_vti_fpxploitation

mshannon@fpxploiter.org

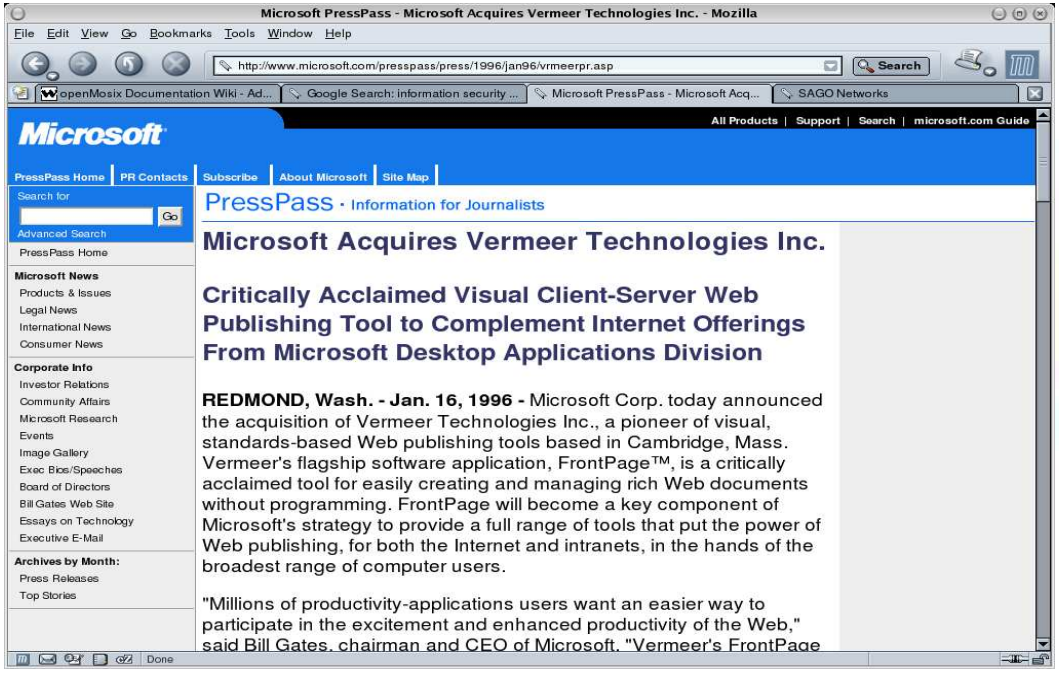
Frontpage: Laying the ground work

What is it?

- Microsoft's integrated Web Site development tool.
- System for adding basic to advanced functionality with little or no web page experience.
- Integrated MS Office package
- Security Nightmare

Who is Vermeer Technologies?

- In early 1995, Vermeer Technologies developed one of the first web publishing tools for simple end users, Frontpage.
- Following enormous success, the application was later bought out by Microsoft and integrated in the Office package.



Frontpage: Decoding the system

Protocol Analysis

Client/Server Protocol Analysis

- Communication between Client and Server.
- Frontpage Client and Server extensions communicate over HTTP PUT requests. The Frontpage client makes requests against Author.dll, Admin.dll, and shtml.exe.

Author.dll(exe)

Authoring commands, uploading, downloading content, reviewing properties, adding enhancements.

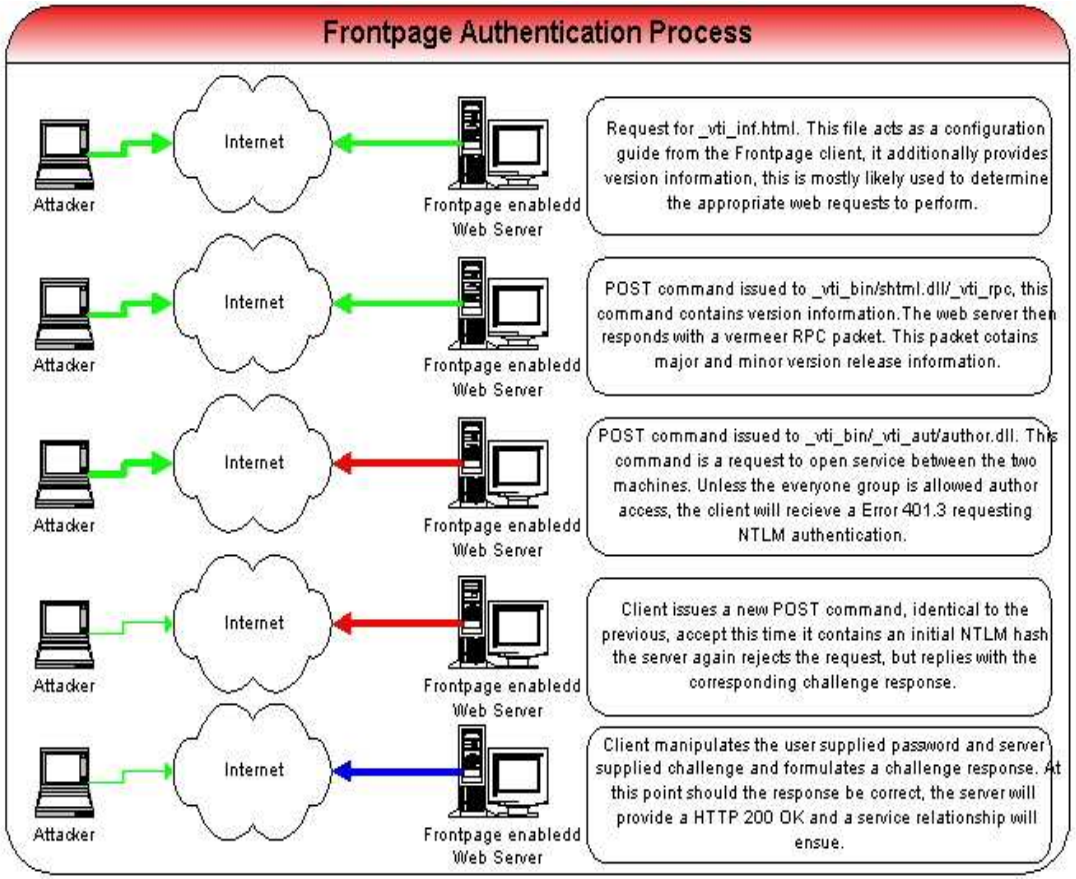
Admin.dll(exe)

