Reinhard Hofer

Sicherheitsanalyse Webserver

Diplomarbeit

Examicus

Fachhochschulstudiengänge Burgenland GmbH
Thomas A. Edison Straße 2
A-7000 Eisenstadt

Studiengang „Information and Communication Solutions"

Diplomarbeit

Sicherheitsanalyse Webserver

Reinhard Hofer

betreut durch

DI Rainer Schmidt

Eisenstadt, Sommersemester 2006

Information and Communication Solutions

1 Ehrenwörtliche Erklärung

Ich habe diese Diplomarbeit selbstständig verfasst, alle meine Quellen und Hilfsmittel angegeben, keine unerlaubten Hilfen eingesetzt und die Arbeit bisher in keiner Form als Prüfungsarbeit vorgelegt.

Mannersdorf, 30.5.2006 Reinhard Hofer

Danksagung

Auch an dieser Stelle möchte ich persönlich darauf hinweisen, dass trotz der Kritik die sowohl kommerziell Softwarehersteller und auch Open Source Entwickler laufend von allen Seiten hinnehmen müssen, die Produkte Internet Information Server und Apache ganz ausgezeichnete sind. Ich kenne selbst noch die Zeit, wo ein Viruskiller die einzige Sicherheitsmaßnahme am Rechner war und auch die ersten Versionen von Windows (DOS), Apache und IIS. Anwender verwünschen oft die Hersteller für deren Entwicklungen, Fehler der Software, Abstürze usw., vergessen aber meiner Meinung nach häufig, dass wenn man die Komplexität der Software heranzieht, es bereits unglaublich ist, dass ein Computer überhaupt bootet. Wenn man die Softwareprodukte im Laufe der Zeit vergleicht und beobachtet, kann man leicht entdecken, dass die Komplexität ständig zunimmt, aber trotzdem Millionen Benutzer ein verwendungsfähiges System vor sich haben.

Persönlich danke ich meinem Betreuer DI. Rainer Schmidt für seine Inputs zu den einzelnen Themen. Sein Fachwissen selbst zu tiefgehenden Themen hat mich bei jedem Gespräch aufs Neue beeindruckt.

Weiters danke ich meinem persönlichen Freund MBA Werner Kölbl für seine kreativen Anmerkungen und seine technische Unterstützung.

Darüber hinaus danke ich dem Team meines Studiengangs für die umfassende und interessante Ausbildung.

Last but not least danke ich meinem persönlichen Freundeskreis für die Geduld, die Unterstützung und das aufgebrachte Verständnis während meines Studiums und während der Erstellung dieser Arbeit.

Reinhard Hofer
Eisenstadt, 30.05.2006

Kurzfassung Deutsch

Die Diplomarbeit setzt am Punkt Internet an, dem zentralen Werkzeug zur Kommunikation bzw. Informationsbeschaffung. Da das Thema Internet und auch Sicherheit ein sehr umfangreiches ist, spezialisiert sich die Arbeit auf die Server, die hinter dem Webseiten stehen und von alltäglichen Benutzern nicht wahrgenommen werden. Es ist nicht Ziel dieser Arbeit, sonstige Bereiche der Kommunikation, Sicherheit, Internet oder Plattformen zu behandeln. Es ist weiters nicht Ziel, neue Sicherheitslöcher in Webserverprodukten aufzudecken oder detailliert auf Mittel und Wege hinzuweisen, Webserver oder Webseiten zu kompromittieren. Sehr wohl ist aber wichtig, nicht nur die Server selbst zu untersuchen, sondern auch grundsätzlich die Clientseite und hier im Speziellen den Sourcecode zu erklären.

