



HNS Newsletter

Issue 170 - 14.07.2003.

<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>.

ALERT: How a Hacker Launches a SQL Injection Attack

It's as simple as placing additional SQL commands into an input box on a web form giving hackers complete access to all your backend data!

Firewalls and IDS will not stop SQL Injection attempts because they are NOT seen as intrusions.

Download this ***FREE*** white paper from SPI Dynamics for a complete guide to protection!

<http://www.spidynamics.com/mktg/sqlinjection56>

Table of contents:

- 1) Security news
- 2) Vulnerabilities
- 3) Advisories
- 4) Articles
- 5) Reviews
- 6) Security world
- 7) Virus news

[Security news]

SWISS TURN UP THE HEAT ON CYBERCRIME

Swiss efforts to combat cybercrime appear to be bearing fruit six months after the government set up a special unit to police the Internet.

<http://www.net-security.org/news.php?id=3048>

WEB HACKING CONTEST CLAIMS 'NO BIG NAMES'

Computer hackers vying in a global contest on Sunday defaced

a slew of Web sites, but the damage was confined to the Internet's backwater of small, unsecured sites, security officials said.

<http://www.net-security.org/news.php?id=3049>

PROMISES TO PROTECT CUSTOMER DATA GET SOME ATTENTION

Most online businesses promise they'll protect customer data as if it were their own. Now the government is holding them to it.

<http://www.net-security.org/news.php?id=3050>

KERNEL ROOTKITS EXPLAINED

In this article the basics of 'rootkitting' will be explained, and how you can protect yourself against them.

<http://www.net-security.org/news.php?id=3051>

DUTCH MASS SPAMMER LOSES GRIP

Martijn Bevelander is not a happy man. The 23 year-old Dutch entrepreneur was exposed last week by the BBC as a mass spammer. Now his company Megaprovider is sinking.

<http://www.net-security.org/news.php?id=3052>

MIT PROJECT LETS CITIZENS 'GOOGLE' FEDS

Its creators hope it will become a Google of government, a massive Internet clearinghouse of information to help citizens track their leaders as effectively as their leaders track them.

<http://www.net-security.org/news.php?id=3055>

START-UP STREAMLINES E-MAIL ENCRYPTION

Voltage Security has its sights set on making sure that more people encrypt their e-mail.

<http://www.net-security.org/news.php?id=3056>

EDS SET TO PROTECT MOBILE DATA

Hoping to cash in on a growing disaster-recovery market, Electronic Data Systems launched a service to protect data held on desktop computers, laptops and personal digital assistants.

<http://www.net-security.org/news.php?id=3057>

RESEARCHERS KEEP AN EYE ON THE FUTURE OF SECURITY

The idea of checking physical characteristics to authenticate a person's identity has a long and distinguished history.

<http://www.net-security.org/news.php?id=3058>

THE FINE ART OF PASSWORD PROTECTION

During a recent European trade show, organizers convinced 90 percent of office workers traveling through a London tube

station to reveal their computer passwords. They merely included the question at the end of a long list of seemingly harmless queries.

<http://www.net-security.org/news.php?id=3059>

REQUIEM FOR A HACKER

Security has become a very big business in IT over the past few years. You'd think its growth as a commercial market would have made all our information more secure. It hasn't.

<http://www.net-security.org/news.php?id=3060>

BASIC HARDENING LINUX

This article includes the essential steps an administrator must follow to harden a Unix system; specifically, a Red Hat Linux system.

<http://www.net-security.org/news.php?id=3061>

ANTIVIRUS CONCERNS IN XP AND .NET ENVIRONMENTS

This article will discuss new antivirus concerns within Microsoft's .NET framework and Windows XP applications.

<http://www.net-security.org/news.php?id=3062>

ORACLE'S SECURITY GUARD

Exec vying to put lock on hot market.

<http://www.net-security.org/news.php?id=3063>

ASSET PROTECTION

Banks come in all shapes and sizes, from global financial services firms down to the smallest credit unions. But finding better ways to ensure security is a common concern.

<http://www.net-security.org/news.php?id=3064>

VIRUS ATTACKS UP 17.5%

Last month's Bugbear-B worm was the most pernicious virus in the first half of 2003. Security firm Sophos received reports about 3,855 new viruses, a 17.5% increase compared to the same period last year, the firm said.