Admin commands, including adding additional users, modify user permissions, listing accounts.

Shtml.exe, vti_rpc

Initial access and service negotiation.

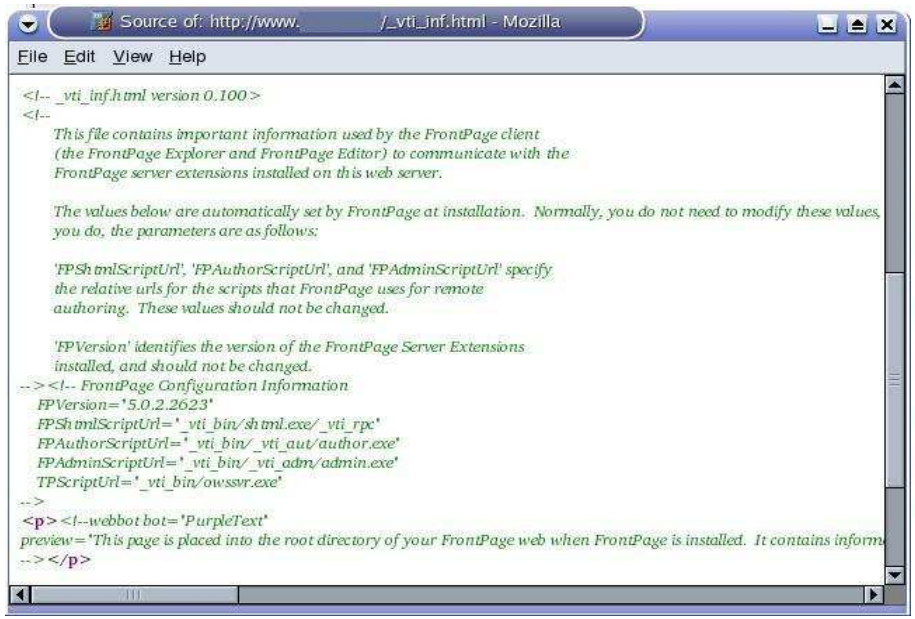
The Authentication System



- This authentication process takes place each time a request is performed, i.e login, upload, download, change permissions, navigate folders, etc.
- While an ineffective use of resources, it does limit attacks based on state.

_vti_inf.html

- _vti_inf.html
  - This file provides configuration information and helps us determine something about the server.



_vti_inf.html Cont.

- Using the following simple guidelines when reading the _vti_inf.html file we can better determine the operating system.

- _vti_inf.html files with references to .exe tools most likely reside on Unix servers.
- _vti_inf.html files with references to .dll tools most likely reside on Windows Servers
- Server extension version numbers can further help us narrow down the options.

_vti_inf Version Table

- Using the information in _vti_inf.html, we can often correctly determine the OS version.

Operating System/Version	*Frontpage Extension Version*
Windows 98/ME Personal Webserver	?
Windows NT 4.0	4.x
Windows 2000	5.x
Windows XP	5.x

