Analysis of Field Data on Web Security Vulnerabilities

José Fonseca, Nuno Seixas, Marco Vieira, Henrique Madeira

Abstract— Most web applications have critical bugs (faults) affecting their security, which makes them vulnerable to attacks by hackers and organized crime. To prevent these security problems from occurring it is of utmost importance to understand the typical software faults. This paper contributes to this body of knowledge by presenting a field study on two of the most widely spread and critical web application vulnerabilities: SQL Injection and XSS. It analyzes the source code of security patches of widely used web applications written in weak and strong typed languages. Results show that only a small subset of software fault types, affecting a restricted collection of statements, is related to security. In order to understand how these vulnerabilities are really exploited by hackers, this paper also presents an analysis of the source code of the scripts used to attack them. The outcomes of this study can be used to train software developers and code inspectors in the detection of such faults, and are also the foundation for the research of realistic vulnerability and attack injectors that can be used to assess security mechanisms, like intrusion detection systems, vulnerability scanners, and static code analyzers.

Index Terms—Security, Internet Applications, Languages, Review and evaluation.

1. INTRODUCTION

MOST information systems and business applications built nowadays have a web front-end and they need to be universally available to clients, employees and partners around the world, as the digital economy is becoming more and more prevalent in the global economy. These web applications, which can be accessed from anywhere, become so widely exposed that any existing security vulnerability will most probably be uncovered and exploited by hackers.

In the context of the present work we use the terminology introduced by [Avizienis04] that considers an error as a "*deviation of an external state of the system from the correct service state*", a fault as "*the adjudged or hypothesized cause of an error*", a vulnerability an "*internal fault that enables an external fault to harm the system*" and an attack is a "*malicious external fault*".

The security of web applications becomes a major concern and it is receiving more and more attention from governments, corporations and the research community [Valeur05, Christey07, Zanero05, David03, Jovanovic06]. Attackers also followed the move to the web and as such more than half of current computer security threats and vulnerabilities affect web applications [IBM11]. Not surprisingly, the number of reported attacks that exploit web application vulnerabilities is increasing [Fossi11]. In fact, numerous data breach attacks are frequently reported due to web application security problems [Mitre07, SANS09, OWASP10, Verizon11, Privacyrights12][1].

Given the preponderant role of web applications in many organizations, one can realize the importance of finding ways to reduce the number of vulnerabilities. This can be helped with a deeper knowledge on software faults behind such vulnerabilities [Howard05, Halfond06, Fogie07, Stuttard07], however this is a vast field and there is still a lot of work to be done, like the one presented by [Scholte12].

This paper contributes to fill this gap by presenting a study on characteristics of source code defects generating major web application vulnerabilities. The main research goal is to understand the typical software faults that are behind the majority of web application vulnerabilities, taking into account different programming languages. To understand the relevance of these kinds of vulner-

- *J. Fonseca is with the UDI of the Institute Polytechnic of Guarda and the CISUC. E-mail: josefonseca@ipg.pt. PEst-OE/EGE/UI4056/2011 – project financed by Science and Technology Foundation*
- *N. Seixas is with the University of Coimbra and he is a researcher at the Centre of Informatics and Systems of the University of Coimbra. Email: naseixas@dei.uc.pt.*
- *M. Vieira is with the University of Coimbra and he is a researcher at the Centre of Informatics and Systems of the University of Coimbra. Email: mvieira@dei.uc.pt.*
- *H. Madeira is with the University of Coimbra and he is a researcher at the Centre of Informatics and Systems of the University of Coimbra. Email: henrique@dei.uc.pt.*

[1] The most relevant vulnerabilities are known for many years, however they are still proliferating, in spite of the development of tools that help automate

Manuscript received (insert date of submission if desired).

Digital Object Indentifier 10.1109/TDSC.2013.37 1545-5971/13/$31.00 © 2013 IEEE