<http://www.net-security.org/news.php?id=3065>

PRO-CHINA SITE HIT BY HACKERS

Last weekend's hacking contest may have struck a high-profile Chinese site.

<http://www.net-security.org/news.php?id=3067>

EXPERTS SAY HACKER HYPE IS THREAT ON ITS OWN

After a widely publicized hacking contest failed to cause as much damage as expected last weekend, computer security experts are advocating a novel response for Internet hackers out for a digital joy ride: ignore them.

<http://www.net-security.org/news.php?id=3068>

SCI-FI SECURITY TECHNOLOGIES A REALITY

Retinal scans, DNA identification access, fingerprint smart cards and voice driven activation.

<http://www.net-security.org/news.php?id=3069>

'SPOOF' E-MAIL SCAM SPREADS

That e-mail may look like it's from a well-known company. But as more people have discovered in recent months, it could be an attempt to defraud you.

<http://www.net-security.org/news.php?id=3070>

SECURITY UNEASE AS GOVERNMENT BUYS SOFTWARE

Sitting at his laptop computer in a hotel near Toronto one day last October, Gregory Gabrenya was alarmed by what he discovered in the sales-support database of his new employer, Platform Software: the names of more than 30 employees of the United States National Security Agency.

<http://www.net-security.org/news.php?id=3071>

HONEYPOTS - HITTING THE SWEET SPOT

Cool new technologies are pushing honeypots closer to prime time. Honeypot guru Lance Spitzner gives us an advance look.

<http://www.net-security.org/news.php?id=3072>

WHO'S WATCHING YOU SURF?

Citizen-rights groups turn to courts, Congress to keep tabs on legal surveillance.

<http://www.net-security.org/news.php?id=3073>

CARELESS PDA USERS THREATEN CORPORATE SECURITY

More people are using PDAs for keeping business data, increasing the security problems faced by corporates, according to the second annual PDA Usage Survey.

<http://www.net-security.org/news.php?id=3074>

USING ETHICAL HACKING TO ENSURE SECURITY

Ethical hacking, also known as internal security auditing, is an effective method to determine security vulnerabilities within IT architectures.

<http://www.net-security.org/news.php?id=3075>

WE'VE FOUND THE PERFECT SOLUTION TO SPAM

The Internet Research Task Force's (IRTF) quest for an effective solution to spam has struck gold in the form of IT specialist Mark McCarron.

<http://www.net-security.org/news.php?id=3076>

WEBCASTERS THREATEN TO SUE RIAA

A group representing small Webcasters is threatening to sue the Recording Industry Association of America on antitrust grounds, fearful that hundreds or thousands of stations will be pushed offline.

<http://www.net-security.org/news.php?id=3079>

FREEBSD 5.1 SHOWS HANDY NEW FEATURES

FreeBSD includes a security utility that can minimize the damage caused by an attack on a service such as BIND or sendmail by running the service within an isolated environment, or jail.

<http://www.net-security.org/news.php?id=3080>

IBM UNVEILS SECURITY LANGUAGE

IBM unveiled a programming language that enables enterprises a way to automate the enforcement of privacy policies across IT applications and systems.

<http://www.net-security.org/news.php?id=3081>

FEDS: SSA VULNERABLE TO IDENTITY THEFT

Congressional investigators working undercover obtained Social Security numbers for nonexistent newborns and used the Social Security numbers of dead people to obtain driver's licenses, exposing weaknesses at the Social Security Administration that could be exploited by identity thieves.

<http://www.net-security.org/news.php?id=3082>

FAKE PAYPAL SITE COULD LEAD TO IDENTITY THEFT

A realistic-looking site purporting to be from PayPal billing is asking for information, including password and PIN details, from users that could enable identity theft.

<http://www.net-security.org/news.php?id=3083>

IE BUGS KEEP COMING

Seventeen days from Bugtraq to patch.

<http://www.net-security.org/news.php?id=3084>

MUMU WORM MAKES A MESS

A worm leaves its mark - and exposes security deficiencies at remote offices.

<http://www.net-security.org/news.php?id=3085>

WLAN SECURITY: DOES ANYBODY CARE?

About half of all enterprises neglect wireless local area network (WLAN) security, according to a new Jupiter Research report.

<http://www.net-security.org/news.php?id=3086>

NETSCREEN PUTS IPV6 IN FIREWALL BETA

Makers of network security gear are lining up to help enterprises and service providers implement IPv6 (Internet Protocol version 6), the next-generation network layer protocol for the Internet that offers a vastly larger number of host addresses.

