



Newsletter  
Issue 119 - 15.07.2002  
<http://net-security.org>

This is a newsletter delivered to you by Help Net Security. It covers weekly roundups of security events that were in the news the past week. Visit Help Net Security for the latest security news - <http://net-security.org>.

=====

SPI Dynamics ALERT:  
Learn how to outsmart the Top 14 Web Application hacks!

=====

ALERT: Test and assess your Web Applications TODAY! Hackers exploiting Web applications gain entry to backend data via Port 80 and 443! Firewalls and IDS don't stop these attacks because hackers using the Web App Layer are NOT seen as intruders.

Are you vulnerable? 15-Day \*Free\* Trial! Download now!  
<http://www.spidynamics.com/mktg/freewebinspect5>

=====

Table of contents:

- 1) Security news
- 2) Vulnerabilities
- 3) Advisories
- 4) Virus news
- 5) Security world
- 6) Featured articles
- 7) Security software

[ General security news ]

-----

#### IBM PURSUES SECURITY AGENDA

Determined to embed its technology at the core of emerging Web services standards, IBM is set to unveil a set of APIs designed to address critical security and third-party integration needs.

>> <http://www.net-security.org/news.php?id=546>

#### SECURING SERVERS WITH PHP

This article by Maguma software developer Jim Barcelona shows how to create a simple yet effective port scanning application in PHP.

>> <http://www.net-security.org/news.php?id=547>

#### X MARKS THE SPOT FOR HACKERS

There are chalked symbols on the walls of Melbourne's city buildings.

They are the marks of the "war chalkers" - hackers who are trying to find open or unguarded wireless computer networks they can penetrate.

>> <http://www.net-security.org/news.php?id=548>

#### PALLADIUM HOLDS PROMISE, AND PERIL

Whether Microsoft's ambitious project is a security solution or a Trojan horse depends much on the company's intentions.

>> <http://www.net-security.org/news.php?id=549>

#### APPLE: TAKING OS X SECURITY SERIOUSLY

Apple hasn't had a great record when it comes to keeping users informed about security vulnerabilities or supplying timely fixes. But the company now seems to be actually trying to improve its rep.

>> <http://www.net-security.org/news.php?id=550>

#### SURVEY: IT EMBRACING SECURITY

Although attackers are becoming more persistent by the day, the defenses that security administrators are putting up around their networks appear to be working to reduce the number of intrusions.

>> <http://www.net-security.org/news.php?id=551>

#### CRYPTO CHALLENGE HAS GEEKS SCRATCHING THEIR HEADS

A cryptography challenge run by Thawte Computing is attracting interest from around the world with entrants from as far as Afghanistan and Barbados struggling to crack the code posted on its Web site.

>> <http://www.net-security.org/news.php?id=552>

#### WORM BLOCKS ACCESS TO THE REGISTER

Virus writers have created a worm which, among other tricks, blocks access to The Register.

>> <http://www.net-security.org/news.php?id=553>

#### MICRONPC UNVEILS A MORE SECURE NOTEBOOK

New T1000 features an embedded biometric fingerprint scanner, allowing you to leave your passwords in the past.

>> <http://www.net-security.org/news.php?id=555>

#### MUCH ADO ABOUT NOTHING

Forget any new laws capping spam and don't expect Uncle Sam to step in and protect your privacy. When it comes to technology, Congress is aggressively doing very little this year.

>> <http://www.net-security.org/news.php?id=556>

#### SHOW US THE BUGS - USERS WANT FULL DISCLOSURE

End-users overwhelmingly support the full disclosure of security vulnerabilities, according to a survey by analysts Hurwitz Group.

>> <http://www.net-security.org/news.php?id=557>

#### FACING THE SECURITY RISKS OF CABLE MODEMS

Cable access is a great value fast connection for tele-workers and small offices. But how do you deal with the security risks?

>> <http://www.net-security.org/news.php?id=558>

#### RESCUING LINUX SYSTEMS

The time comes when every Linux system administrator experiences a system failure...

>> <http://www.net-security.org/news.php?id=559>

#### HACKERS' PARADISE

Which part of the world has the dubious distinction of being the most active hotbed of computer hacking?

