Information Extraction
Art of Testing Network Peripheral Devices

Aditya K Sood , SecNiche Security
(adi_ks@secniche.org)

Mauro Risonho de Paula Assumpção
(firebits@backtrack.com.br)

OWASP AppSec Brasil 2010

Disclaimer

All the views solely based on the work conducted by SecNiche Security.

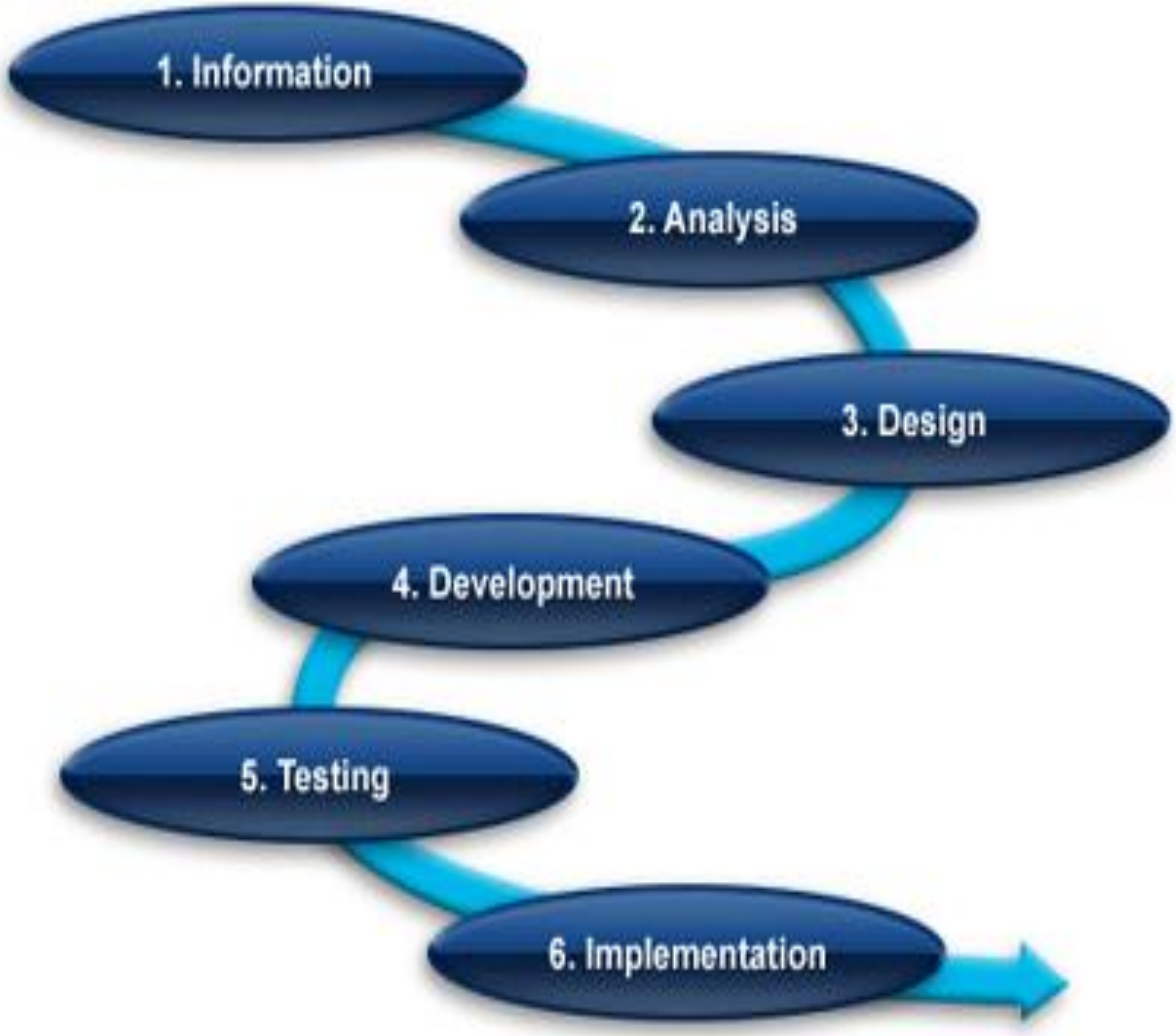
(C) SecNiche Security | http://www.secniche.org

Content should be used with the permission of SecNiche

Agenda

- Why Information Gathering?
- Information Gathering Patterns
- Web Network Devices – Case Studies
- Proxy and Anonoymous Services
- Bad Design Practices
- Free Web
- Conclusion

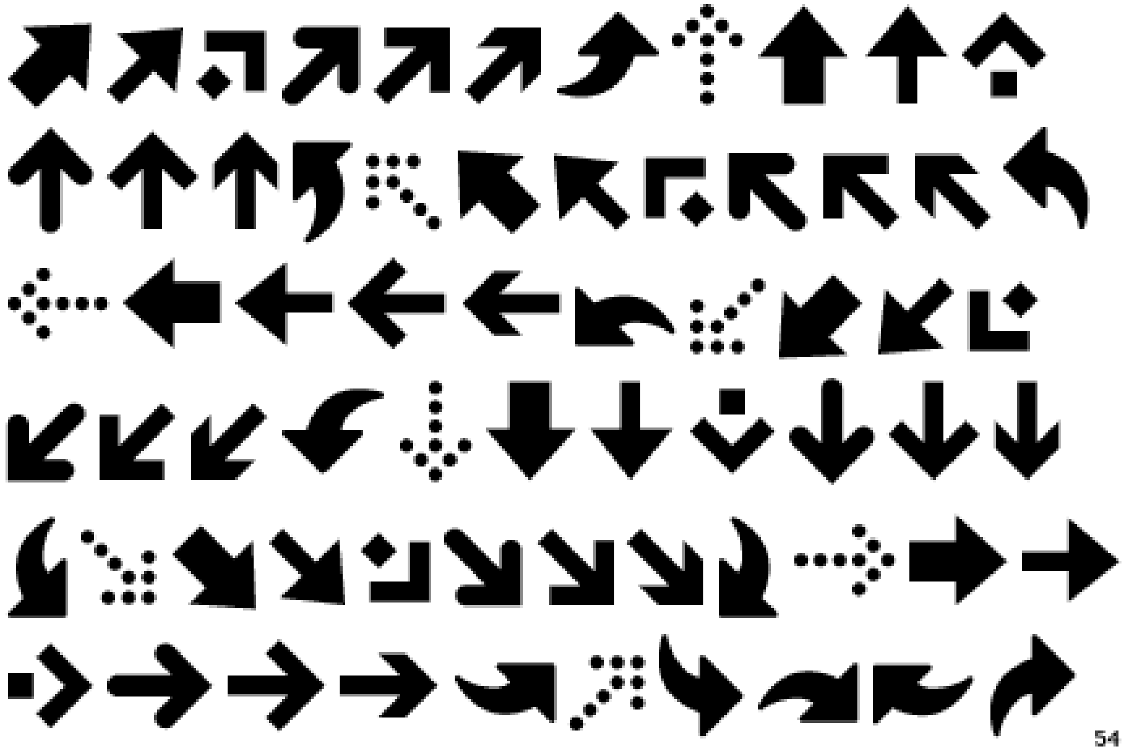
Information Gathering – First Critical Step



1. Information
2. Analysis
3. Design
4. Development
5. Testing
6. Implementation

Information Gathering Facets on Web

- Complex web networks
- Peripheral network devices securing web
- Ofcourse, World Wide Web is random



Why Information Gathering ?

- Criticality in determining the internal structure.
- HTTP request parameters are manipulated.
- 301 moved permanently response code is thrown.
- Devices used to spoof the internal IP addresses.
- Every device has its own working approach
- Used to **Set Cookie** in a different manner.
- Used to change the parameter of HTTP header.
- Analyzing the change in HTTP headers.

Web Information Patterns are Important

Why ?

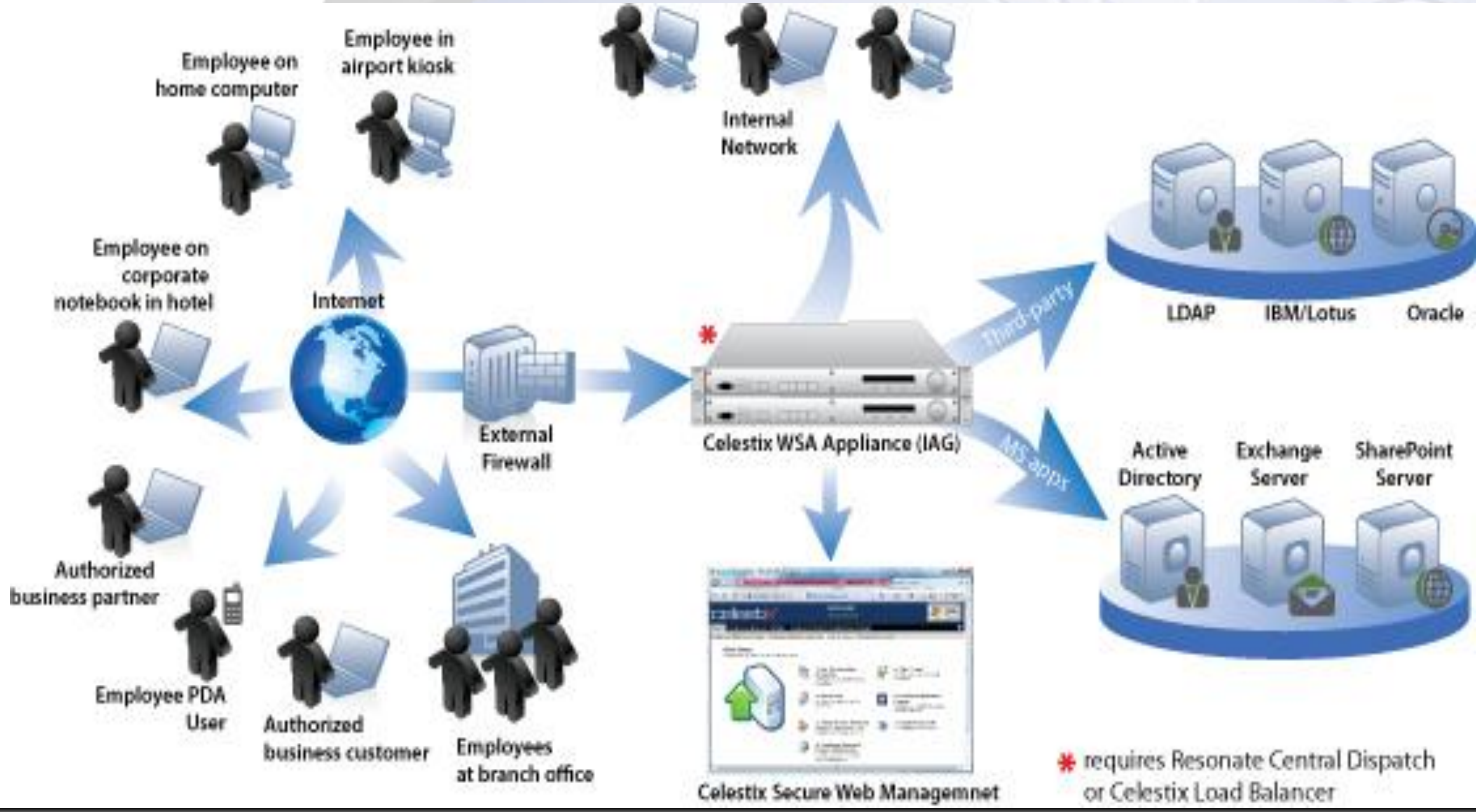
- When “server” header is removed from responses
  - Most of detection signatures are gone
- Banner grabbing does not provide enough information
- Headers reveal less information

Web Network Devices Functionality

- Server Cloaking
- Setting Set-Cookie parameter with unique names
- Response header manipulation
- Different combination and sequence of HTTP responses

Server Cloaking – Anti Information Gathering Rule

- HTTP response camouflaging
- Behavior variation in response to **Searh Engine and Browser**
- Delivering content based on HTTP request


Employee on home computer
Employee in airport kiosk
Internal Network
Employee on corporate notebook in hotel
Internet
LDAP
IBM/Lotus
Oracle
Third-party
External Firewall
Celestix WSA Appliance (IAG)
MS apps
Active Directory
Exchange Server
SharePoint Server
Authorized business partner
Employee PDA User
Authorized business customer
Employees at branch office
Celestix Secure Web Managemnet
* requires Resonate Central Dispatch or Celestix Load Balancer

Case Studies

Almost 80% of the Signatures are new for detection of various web based network devices.

We will show some of the new patterns.

Embedded Devices

HTTP Response Headers Scrambling and Modifications

1. Citrix NetScaler Devices
2. Radware Devices
3. Juniper Devices
4. WatchGuard Firewall
5. Barracuda Devices
6. Profense
7. BinaryCheck
8. Many more..................