<http://www.net-security.org/news.php?id=3087>

DECODING MOBILE DEVICE SECURITY

In view of the proliferation of mobile devices, it's surprising how few are appropriately secured against the financial, legal and regulatory risks associated with the potential exposure of sensitive data.

<http://www.net-security.org/news.php?id=3088>

ADOBE AND IBM JOIN TO BOOST PDF SECURITY

IBM is expected to announce a partnership with software maker Adobe Systems on Thursday to boost security in documents created with Adobe's Acrobat software.

<http://www.net-security.org/news.php?id=3089>

WATCH OUT FOR THE SCAMMERS

SurfControl is warning people to use extra security precautions against "brand spoofing," which is a tactic used to defraud people.

<http://www.net-security.org/news.php?id=3090>

SPAM FIGHT DIVIDES ON PARTY LINES

Once thoroughly bipartisan, the debate in Washington over how to reduce the flow of bulk e-mail is now pitting Democrats against Republicans--a development that threatens to complicate enactment of laws regulating spam.

<http://www.net-security.org/news.php?id=3091>

CONNECT SECURELY WITH SSH

You'll undoubtedly want to use ssh to work on your servers from remote sites, but it takes an assortment of tricks to keep progress rolling smoothly.

<http://www.net-security.org/news.php?id=3092>

AUSSIE DEFACER ARRESTED IN PARIS

A 17-year-old French cracker who defaced websites in Australia, Britain, and the United States with political messages has been arrested in Paris and ordered to stay away from the Internet while on parole, police revealed.

<http://www.net-security.org/news.php?id=3093>

SETTING UP A SECURE WIRELESS NETWORK

If you have a low-end access point, your security will be limited to Wired Equivalent Privacy (WEP) and MAC address filters. With a

higher end access point, you'll be able to turn on Temporal Key Integrity Protocol (TKIP).
<http://www.net-security.org/news.php?id=3094>

HOW SECURE IS YOUR BROWSER?

Results of a survey conducted by the Belgian IT security company, ScanIT, indicates that many of the worlds computers are "sitting targets" for attackers, despite the use of virus protection software and firewalls.
<http://www.net-security.org/news.php?id=3095>

IBM INTRODUCES EPAL FOR PRIVACY MANAGEMENT

IBM introduced a set of tools that will help companies automatically set and manage privacy policies that govern access to sensitive data stored in corporate applications and databases.
<http://www.net-security.org/news.php?id=3096>

RFID SPY-CHIPPERS LEAK CONFIDENTIAL DATA ON THE WEB

Public relations flacks eager to win the public over to the benefits of mass RFID (Radio Frequency Identification) chip proliferation have ironically managed to leave their own confidential plans unprotected on the Web.
<http://www.net-security.org/news.php?id=3097>

A HOLISTIC APPROACH TO SECURITY

Time to swap medieval security policies for a more collaborative attitude.
<http://www.net-security.org/news.php?id=3098>

[**Vulnerabilities**]

All vulnerabilities are located here:
http://www.net-security.org/archive_vuln.php

Acroread 5.0.7 Buffer Overflow Vulnerability
<http://www.net-security.org/vuln.php?id=2817>

Gattaca Server 2003 Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=2816>

Microsoft Utility Manager Local Privilege Escalation Vulnerability

<http://www.net-security.org/vuln.php?id=2815>

Apache HTTP Server Type-Map File Denial of Services
<http://www.net-security.org/vuln.php?id=2814>

Named Pipe Filename Local Privilege Escalation Vulnerability
<http://www.net-security.org/vuln.php?id=2813>

TerminatorX Local Root Compromise Vulnerability
<http://www.net-security.org/vuln.php?id=2812>

QShop Priviledge Escalation Vulnerability
<http://www.net-security.org/vuln.php?id=2811>

Bitboard2 Information Disclosure Vulnerability
<http://www.net-security.org/vuln.php?id=2810>

Rockliffe Mailsite Express Unauthorized Mail
Attachments Retrieving Vulnerability
<http://www.net-security.org/vuln.php?id=2809>

Knoppix 3.1 Qt Temporary Files Race Condition Vulnerability
<http://www.net-security.org/vuln.php?id=2808>

IglooFTP PRO Multiple Buffer Overflow Vulnerabilities
<http://www.net-security.org/vuln.php?id=2807>

Microsoft Outlook Web Access Cross Site Scripting Vulnerability
<http://www.net-security.org/vuln.php?id=2806>

ICQ 2003a Password Bypass Vulnerability
<http://www.net-security.org/vuln.php?id=2805>

Canon GP300 Denial of Service Vulnerability
<http://www.net-security.org/vuln.php?id=2804>

VP-ASP SQL Injection Vulnerability
<http://www.net-security.org/vuln.php?id=2803>

cPanel Malicious HTML Tags Injection Vulnerability
<http://www.net-security.org/vuln.php?id=2802>

myServer Denial of Service Vulnerability
<http://www.net-security.org/vuln.php?id=2801>

[**Advisories**]

All advisories are located at:
http://www.net-security.org/archive_advi.php

Conectiva Linux Security Announcement - pam
<http://www.net-security.org/advisory.php?id=2217>

OpenPKG Security Advisory - imagemagick
<http://www.net-security.org/advisory.php?id=2216>

OpenPKG Security Advisory - infozip
<http://www.net-security.org/advisory.php?id=2215>

Cisco Security Advisory - Denial-of-Service of
TCP-based Services in CatOS
<http://www.net-security.org/advisory.php?id=2214>

Debian Security Advisory - New teapop packages
fix SQL injection
<http://www.net-security.org/advisory.php?id=2213>

Microsoft Security Bulletin MS03-023 - Buffer Overrun
In HTML Converter Could Allow Code Executio
<http://www.net-security.org/advisory.php?id=2212>

Turbolinux Server Security Announcement - unzip
<http://www.net-security.org/advisory.php?id=2211>

Debian Security Advisory - New teapop packages
fix SQL injection
<http://www.net-security.org/advisory.php?id=2210>

Debian Security Advisory - New phpsysinfo packages
fix directory traversal
<http://www.net-security.org/advisory.php?id=2209>

Debian Security Advisory - New xbl packages fix
buffer overflow

<http://www.net-security.org/advisory.php?id=2208>

Debian Security Advisory - New unzip packages fix directory traversal

<http://www.net-security.org/advisory.php?id=2207>

Debian Security Advisory - New skk, ddskk packages fix insecure temporary file creation

<http://www.net-security.org/advisory.php?id=2206>

Conectiva Linux Security Announcement - php4

<http://www.net-security.org/advisory.php?id=2205>

Conectiva Linux Security Announcement - imp

<http://www.net-security.org/advisory.php?id=2204>

Mandrake Linux Security Update Advisory - unzip

<http://www.net-security.org/advisory.php?id=2203>

Debian Security Advisory - New mozart packages fix unsafe mailcap configuration

<http://www.net-security.org/advisory.php?id=2202>

Debian Security Advisory - New liece packages fix insecure temporary file creation

<http://www.net-security.org/advisory.php?id=2201>

OpenPKG Security Advisory - php, apache

<http://www.net-security.org/advisory.php?id=2200>

Debian Security Advisory - New x-face-el packages fix insecure temporary file creation

<http://www.net-security.org/advisory.php?id=2199>

Debian Security Advisory - New semi, wemi packages fix insecure temporary file creation

<http://www.net-security.org/advisory.php?id=2198>

Conectiva Linux Security Announcement - openldap

<http://www.net-security.org/advisory.php?id=2197>

Conectiva Linux Security Announcement - ml85p

<http://www.net-security.org/advisory.php?id=2196>

Conectiva Linux Security Announcement - xpdf
<http://www.net-security.org/advisory.php?id=2195>

[**Featured articles**]

All articles are located at:
http://www.net-security.org/articles_main.php

Articles can be contributed to staff@net-security.org

21ST CENTURY INFAMOUS COMPETITIONS
In yet another opinion article, Panda Software's Fernando de la Cuadra, shares his view on virus writers and their contests.
<http://www.net-security.org/article.php?id=522>

MIT KERBEROS 5 RELEASE 1.3 ANNOUNCED
The MIT Kerberos Team announced the availability of the new version of MIT Kerberos. Read on to discover where you can get it as well as the major changes since release 1.2.8.
<http://www.net-security.org/article.php?id=523>

NEW WIRELESS SECURITY SOLUTION FROM AIRDEFENSE
AirDefense introduced its AirDefense Guard 1120 as an entry-level solution to provide the highest level of security and support for enterprise wireless LANs at an affordable price.
<http://www.net-security.org/article.php?id=524>

[**Reviews**]

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

BUILD YOUR OWN SERVER
I've had the pleasure of reading several books that build system administration skills essential for successfully managing a system. This time I went through a title that covers not only the configuration of an operating system on a server but also the actual building of a server. Do the step-by-step instructions deliver? Read on to find out.
<http://www.net-security.org/review.php?id=86>

REVIEW - WIFI SECURITY

Books like the one I'm taking a look at today, clearly show that wireless security is not just about the infamous WEP. This is a hot topic, but is this book worth buying?