>> <http://www.net-security.org/news.php?id=560>

#### CHINA VOWS TO PUNISH FALUN GONG FOR TV PIRACY INCIDENT

Officials in Beijing are vowing to hunt down and punish sympathizers of the Falun Gong spiritual movement, who have been hijacking Chinese satellite TV signals.

>> <http://www.net-security.org/news.php?id=562>

#### HACKERS WARN OF 'CRACKERS'

Meet Mack and Jack, not their real names. They are hackers or whiz kids of the computer. Mack, 17, is a student, Jack, 29, is in business. Neither wants his name used, nor to be identified.

>> <http://www.net-security.org/news.php?id=563>

#### REPORT: CYBERATTACKS AGAINST ENERGY FIRMS RISE

Power and energy companies have become targets for hackers, who have managed to penetrate their networks and other systems.

>> <http://www.net-security.org/news.php?id=564>

#### FREEDOM DOWNTIME LA SCREENING

The 2600 documentary on the hacker culture and the Free Kevin movement will be screening in Los Angeles on Sunday, July 21. Mitnick will be there.

>> <http://www.net-security.org/news.php?id=566>

#### APPLE WARNED OF UPDATE EXPLOIT

Apple is under the gun to address a reported security gap that could allow attackers to attach malicious code to automatic updates for Mac OS X.

>> <http://www.net-security.org/news.php?id=567>

#### HARD DRIVE SECURITY TOOL SHIPS

PC Guardian Updates Encryption Plus, on-the-fly file encryption program for networked PCs.

>> <http://www.net-security.org/news.php?id=568>

#### GIANTS MOVE FORWARD ON SECURITY STANDARD

A long-awaited Web services security specification will soon be

submitted to the Organisation for the Advancement of Structured Information Standards standards body.

>> <http://www.net-security.org/news.php?id=569>

#### SECURITY BREACH LEAVES STUDENT DATA OPEN

The breach allowed outsiders to search for the names, Social Security numbers, and addresses of about 2,000 students who registered with Resicom via its Web site.

>> <http://www.net-security.org/news.php?id=570>

#### ITALIAN POLICE BLACK OUT 'BLASPHEMOUS' WEBSITES

Italian authorities have shut down five Internet sites which reportedly carried blasphemies against God and the Virgin Mary, following a complaint by the Vatican's newspaper.

>> <http://www.net-security.org/news.php?id=571>

#### TOOLS FOR SECURE NETWORKS

A vast number of programs can be loosely described as network management tools. This reflects both users' desperate need for help and the broad range of problems you can encounter on a network.

>> <http://www.net-security.org/news.php?id=572>

#### USE SNORT FOR LIGHTWEIGHT INTRUSION DETECTION

Snort is a free, cross-platform packet sniffer, logger, and intrusion detector for monitoring smaller TCP/IP networks. It takes mere minutes to install and start using it.

>> <http://www.net-security.org/news.php?id=573>

#### AUTOMATING SECURITY SYSTEMS

Automation is a key factor in the formulation of a resilient security strategy, says Idris Cassim, business unit manager: security at Datacentrix.

>> <http://www.net-security.org/news.php?id=575>

#### FOCUS TURNED ON SECURITY OFFICIALS

Updated guidance for agencies' annual reports on information security management capabilities includes a new focus on performance measures for officials who are accountable for systems security.

>> <http://www.net-security.org/news.php?id=577>

#### SECURITY DEVICE MAKERS WANT SHIELD FROM LAWSUITS

The companies making new homeland security devices, such as bomb detectors and biological weapon alarms, want the government to pick up the tab if their products fail and they are sued.

>> <http://www.net-security.org/news.php?id=578>

#### DIGITAL COPYRIGHT PROTECTION GOES MOBILE

Technology designed to prevent mobile phone users sharing copyrighted ring tones, graphics and games is to be developed under a new agreement between IBM and Nokia.

>> <http://www.net-security.org/news.php?id=579>

#### XML SECURITY: A WHO'S WHO

When a standard is deployed as openly as XML, businesses are bound to have security concerns.

>> <http://www.net-security.org/news.php?id=580>

#### MORE THEN 400,000 OPTUS ACCOUNTS SNATCHED

Sydney resident has been charged over accusations he hacked Optus and got information on more than 400,000 dial up accounts.

