Security of Web Servers and Web Services

Volker Hockmann
Techniker Krankenkasse, Hamburg, Germany

Heinz D. Knoell
University of Lueneburg, Germany

Ernst L. Leiss
University of Houston, USA

INTRODUCTION

Web servers and the Web services associated with them have become increasingly important in the last few years. Online banking, e-mail, and money, business-to-business (B2B), and business-to-client (B2C) transactions are growing rapidly. It is difficult to imagine modern business without these forms of networking.

However, there are also significant negative aspects. In many cases, due to competitive pressures, companies and government agencies had to implement these services very fast, often too fast and without any appreciation of the concepts of security and protection. As a consequence, it turns out that a hacker can misuse with little effort these Web services or compromise the underlying database (e.g., to obtain access to credit cards numbers or social insurance information).

A very significant percentage of the population in developed and developing countries is using wired and wireless connections for reading e-mails, accessing newsgroups, or using Internet banking. All these services are running on a Web server. Most Web servers are running the Apache or the Microsoft Internet Information Server (IIS) (all versions of both servers [Apache 1.3.x/2.x, IIS 3-6]) (Netcraft, 2006). Of these, older versions of the Internet Information Server are especially vulnerable to numerous attacks. Therefore, an attacker is in a position to break, with little effort, into many Web servers running IIS 4 or 5.

However, the Apache Web server (running on Windows systems) is also vulnerable to similar attacks. Moreover, using a Web server based on UNIX or Linux is not a guarantee for a secure system. UNIX and Linux systems are also affected by inherent weaknesses and vulnerabilities such as buffer overflows and the handling of format strings (ZDNet, 2006).

Readers who like to have more general insight are referred to works by Leiss (1990) and Garfinkel and Spafford (2002). These books give broader perspectives on Internet security.

HACKER, CRACKER, AND ATTACKER

In many technical articles as well as in the popular IT press one can read about hackers and crackers; sometimes there are references to cyberpunks and script-kiddies. But, what is a hacker, when is a hacker a cracker? What is the definition of a script-kiddie?

A hacker is someone with substantial technical know-how. A hacker (and it is almost always a male) is very interested in developing and administrating systems. The hacker is frequently motivated by a search for knowledge and interest in improving the hacker's systems and programs. A cracker on the other hand is someone who is often more interested in breaking into a server to access data or to subvert the functioning of the server. The cracker may also break into systems for money (Davis, 2002; Pipkin, 2002).

Script-kiddie is a derogative term for someone who is interested in computers but does not have enough knowledge to break into systems using personal ideas or scripts. Therefore, a scrip-kiddie uses existing and frequently well-known and easy-to-find (often downloadable) techniques and programs. A very dangerous aspect of this process is that script-kiddies do not know enough about the tools and relations between the tools and the compromised system. Often they are destroying more with their lack of knowledge than they intended (HoneyNet, 2000).

However, for the affected user, it does not greatly matter what kind of attacker is trying to break into the system. Maybe it is one of the company's own employees, who only wants to “improve” a system. Or it is a former employee who wants to retaliate for some perceived injustice. Or a script-kiddie just found a new and interesting tool to hack into a **Web server** and has by pure coincidence deleted all customer data on a company’s server.

All of these attackers are in a position to hack into a system, either intentionally and knowingly or more or less accidentally. In the next section we will talk about “the attacker.” This means all types of persons who are able to destroy, change, or delete data on systems.

It is very important to secure systems and servers against all kind of menaces, internal or external. The primary aim of an attacker is to assert oneself, to leverage some knowledge, and to bully one’s way into the system to steal credit card numbers, customer data, or other data of value to a business (Catless, 2006). Another goal is for attackers to subvert the functioning of servers, either to install back doors for future use or processes that can be used for subsequent attacks, such as a distributed denial-of-service attack.

For every company and especially for every administrator, it is a primary task to protect the running systems against all attackers. In some cases there are relatively simple ways to realize a security concept with “on-board tools,” tools, and product documentation. On-board tools might be extensions of the Apache Web server, such as ModSecurity (ModSecurity, 2006). With little effort the administrator may be able to make a server more secure using these tools. Another open source software that can be used to protect the systems is SNORT (Snort, 2006). SNORT is an intrusion detection system for Linux and Windows systems.

EXAMPLE OF WEB SERVER ATTACKS

In this section we present short and simple attacks against the Microsoft IIS Web server (Versions 4 and 5). We are using at first some real example data. In later sections, we will work only in a test environment. All URLs and IP addresses are disguised. A detailed description and more extensive explanation can be found by Hockmann (2004).

The reader should be careful with all given examples and try them only in a test environment, not with actual systems running real-time services.