<http://net-security.org/review.php?id=85>

THE COMPLETE C++ TRAINING COURSE 4/E

This course could just be the right one to show that object orientation is the most efficient approach to solving software engineering problems. In this sense, it's an excellent choice for newcomers and for experienced C programmers, as both will find its C++ object oriented approach very convincing and understandable.

<http://www.net-security.org/review.php?id=84>

[Security world]

All press releases are located at:

http://www.net-security.org/press_main.php

RSA Security Extends Identity and Access Management to Mainframe Environments

<http://www.net-security.org/press.php?id=1531>

PivX Security Heads Up - Millions of Windows Users Vulnerable

<http://www.net-security.org/press.php?id=1530>

CyberGuard Unveils New Multi-Gigabit Security Appliance Powerhouse

<http://www.net-security.org/press.php?id=1529>

Diversinet Earns NIST Listing for Passport Mobile Security Solution

<http://www.net-security.org/press.php?id=1528>

GFI White Paper Exposes How Hackers Can Elude Anti-Virus Software With Custom Trojans

<http://www.net-security.org/press.php?id=1527>

Leading Market Research Firm Confirms That Websense
Is the World's Foremost Provider of Web Filtering Solutions
<http://www.net-security.org/press.php?id=1526>
Sapo Portal's Web Mail Protected by Panda Software
<http://www.net-security.org/press.php?id=1525>

Equant Selects Ubizen As Global Managed Security Partner
<http://www.net-security.org/press.php?id=1524>

Do Not Spam List May Be Inevitable, But Much Work Required
<http://www.net-security.org/press.php?id=1523>

NetScreen First To Demonstrate IPv6 Support for
Both Firewall and VPN Functions
<http://www.net-security.org/press.php?id=1522>

Zix Corporation Provides Secure Email Services to Jewish
Hospital HealthCare Services and Expands Kentucky Presence
<http://www.net-security.org/press.php?id=1521>

Kingston Communications and Integralis to Offer
Customers Access to Security Expertise
<http://www.net-security.org/press.php?id=1520>

Sygate Achieves Leader Quadrant Position In
Personal Firewall Magic Quadrant
<http://www.net-security.org/press.php?id=1519>

Sygate's Security Solution Receives Ongoing
Industry Validation
<http://www.net-security.org/press.php?id=1518>

Neoteris Unveils The Meeting Series Product Family, Extending
The Instant Virtual Extranet Platform With Secure Online
Meeting Appliances
<http://www.net-security.org/press.php?id=1517>

Rainbow's iKey USB Token Integrated Into Web-based
Secure E-mail S-Mail.com
<http://www.net-security.org/press.php?id=1516>

Intrusion Inc. Software-Appliance CD Turns Standard
Server Platform into IDS Appliance
<http://www.net-security.org/press.php?id=1515>

StarForce Technology and OEM Allied to Protect
European CD-Rs
<http://www.net-security.org/press.php?id=1514>
[**Virus News**]

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

Weekly Virus Report - IRC.Sx2 Trojan, Graps and Ronoper.B Worms
http://www.net-security.org/virus_news.php?id=270

Viruses Reach Record High For Year
http://www.net-security.org/virus_news.php?id=269

Questions, contributions, comments or ideas go to:

Help Net Security staff
staff@net-security.org
<http://net-security.org>

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

Unsubscribe by sending the e-mail address you are subscribed
with to: 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

ALERT: How a Hacker Launches a SQL Injection Attack

It's as simple as placing additional SQL commands into an input
box on a web form giving hackers complete access to all your
backend data!

Firewalls and IDS will not stop SQL Injection attempts because
they are NOT seen as intrusions.

Download this ***FREE*** white paper from SPI Dynamics for a
complete guide to protection!

<http://www.spidynamics.com/mktg/sqlinjection56>