>> <http://www.net-security.org/news.php?id=581>

#### ATTACK OF THE CYBER-TERROR STUDIES

Last month's BSA report on cyber security concluded that cyber terrorism was going to be really serious. The Reg has a rant on this study.

>> <http://www.net-security.org/news.php?id=582>

#### APPGATE RECEIVES MORE VC

VPN vendor AppGate received its second venture capital investment this year, with \$2.5 million in new funding, the company said.

>> <http://www.net-security.org/news.php?id=583>

#### NETCRAFT SURVEY FOR JUNE 2002

A June 2002 survey by Netcraft shows that Web sites are more vulnerable than ever because of several recently reported security problems with MS IIS and Apache Web server.

>> <http://www.net-security.org/news.php?id=585>

#### GETTING TOUGH WITH ONLINE FRAUDSTERS

The UK Government is to get tough with rogue online traders in an attempt to make e-commerce more attractive to consumers.

>> <http://www.net-security.org/news.php?id=587>

#### UNCLE SAM'S INFO-TECH CRISIS

Upgrading agencies' info-handling and data-mining capabilities will be costly. Not doing so could exact an even more horrific price.

>> <http://www.net-security.org/news.php?id=588>

#### COALITION TO UNVEIL NET ID SYSTEM

An industry coalition is set to unveil standards for identity authentication on the Internet, the first step toward making the task of remembering long lists of Web site passwords a thing of the past.

>> <http://www.net-security.org/news.php?id=589>

#### EXCHANGE 2000 TO GET SECURITY SWEEP FIXES

Microsoft is planning to release the third service pack for its Exchange 2000 server software, which will include fixes for bugs discovered as part of its lengthy review of the software code.

>> <http://www.net-security.org/news.php?id=590>

TIME FOR A SPYWARE TAKEDOWN

While legislators jabber on about limiting spam, putting a choke collar on ICANN spyware is being perfected.

>> <http://www.net-security.org/news.php?id=591>

LOCK SPAM AND VIRUSES OUT OF SENDMAIL

Let's take a look at some methods for locking down a popular mail server in the Linux and UNIX realm: Sendmail.

>> <http://www.net-security.org/news.php?id=592>

CYBERTERRORISTS DON'T CARE ABOUT YOUR PC

Forget about viruses. America's real cybersecurity concerns are the vulnerable computer systems that control our power and water supplies. Here are a few ideas about how to keep the infrastructure safe.

>> <http://www.net-security.org/news.php?id=593>

USA TODAY SWATS HACK ATTACK - BUT NOT ENTIRELY

USA Today experienced a hacker attack last night, which took it out of service for three hours.

>> <http://www.net-security.org/news.php?id=594>

NEW CALIFORNIA UNIT TO DEAL WITH SECURITY ISSUES

The State of California must cobble together procedures to both procure and secure its multibillion-dollar IT systems.

>> <http://www.net-security.org/news.php?id=595>

-----

=====  
Computer Security Institute Survey: 90% Say Systems Hacked.

How Secure Is Your Network? Get a FREE Assessment!

<http://www.net-security.org/lm/ads/ads.pl?banner=scannerx1>

=====

[ Vulnerabilities ]

All vulnerabilities are located here:

[http://www.net-security.org/archive\\_vuln.php](http://www.net-security.org/archive_vuln.php)

-----

Multiple Vulnerabilities with Pingtel xpressa SIP Phones

>> <http://www.net-security.org/vuln.php?id=1859>

Microsoft SQL Server 2000 BULK INSERT Buffer Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=1858>

Remote PGP Outlook Encryption Plug-in Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1857>

Carello 1.3 Remote File Execution Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1856>

GoAhead Web Server Directory Traversal and Cross Site Scripting Vulnerabilities  
>> <http://www.net-security.org/vuln.php?id=1855>

Apache Tomcat Cross Site Scripting Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1854>

Internet Explorer Universal Cross Domain Scripting Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1853>

Sun iPlanet Web Server Remote File Viewing Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1852>

iPlanet Search Buffer Overflow Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1851>

Watchguard Firebox Dynamic VPN Configuration Protocol Denial of Service Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1850>

