WEB APPLICATION SECURITY IS A STACK

How to CYA (Cover Your Apps) Completely

Lori Mac Vittie

information security buzz

itgp™

Web Application Security is a Stack

How to CYA (Cover Your Apps) Completely

Lori MacVittie

IT Governance Publishing

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publisher and the author cannot accept responsibility for any errors or omissions, however caused. Any opinions expressed in this book are those of the author, not the publisher. Websites identified are for reference only, not endorsement, and any website visits are at the reader's own risk. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom
www.itgovernance.co.uk

First published in the United Kingdom in 2015
by IT Governance Publishing

ISBN: 978-1-84928-705-0

ABOUT THE AUTHOR

Lori MacVittie is responsible for education and evangelism of application services available across F5's entire product suite. Her role includes authorship of technical materials and participation in a number of community-based forums and industry standards organisations, among other efforts. She currently focuses on Cloud Computing, infrastructure, DevOps, data centre architecture and security-related topics. MacVittie has extensive development and technical architecture experience in both high-tech and enterprise organisations, in addition to network and systems administration expertise. Prior to joining F5, MacVittie was an award-winning technology editor at *Network Computing* magazine.

She holds a BS in Information and Computing Science from the University of Wisconsin at Green Bay, and an MS in Computer Science from Nova Southeastern University. She is Technical Editor and a member of the steering committee for CloudNOW, a non-profit consortium of the leading women in Cloud Computing.

CONTENTS

CHAPTER 1: INTRODUCTION

The modern threat

In 2011 an exploit taking advantage of a vulnerability in the Apache web server rapidly circulated across the Internet. Apache, at the time, was used by more than 65% of websites, according to Netcraft, so this was a serious issue which required immediate remediation. The exploit took advantage of a little-known vulnerability in the way Apache handled two HTTP headers. Exploitation of this vulnerability resulted in, as described by CVE-2011-3192, "very significant memory and CPU usage on the server", resulting in a distributed denial-of-service attack (DDoS) through resource exhaustion.

In late 2013, a highly complex DDoS attack[1] on a prominent member of an online trading community was detected and mitigated. In addition to the overwhelming network traffic generated, post-mortem analysis discovered a significant amount of application layer traffic. What had originally appeared to be simply an unusual spike in human interaction was, in truth, driven by a network of nearly 20,000 compromised browsers, all infected with a variant of the PushDo malware.

In early 2014, another vulnerability would shake the foundations of the Internet. Within the implementation of SSL as supported by the open source library, OpenSSL, existed the potential for attacks to exploit a buffer-

[1] Application-layer DDoS attacks are becoming increasingly sophisticated, PC World, Oct 2013 *http://www.pcworld.com/article/2056805/applicationlayer-ddos-attacks-are-becoming-increasingly-sophisticated.html*

overflow, enabling the extraction of sensitive consumer and corporate data. The open source library was widely used by web servers, as well as a wide variety of open and closed software and hardware around the world. Its discovery led to disruption of business and consumer fears regarding just what data attackers may have been able to extract.

None of these very serious web application vulnerabilities fall under what is traditionally considered the domain of application developers. The term 'web application security' usually conjures up thoughts of the more well-known web application attack vectors, such as SQL injection and cross-site scripting. But the reality is that web application security is not just about the application, but about the 'Web' too. Exploitation of web application platform and protocol implementation is becoming more common and, ultimately, is far more likely to produce the result desired by attackers.

These results are not always the theft of data, as is traditionally put forth. The rise of hacktivism – attacking organisations through their web presence as a means of protest against some business practice or to highlight a social cause – has resulted in a dramatic increase in attacks intended not to steal data or information but to disrupt business operations. These denial-of-service (DoS) attacks generate a lot of press, in addition to the financial costs incurred while applications are unavailable, not to mention the costs to remediate.

Also on the rise are attempts to use vulnerabilities in applications as a delivery vehicle for malware and remote access. Attackers seek not to attack applications themselves, but rather its consumers. By using vulnerabilities in the application layer, attackers can plant, and subsequently deliver, malware and malicious code to a much larger set of victims, some of whom are certain to be compromised and deliver to attackers the resources, data or credentials they are seeking.

The WhiteHat 'Website Security Statistics Report' from May 2013 notes that "23% of organisations website(s) said they experienced a data or system breach as a result of an application layer vulnerability"[2]. An HP TippingPoint sponsored security survey[3] noted that "nearly three in five IT professionals are concerned with application DDoS".

Much of the blame for successful attacks against web applications is laid solely at the feet of the developers who design and build the applications. While many of the attacks rely on common mistakes made during development, it is increasingly the case that attackers are targeting other areas of the web application stack, namely protocols and platforms. Recognising that 'application' security is really a stack, ensures that a growing vector of attacks does not go ignored. Protocol and metadata manipulation attacks are a dangerous source of DDoS and other disruptive techniques that can interrupt business and have a serious impact on the business' bottom line, as well as its reputation.

[2] Website Security Statistics Report, May 2013 www.whitehatsec.com/assets/WPstatsReport_052013.pdf.

[3] http://h30499.www3.hp.com/t5/HP-Security-Products-Blog/TippingPoint-network-security-survey-reveals-top-network/ba-p/6587710#.VAceWvmwLYg.

A holistic web application security strategy must therefore necessarily view its attack surface as the entire web application stack.