Die Arbeit ist in drei Abschnitte unterteilt. Der einleitende Abschnitt beinhaltet Theorie zu gängigen Angriffsformen auf Webserver und Webseiten und beinhaltet damit auch gängige Formen zum widerrechtlichen Erlangen von Passworten oder zum Umgehen von passwortgeschützten Techniken. Zusätzlich zum theoretischen Ansatz beinhaltet dieses Dokument Beispiele für mögliche Techniken und deren Schwachstellen. Im Sourcecode-Abschnitt wird gezeigt, wie man den Zugang zu Webserverressourcen beschränken kann und worauf man dabei achten muss bzw. wo und wie Angreifer ansetzen können. Dazu gibt es mehrere Beispiele, die an Komplexität zunehmen und aufsteigend angeführt werden.

Die beiden anderen Abschnitte behandeln die beiden Webserver Internet Information Server 6 und Apache 2.2 und sind gleich aufgebaut und zeigen eine vergleichende Sicht auf das jeweilige Produkt. Im Vordergrund steht auch hier der Sicherheitsaspekt. Welche Schwachstellen weist das jeweilige System auf und wie kann man sich schützen? Die Beschreibung der Konfiguration bzw. der Schritte zur Absicherung des Systems zeigen auch, wo die jeweiligen Schwachstellen liegen und welcher Konfigurationsaufwand dabei entsteht. Das Abschlusskapitel zeigt die resultierenden Ergebnisse.

Kurzfassung Englisch

Security is no longer about a second lock for your door or about buying an alarm system. Today's networking and the geographical extension of computers and Internet leads to new security threats. The Internet is today's centre of communication and information gathering. As web servers are at the centre of almost all online communication and are therefore the centre for security measures, this thesis focuses on the servers which are not visible by common users. The aim of this work is not to explain operating systems, Internet communication, platforms etc. Furthermore, the author doe not intend to discover new security leaks in actual web server software or to explain in detail how to compromise a web server system. That is to say, it takes a look at the clients and explains the source code executed on their side.

The thesis is divided into three sections. The introductory section includes the theoretical background of common attack scenarios on web servers and websites. It also refers to common ways of avoiding or bypassing password protected techniques. In addition to the theoretical part, the thesis includes examples of source code and their weaknesses. This section shows methods to restrict access to resources and describes the possibilities available to hostile users. The complexity of the examples increases and is in ascending order. The examples shown describe client side and server side code and are written in script languages like PHP, JavaScript, VB.(NET) and JSP.

The other sections cover the two web servers that have the largest market share. The chapters about Internet Information Server 6 and Apache 2.2 have the same structure and compare both products. Certainly, security is given priority. Which weaknesses are there and how can one protect oneself? Additionally both chapters mention basic security measures. The explanation of configuration and first steps show the complexity and effort needed. Besides the substantial research the reader can find multiple analyses on network traffic as well as scans of the server systems and a comparison of security holes. The final chapter shows the results.

Inhaltsverzeichnis

Seite
1 Einleitung 1
1.1 Problemstellung 1
1.2 Zielsetzung 2
2 Quellcode 4
2.1 Fehler und Risiken 4
2.2 Passwortgeschützter Zugang 6
2.2.1 HTML und clientseitige Skripte 6
2.2.2 Serverseitige Skripte 7
2.2.3 Referer Header und Cookies 8
2.2.4 Codebeispiele 10
2.2.4.1 Beispiel 1 - Sourcecodeanalyse 10
2.2.4.2 Beispiel 2 – Sourcefehler 13
2.2.4.3 Beispiel 3 - Sessions 16
2.2.4.4 Beispiel 4 – Skriptinjections & Referer & Cookies 16
2.2.4.5 Beispiel 5 – Dateien außerhalb des Webverzeichnisses / Includes 19
2.2.4.6 Beispiel 6 – SQL-Injections 20
2.3 Angriffsmethoden 26
2.3.1 Spoofing 26
2.3.1.1 Adress Resolution Protocol-Spoofing 27
2.3.1.2 Domain Naming Service-Spoofing 30
2.3.1.3 IP-Spoofing 32
2.3.1.4 Route-Spoofing 35
2.3.2 Denial of Service 36
2.3.2.1 Flooding 36
2.3.2.2 Intern Control Message Protocol - Angriffe 37
2.3.3 Scanning 38
2.3.3.1 Portscanning 38
2.3.3.2 Sniffing 39
2.3.4 Cracking 40
2.3.5 Phishing 42
3 Internet Information Server 45
3.1 Risiken 45
3.2 Standardeinstellungen und Konfiguration 46
3.2.1 Änderungen an den Standardeinstellungen 46
3.2.2 Sicherheitsmaßnahmen 48
3.2.2.1 Sicherheitsrichtlinie 48
3.2.2.2 Logging 49
3.2.2.3 Checkliste 52
3.2.3 Verbesserungen gegenüber IIS 5 54
3.3 Security Analyse 56
3.4 Hotfixes 59
3.4.1 Aktuelle Sicherheitslöcher 59
3.4.1.1 Kompressionsfehler verursacht Zugriffsverletzungen 59
3.4.1.2 Kennwortänderungsseiten 60