KF Web Server v1.0.2 Arbitrary File and Directory Information Reading Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1849>

Buffer Overflow in MyWebServer  
>> <http://www.net-security.org/vuln.php?id=1848>

BadBlue 1.73 EXT.DLL Cross Site Scripting Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1847>

Technical Details of BadBlue EXT.DLL Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1846>

Bea Weblogic Performance Pack Denial of Service  
>> <http://www.net-security.org/vuln.php?id=1845>

MacOS X SoftwareUpdate Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1844>

---

[ Advisories ]

All advisories are located at:  
[http://www.net-security.org/archive\\_advi.php](http://www.net-security.org/archive_advi.php)

---

SuSE Security Advisory - DNS resolver vulnerability  
>> <http://www.net-security.org/advisory.php?id=847>

CERT Advisory CA-2002-20 - Multiple Vulnerabilities in CDE ToolTalk  
>> <http://www.net-security.org/advisory.php?id=846>

SuSE Security Announcement - bind, glibc  
>> <http://www.net-security.org/advisory.php?id=845>

SuSE Security Announcement - squid  
>> <http://www.net-security.org/advisory.php?id=844>

---

[ Virus News ]

All virus news are located at:  
<http://www.net-security.org/viruses.php>

---

New Panda PerimeterScan Qmail Edition Released  
>> [http://www.net-security.org/virus\\_news.php?id=49](http://www.net-security.org/virus_news.php?id=49)

Benjamin Worm Gets a "B" Version  
>> [http://www.net-security.org/virus\\_news.php?id=48](http://www.net-security.org/virus_news.php?id=48)

Panda Software: Klez.I Leads the Top Ten List  
>> [http://www.net-security.org/virus\\_news.php?id=47](http://www.net-security.org/virus_news.php?id=47)

Etap Author Tells Us The Score  
>> [http://www.net-security.org/virus\\_news.php?id=46](http://www.net-security.org/virus_news.php?id=46)

---

[ Security world ]

All press releases are located at:  
[http://www.net-security.org/press\\_main.php](http://www.net-security.org/press_main.php)

---

Datakey Smart Card Technology Deployed To Secure Online Submission Of Commercial Documents

>> <http://www.net-security.org/press.php?id=894>

Rainbow eSecurity and i-SSL Integrate Security Solutions for USB Keys and SSL Acceleration Devices

>> <http://www.net-security.org/press.php?id=893>

Secos Continues Rapid Expansion Of Successful Information Security Partnership Program

>> <http://www.net-security.org/press.php?id=892>

Zero-Knowledge Systems' Stephanie Perrin to Speak at Comdex Canada's "Security Versus Privacy" Keynote Panel

>> <http://www.net-security.org/press.php?id=891>

Security Company-PivX, Adds World Class Security Researcher and Announces Major New Vulnerability in Internet Explorer

>> <http://www.net-security.org/press.php?id=890>

Black Hat Briefings 2002 Keynotes Include NSA Director And Special Advisor To The President

>> <http://www.net-security.org/press.php?id=889>

RSA Security Embraces SAML Standard Across Product Lines

>> <http://www.net-security.org/press.php?id=888>

GFI Launches Email Exploit Engine - New Technology To Block Email Threats

>> <http://www.net-security.org/press.php?id=887>

McAfee.com Reaches Two Million Subscription Milestone

>> <http://www.net-security.org/press.php?id=886>

Rainbow Ships NetSwift iGate Web Security Appliance for Instant Private Webs

>> <http://www.net-security.org/press.php?id=885>

Major U.S. bank deploying Datakey's new Card Management System

>> <http://www.net-security.org/press.php?id=884>

[ Featured articles ]

All articles are located at:

[http://www.net-security.org/articles\\_main.php](http://www.net-security.org/articles_main.php)

Articles can be contributed to [staff@net-security.org](mailto:staff@net-security.org)

---

#### SECURITY IN OPEN VERSUS CLOSED SYSTEMS - THE DANCE OF BOLTZMANN, COASE AND MOORE

Some members of the open-source and free software community argue that their code is more secure, because vulnerabilities are easier for users to find and fix. Meanwhile the proprietary vendor community maintains that access to source code rather makes things easier for the attackers.