Understanding Vermeer RPC Packets

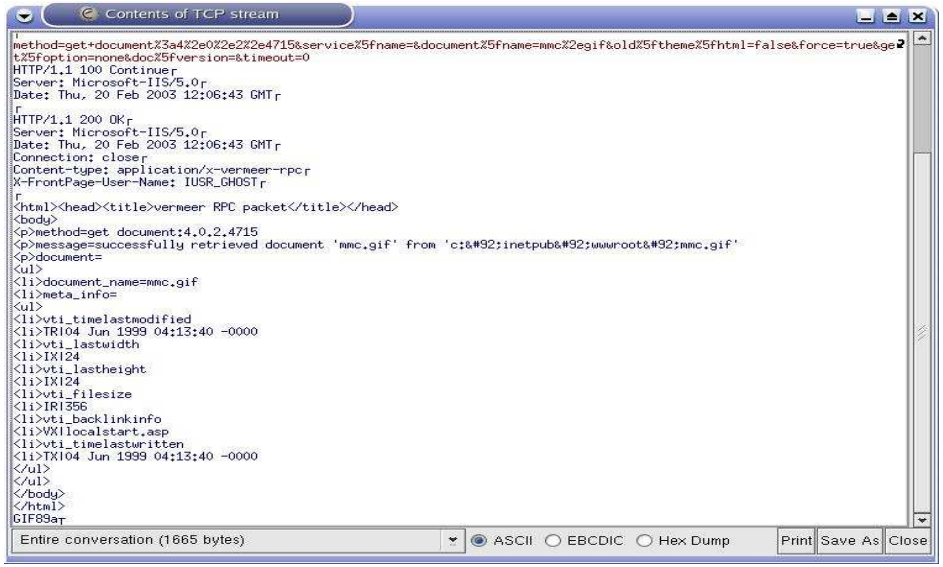
- All responses from Frontpage Server Extensions come in the form of Vermeer RPC Packets.
- Vermeer Packets closely resemble HTML pages.

Information is coded within these packets based on position within HTML tags.

An early precursor to XML?

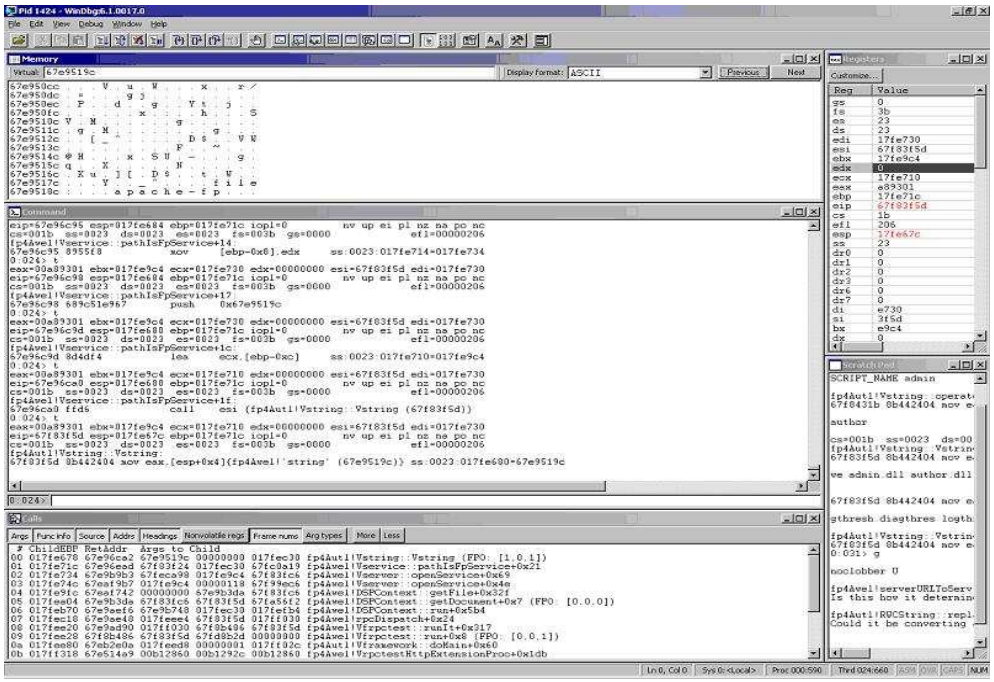
Sample Vermeer RPC Packet

- The following sample VTI Packet contains large amounts of information, including physical drive locations.
  - Physical drive paths may be useful for Unicode exploits.



Debugging Server Extensions

- Using Windbg (Microsoft Debugger) we can explore Frontpage Server Extensions.



How to obtain and configure Windbg

- Download Windbg from Microsoft Debugging Website.
- http://www.microsoft.com/whdc/ddk/debugging/default.mspx

Configure Symbols Server
Symbols are required to determine the functions being called.
http://www.microsoft.com/whdc/ddk/debugging/symbols.mspx

Frontpage Server Extension Dlls

- Based on past debugging exercises, the following is a partial list of dlls used by Frontpage Server Extensions.
  - fp4Autl.dll
  - ffp4Awel.dll
  - fp4amsft.dll
  - fp4Avss.dll
  - Author.dll
  - Admin.dll

Basic tips for getting started in debugging

- Multiple guides and tutorials available for debugging.
  - Windbg specific help files
  - Google
- Simple commands to remember
  - bm
    - Set Breakpoints
      - (ex, bm fp4Awel!*)
  - bc
    - Clear Breakpoints
  - g
    - Go
  - p
    - pause

Interesting Discoveries

- Fp4Awel!Vservice
  - Forms a listing of all documents on the defined web prior to accepting a request. References listing when replying to a request.

Fp4Awel!DSPContext:getFile, get Document

Called when downloading a file via Frontpage, perhaps there are options for Buffer overruns?

NTDLL

Called during authentication, do some of the prior attack vectors still apply?

Frontpage: Knocking on the door

Custom Tools

fpxploiter -> Frontpage Vulnerability Scanner

Perl-Gtk Scanning tool

Summary

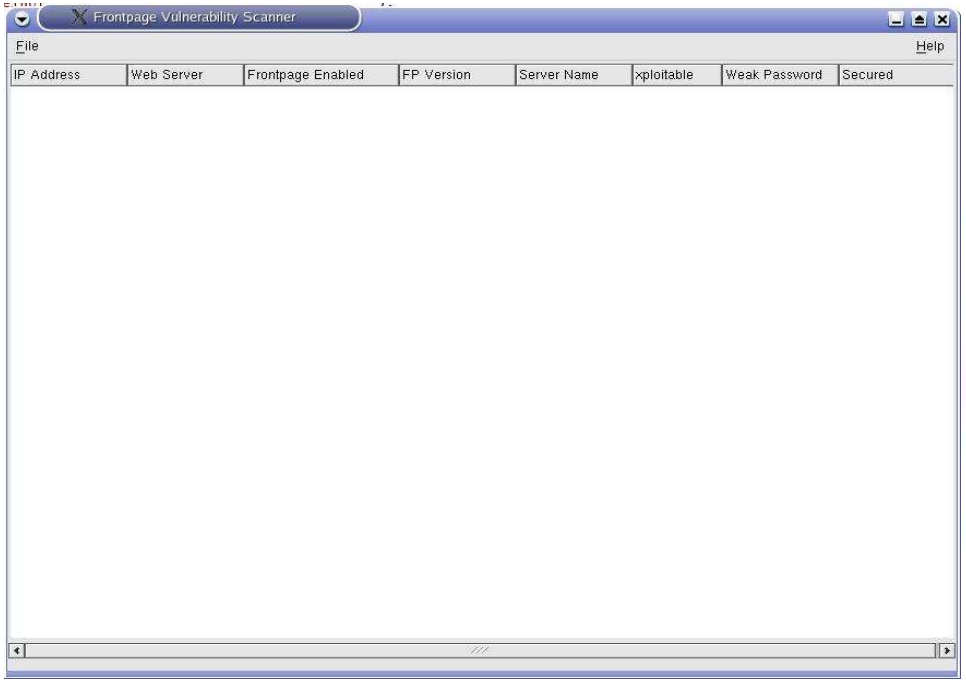
- Now that we have a better understanding of how Frontpage works, let's see about finding vulnerable targets.
- This is what brought about fpxploiter.

It's a Perl-Gtk application the provides capability for:

- Locating Frontpage accessible webservers, using default options, or user defined accounts and passwords.
  - Servers without passwords
  - Servers with weak passwords

Using fpxploiter: How to Start

- Start fpxploiter with the command fpxploiter.
- Application opens with main window.

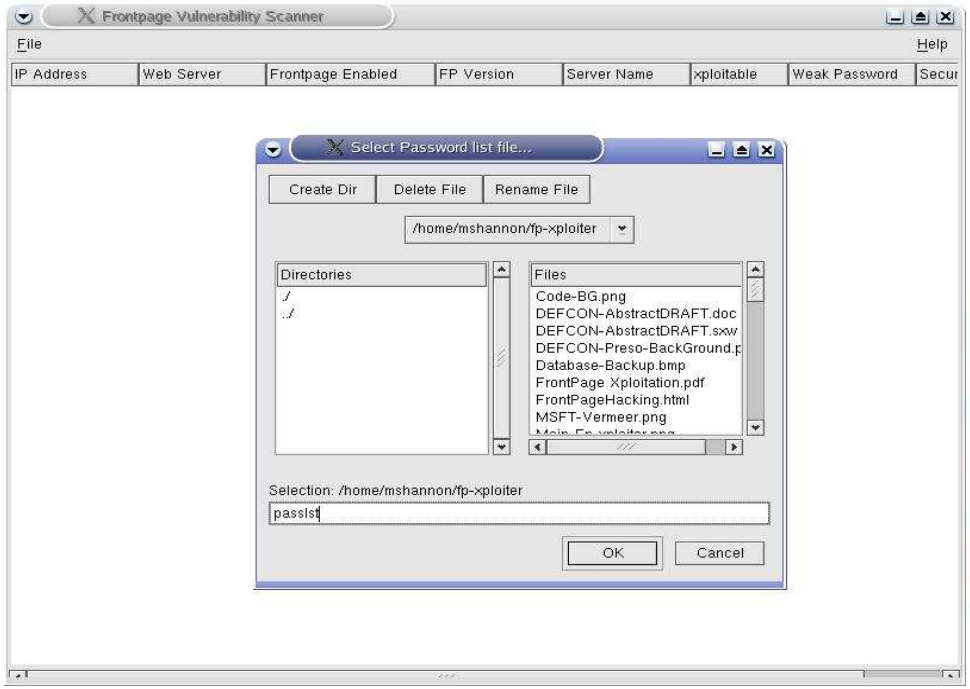


Using fpxploiter: How the scanner works?

- Start by providing a target list, the current configuration of the tool does not allow scanning of more than one Class C at a time.
- Select File->Set Targets or press Ctrl-T.
- Enter the host targets.

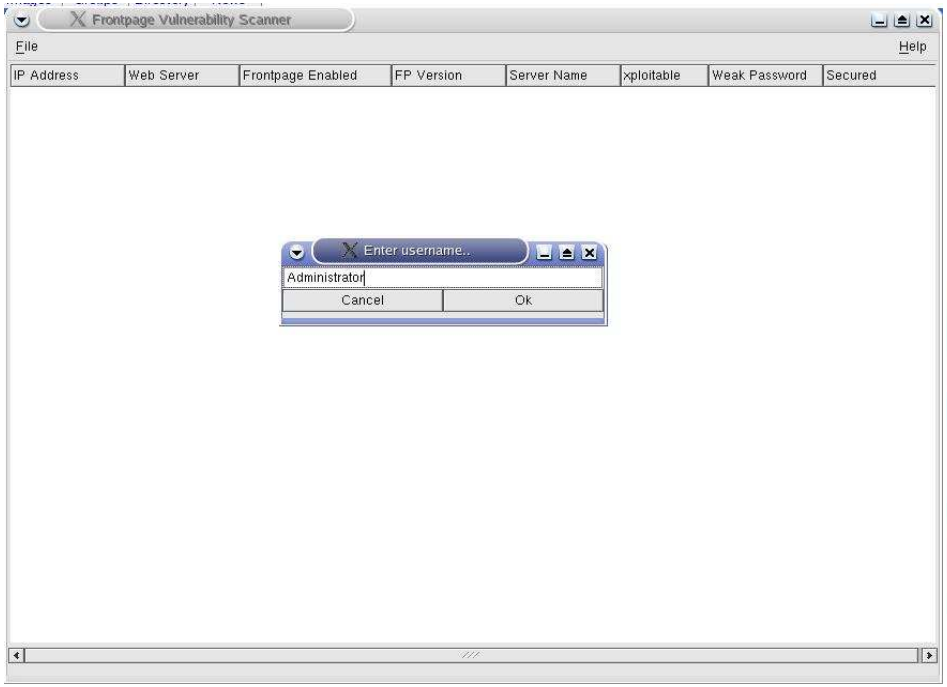
Using fpxploiter: How modify the password list?

- Select File->Set Password List and select you new password list file.



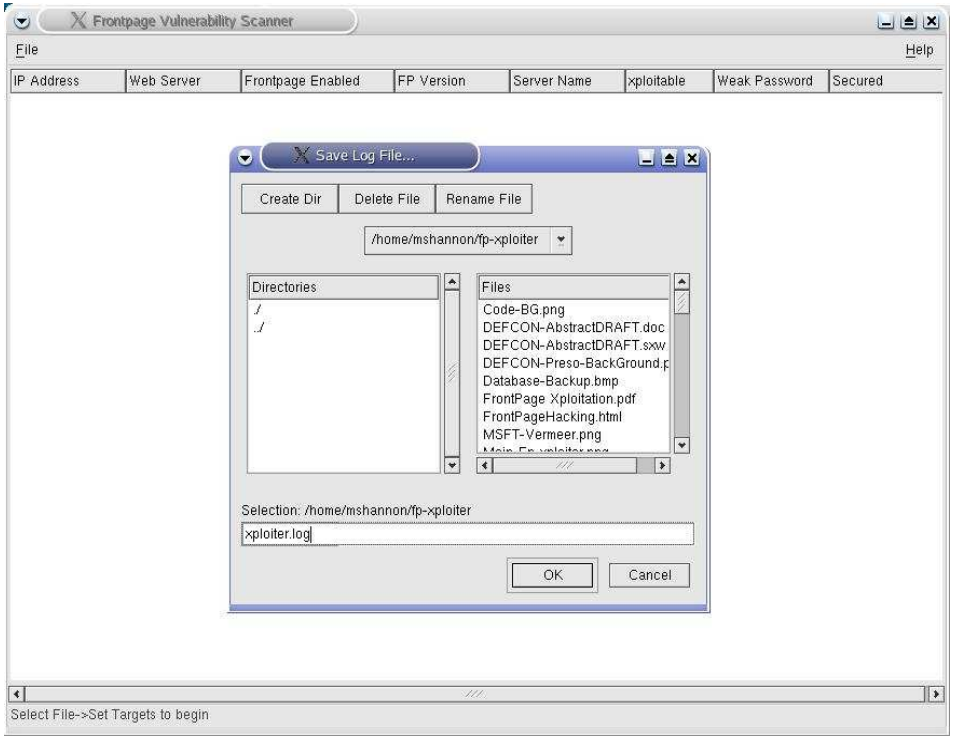
Using fpxploiter: How modify the default user account?

- Select File->Set User account and enter your new user account.