CYA: Cover Your Apps

Web application security must evolve along with the threat spectrum, to ensure complete coverage. Therefore, we will look not only at traditional application logic and data related security issues, but also at protocol and platform concerns. As emerging technologies and architectures, such as Cloud Computing and SDN (Software Defined Networking) continue to advance, application developers are increasingly responsible not only for ensuring compliance with best practices regarding web applications security, but in defining and managing the application policies and procedures that ensure application security at the platform and protocol layers.

Conversely, operators in other organisations are being forced to become more intimately familiar with web applications, in order to implement continuous deployment and delivery in response to pressures to move applications to market faster. Operators must therefore understand the attack vectors against which they must protect those applications, and the various methods which can be used to effectively combat successful exploitation.

With this in mind, this book is intended for application developers, system administrators and operators, as well as networking professionals who need a comprehensive top level view of web application security in order to better defend and protect both the 'Web' and the 'application' against potential attacks. It is not intended to be all encompassing but rather a look at the most common, fundamental attack vectors and defence techniques used to combat such attacks.

CHAPTER 2: ATTACK SURFACE

Web application security tends to be viewed as the purview of developers. It is, after all, about the application, and thus much of the focus on protecting against attacks falls to application developers. The OWASP Top 10, for example, focuses primarily on the methods used by attackers to manipulate application data to gain system access, execute remote commands and generally extract data beyond security controls that may be in place. These attacks target the data exchanged between a client and the application, taking advantage of vulnerabilities in parsing and lax security practices in input validation.

But a web application can also be exploited in other ways. The very logic encoded in an application may be vulnerable. URI or path traversal attacks attempt to exploit a lack of security to access files not intended to be accessed.

These types of attacks are made possible due to assumptions made as to the flow of logic through an application, as well as the methods used to maintain the current state of a web application. The use of cookies as a means to track user location within a workflow, has led to exploitation, as it is rarely the case that such mechanisms are protected against tampering while residing on the client in the browser.

In recent years it has also become commonplace for attackers to target the web application platform and protocols prevalent today. In 2011 a widespread attack on

Apache, known as 'Apache Killer', took advantage of poor handling of an HTTP header in the ubiquitous web server platform to affect a denial of service attack against organisations relying on the web server. As the web server served more than 65% of the sites on the Internet at the time, as tracked by Netcraft[4], the vulnerability rapidly gained the attention of the entire security community.

The result is that the modern web application attack surface should be viewed as a stack, comprising both protocol and more application-specific categories of potential attack surfaces. It is not enough to simply tighten input validation, or apply system-level security to files that should remain inaccessible. The entire stack must be secured against potential attack, lest it be exploited by attackers.

The web application security stack

Those concerned with web application security – whether operators or developers – must view the application layer as comprising its own 'stack', and apply security strategies appropriately.

There are two primary attack surfaces for modern web applications: the web application itself and the platform upon which it is deployed. The two are inseparable; you cannot deploy a web application without a platform on which it can run. Apache, NGINX, IBM WebSphere and Microsoft IIS are among the most popular platforms upon which web applications are deployed. Attacks on web

[4] http://news.netcraft.com/archives/2011/07/08/july-2011-web-server-survey.html.

applications, as well as their underlying platforms, are common, and the reliance of web applications on the platform to provide data regarding state, and other relevant information, introduces additional risk.

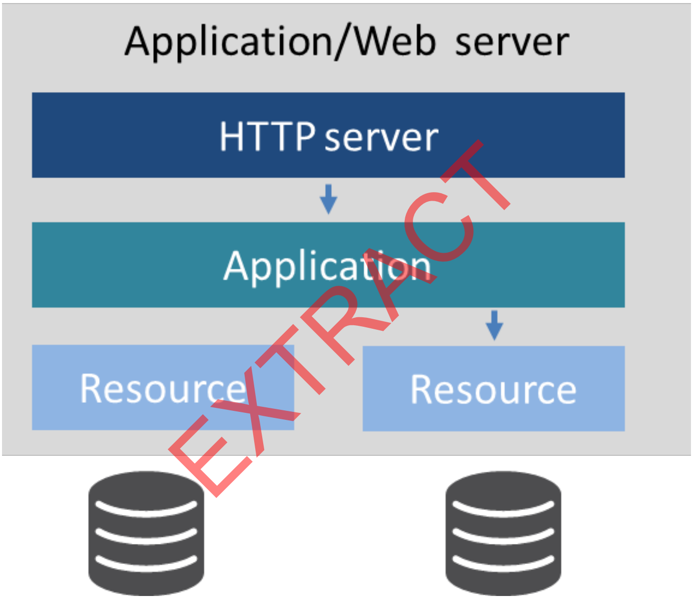
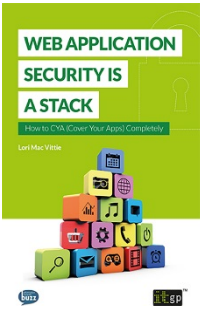


Figure 1: High-level architecture of a typical web application

<<< END OF EXTRACT >>>

Web Application Security is a Stack



- Provides an overview of the main threats from web application attacks, helping readers to improve their cyber defences.
- A comprehensive top-level view of web application security, covered concisely so that organisations can quickly apply their newly gained knowledge.
- Buy now and see how protecting your web applications significantly improves your cyber defences.

Buy your copy today

www.itgovernance.co.uk/shop/p-1688-web-application-security-is-a-stack-how-to-cya-cover-your-apps-completely.aspx

www.itgovernanceusa.com/shop/p-1464-web-application-security-is-a-stack-how-to-cya-cover-your-apps-completely.aspx

www.itgovernance.eu/p-1114-web-application-security-is-a-stack-how-to-cya-cover-your-apps-completely.aspx