Chapter 7.8
Security Threats in Web–Powered Databases and Web Portals

Theodoros Evdoridis
University of the Aegean, Greece

Theodoros Tzouramanis
University of the Aegean, Greece

INTRODUCTION

It is a strongly held view that the scientific branch of computer security that deals with Web-powered databases (Rahayu & Taniar, 2002) than can be accessed through Web portals (Tatnall, 2005) is both complex and challenging. This is mainly due to the fact that there are numerous avenues available for a potential intruder to follow in order to break into the Web portal and compromise its assets and functionality. This is of vital importance when the assets that might be jeopardized belong to a legally sensitive Web database such as that of an enterprise or government portal, containing sensitive and confidential information. It is obvious that the aim of not only protecting against, but mostly preventing from potential malicious or accidental activity that could set a Web portal's asset in danger, requires an attentive examina-

tion of all possible threats that may endanger the Web-based system.

BACKGROUND

Security incidents have been bound to the Internet since the very start of it, even before its transition from a government research project to an operational network. Back in 1988, the ARPANET, as it was referred to then, had its first automated network security incident, usually referred to as "the Morris worm." A student at Cornell University (Ithaca, NY), Robert T. Morris, wrote a program that would connect to another computer, find and use one of several vulnerabilities to copy itself to that second computer, and begin to run the copy of itself at the new location (CERT Coordination Center Reports, 2006). In 1989, the ARPANET of-

ficially became the Internet and security incidents employing more sophisticated methods became more and more apparent. Among the major security incidents were the 1989 WANK/OILZ worm, an automated attack on VMS systems attached to the Internet, and exploitation of vulnerabilities in widely distributed programs such as the sendmail program (CERT Coordination Center Reports, 2006).

However, without underestimating the impact that such incidents of the past had to all involved parties, analysts support that the phenomenon has significantly escalated not only with respect to the amount of incidents but mostly to the consequences of the latter. The most notorious representative of this new era of cyber crime is the CardSystems incident (Web Application Security Consortium, 2006). In that crime scheme, hackers managed to steal 263,000 credit card numbers, expose 40 million more and proceed to purchases worth several million dollars using these counterfeit cards. CardSystems is considered by many the most severe publicized information security breach ever and it caused company shareholders, financial institutes and card holders damage of millions of dollars. The latest security incident occurred on April 25, 2006 when a hacker successfully managed to abuse a vulnerability in the Horde platform to penetrate the site owned by the National Security Agency of the Slovak Republic, jeopardizing sensitive information (Web Application Security Consortium, 2006).

LEGALLY SENSITIVE WEB-POWERED DATABASES

Even though legally sensitive portals, in other words, Web portals containing legally sensitive data, have been included in the Web portal family no sooner than the late 1990s (Wikipedia.org, 2006), the specific addition signaled the beginning of a new era in the Web portal scientific field. More specifically, portals took a converse approach with respect not only to the nature of services that they offered but also to the target group to which these services were offered. The end user from the perception of the Web portal was no longer exclusively the anonymous user, but could also be a very specific individual whose personalization data were frequently hosted inside the portal itself.

These types of portals, while often operating like ordinary Web portals serving millions of unaffiliated users, utilised some of its privately accessed aspects to harmonise the communications and work flow inside the corporation. This innovative approach proved to be both a money and labour saving initiative (Oracle Corporation, 2003). On the other hand, government portals that aimed at supporting instructing and aiding citizens to various socially oriented activities proved to be an important step towards the information society era.

It is obvious that these kinds of portals playing such an important role in the social or the enterprise context could not operate without information of equivalent potential and importance. As a result, the aforementioned Web portals were powered by databases hosting information of extreme fragility and sensitivity, a fact that inescapably attracted various nonlegitimate users, driven by ambition, challenge, or malice and who aimed to compromise the information, mangling the Web portal and making it non-operational. To impede all possible attacks against the Web portal and the hosted information, it is considered wise to identify all possible actions that could threaten and distort their functionality. The most ordinary Web portal architecture is examined and a threat area is defined, partitioned into four different sections, every one of which relates to a corresponding point of breaking-into the Web portal's normal operation.

7 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/security-threats-web-powered-databases/8024

Related Content

Comparing Metamodels for ER, ORM and UML Data Models
Terry Halpin (2004). *Advanced Topics in Database Research, Volume 3 (pp. 23-44).*
www.irma-international.org/chapter/comparing-metamodels-orm-uml-data/4352

Theoretical vs. Practical Complexity: The Case of UML
Keng Siau, John Ericksonand LihYunn Lee (2005). *Journal of Database Management (pp. 40-57).*
www.irma-international.org/article/theoretical-practical-complexity/3336

Making Query Coding in SQL Easier by Implementing the SQL Divide Keyword: An Experimental Query Rewriter in Java
Eric Draken, Shang Gaoand Reda Alhajj (2011). *Advanced Database Query Systems: Techniques, Applications and Technologies (pp. 287-303).*
www.irma-international.org/chapter/making-query-coding-sql-easier/52306

Deciding Query Entailment in Fuzzy OWL Lite Ontologies
Jingwei Cheng, Z. M. Maand Li Yan (2011). *Advanced Database Query Systems: Techniques, Applications and Technologies (pp. 247-268).*
www.irma-international.org/chapter/deciding-query-entailment-fuzzy-owl/52304

Comparing Object-Oriented and Extended-Entity-Relationship Data Models
Bill C. Hardgraveand Nikunj P. Dalal (1995). *Journal of Database Management (pp. 15-22).*
www.irma-international.org/article/comparing-object-oriented-extended-entity/51151