3.4.1.3 WebDAV-XML Message Handler 60
3.4.1.4 FTP-Resume-Feature 61
3.4.1.5 ASP.NET und Set-Cookie 61
3.4.2 Herstellerverhalten 62
3.5 Systeme die auf den Webserver einwirken 64
3.5.1 Betriebssystem 64
3.5.2 Intrusion Detection System 66
3.5.3 Demilitarized Zone 67
3.5.4 Firewall 69
3.5.5 Viruskiller 71
4 Apache 75
4.1 Risiken 75
4.2 Standardeinstellungen und Konfiguration 76
4.2.1 Änderungen an den Standardeinstellungen 76
4.2.2 Sicherheitsmaßnahmen 77
4.2.2.1 Logging 77
4.2.2.2 Checkliste 79
4.2.3 Verbesserungen gegenüber Apache 1.3 bzw. 2.0 81
4.2.3.1 Verbesserungen von Apache 2.0 gegenüber 1.3 81
4.2.3.2 Verbesserungen von Apache 2.2 gegenüber 2.0 82
4.3 Securityanalyse 83
4.4 Updates 85
4.4.1 Aktuelle Sicherheitslöcher 85
4.4.1.1 Referer Cross-Site Scripting 85
4.4.1.2 Behobene Sicherheitslöcher in Version 2.0.58 85
4.4.1.3 Behobene Sicherheitslöcher in Version 2.0.55 86
4.4.2 Herstellerverhalten 86
4.5 Systeme die auf den Webserver einwirken 88
4.5.1 Betriebssystem 88
4.5.2 Intrusion Detection System 89
4.5.3 Demilitarized Zone 89
4.5.4 Firewall 89
4.5.5 Viruskiller 89
5 Ergebnisse und Schlussfolgerungen 90
6 Zusammenfassung 96
7 Verzeichnisse 98
7.1 Literaturverzeichnis 98
7.2 Abbildungsverzeichnis 101
7.3 Tabellenverzeichnis 102
7.4 Listingverzeichnis 102
7.5 Formelzeichen, Indizes und Abkürzungen 103

1 Einleitung

1.1 Problemstellung

Bereits der Amerikaner Abraham H. Maslow hat in seinem Studium über die Bedürfnisse der Menschen Sicherheit als wesentlichen Bestandteil aufgenommen. Genauer ist in seiner „Hierarchy of the prepotency of human needs", übersetzbar mit Bedürfnispyramide, der Punkt Sicherheit auf Stufe 2 und somit unmittelbar nach den Grundbedürfnissen. Sicherheit ist ein Begriff der viele Aspekte im Leben und in der Gesellschaft vereint und eine Möglichkeit zum Befriedigen des Sicherheitsbedürfnisses ist Vorbeugung bzw. Implementierung von Schutzmechanismen.