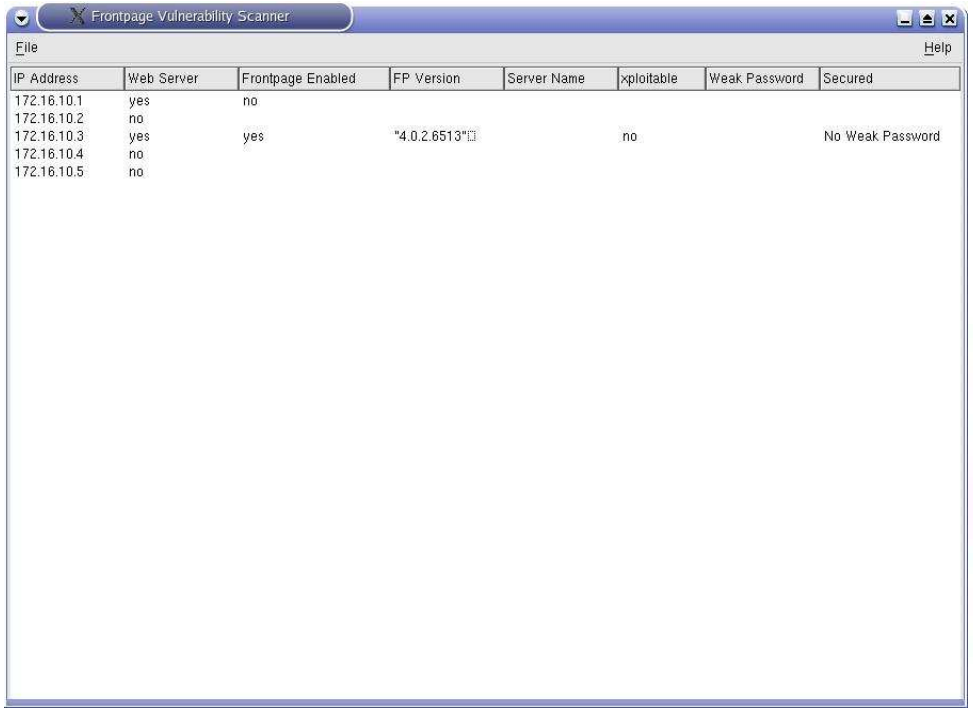
Using fpxploiter: How to export the results?

- Select File->Save Log and select the destination for your log file, use this AFTER the scanning is complete.



Additional Screen Captures

- Fpxploiter during a scanning session.



Future Directions

- Support for Apache Frontpage extensions.
- Redesign of the fpxploiter tool to provide generic Frontpage access library.
- Rebuild in C/Gtk or C++/QT.
- Support for uploading content.

Code

- All Code for fpxploiter is available the the following website.
  - http://www.fpxploiter.org
- Additionally it's on the DEFCON CD.

Frontpage: What to do when your there

ASP for Hackers

SQL Server Database Hunting

- SQL Server Database Access Tools
- Custom ASP pages that allow us to execute queries and explore SQL Servers.
- Using fpxploiter to locate vulnerable servers.

Tie it all together with ASP pages to execute sql queries against the database.

Summary

- Fpxploiter helps us find vulnerable web servers.
- SQLUltimate.asp contains custom asp code that functions as a SQL Analyzer.
  - Ideas?

    Add SQL Server users (if your in the System Admin role)
    Access corporate data
    Execute extended stored procedures
    Locate application accounts and passwords

Screen Capture

- The following screen capture shows the SQLUltimate.asp and a resulting query result.

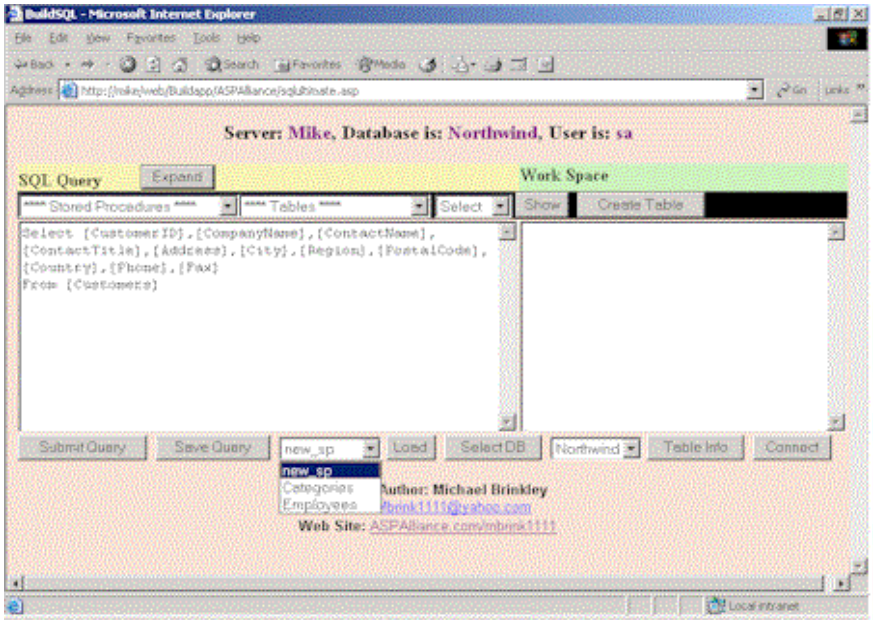


Image taken from http://ASPAlliance.com/mbrink1111/
Copyright 2003 Michael Brinkley, All Rights Reserved
Used with Permission

Code

- All Code for SQLUltimate.asp is available the the following website.
  - ASPAlliance.com
    - http://aspalliance.com/mbrink1111/SQLAnalyzer.asp

Command Line ASP

- ASP Page built to execute console commands and return the results.
- Built by Maceo <maceo @ dogmile.com>

Allows execution of simple commands, good examples include

- netstat -a
- ipconfig -all
- Ver
- set
- net users
- Net localgroup

Summary

- Fpxploiter helps us find vulnerable web servers.
- cmdasp.asp contains custom asp code to execute simple console commands.
  - Ideas?

