Chapter 6

Threats and Attacks on E-Commerce Sites

Kannan Balasubramanian
Mepco Schlenk Engineering College, India

ABSTRACT

In this chapter, a detailed knowledge of some of the most devastating attacks against Web applications and common tools in the attacker’s arsenal is discussed. There are many ways of categorizing and classifying attacks: based on the complexity to mount them, the effect they have on the target system, the type of vulnerability that they exploit, the assets that they expose, the difficulty of detecting and fixing them, and so on. There are different methodologies for Vulnerability Assessment and Threat Analysis (VATA) and many sources to consult for assessing the risk of each attack. Among other sources, in this chapter we pay special attention to the methodology of Open Web Application Security Project (OWASP) because OWASP is one of the most active security communities on the Web. Other good resources to follow the attack and vulnerability trends are Common Vulnerabilities and Exposures (CVE), National Vulnerability Database (NVD), United States CERT Bulletins (US-CERT), and SANS.

INTRODUCTION

In Computer Programming everyone knows that debugging is twice as hard as writing a program in the first place. You first need to understand what the code was originally designed to do, and then why it’s not doing it. Therefore, you need to be twice as smart debugging a program than coding it in the first place. Finding and exploiting a security vulnerability in a program is twice as hard as debugging it. The moral of the story is that the attackers are very smart. We should never underestimate our adversaries.

Attackers have two more advantages. First cryptographers tell you that you cannot enumerate all the attacks because solving all security flaws in a complex program becomes an intractable problem that leads to state-space combinatorial explosion. In English, this means that the hackers have a larger pool to find ways to break a program than the defenders have to fix them. Another advantage for attackers is that they only need to be successful in their attacks once; you, as the security professional in charge of protecting your Web commerce infrastructure and its users must be successful in your defense all the
In this chapter, we give you detailed knowledge of some of the most devastating attacks against Web applications and common tools in the attacker’s arsenal. There are many ways of categorizing and classifying attacks: based on the complexity to mount them, the effect they have on the target system, the type of vulnerability that they exploit, the assets that they expose, the difficulty of detecting and fixing them, and so on. There are different methodologies for Vulnerability Assessment and Threat Analysis (VATA) and many sources to consult for assessing the risk of each attack. Among other sources, in this chapter we pay special attention to the methodology of Open Web Application Security Project (OWASP) because OWASP is one of the most active security communities on the Web. It is an open project, and it is free, and therefore has participants from various players in the industry — from corporations to academia and individuals contributing to it. Other good resources to follow the attack and vulnerability trends are Common Vulnerabilities and Exposures (CVE), National Vulnerability Database (NVD), United States CERT Bulletins (US-CERT), and SANS.

In this chapter, the attacks are sorted alphabetically because, as we explained earlier, there are many criteria for ranking them; depending on your specific security and protection requirements the sorting would change. However, we have provided more details on the top ten attacks at the time of this writing. Furthermore, the list of attacks that are covered in this chapter is by no means exhaustive. Choosing which items to include has been a monumental task; the attacks that we have deemed most relevant to Web commerce are covered here. Before we dive into the depth of vulnerabilities, exploits, and attacks, let us have a quick glance at some basic definitions and become familiar with the terminology of the field.

BASIC DEFINITIONS

In this section we are going to define basic concepts that will help better understand the terminologies used in the rest of this chapter.

- **Target**: A target system is defined from a hacker’s perspective: That is, it is your system! It is referred to as a “target” because it is targeted by hackers. Although the term “target” is singular, all of your system components, including hardware, networking infrastructure, applications, frameworks, storage mechanisms, and the sensitive data they contain, together serve as the target for your adversaries. As it pertains to the application space, the two important classes of target are:
  - **Native Applications**: Programs that run directly at the operating system level and do not depend on an intermediary runtime environment such as a Java Virtual Machine (JVM), a Microsoft.NET Common Language Runtime (CLR), or any other runtime to execute. Native applications can run standalone and could potentially have more privileges than their Web application counterparts.
  - **Web Apps**: Programs that run inside a JVM, a CLR, or any other runtime, and depend on the services that are made available to them by the runtime, and therefore cannot run standalone.
- **Threat**: Security is a function of threat: Without a threat, security becomes an abstract concept that may not be of practical value to you. A threat is the potential for the threat-source to exploit a specific vulnerability or mount an actual attack. A threat-source is the intent or method that is targeted at the exploitation of vulnerability.
Related Content

Mobile Workforce Management in a Service-Oriented Enterprise: Capturing Concepts and Requirements in a Multi-Agent Infrastructure
[www.igi-global.com/chapter/mobile-workforce-management-service-oriented/26427?camid=4v1a](www.igi-global.com/chapter/mobile-workforce-management-service-oriented/26427?camid=4v1a)

B2C Failures: Toward an Innovation Theory Framework
[www.igi-global.com/article/b2c-failures-toward-innovation-theory/3456?camid=4v1a](www.igi-global.com/article/b2c-failures-toward-innovation-theory/3456?camid=4v1a)

Customer Value and New Product Retailing Dynamics: An Analytical Construct for Gaining Competetive Advantage
Dr. Rajagopal (2009). *Information Communication Technologies and Globalization of Retailing Applications* (pp. 49-71).
[www.igi-global.com/chapter/customer-value-new-product-retailing/22604?camid=4v1a](www.igi-global.com/chapter/customer-value-new-product-retailing/22604?camid=4v1a)

Building Competitive Advantage through E-CRM Analytics and Data Integration
[www.igi-global.com/chapter/building-competitive-advantage-through-crm/30404?camid=4v1a](www.igi-global.com/chapter/building-competitive-advantage-through-crm/30404?camid=4v1a)