Q2: What are the existing approaches used to solve this problem?
- Q3: What are the weaknesses and strengths of existing approaches?
- Q4: Which area should be focused for better results?

Literature to conduct this study was collected from following online databases:

Corresponding Author: Nayeem Khan, Faculty of Computer Science and Information Technology, Universitiy Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia