

FrontPage: 2003

Exploiting, Abusing, and Securing the FrontPage
Server Extensions on Windows Server 2003

Mark Burnett

FrontPage: 2003

Exploiting, Abusing, and Securing the FrontPage
Server Extensions on Windows Server 2003

Mark Burnett

Background

History of the FPSE

Different names, same old holes

What products include FPSE?

Risks

Are the FPSE as insecure as everyone says?

What are the real risks?

- Increased attack surface
- Entry point
- Information gathering
- Running on system partition
- Insufficient logging
- Storing files within the web root

Risks

What are some greater risks?

- Confusing security model
- Running in-process with inetinfo.exe
- Relaxed NTFS permissions
- Cannot be secured without NTFS

The FPSE Files

The same files?

- _vti_bin/shtml.dll
- _vti_bin/_vti_aut/author.dll
- _vti_bin/_vti_adm/admin.dll

FPSE 2002

- _vti_bin/owssvr.dll
- _vti_bin/_vti_adm/fpadm.dll

FPSE Directories

_vti_bin – FPSE Binaries

_private -

_vti_cnf

_vti_pvt

_vti_script

_vti_txt

Decoding vti_rpc

Sending vti_rpc methods

- POST to FPSE binaries
- GET to owssvr.dll
- Multiple posts using CAML

Interpreting output

Sample Output

- `<html><head><title>vermeer RPC packet</title></head>`
- `<body>`
- `<p>method=list services:4.0.2.0`
- `<p>services_list=`
- ``
- `SR|msiis`
- `vti_usagevisitsbyweek`
- `UX|337 380 423 501 297`
- `vti_usagebymonth`
- `UX|88 4195 2667 3497 90`
- `vti_welcomenames`
- `VX|Default.htm Default.asp Default.aspx`
- `vti_adminurl`
- `SR|/_vti_bin/_vti_adm/fpadmdll.dll`

Cool vti_rpc Tricks

Finding unprotected web sites

Listing webs

Other info gathering

```
method=list+services:4.0.2.0000&service_name=
```

vti_rpc Exploits

New exploits to be announced

Other Exploits

New exploits to be announced

Updating the FPSE

Finding product updates

Confusing and inconsistent

Manual fixes

Manual Fixes

Htimage.exe and Imagemap.exe

- Microsoft's solution
- Another Microsoft solution
- The real solution?

The Security Model

Browse, Author, and Administer
NTFS Permissions on web root
Common Mistakes

Installing & Uninstalling

Why are the directories there on a clean install?

Why won't they uninstall?

How do you remove them?

Moving the FPSE

1. Move the binaries
2. Update the registry
3. Update the metabase

Securing the FPSE

The FPSE can be used safely if you:

- Secure user accounts

- Set proper NTFS permissions

- Set proper IIS permissions

- Configure the registry defaults

- Keep patched

- Use SSL for authoring

- Manage log files

- Set IP Restrictions

Advanced Techniques

Mirror sites

URLScan Rules

Custom ISAPI filter

FPSE neutered

- NTFS restrictions

- Remove directories

- Disable authoring

FPSE Intrusions

Spotting attacks

Log entries

Other trails

FPSE vs. WebDAV

Snort Rules

Updated Snort rules

Logging FPSE authoring with
Snort

FrontPage Tools

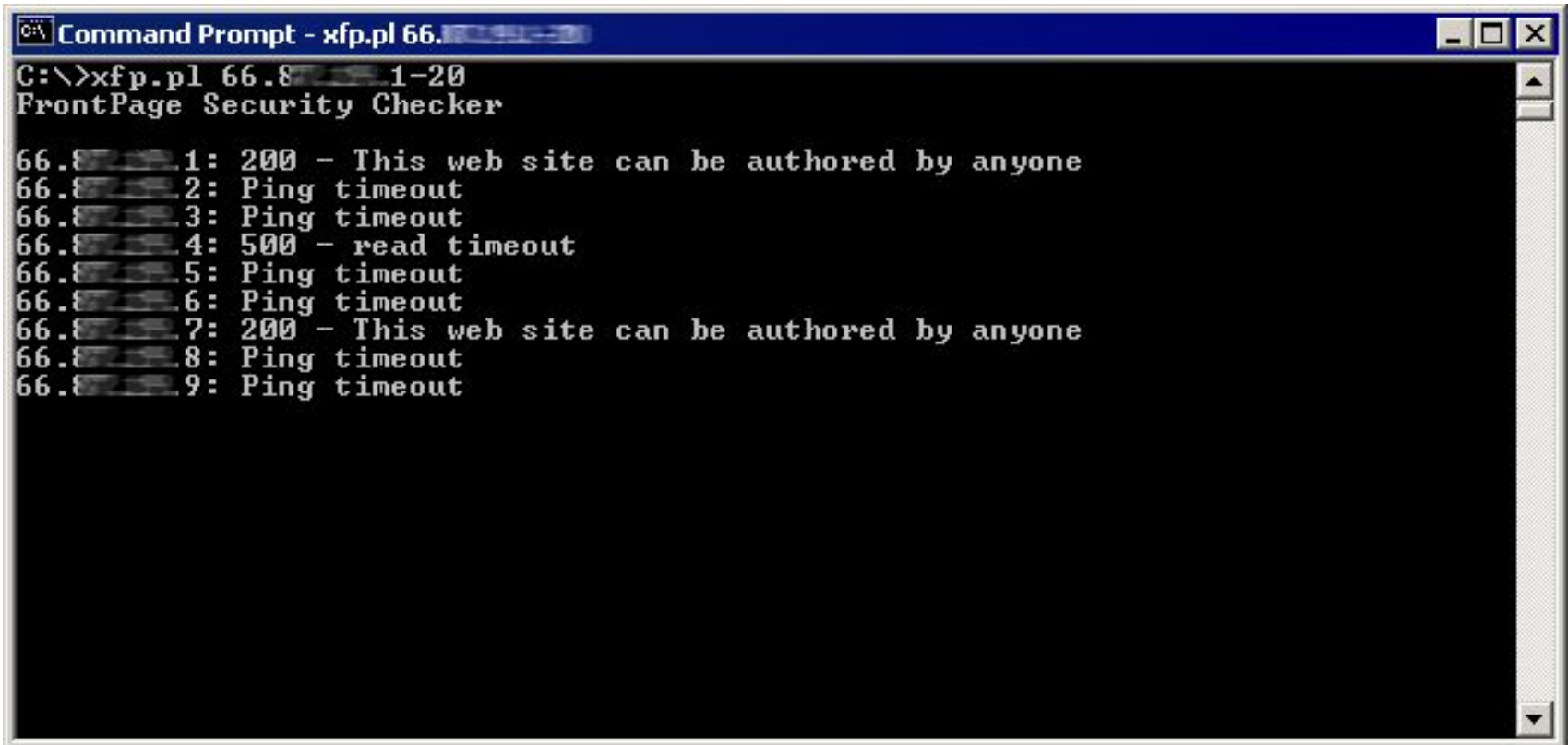
Xfp.pl – FrontPage security scanner

Fpseinfo.pl – FrontPage info gathering

SecureFPSE.cmd – Harden FrontPage Server Extensions

fpBlock – ISAPI filter for FrontPage IP restrictions

Xfp.pl



```
Command Prompt - xfp.pl 66.8...1-20
C:\>xfp.pl 66.8...1-20
FrontPage Security Checker

66.8...1: 200 - This web site can be authored by anyone
66.8...2: Ping timeout
66.8...3: Ping timeout
66.8...4: 500 - read timeout
66.8...5: Ping timeout
66.8...6: Ping timeout
66.8...7: 200 - This web site can be authored by anyone
66.8...8: Ping timeout
66.8...9: Ping timeout
```

Fpseinfo.pl

Returns FPSE information

- Web server platform
- Anonymous user account
- Site statistics
- Hidden directories
- More

SecureFPSE.cmd

Removes htimage.exe and
imagemap.exe

Moves binaries

Registers components in new
Icoation

Updates metabase

Updates registry