>> <http://www.net-security.org/article.php?id=145>

#### MICROSOFT SQL SERVER PASSWORDS (CRACKING THE PASSWORD HASHES)

SQL Server uses an undocumented function, `pwdencrypt()` to produce a hash of the user's password, which is stored in the `sysxlogins` table of the master database. This is probably a fairly common known fact. What has not been published yet are the details of the `pwdencrypt()` function. This paper will discuss the function in detail and show some weaknesses in the way SQL Server stores the password hash. In fact, as we shall see, later on I should be saying, 'password hashes'.

>> <http://www.net-security.org/article.php?id=146>

#### DSL SECURITY WHITEPAPER

This contribution provides an overview of some of the security aspects of DSL-based corporate networks.

>> <http://www.net-security.org/article.php?id=147>

#### PGP OUTLOOK ENCRYPTION PLUG-IN VULNERABILITY

eEye staffers Marc Maiffret and Riley Hassell, were again busy on finding the bugs, so a new advisory hit the "streets" today. This time, there is a remote vulnerability in NAI PGP Outlook plug-in which is included in these products: NAI PGP Desktop Security 7.0.4, NAI PGP Personal Security 7.0.3 and NAI PGP Freeware 7.0.3.

>> <http://www.net-security.org/article.php?id=148>

---

[ Security Software ]

Windows software is located at:  
[http://net-security.org/software\\_main.php?cat=1](http://net-security.org/software_main.php?cat=1)

Linux software is located at:  
[http://net-security.org/software\\_main.php?cat=2](http://net-security.org/software_main.php?cat=2)

---

TOSKA 0.8BETA

TOSKA (Toolkit for OpenSSH Key Administration) provides a way for network administrators to centralize their SSH key management.

>> <http://www.net-security.org/software.php?id=190>

PPTPPROXY 1.6

This program will forward a PPTP VPN connection through a Linux firewall.

>> <http://www.net-security.org/software.php?id=191>

ATRANS 0.9

aTrans is a secure, easy to use, easy to move, P2P chat and file transfer utility.

>> <http://www.net-security.org/software.php?id=192>

FREERADIUS 0.6

The FreeRADIUS Server Project is a high-performance and highly configurable RADIUS server.

>> <http://www.net-security.org/software.php?id=193>

LINKSYSMON 1.0.1

linksysmon is a tool for monitoring Linksys BEFSR41 and BEFSR11 firewalls under Linux and other Unix-like operating systems.

>> <http://www.net-security.org/software.php?id=194>

FOUREYES 1.0

FourEyes allows network administrators to enforce a four eyes policy on Windows NT, 2000 and XP by requiring two users to authenticate during a local logon.

>> <http://www.net-security.org/software.php?id=195>

DYNAMICAL PASSWORDS 1.0

With "Dynamical Passwords" you may generate passwords on any date (even each day). There is no need to remember or save all these generated passwords as far as you can remember your personal password (key) and the date.

>> <http://www.net-security.org/software.php?id=196>

XML SECURITY LIBRARY 0.0.7

XML Security Library is a C library based on LibXML2 and OpenSSL.

>> <http://www.net-security.org/software.php?id=197>

### BIG CROCODILE 3.3

Big Crocodile is a powerful, secure password manager. Storage of all your passwords, logins and hyperlinks in a securely encrypted file.

>> <http://www.net-security.org/software.php?id=198>

### MESSAGEWALL 0.9.33

MessageWall is a free software SMTP proxy. It sits between the outside world and your mail server and keeps out viruses, spam and mail relaying.

>> <http://www.net-security.org/software.php?id=199>

-----  
Questions, contributions, comments or ideas go to:

Help Net Security staff  
[staff@net-security.org](mailto:staff@net-security.org)  
<http://net-security.org>

-----  
Subscribe to this weekly digest on:  
<http://www.net-security.org/subscribe.php>

Unsubscribe by sending your e-mail address to:  
[info@net-security.org](mailto:info@net-security.org) with UNSUBSCRIBE in the message body.

The archive of the newsletter in TXT and PDF format is available  
[http://www.net-security.org/newsletter\\_archive.php](http://www.net-security.org/newsletter_archive.php)