HTTP Header Manipulation – Case Check 1 (a)

Load Balancer Behavior

Response Check 1

HTTP/1.1 200 OK\r\n
Date: Tue, 05 Jul 2007 17:05:18 GMT\r\n
Server: Server\r\n
Vary: Accept-Encoding,User-Agent\r\n
Content-Type: text/html;
charset=ISO-8859-1\r\n
nnCoection: close\r\n
Transfer-Encoding: chunked\r\n

Citrix Net Scaler Devices

Response Check 2

→send: 'GET /?Action=DescribeImages&AWSAccessKeyId=0CZQCKRS3J69PZ6QQQR2&Owner.1 =084307701560&SignatureVersion=1&Version=2007-01- 03&Signature=<signature removed> HTTP/1.1\r\nHost: ec2.amazonaws.com:443\r\nAccept- Encoding: identity\r\n\r\n' reply: 'HTTP/1.1 200 OK\r\n' header: Server: Apache-Coyote/1.1 header: Transfer-Encoding: chunked header: Date: Thu, 15 Feb 2007 17:30:13 GMT

→send: 'GET /?Action=ModifyImageAttribute&Attribute=launchPermission&AWSAccessKeyId =0CZQCKRS3J6 9PZ6QQQR2&ImageId=ami-00b95c69&OperationType=add&SignatureVersion=1& Timestamp=2007- 02-15T17%3A30%3A14&UserGroup.1=all&Signature=<signature removed> HTTP/1.1\r\nHost: ec2.amazonaws.com:443\r\nAccept-Encoding: identity\r\n\r\n' reply: 'HTTP/1.1 400 Bad Request\r\n' header: Server: Apache-Coyote/1.1 header: Transfer-Encoding: chunked header:

Date: Thu, 15 Feb 2007 17:30:14 GMT header: nnCoection: close

HTTP Header Manipulation – Case Check 1 (b)

Load Balancer Behavior

Request /Response Check

```
GET / HTTP/1.1
Host	example.com
User-Agent	Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.2.12) Gecko/20101026 Firefox/3.6.12
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
 Keep-Alive	115
Connection	keep-alive

(Status-Line)	HTTP/1.1 301 Moved Permanently
Date	Mon, 08 Nov 2010 19:49:23 GMT
Cneonction	close
Content-Type	httpd/unix-directory
Set-Cookie
uu=9mjpm8rn90Duu4CQwFOZbQPyOCTl4V6yoHENgcCxLaHVsZ3h5dQ99JSlTTGlpO4Tw/IehNChDcKgwZ4S
kLD98SNSnGEggS3RM4FdkEVkaDIDUknUIRRI9fOEyYXz10uCA9bKIgdm+sIHNgpXl6YLh+ChPhIREU2wQK
D9obDCvgGQ0Y3BwNGN8eNSvhGz0h6ypaRIUuPyHvWQ8paioPEtkaDRnSGAwr4RsLFNwcDRnSGDwr4Rs9
IesqPUWCLgwh6yoME9ocDRnSGT4r4Rs9IesqPyHvLjom6Co=;expires=Thu, 30 Dec 2037 00:00:00
GMT;path=/;domain=.imdb.com
Set-Cookie	session-id=284-9245763-9527093;path=/;domain=.imdb.com
Set-Cookie	session-id-time=1289332163;path=/;domain=.imdb.com
Vary	Accept-Encoding,User-Agent
Content-Encoding	gzip
P3P	policyref="http://i.imdb.com/images/p3p.xml",CP="CAO DSP LAW CUR ADM IVAo IVDo CONo OTPo
OUR DELi PUBi OTRi BUS PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA HEA PRE LOC GOV OTC "
Content-Length	20
```

Citrix Net Scaler Devices

HTTP Header Manipulation – Case Check 1 (c)

Response Check

```
(Status-Line)     HTTP/1.1 200 OK
Cteonnt-Length 3705
Content-Type      application/x-javascript
Last-Modified     Mon, 21 May 2007 12:47:20 GMT
Accept-Ranges bytes
Etag      "07c7f2ba69bc71:eda"
Server   Microsoft-IIS/6.0
X-Powered-By   ASP.NET
Date      Mon, 08 Nov 2010 19:55:47 GMT
Cache-Control   private
Content-Encoding    gzip
Content-Length 1183

(Status-Line)     HTTP/1.1 200 OK
Date      Mon, 08 Nov 2010 19:55:47 GMT
Server   Microsoft-IIS/6.0
X-Powered-By   ASP.NET
ntCoent-Length 27166
Content-Type      text/html
Cache-Control   private
Content-Encoding    gzip
Content-Length 8276
```

Citrix Net Scaler Devices

HTTP Header Manipulation – Case Check 2

Response Check 1

```
HTTP/1.0 404 Not Found\r\n
Xontent-Length: \r\n
Server: thttpd/2.25b 29dec2003\r\n
Content-Type: text/html; charset=iso-8859-1\r\n
Last-Modified: Tue, 05 Jul 2010 17:01:12 GMT\r\n
Accept-Ranges: bytes\r\n
Cache-Control: no-cache, no-store\r\n
Date: Tue, 05 Jun 2010 17:01:12 GMT\r\n
Content-Length: 329\r\n
Connection: close\r\n
```

```
HTTP/1.0 302 Moved Temporarily
Age: 0
Date: Thu, 11 Mar 2010 12:01:55 GMT
Xontent-Length:
Connection: Close
Via: NS-CACHE-7.0: 11
ETag: "KXIPDABNAPPNNTZS"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-Powered-By: PHP/5.1.6
Location: http://216.99.132.20/smb/index.php
Content-type: text/html
```

Xontent-Length: \r\n:”

NetScaler & Radware Devices

HTTP Header Combination – Case Check 3

Response Check (200 OK & 301 Moved Permanently)

Via: 1.1 kitjlb01
Set-Cookie: rl-sticky-key=0a4b16a1; path=/; expires=Tue, 09 Nov 2010 02:53:38 GMT

Via: 1.1 prijlb01
Set-Cookie: rl-sticky-key=c0a80a35; path=/; expires=Wed, 10 Nov 2010 09:42:14 GMT...

Via: 1.1 kitjlb01
Set-Cookie: rl-sticky-key=0a4b16a1; path=/; expires=Tue, 09 Nov 2010 02:53:38 GMT

Via: 1.1 sdcdx38f
Set-Cookie: rl-sticky-key=0a03090a1f96; path=/; expires=Mon, 08 Nov 2010 08:00:39 GMT

Via: 1.1 rl2650
Set-Cookie: rl-sticky-key=24dcf3f31e7ea5c3...

Via: 1.1 DX3200UCI01
Set-Cookie: rl-sticky-key=eb281a3dd74de7264188f6e2b4cd56c9; path=/;

Juniper Networks Application
Acceleration Platform

HTTP Header Combination – Case Check 4

Response Check (It Uses combination of both Digest And Basic Realm for Authentication)

```
HTTP/1.0 401 Authentication Required
www-authenticate: Digest realm="Firebox Local
User",qop="auth",nonce="f2a0ee2ddeff937bb382f6f5e1d002cd"
www-authenticate: Basic realm=" Configuration"
Content-type: text/plain

HTTP/1.0 401 Authentication Required
 www-authenticate: Digest realm="SOHO
Configuration",qop="auth",nonce="1ec86c0e135261685b4cbf78986860d4"
www-authenticate: Basic realm="SOHO Configuration"
Content-type: text/plain

HTTP/1.0 401 Authentication Required
www-authenticate: Digest realm="Local
User",qop="auth",nonce="2bb1bdded2ed59dd6ca961acabd43e2e"
www-authenticate: Basic realm="X5 Configuration"
Content-type: text/plain
```

Watch Guard Firewall
SOHO Devices
Firebox

HTTP Header Combination – Case Check 5

Response Check (It uses Set_Cookie with “Barracuda” name parameter)

```
HTTP/1.0 500 Internal Server Error
Date: Thu, 11 Nov 2010 05:52:54 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 5145
Set-Cookie: BNI__BARRACUDA_LB_COOKIE=df0fa8c000005000; Path=/; Max-age=1020

HTTP/1.0 400 Bad Request
Content-Type: text/html
Date: Thu, 11 Nov 2010 05:02:23 GMT
Connection: close
Content-Length: 39
Set-Cookie: BARRACUDA_LB_COOKIE=192.168.155.11_80; path=/

HTTP/1.0 200 OK
Date: Thu, 11 Nov 2010 10:29:51 GMT
Server: BarracudaServer.com (Windows)
Connection: Keep-Alive
Content-Type: text/html
Cache-Control: No-Cache
Transfer-Encoding: chunked
Set-Cookie: BarracudaDrive=3.2.1; expires=Wed, 07 Sep 2011 10:29:51 GMT
```

Barracuda Devices

HTTP Header Combination – Case Check 6

Response Check (It uses Set_Cookie with “PLBSID” name parameter)

```
HTTP/1.0 200 OK
Date: Mon, 01 Nov 2010 02:59:47 GMT
Content-length: 9783
Content-Type: text/html
Via: 1.1 217.22.135.104
Set-Cookie: PLBSID=0.s1; path=/
Cache-Control: no-store
Vary: Accept-Encoding

HTTP/1.0 200 OK
Date: Mon, 01 Nov 2010 02:59:47 GMT
Content-length: 9783
Content-Type: text/html
Via: 1.1 217.22.135.104
Set-Cookie: PLBSID=0.s2; path=/
Cache-Control: no-store
Vary: Accept-Encoding
```

Usually, Server header is used as mark point for detecting Profense. If “Server” header is missing “PLBSID” is the parameter to look for.

HTTP Header Combination – Case Check 7

Response Check (It uses Set_Cookie with “PLBSID” name parameter)

```
HTTP/1.0 200 OK
 Date: Wed, 25 Aug 2010 08:45:45 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Last-Modified: Wed, 25 Aug 2010 08:45:46 GMT
X-BinarySEC-Via: frontal2.re.saas.example.com

HTTP/1.0 301 Moved Permanently
Content-length: 0
Content-language: fr
X-binarysec-cache: saas.example.com
 Connection: keep-alive
Location: http://www.binarysec.fr/cms/index.html
Date: Tue, 24 Nov 2009 22:49:01 GMT
Content-type: text/html

Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Last-Modified: Wed, 25 Aug 2010 08:45:46 GMT
X-BinarySEC-Via: frontal2.re.saas.examplecom
```

BinarySec WAF is now using its own response headers “X-BinarySEC”

Embedded Devices

Cookies Layout
Session Management Tricks

1. Big IP Server Devices
2. Juniper Devices

Cookie Layout – Dissecting HTTP Sessions
IP Based Session Management

Request / Response

```
E:\audit>nc example.com 80
GET / HTTP/1.1
HOST:example.com

HTTP/1.1 302 Object moved
Server: Microsoft-IIS/5.0
Date: Mon, 08 Nov 2010 17:41:56 GMT
X-Powered-By: ASP.NET
Location: http://www.example.com/us/index.asp
Content-Length: 159
Content-Type: text/html
Set-Cookie: ASPSESSIONIDCCCCSBAA=AHLDLDDANEKJOOPHGOHAAKBA; path=/
Cache-control: private
Set-Cookie: http.pool=167880896.20480.0000; path=/

<head><title>Object moved</title></head>
<body><h1>Object Moved</h1>This object may be found <a
HREF="http://www.example.com/us/index.asp">here</a>.</body>
```

Cookie Layout – Dissecting HTTP Sessions
IP Based Session Management

Request / Response

E:\audit>nc example.com 80
GET / HTTP/1.1
HOST:example.com

HTTP/1.1 302 Object moved
Set-Cookie: http.pool=167880896.20480.0000; path=/
Converting to Binary: Binary (cookie) Part == 000010100000000011010100011000000

Big IP Server Device

Converting to blocks of 4 □
00001010
00000001
10101000
11000000

00001010 □ 10
00000001 □ 1
10101000 □ 168
11000000 □ 192

192.168.1.10

Cookie Layout – Dissecting HTTP Sessions

Geo Location Based Session Management

Request / Response

(Request-Line) GET / HTTP/1.1
Host www.example.net
User-Agent Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.2.12) Gecko/20101026 Firefox/3.6.12
Accept text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language en-us,en;q=0.5
Accept-Encodinggzip,deflate
Accept-Charset ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive 115
Connection keep-alive

Juniper Network Device

(Status-Line)HTTP/1.1 200 OK
Accept-Ranges bytes
Content-Type text/html; charset=UTF-8
Date Mon, 08 Nov 2010 18:48:02 GMT
Connection keep-alive
Set-Cookie rl-sticky-key=b159fd3052f1f60eea47e0dc56d57d62; path=/; expires=Mon, 08 Nov 2010 19:35:22 GMT
Set-Cookie
CT_Akamai=georegion=264,country_code=US,region_code=MI,city=EASTLANSING,dma=551,msa=4040,areacode=517,county=INGHAM,fips=26065,lat=42.7369,long=-84.4838,timezone=EST,zip=48823-48826,continent=NA,throughput=vhigh,bw=1000,asnum=237,location_id=0; path=/; domain=example.net

Proxy Detection

1. Web Proxy Auto Detection Protocol – WPAD
2. Proxy Auto Configuration (PAC)

Walk Through - WPAD

- Protocol used in discovering network proxy automatically.
- Configuration file contains Intranet Addresses inherently.
- WPAD works on DHCP Behavior. [DHCPINFORM Query]
- No DNS lookup is required if DHCP issues a request
- DHCP Query through Uniform Resource Locator [URL]
- DNS Query through wpad.dat , File located in WPAD root directory
- Function □ FindProxyForURL()

Walk Through – WPAD Unique Insecurities

- wpad.dat is not stored in a secure manner. Should be placed in default virtual directory.

- No referrer check on the request to wpad.dat file.

- Generic scan to detect the presence of wpad.dat

.

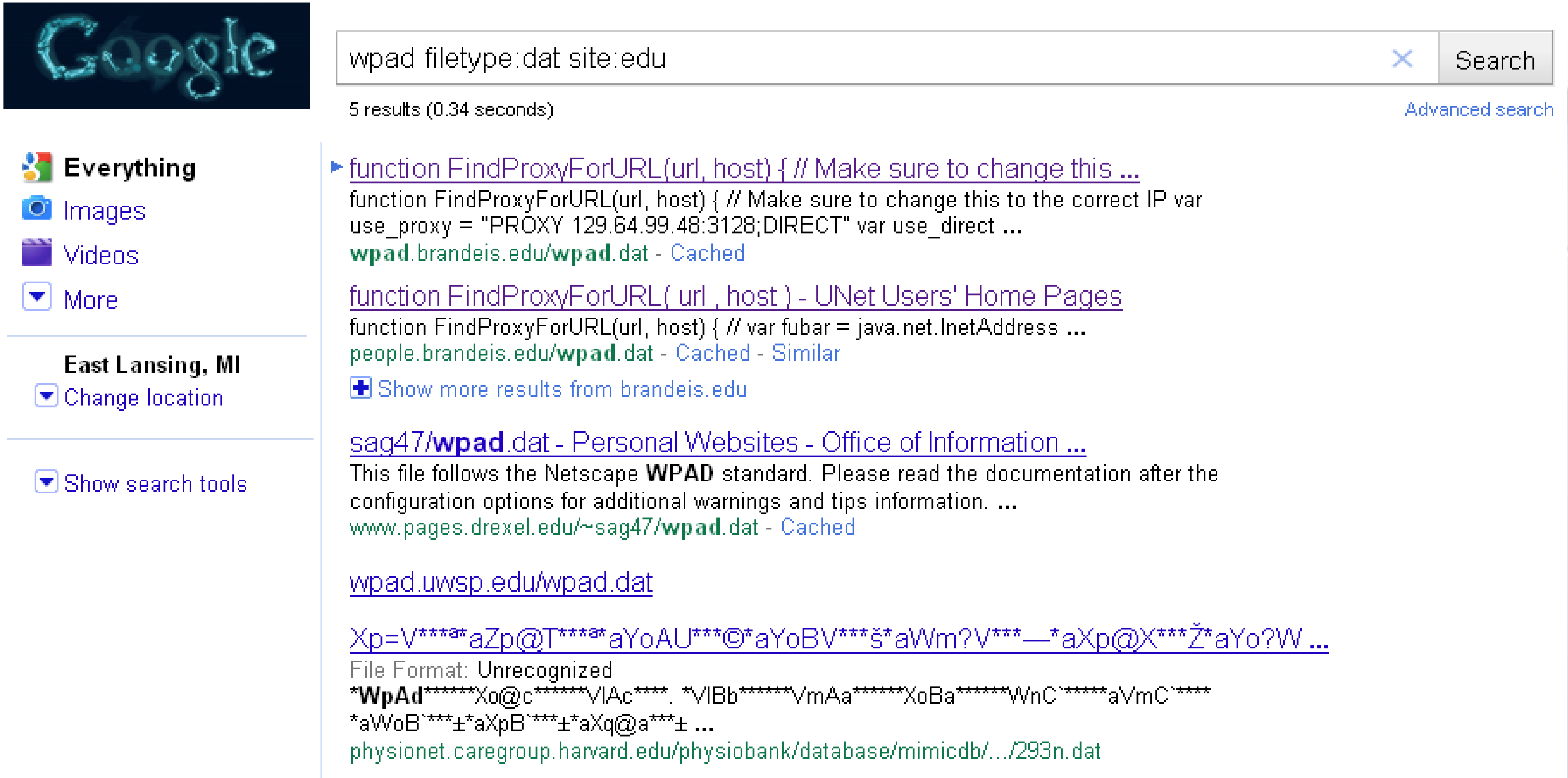
- When a DHCP request is issued no DNS required.

  →Rogue DHCP server on LAN can result in differential attacks.

- Wpad.dat use JavaScript to set browsers for proxy settings.

WPAD – Case Study

- Example - Check



Google

wpad filetype:dat site:edu

5 results (0.34 seconds)

function FindProxyForURL(url, host) { // Make sure to change this ...
function FindProxyForURL(url, host) { // Make sure to change this to the correct IP var use_proxy = "PROXY 129.64.99.48:3128;DIRECT" var use_direct ...
wpad.brandeis.edu/wpad.dat - Cached

function FindProxyForURL(url , host) - UNet Users' Home Pages
function FindProxyForURL(url, host) { // var fubar = java.net.InetAddress ...
people.brandeis.edu/wpad.dat - Cached - Similar

Show more results from brandeis.edu

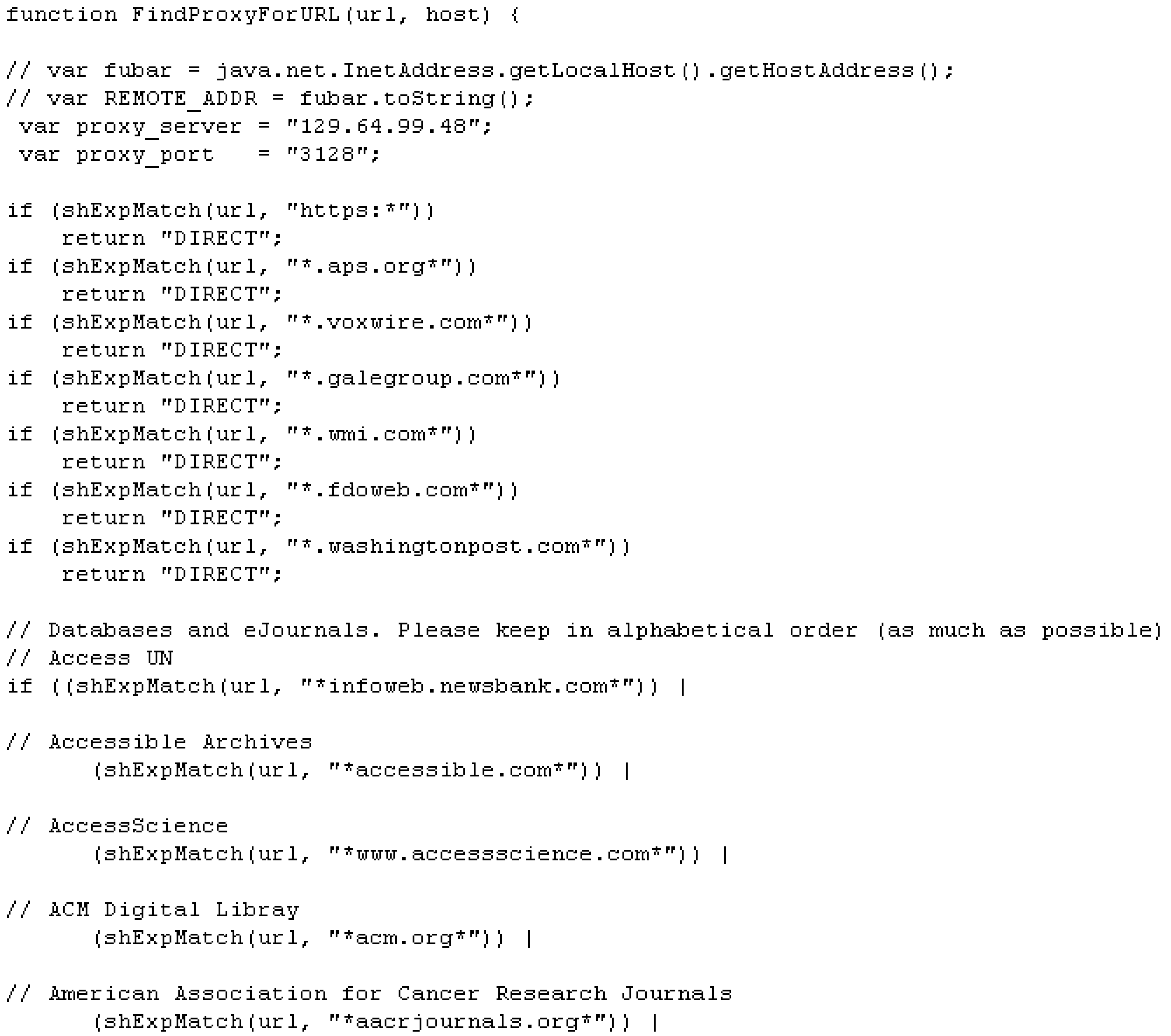
sag47/wpad.dat - Personal Websites - Office of Information ...
This file follows the Netscape **WPAD** standard. Please read the documentation after the configuration options for additional warnings and tips information. ...
www.pages.drexel.edu/~sag47/wpad.dat - Cached

wpad.uwsp.edu/wpad.dat

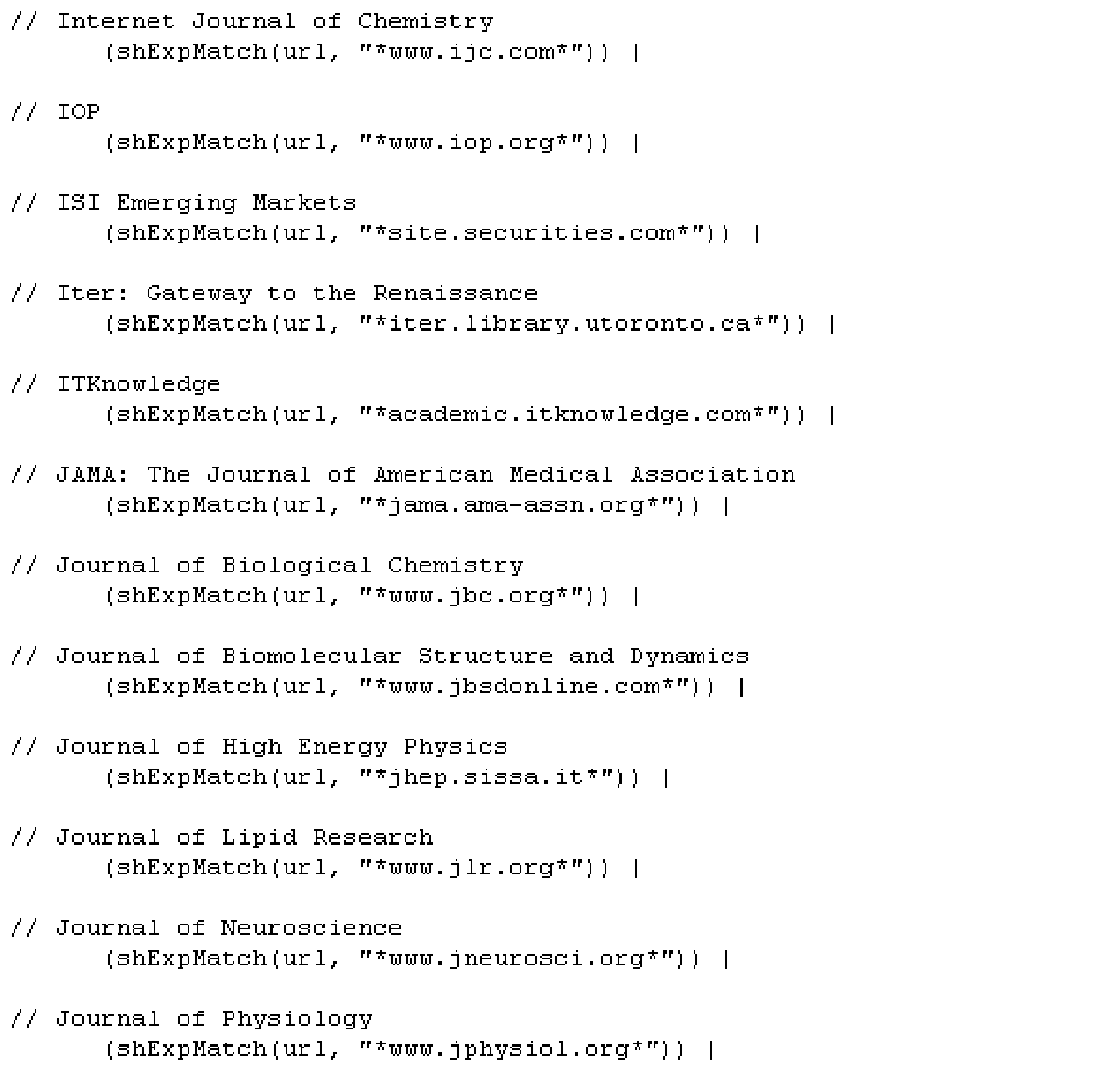
Xp=V***ª*aZp@T***ª*aYoAU***©*aYoBV***š*aWm?V***—*aXp@X***Ž*aYo?W ...
File Format: Unrecognized
*WpAd******Xo@c******VlAc****. *VlBb******VmAa******XoBa******WnC`*****aVmC`****
*aWoB`***±*aXpB`***±*aXq@a***± ...
physionet.caregroup.harvard.edu/physiobank/database/mimicdb/.../293n.dat

WPAD – Case Study

- Example - Check



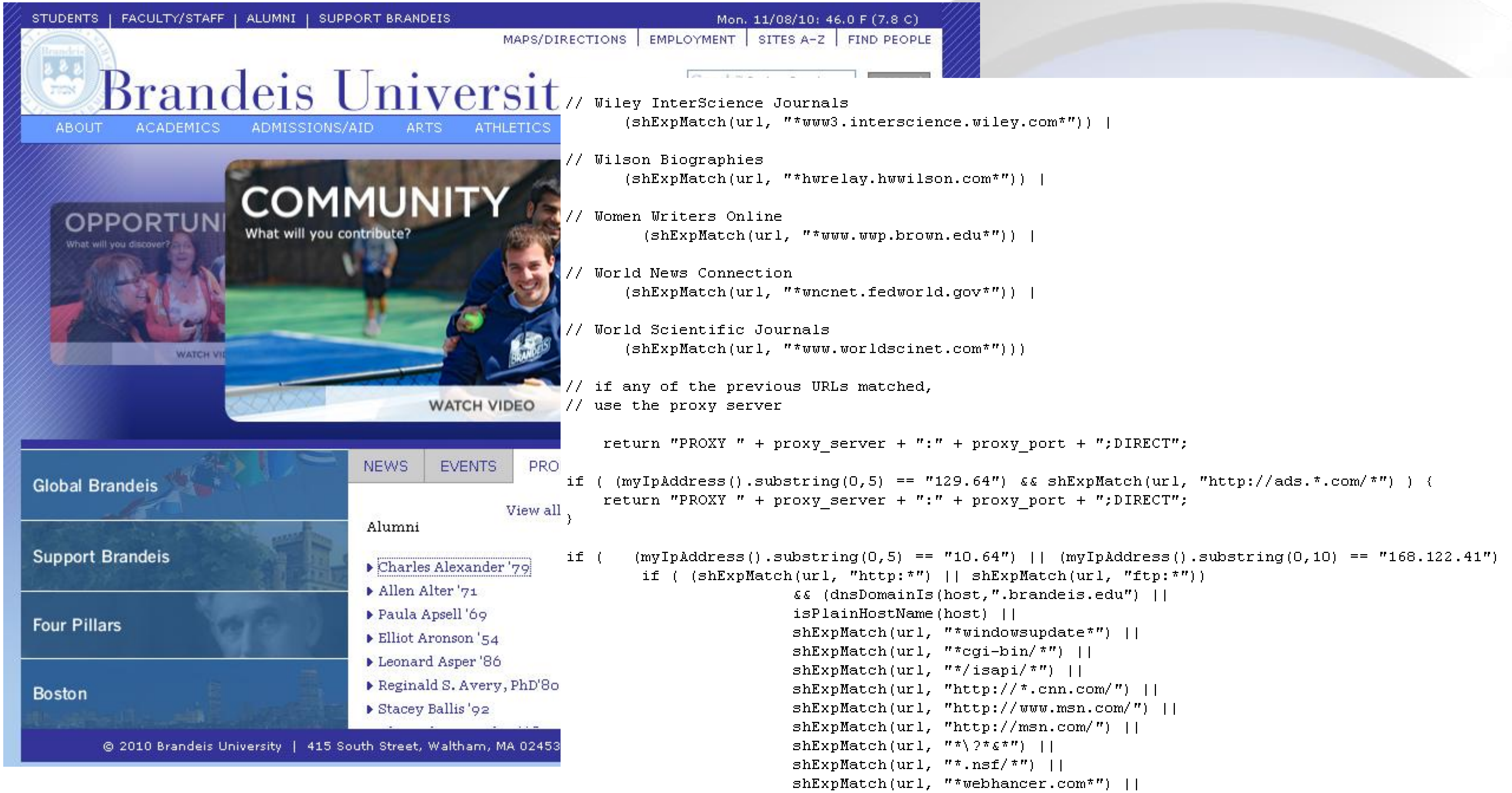
```
function FindProxyForURL(url, host) {

// var fubar = java.net.InetAddress.getLocalHost().getHostAddress();
// var REMOTE_ADDR = fubar.toString();
 var proxy_server = "129.64.99.48";
 var proxy_port   = "3128";

if (shExpMatch(url, "https:*"))
    return "DIRECT";
if (shExpMatch(url, "*.aps.org*"))
    return "DIRECT";
if (shExpMatch(url, "*.voxwire.com*"))
    return "DIRECT";
if (shExpMatch(url, "*.galegroup.com*"))
    return "DIRECT";
if (shExpMatch(url, "*.wmi.com*"))
    return "DIRECT";
if (shExpMatch(url, "*.fdoweb.com*"))
    return "DIRECT";
if (shExpMatch(url, "*.washingtonpost.com*"))
    return "DIRECT";

// Databases and eJournals. Please keep in alphabetical order (as much as possible)
// Access UN
if ((shExpMatch(url, "*infoweb.newsbank.com*")) |

// Accessible Archives
      (shExpMatch(url, "*accessible.com*")) |

// AccessScience
      (shExpMatch(url, "*www.accessscience.com*")) |

// ACM Digital Libray
      (shExpMatch(url, "*acm.org*")) |

// American Association for Cancer Research Journals
      (shExpMatch(url, "*aacrjournals.org*")) |
```



```
// Internet Journal of Chemistry
      (shExpMatch(url, "*www.ijc.com*")) |

// IOP
      (shExpMatch(url, "*www.iop.org*")) |

// ISI Emerging Markets
      (shExpMatch(url, "*site.securities.com*")) |

// Iter: Gateway to the Renaissance
      (shExpMatch(url, "*iter.library.utoronto.ca*")) |

// ITKnowledge
      (shExpMatch(url, "*academic.itknowledge.com*")) |

// JAMA: The Journal of American Medical Association
      (shExpMatch(url, "*jama.ama-assn.org*")) |

// Journal of Biological Chemistry
      (shExpMatch(url, "*www.jbc.org*")) |

// Journal of Biomolecular Structure and Dynamics
      (shExpMatch(url, "*www.jbsdonline.com*")) |

// Journal of High Energy Physics
      (shExpMatch(url, "*jhep.sissa.it*")) |

// Journal of Lipid Research
      (shExpMatch(url, "*www.jlr.org*")) |

// Journal of Neuroscience
      (shExpMatch(url, "*www.jneurosci.org*")) |

// Journal of Physiology
      (shExpMatch(url, "*www.jphysiol.org*")) |
```

WPAD – Case Study

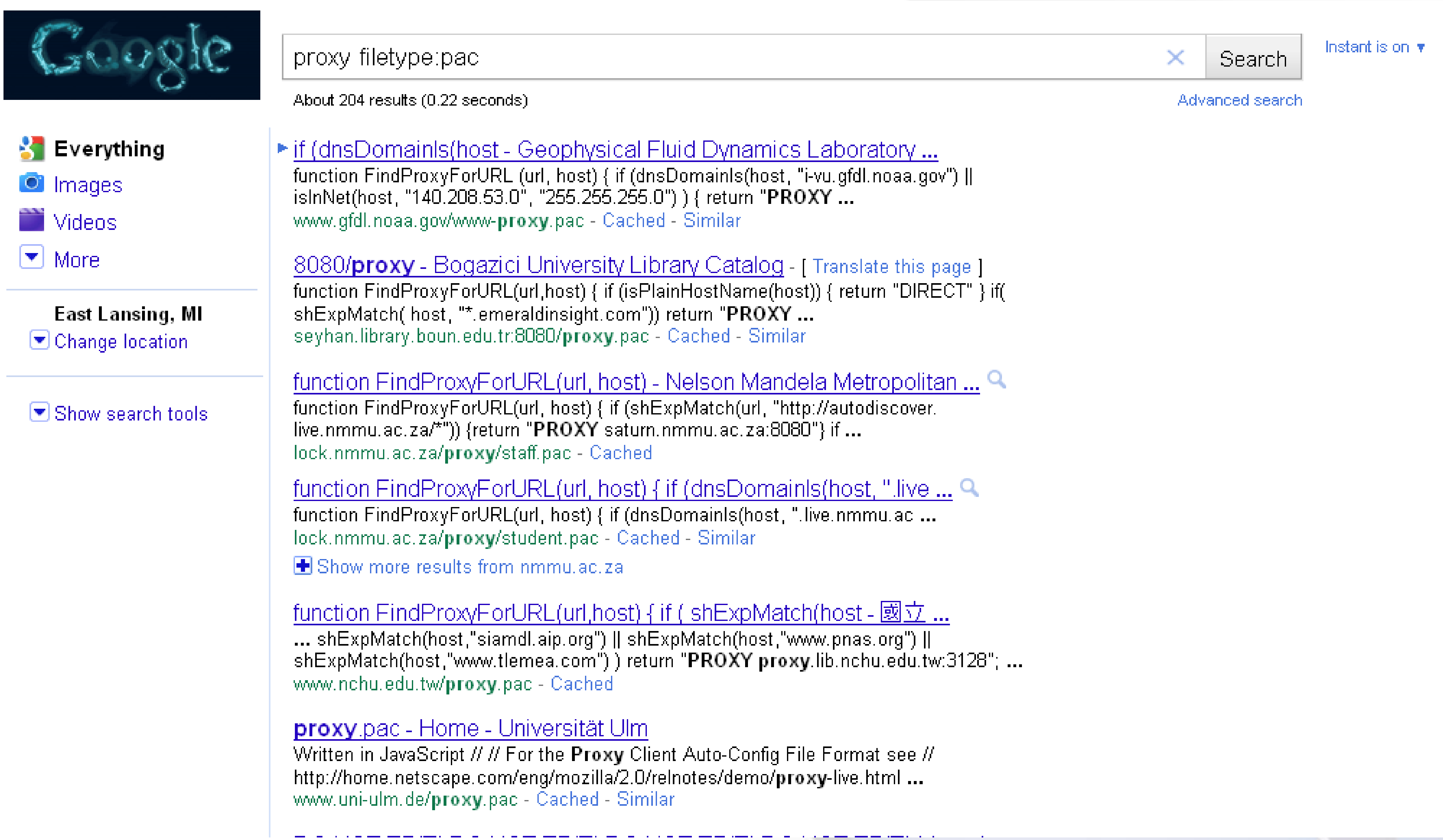
- Example – Full proxy settings are revealed.



```
// Wiley InterScience Journals
    (shExpMatch(url, "*www3.interscience.wiley.com*")) |

// Wilson Biographies
    (shExpMatch(url, "*hwrelay.hwwilson.com*")) |

// Women Writers Online
      (shExpMatch(url, "*www.wwp.brown.edu*")) |

// World News Connection
    (shExpMatch(url, "*wncnet.fedworld.gov*")) |

// World Scientific Journals
    (shExpMatch(url, "*www.worldscinet.com*")))

// if any of the previous URLs matched,
// use the proxy server

    return "PROXY " + proxy_server + ":" + proxy_port + ";DIRECT";

if ( (myIpAddress().substring(0,5) == "129.64") && shExpMatch(url, "http://ads.*.com/*") ) {
    return "PROXY " + proxy_server + ":" + proxy_port + ";DIRECT";
}

if (   (myIpAddress().substring(0,5) == "10.64") || (myIpAddress().substring(0,10) == "168.122.41")
        if ( (shExpMatch(url, "http:*") || shExpMatch(url, "ftp:*"))
                        && (dnsDomainIs(host,".brandeis.edu") ||
                        isPlainHostName(host) ||
                        shExpMatch(url, "*windowsupdate*") ||
                        shExpMatch(url, "*cgi-bin/*") ||
                        shExpMatch(url, "*/isapi/*") ||
                        shExpMatch(url, "http://*.cnn.com/") ||
                        shExpMatch(url, "http://www.msn.com/") ||
                        shExpMatch(url, "http://msn.com/") ||
                        shExpMatch(url, "*\?*&*") ||
                        shExpMatch(url, "*.nsf/*") ||
                        shExpMatch(url, "*webhancer.com*") ||
```

PAC – Case Study

- Example – Check



About 204 results (0.22 seconds)

if (dnsDomainIs(host - Geophysical Fluid Dynamics Laboratory ...
function FindProxyForURL (url, host) { if (dnsDomainIs(host, "i-vu.gfdl.noaa.gov") || isInNet(host, "140.208.53.0", "255.255.255.0")) { return "**PROXY** ...
www.gfdl.noaa.gov/www-**proxy**.pac - Cached - Similar

8080/**proxy** - Bogazici University Library Catalog - [Translate this page]
function FindProxyForURL(url,host) { if (isPlainHostName(host)) { return "DIRECT" } if(shExpMatch(host, "*.emeraldinsight.com")) return "**PROXY** ...
seyhan.library.boun.edu.tr:8080/**proxy**.pac - Cached - Similar

function FindProxyForURL(url, host) - Nelson Mandela Metropolitan ...
function FindProxyForURL(url, host) { if (shExpMatch(url, "http://autodiscover. live.nmmu.ac.za/*")) {return "**PROXY** saturn.nmmu.ac.za:8080"} if ...
lock.nmmu.ac.za/**proxy**/staff.pac - Cached

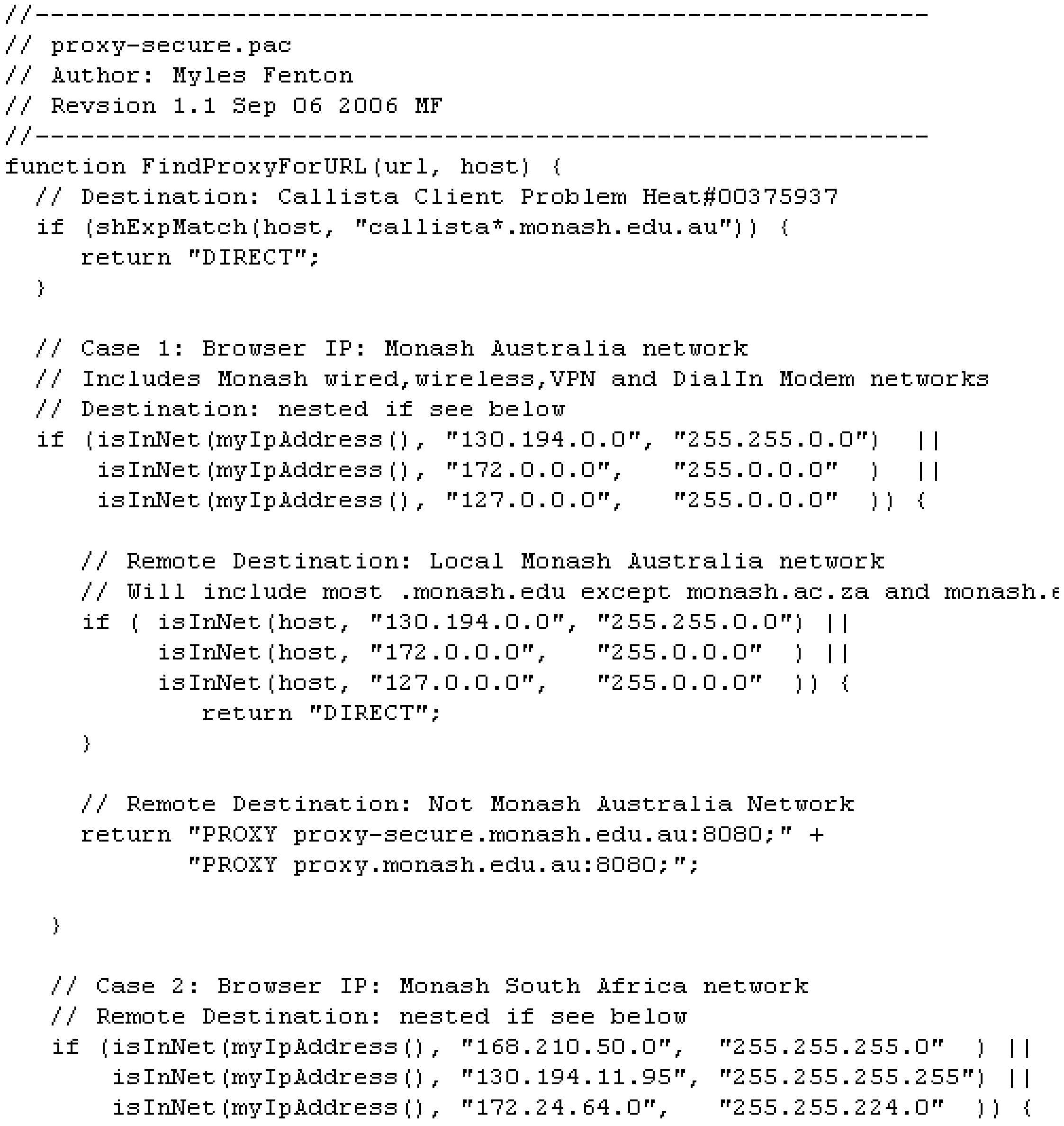
function FindProxyForURL(url, host) { if (dnsDomainIs(host, ".live ...
function FindProxyForURL(url, host) { if (dnsDomainIs(host, ".live.nmmu.ac ...
lock.nmmu.ac.za/**proxy**/student.pac - Cached - Similar
Show more results from nmmu.ac.za

function FindProxyForURL(url,host) { if (shExpMatch(host - 國立 ...
... shExpMatch(host,"siamdl.aip.org") || shExpMatch(host,"www.pnas.org") || shExpMatch(host,"www.tlemea.com")) return "**PROXY proxy**.lib.nchu.edu.tw:3128"; ...
www.nchu.edu.tw/**proxy**.pac - Cached

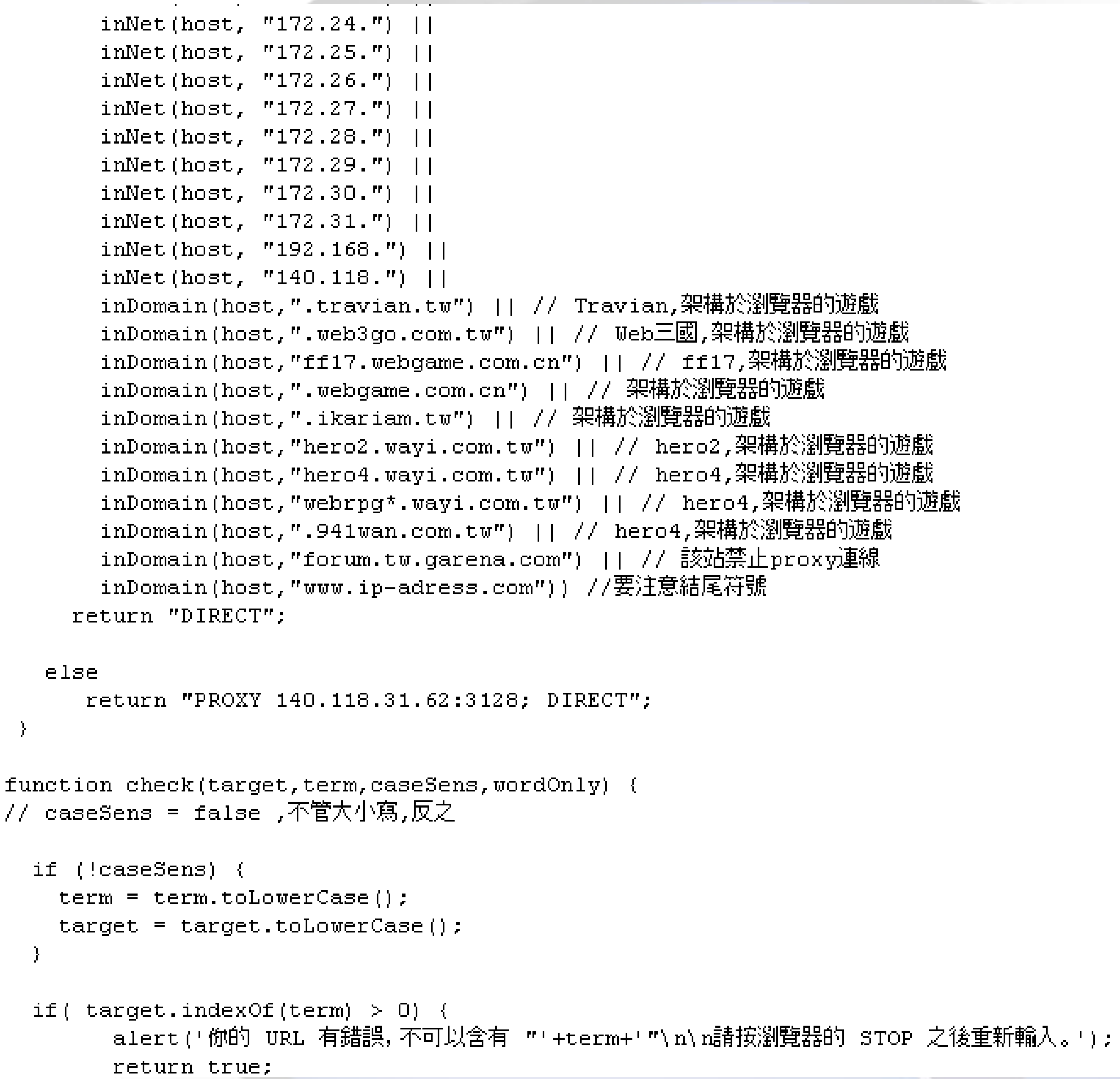
proxy.pac - Home - Universität Ulm
Written in JavaScript // // For the **Proxy** Client Auto-Config File Format see // http://home.netscape.com/eng/mozilla/2.0/relnotes/demo/**proxy**-live.html ...
www.uni-ulm.de/**proxy**.pac - Cached - Similar

PAC – Case Study

- Example – Lot of Information



```
//-----------------------------------------------------------
// proxy-secure.pac
// Author: Myles Fenton
// Revsion 1.1 Sep 06 2006 MF
//-----------------------------------------------------------
function FindProxyForURL(url, host) {
  // Destination: Callista Client Problem Heat#00375937
  if (shExpMatch(host, "callista*.monash.edu.au")) {
     return "DIRECT";
  }

  // Case 1: Browser IP: Monash Australia network
  // Includes Monash wired,wireless,VPN and DialIn Modem networks
  // Destination: nested if see below
  if (isInNet(myIpAddress(), "130.194.0.0", "255.255.0.0")  ||
      isInNet(myIpAddress(), "172.0.0.0",   "255.0.0.0"  )  ||
      isInNet(myIpAddress(), "127.0.0.0",   "255.0.0.0"  )) {

     // Remote Destination: Local Monash Australia network
     // Will include most .monash.edu except monash.ac.za and monash.e
     if ( isInNet(host, "130.194.0.0", "255.255.0.0") ||
          isInNet(host, "172.0.0.0",   "255.0.0.0"  ) ||
          isInNet(host, "127.0.0.0",   "255.0.0.0"  )) {
             return "DIRECT";
     }

     // Remote Destination: Not Monash Australia Network
     return "PROXY proxy-secure.monash.edu.au:8080;" +
            "PROXY proxy.monash.edu.au:8080;";

   }

   // Case 2: Browser IP: Monash South Africa network
   // Remote Destination: nested if see below
   if (isInNet(myIpAddress(), "168.210.50.0",  "255.255.255.0"  ) ||
       isInNet(myIpAddress(), "130.194.11.95", "255.255.255.255") ||
       isInNet(myIpAddress(), "172.24.64.0",   "255.255.224.0"  )) {
```



```
      inNet(host, "172.24.") ||
      inNet(host, "172.25.") ||
      inNet(host, "172.26.") ||
      inNet(host, "172.27.") ||
      inNet(host, "172.28.") ||
      inNet(host, "172.29.") ||
      inNet(host, "172.30.") ||
      inNet(host, "172.31.") ||
      inNet(host, "192.168.") ||
      inNet(host, "140.118.") ||
      inDomain(host,".travian.tw") || // Travian,架構於瀏覽器的遊戲
      inDomain(host,".web3go.com.tw") || // Web三國,架構於瀏覽器的遊戲
      inDomain(host,"ff17.webgame.com.cn") || // ff17,架構於瀏覽器的遊戲
      inDomain(host,".webgame.com.cn") || // 架構於瀏覽器的遊戲
      inDomain(host,".ikariam.tw") || // 架構於瀏覽器的遊戲
      inDomain(host,"hero2.wayi.com.tw") || // hero2,架構於瀏覽器的遊戲
      inDomain(host,"hero4.wayi.com.tw") || // hero4,架構於瀏覽器的遊戲
      inDomain(host,"webrpg*.wayi.com.tw") || // hero4,架構於瀏覽器的遊戲
      inDomain(host,".941wan.com.tw") || // hero4,架構於瀏覽器的遊戲
      inDomain(host,"forum.tw.garena.com") || // 該站禁止proxy連線
      inDomain(host,"www.ip-adress.com")) //要注意結尾符號
    return "DIRECT";

  else
     return "PROXY 140.118.31.62:3128; DIRECT";
 }

function check(target,term,caseSens,wordOnly) {
// caseSens = false ,不管大小寫,反之

  if (!caseSens) {
    term = term.toLowerCase();
    target = target.toLowerCase();
  }

  if( target.indexOf(term) > 0) {
        alert('你的 URL 有錯誤,不可以含有 "'+term+'"\n\n請按瀏覽器的 STOP 之後重新輸入。');
        return true;
```

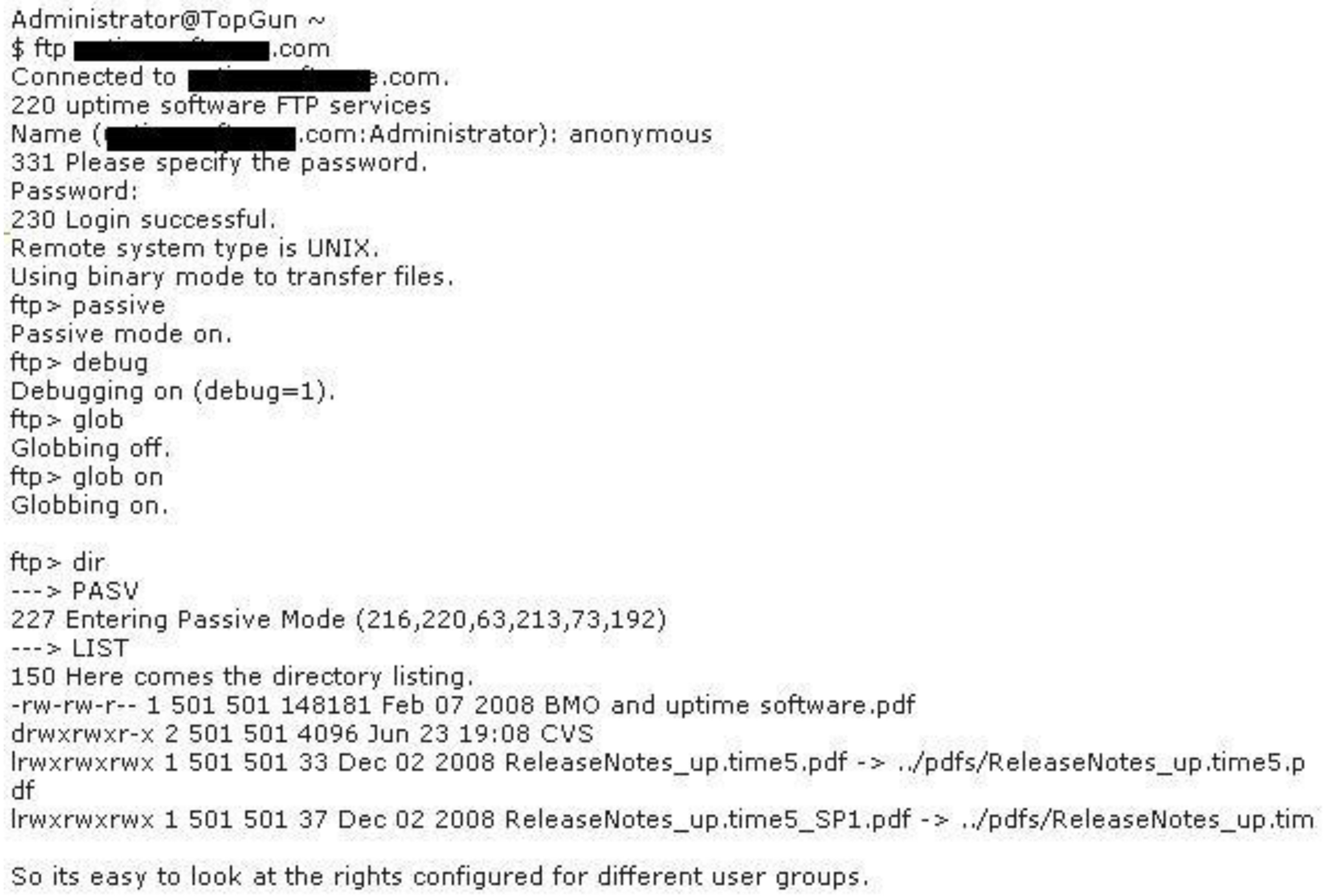
Anonymous Services

1. Enumerating Users On the Fly
2. Information Gathering
3. Entry point of XSS in Vulnerable Devices

Open Services and Anonymous Access

- Open services such as FTP etc.
- Why open FTP? Why not a credential based access?
- Scrutinize the deployment strategy whether it has to be applied at internet or intranet.
- Why not to put these services on VPN considering the business need.
- Open services are tactically exploited to gain information and reconnaissance.
- These can be used to scan third party targets too.

FTP Anonymous Access – How deeper we can go ?

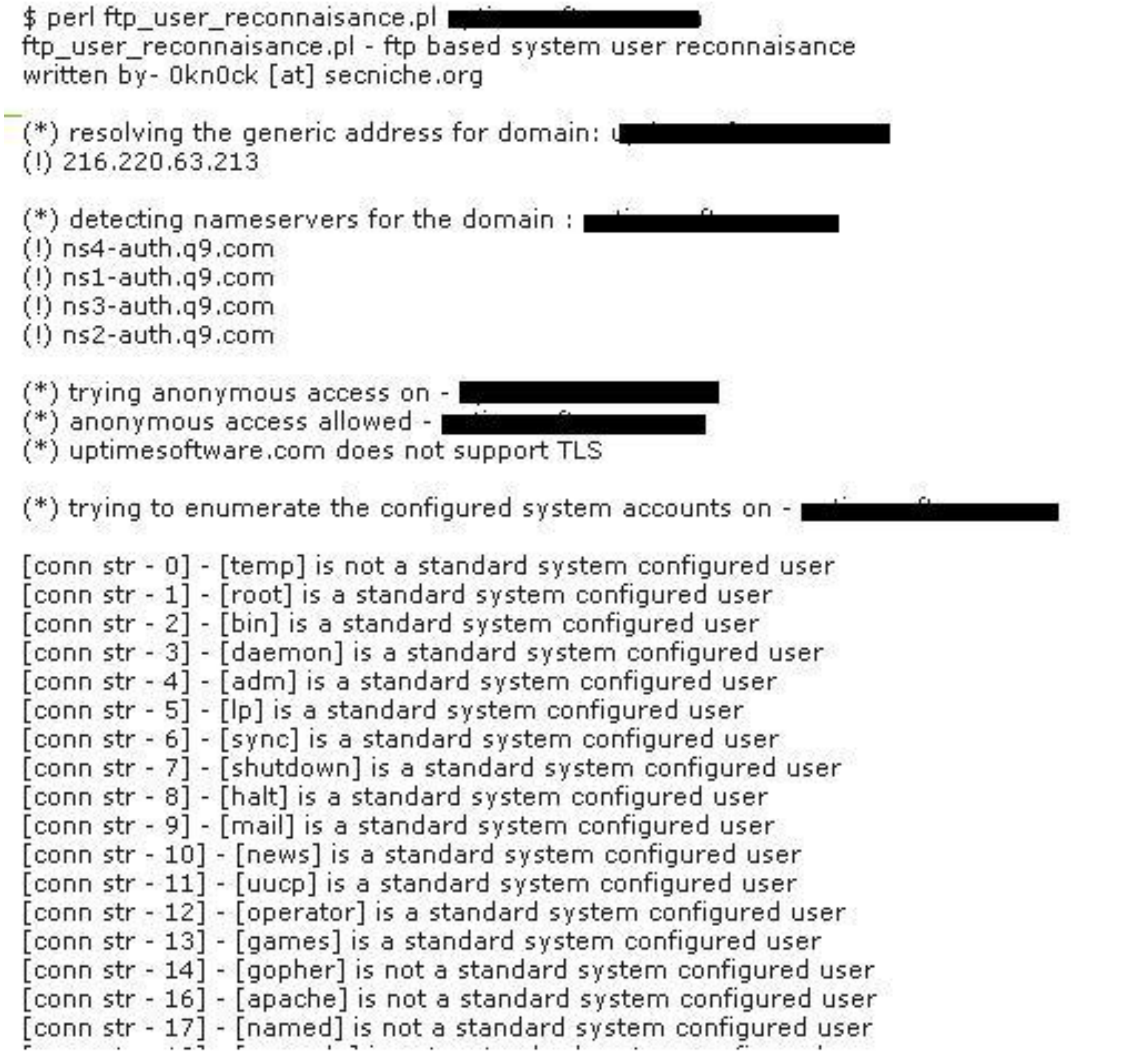


```
Administrator@TopGun ~
$ ftp [redacted].com
Connected to [redacted].com.
220 uptime software FTP services
Name ([redacted].com:Administrator): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> passive
Passive mode on.
ftp> debug
Debugging on (debug=1).
ftp> glob
Globbing off.
ftp> glob on
Globbing on.

ftp> dir
---> PASV
227 Entering Passive Mode (216,220,63,213,73,192)
---> LIST
150 Here comes the directory listing.
-rw-rw-r-- 1 501 501 148181 Feb 07 2008 BMO and uptime software.pdf
drwxrwxr-x 2 501 501 4096 Jun 23 19:08 CVS
lrwxrwxrwx 1 501 501 33 Dec 02 2008 ReleaseNotes_up.time5.pdf -> ../pdfs/ReleaseNotes_up.time5.p
df
lrwxrwxrwx 1 501 501 37 Dec 02 2008 ReleaseNotes_up.time5_SP1.pdf -> ../pdfs/ReleaseNotes_up.tim
```

So its easy to look at the rights configured for different user groups.

Is that all ?

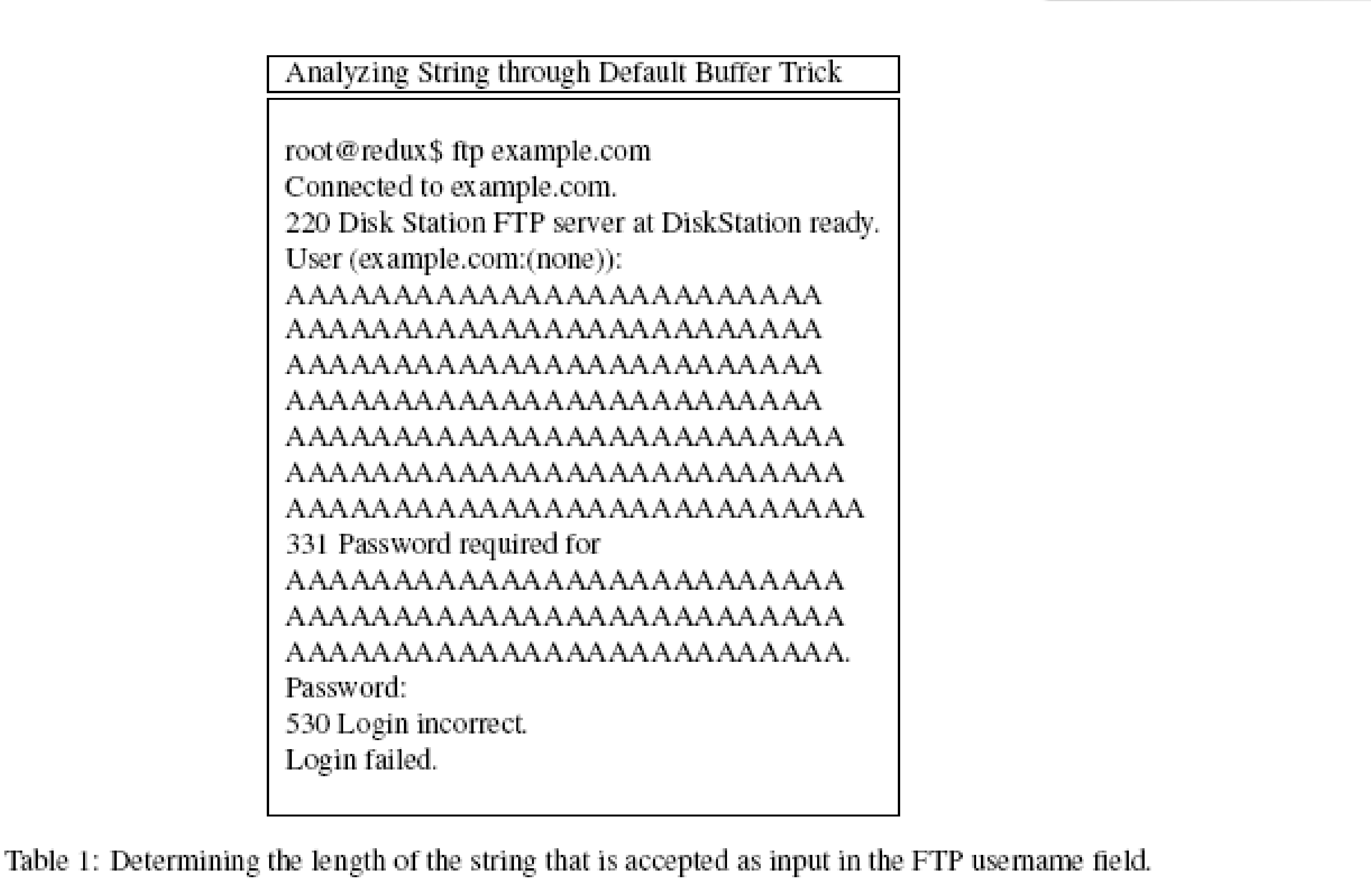
FTP – Default Design – Lot of Information



```
$ perl ftp_user_reconnaisance.pl [redacted]
ftp_user_reconnaisance.pl - ftp based system user reconnaisance
written by- 0kn0ck [at] secniche.org

(*) resolving the generic address for domain: [redacted]
(!) 216.220.63.213

(*) detecting nameservers for the domain : [redacted]
(!) ns4-auth.q9.com
(!) ns1-auth.q9.com
(!) ns3-auth.q9.com
(!) ns2-auth.q9.com

(*) trying anonymous access on - [redacted]
(*) anonymous access allowed - [redacted]
(*) uptimesoftware.com does not support TLS

(*) trying to enumerate the configured system accounts on - [redacted]

[conn str - 0] - [temp] is not a standard system configured user
[conn str - 1] - [root] is a standard system configured user
[conn str - 2] - [bin] is a standard system configured user
[conn str - 3] - [daemon] is a standard system configured user
[conn str - 4] - [adm] is a standard system configured user
[conn str - 5] - [lp] is a standard system configured user
[conn str - 6] - [sync] is a standard system configured user
[conn str - 7] - [shutdown] is a standard system configured user
[conn str - 8] - [halt] is a standard system configured user
[conn str - 9] - [mail] is a standard system configured user
[conn str - 10] - [news] is a standard system configured user
[conn str - 11] - [uucp] is a standard system configured user
[conn str - 12] - [operator] is a standard system configured user
[conn str - 13] - [games] is a standard system configured user
[conn str - 14] - [gopher] is not a standard system configured user
[conn str - 16] - [apache] is not a standard system configured user
[conn str - 17] - [named] is not a standard system configured user
```

Enumerating Users

FTP – Default Design – XSS Entry Point



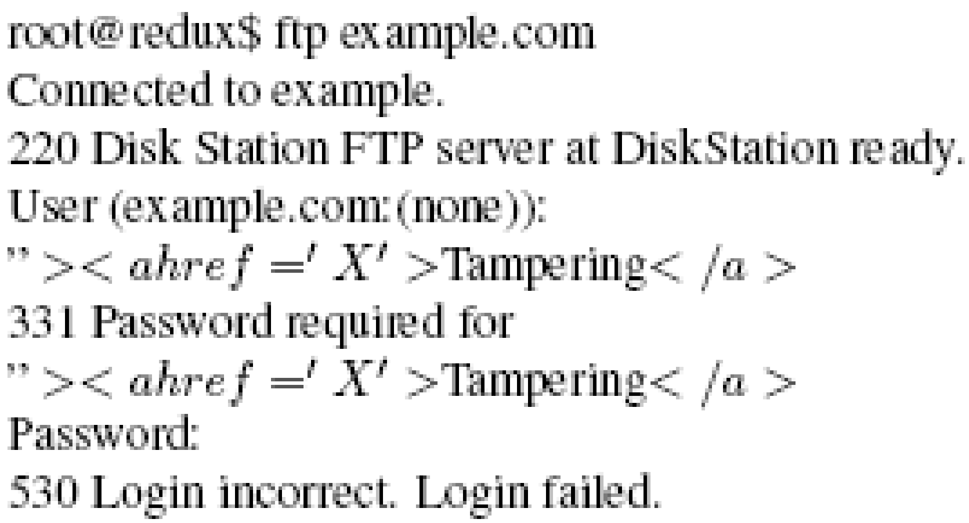
Analyzing String through Default Buffer Trick

```
root@redux$ ftp example.com
Connected to example.com.
220 Disk Station FTP server at DiskStation ready.
User (example.com:(none)):
AAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAA
331 Password required for
AAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAA.
Password:
530 Login incorrect.
Login failed.
```

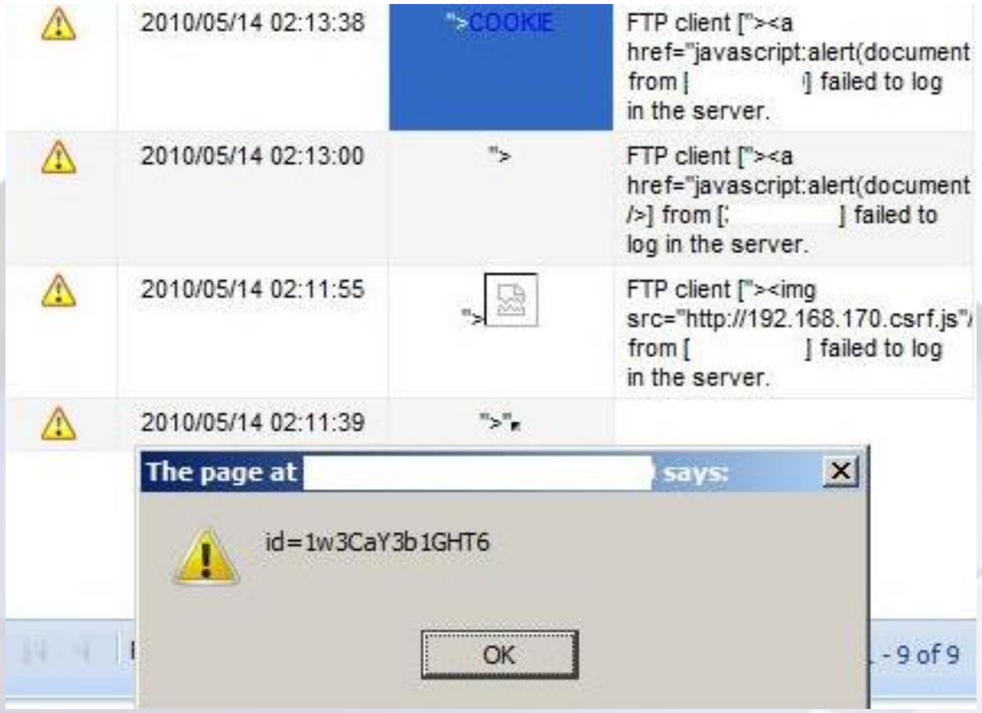
Table 1: Determining the length of the string that is accepted as input in the FTP username field.

Default buffer trick

FTP – Default Design – XSS Entry Point



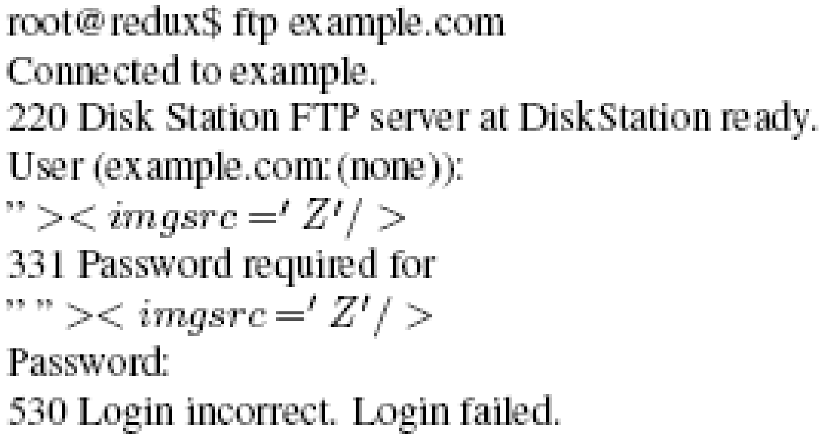
```
root@redux$ ftp example.com
Connected to example.
220 Disk Station FTP server at DiskStation ready.
User (example.com:(none)):
" >< ahref =' X' >Tampering< /a >
331 Password required for
" >< ahref =' X' >Tampering< /a >
Password:
530 Login incorrect. Login failed.
```



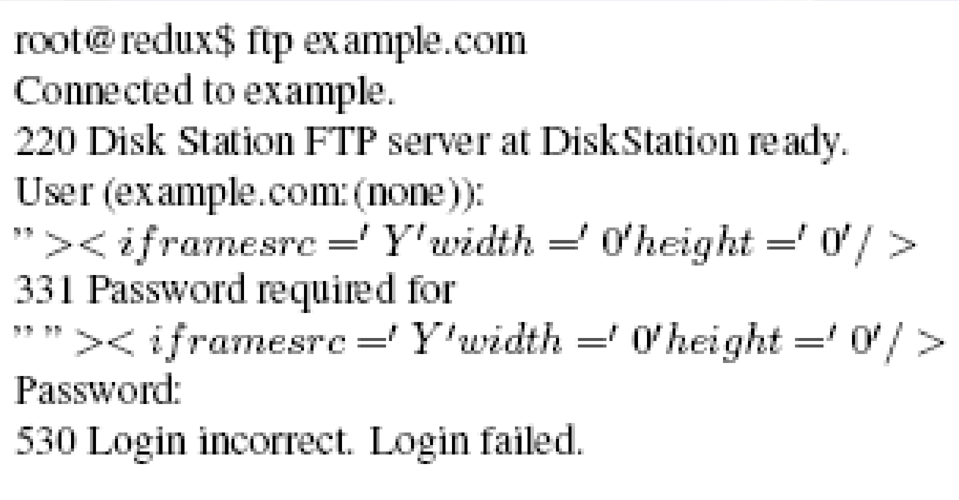
⚠	2010/05/14 02:13:38	">COOKIE	FTP client ["><a href="javascript:alert(document from [[redacted]] failed to log in the server.
⚠	2010/05/14 02:13:00	">	FTP client ["><a href="javascript:alert(document />] from [[redacted]] failed to log in the server.
⚠	2010/05/14 02:11:55	">	FTP client ["><img src="http://192.168.170.csrf.js"/ from [[redacted]] failed to log in the server.
⚠	2010/05/14 02:11:39	">"	

The page at [redacted] says:

id=1w3CaY3b1GHT6



```
root@redux$ ftp example.com
Connected to example.
220 Disk Station FTP server at DiskStation ready.
User (example.com:(none)):
" >< imgsrc =' Z' / >
331 Password required for
" " >< imgsrc =' Z' / >
Password:
530 Login incorrect. Login failed.
```



```
root@redux$ ftp example.com
Connected to example.
220 Disk Station FTP server at DiskStation ready.
User (example.com:(none)):
" >< iframesrc =' Y' width =' 0' height =' 0' / >
331 Password required for
" " >< iframesrc =' Y' width =' 0' height =' 0' / >
Password:
530 Login incorrect. Login failed.
```

Advisory : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3684

Bad Design Practices

1. URL Based Detection – Binary Control
2. Case Studies in the Wild

Bad Design over HTTP

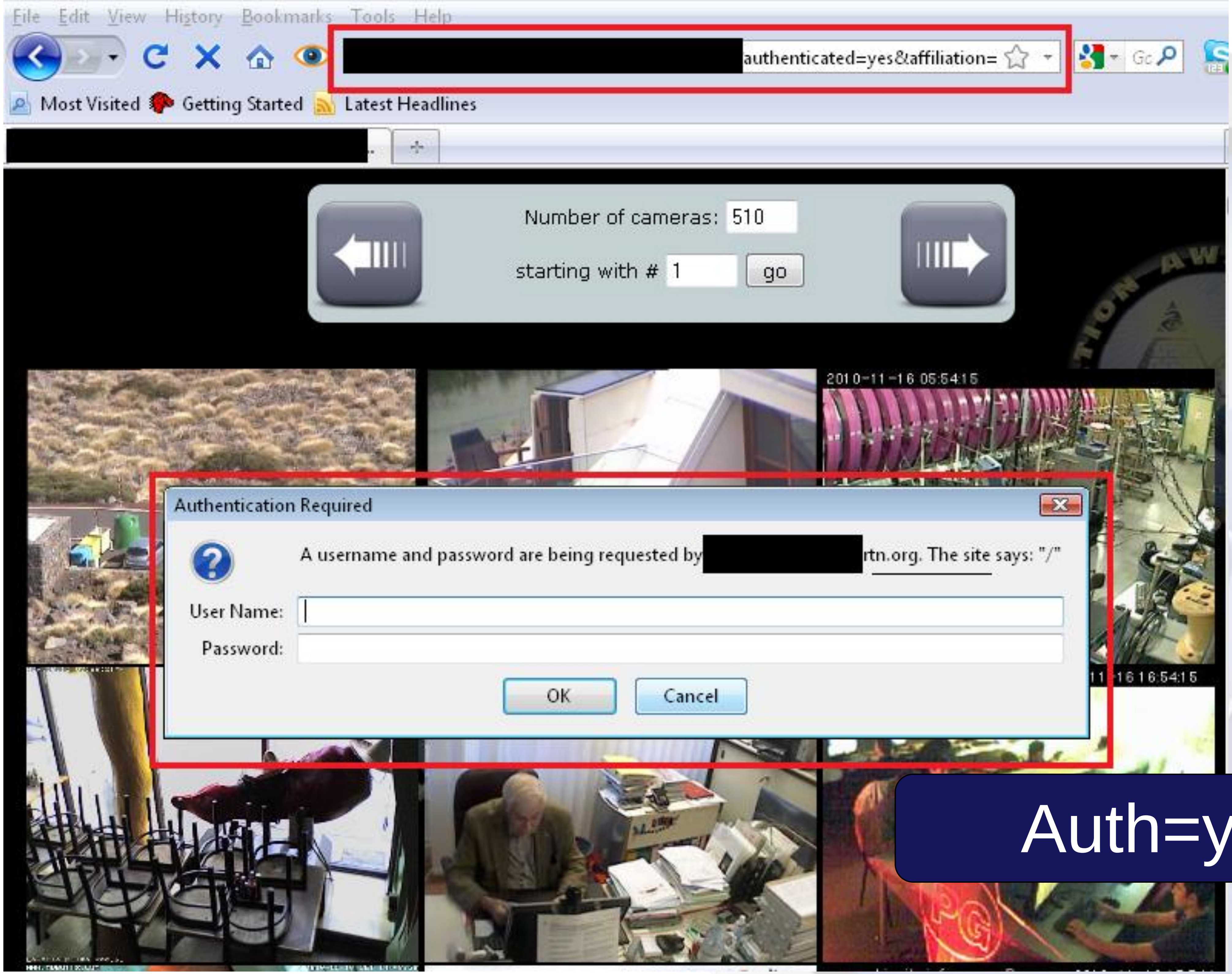
Why ?

- Everything is open on port 80
  - Firewall bypass easy.
- URL patterns play a critical role
- Binary control sequence is used in the network devices
- [YES|NO] [0|1] – Play around to bypass the authentication

Examples:

- *http://router.ip/enblUpnp.cgi?enblUpnp=1 | 0*
- *http://192.168.1.1/application.cgi?authenticated=yes | no*

Bad Design over HTTP – Case Study (1)



[redacted]authenticated=yes&affiliation=

[redacted]

Number of cameras: 510

starting with # 1 go

Authentication Required

A username and password are being requested by [redacted]rtn.org. The site says: "/"

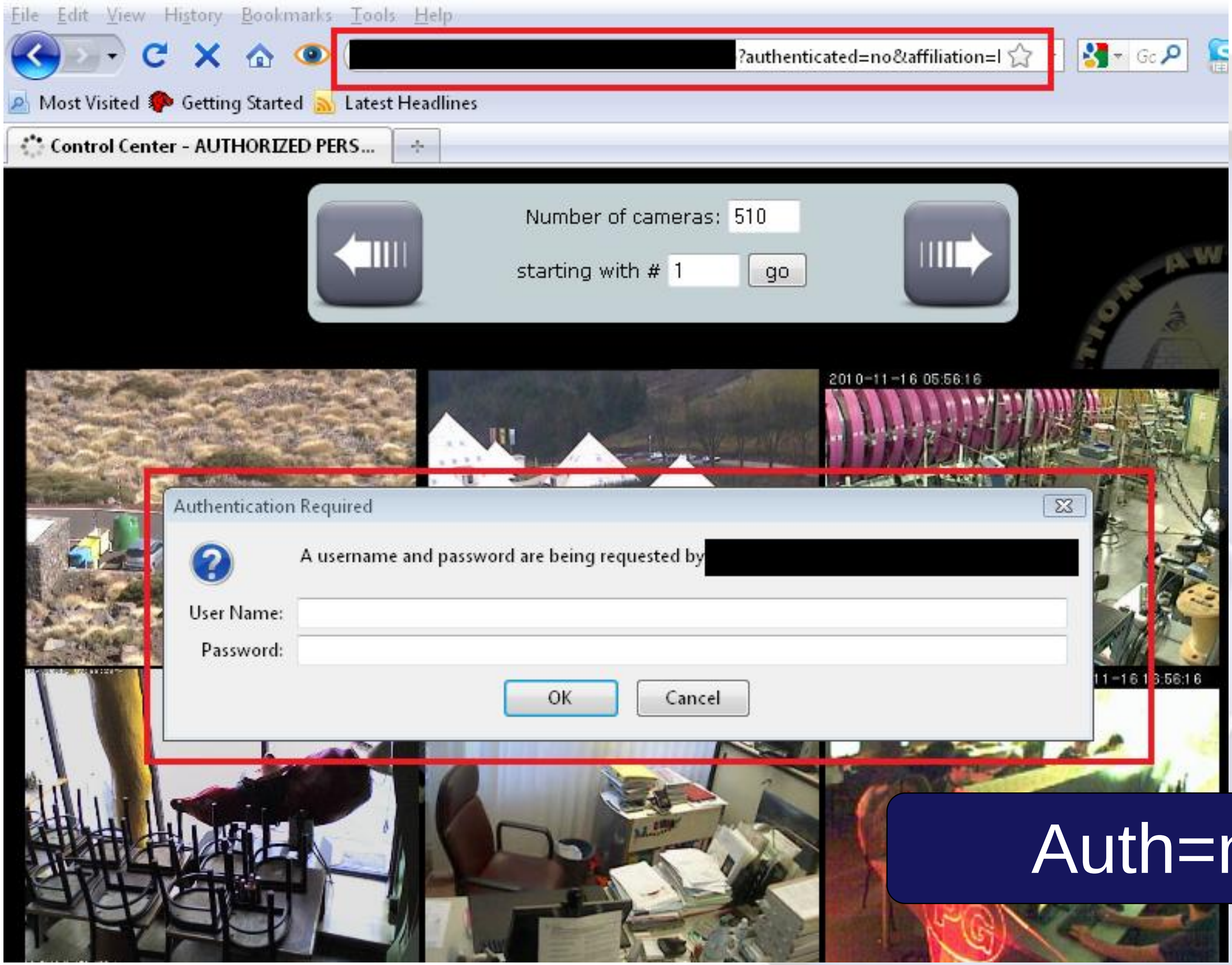
User Name:

Password:

OK Cancel

Auth=yes

Bad Design over HTTP – Case Study (1)



[redacted]?authenticated=no&affiliation=l

File Edit View History Bookmarks Tools Help
Most Visited
Getting Started
Latest Headlines
Control Center - AUTHORIZED PERS...