Betrachtet man das Thema Sicherheit im Rahmen der IT, dann wird deutlich, wie weit verzweigt dieses Thema wirklich ist. IT-Sicherheit war mehr als 20 Jahre nicht von Nöten. Das Urnetz ARPANET war eine Vernetzung von vier Rechnern zwischen Universitäten in den USA. Die Teilnehmer kannten sich untereinander. Das World Wide Web, das 1989 von Cern entwickelt wurde, hat die Situation geändert. Plötzlich war die Allgemeinheit eingebunden und damit das Netzwerk unkontrollierbar. Reichte vor einem Jahrzehnt noch ein guter Virenkiller aus, so ist heutzutage ein ungeschützter Server im Internet innerhalb von Minuten das Opfer irgendeiner Form eines Angriffs.

Von allen Sicherheitsmechanismen wie Intrusion Detection Systems, Honeypots, Sicherheitsrichtlinien usw. ist in dieser Arbeit vor allem die Sicherheit von Webservern im Vordergrund. Ein Webserver steht natürlich nicht auf sich selbst gestellt im Netz. Eine Firewall ist obligatorisch und jedes System, das das Netzwerk bzw. den Server selbst schützt, unterstützt die Sicherheit des Webserver mit. Die Fragen, die sich stellen sind, welchen Webserver man verwenden soll und worauf man achten muss bzw. welche Möglichkeiten man bei der Konfiguration hat. Der heute marktführende Webserver ist Apache, gefolgt vom Internet Information Server. Es gibt weitere Webserver die mitunter spezialisiert in einem

bestimmten Bereich sind. Tomcat beispielsweise ist weniger ein Webserver, sondern eine Servletengine[1]. MyServer ist ein weiteres Open Source Project mit GNU General Public License (GPL) oder Zeus stellt einen High Performance Webserver dar. Im Zuge dieser Arbeit werden die beiden wohl bekanntesten, sicher aber wichtigsten Server Apache und IIS evaluiert und verglichen.

1.2 Zielsetzung

Ziel ist, die Risiken beim Einsatz von Webservern aufzuzeigen und auf entsprechende Lösungen hinzuweisen. Die Arbeit beantwortet, welcher Webserver unter welchen Bedingungen der bessere und sichere ist. Dies beginnt bei der Konfiguration, die bei beiden Produkten sehr umfangreich und oft verwirrend ist. Jeder Server hat seine eigenen Schwächen, wobei einige bekannt sind bzw. von den Herstellern behoben, andere nicht. Vor allem die Möglichkeiten zur Beeinträchtigung der Funktionalität und Erlangen von geheimer Information sind wichtig. Welche Möglichkeiten gibt es, sich vor Eindringlingen zu schützen? Welche Risiken bestehen generell? Nicht nur das fertige Endprodukt wird untersucht, sondern auch das Verhalten der Hersteller. Nur Microsoft und die Apache Software Foundation können Sicherheitsmängel beheben. Hier wird untersucht, wie das Verhalten der Hersteller ist und wie schnell aufgedeckte Mängel behoben werden.

Die benutzten Betriebssysteme stehen hier im Hintergrund. Apache läuft zwar auf allen Linuxderivaten und auf Windows, jedoch ist für IIS Windows Voraussetzung. Die Systeme rund um den Webserver stehen im Hintergrund. Selbstverständlich wird auf Entsprechendes hingewiesen, es ist jedoch nicht Ziel dieser Arbeit, die Konfiguration des Netzwerks oder eine Anleitung zur Erstellung von Sicherheitsrichtlinien zu liefern. Noch weniger ist es Ziel eine Anleitung zum Hacken zu liefern. Viel mehr werden Fehler aufgezeigt und die Möglichkeit zur Vermeidung eben dieser.

Ein Kapitel widmet sich dem Sourcecode selbst. Jeder Webserver dient letztendlich nur der Umwandlung der Source in lesbaren Text, d.h. der Ausgabe für den

[1]Eine Servletengine dient zum Ausführen von Programmcode. Im Fall von Tomcat zum Ausführen von Javacode bzw. von Java Server Pages.

Browser. Der beste Server kann nicht verhindern, dass das Passwort der Seite im Sourcecode steht. Solche Fehler im Sourcecode sind natürlich ebenfalls zu vermeiden.