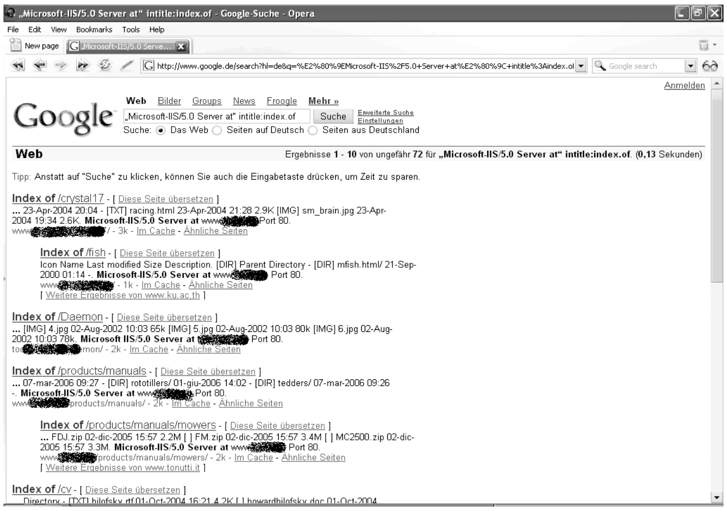
First Step: Providing Information

The first step includes obtaining information about the system the attacker wants to hack. Relevant information might be software version of the Web server, patch level, installed operating system, other services running on this system, IP address, and shared directories.

Often, it is very simple to find such information, for example using Google.

If one types into Google the search string—*Microsoft-IIS/5.0 Server at“ intitle:index.of*—some very interesting listings will result. Figure 1 gives some very interesting details about Web servers. To begin, it shows the version (“Microsoft-IIS/5.0”) and the port on which the Web server is listening (“Port 80”).

Figure 1. Google search results



http://www.google.de/search?hl=de&q=%E2%80%9EMicrosoft-IIS%2F5.0+Server+at%E2%80%9C+intitle%3Aindex.of

„Microsoft-IIS/5.0 Server at" intitle:index.of

Suche: ● Das Web ○ Seiten auf Deutsch ○ Seiten aus Deutschland

Web Ergebnisse **1** - **10** von ungefähr **72** für **„Microsoft-IIS/5.0 Server at“ intitle:index.of**. (**0,13** Sekunden)

Tipp: Anstatt auf "Suche" zu klicken, können Sie auch die Eingabetaste drücken, um Zeit zu sparen.

Index of /crystal17 - [Diese Seite übersetzen]
... 23-Apr-2004 20:04 - [TXT] racing.html 23-Apr-2004 21:28 2.9K [IMG] sm_brain.jpg 23-Apr-2004 19:34 2.6K. **Microsoft-IIS/5.0 Server at** www[redacted]Port 80.
www[redacted]/ - 3k - Im Cache - Ähnliche Seiten

Index of /fish - [Diese Seite übersetzen]
Icon Name Last modified Size Description. [DIR] Parent Directory - [DIR] mfish.html/ 21-Sep-2000 01:14 -. **Microsoft-IIS/5.0 Server at** www[redacted] Port 80.
www[redacted]/ - 1k - Im Cache - Ähnliche Seiten
[Weitere Ergebnisse von www.ku.ac.th]

Index of /Daemon - [Diese Seite übersetzen]
... [IMG] 4.jpg 02-Aug-2002 10:03 65k [IMG] 5.jpg 02-Aug-2002 10:03 80k [IMG] 6.jpg 02-Aug-2002 10:03 78k. **Microsoft IIS/5.0 Server at** [redacted] Port 80.
to[redacted]mon/ - 2k - Im Cache - Ähnliche Seiten

Index of /products/manuals - [Diese Seite übersetzen]
... 07-mar-2006 09:27 - [DIR] rototillers/ 01-giu-2006 14:02 - [DIR] tedders/ 07-mar-2006 09:26 -. **Microsoft-IIS/5.0 Server at** www[redacted]Port 80.
www[redacted]products/manuals/ - 2k - Im Cache - Ähnliche Seiten

Index of /products/manuals/mowers - [Diese Seite übersetzen]
... FDJ.zip 02-dic-2005 15:57 2.2M [ ] FM.zip 02-dic-2005 15:57 3.4M [ ] MC2500.zip 02-dic-2005 15:57 3.3M. **Microsoft-IIS/5.0 Server at** www[redacted] Port 80.
www[redacted]/products/manuals/mowers/ - 2k - Im Cache - Ähnliche Seiten
[Weitere Ergebnisse von www.tonutti.it]

Index of /cv - [Diese Seite übersetzen]
Directory - [TXT] hilofsky.rtf 01-Oct-2004 16:21 4.2K [ ] howardhilofsky.doc 01-Oct-2004