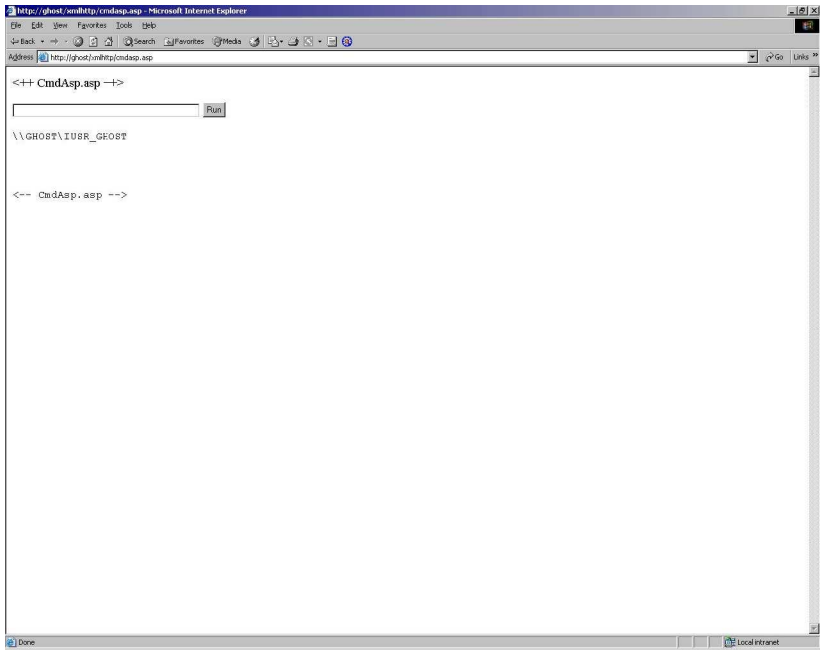
    Use netstat -an & netstat -a as make shift reverse DNS.

    Use net localgroup and net view to understand drive mappings and groups.

    Use ping to find additional servers

Screen Capture

- The following screen capture shows cmdasp.asp in action.



Code

- All Code for cmdasp.asp is available the the following website.
  - http://www.securiteam.com/tools/5AP020U35C.html

Future Ideas

- ASP Code can be used in conjunction with the winsock control to provide “scanning” from the webserver.
- ASP Code can be used to view SMB Shares and Remote Administration (See http: //cifs.novotny.org/, amazing work with ASP.NET)
- ASP Code can be used with xmlhttp controls to navigate internal web sites (Intranets)

Frontpage: Holding down the fort

Securing Frontpage through best practices

Strong Passwords

- As in most systems, your last line of defense is your password, and Frontpage is no different.

  Choose strong passwords, consisting of upper and lowercase characters (with LANMAN this is *rather meaningless*), numbers, and special characters.

  Stick with passwords over eight characters in length.

Changed Admin Account

- As is good practice, consider changing the name of your Administrator account.
- Choose something meaningful, however avoid the typical choices, such as:
  - Root
  - Admin
  - 123
  - Password

Concept of least privilege

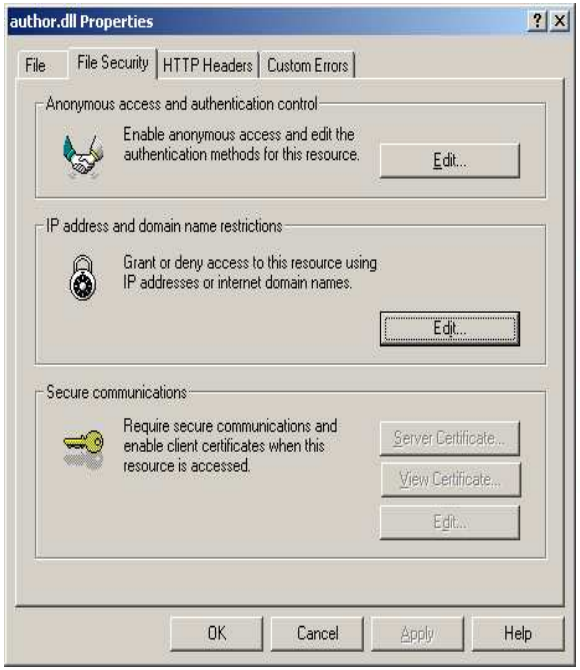
- Only provide the access necessary to get the job done.

  Use the Frontpage roles to assign users Author rights to specific webs as appropriate.

  Reserve Admin rights for specific accounts.

IP Restrictions

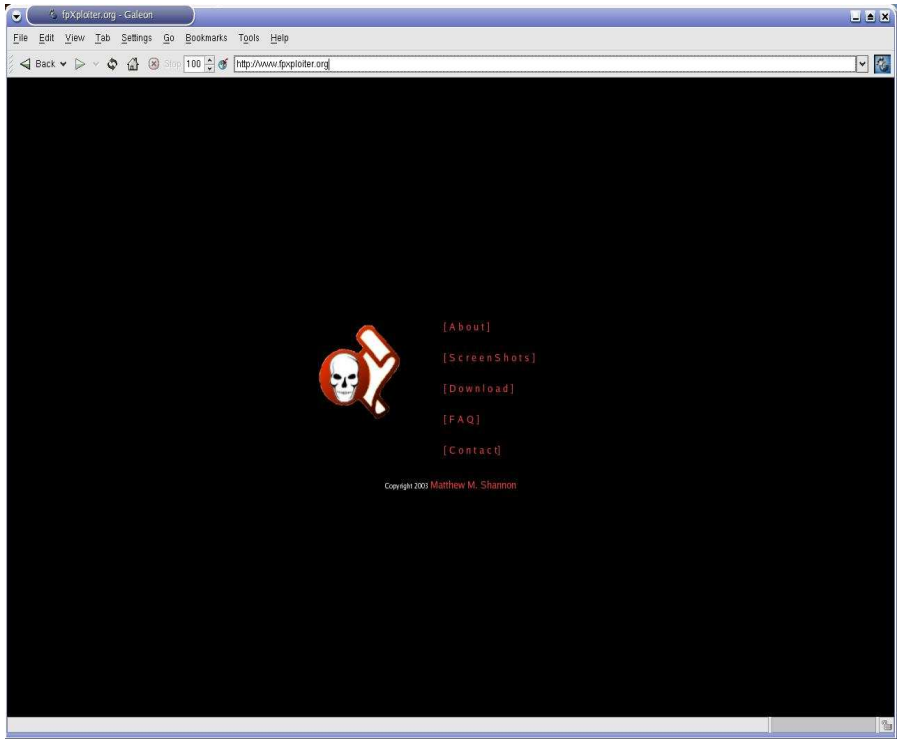
- Using IIS native IP based restrictions you can effectively block a large portion of Frontpage attacks.
- Use the IIS Access tab to block access to the admin.dll and author.dll to IP addresses outside of your internal range.
  - Additionally, consider segmenting your developers and giving this group access only.



Frontpage: Closing words

Fpxploiter.org Site

- Clearing house for code and commentary.



References and Links

- References to the many sources used in this research, and a thanks to all involved.

Older Frontpage Hacking Texts

http://www.insecure.org/sploits/Microsoft.frontpage.insecurities.html

Perl-Gtk Tutorial

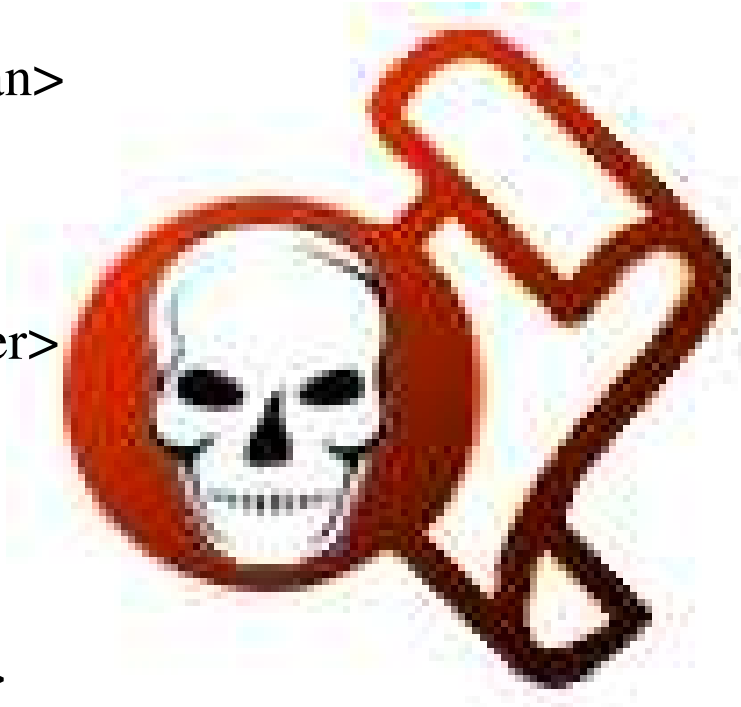
http://personal.riverusers.com/~swilhelm/gtkperl-tutorial/

Microsoft Frontpage MSDN

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnservext/html/fpse02win.asp

Thanks and Credits

- This project would never have been made possible without the support of the following people.
  - Mary Shannon <Wife and Greatest Fan>
  - Matthew Decker <Mentor>
    - mjdecker@kpmg.com
  - Michael D'Andrea <Graphics Designer>
    - centralsource@hotmail.com
  - Stephen Bickle <Technical Review>
    - steve@xsec.net
  - Stephen Wilhelm <Perl-Gtk Tutorial>



Questions or Comments?