COUNTERING WEB INJECTION ATTACKS

A dissertation submitted to the University of Manchester for the degree of Master of Science in the Faculty of Engineering and Physical Sciences

2012

PAUL MATHEW

School of Computer Science

Abstract

"Web Injection" is the act of loading malicious content on to websites that are vulnerable to attacks, intending to exploit the web content. Most of the websites created are prone to attacks due to the lack of awareness about the security measures & poor coding practices which leaves a set of vulnerabilities which can exploit the website content. The attacks are mainly aimed to take the control over the whole system, which in turn can lead to access confidential data or damage/manipulation of database by malicious code, website being not available to legitimate user, with the ultimate aim of gaining the control of the system. Despite the number of threat detection tools and scanners, the attack is being increasing dramatically, and as a result of this, almost all the victims are legitimate web owners or users. This project will provide solution and awareness about the security measures to be implemented in various places.

The project consists of an elaborate literature review on web injection attacks and some existing detection and prevention solutions. The project mainly focuses on a type of attack recently discovered called Mass Meshing. On the basis of the literature study carried out, a solution has been designed and implemented and in addition to that a technical awareness guide is also developed. The solution is a Vulnerability Scanner which is designed particularly for the detection and removal of Mass Meshing attack. In order to test the scanner an attack is simulated and a demo web site is developed on which the attack is performed. The technical awareness guide describes about the security measures to be implemented in different levels for Mass Meshing and also a guide on a general web security.

Recommendations on future work can the addition of features to detect all incoming requests to the web server and allowing only legitimate and authorized requests. Another feature is to be able to incorporate with any website, so once the server starts the scanners starts automatically.