Number of cameras: 510

starting with # 1 go

Authentication Required

A username and password are being requested by [redacted]

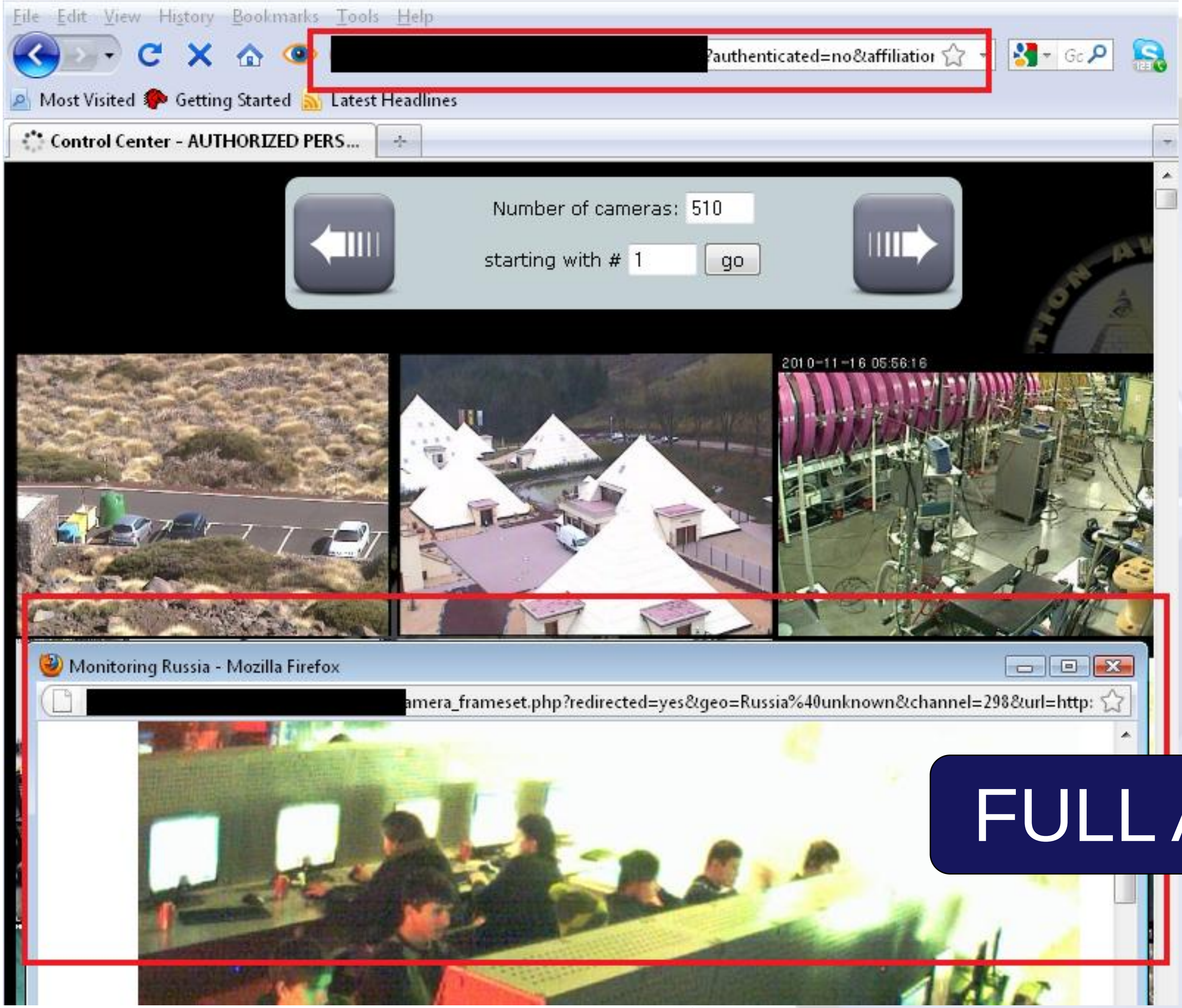
User Name:

Password:

OK Cancel

Auth=no

Bad Design over HTTP – Case Study (1)


File Edit View History Bookmarks Tools Help
Most Visited
Getting Started
Latest Headlines
Control Center - AUTHORIZED PERS...
2010-11-16 05:56:16

[redacted]?authenticated=no&affiliatio

Number of cameras: 510

starting with # 1 go

Monitoring Russia - Mozilla Firefox

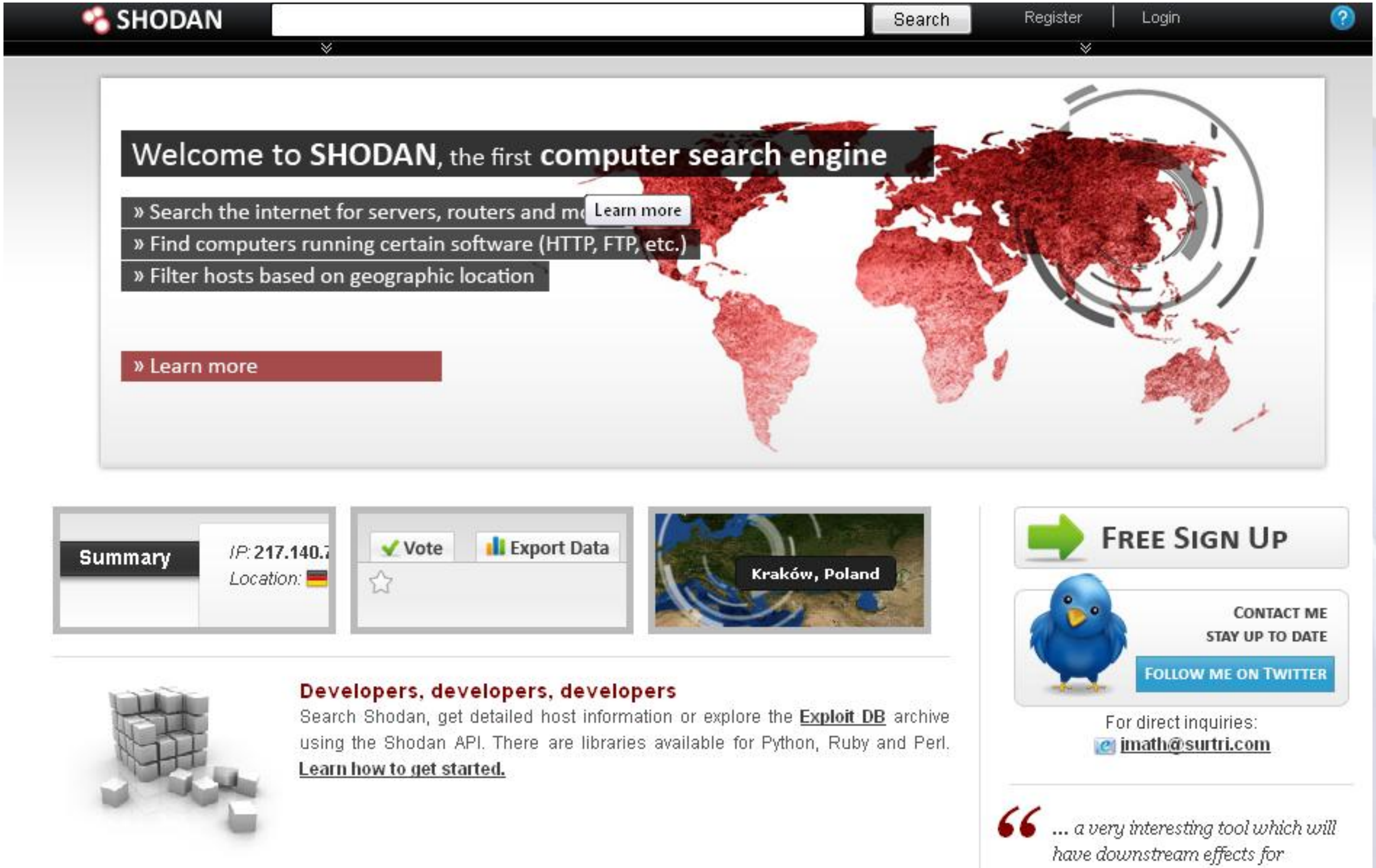
[redacted]amera_frameset.php?redirected=yes&geo=Russia%40unknown&channel=298&url=http:

FULL ACCESS

Free Web – Network Devices Check

1. Search engines such as Shodan
2. Google Dorks

SHODAN – Information Helps in Automated Tool Design



Welcome to SHODAN, the first computer search engine

» Search the internet for servers, routers and mo Learn more

» Find computers running certain software (HTTP, FTP, etc.)

» Filter hosts based on geographic location

» Learn more

IP: 217.140.7

Location:

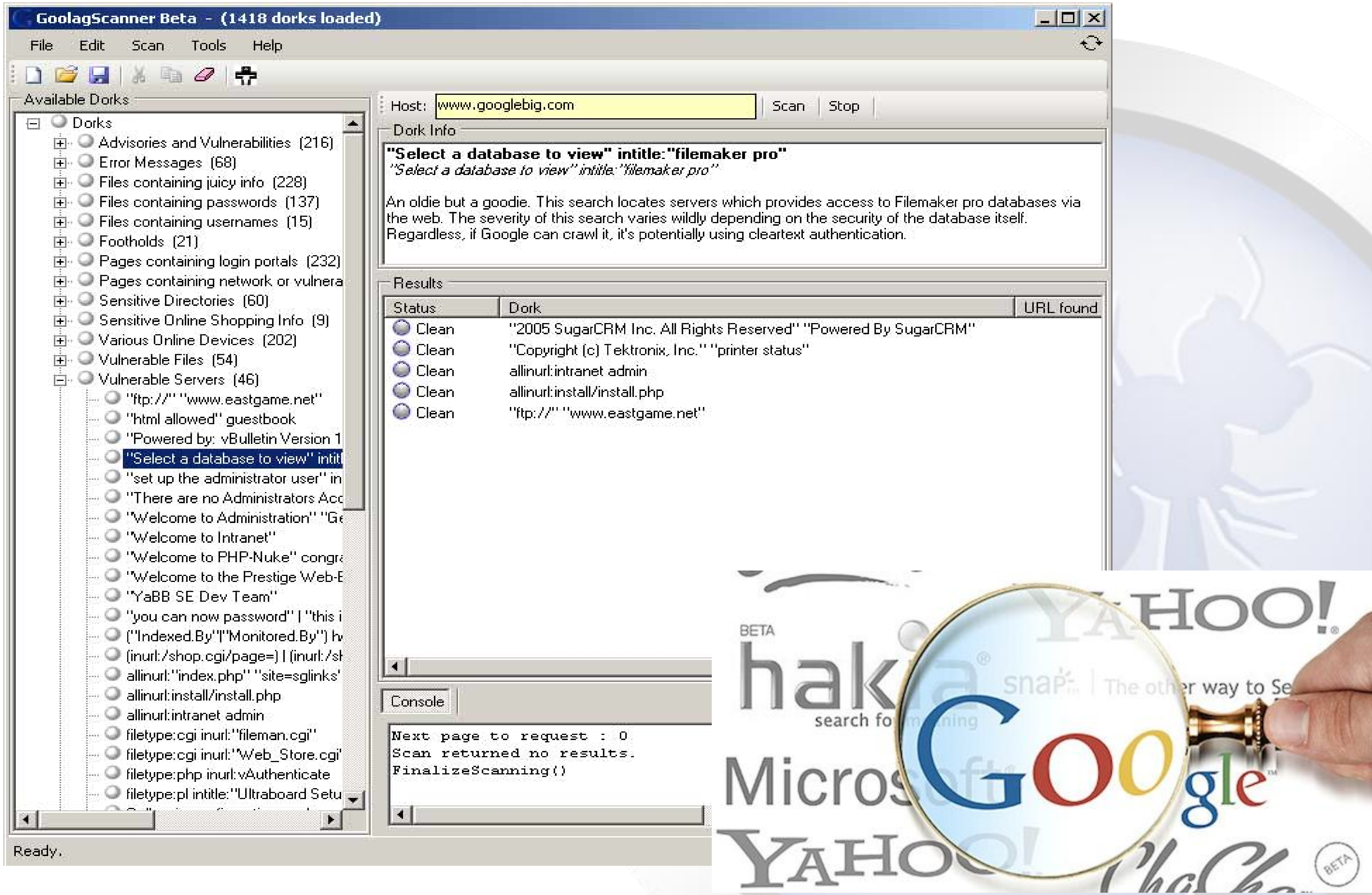
Developers, developers, developers

Search Shodan, get detailed host information or explore the Exploit DB archive using the Shodan API. There are libraries available for Python, Ruby and Perl. Learn how to get started.

For direct inquiries:
jmath@surtri.com

“ ... *a very interesting tool which will have downstream effects for*

Google Dorks – Long Live



GoolagScanner Beta - (1418 dorks loaded)

Available Dorks

- Dorks
  - Advisories and Vulnerabilities (216)
  - Error Messages (68)
  - Files containing juicy info (228)
  - Files containing passwords (137)
  - Files containing usernames (15)
  - Footholds (21)
  - Pages containing login portals (232)
  - Pages containing network or vulnera
  - Sensitive Directories (60)
  - Sensitive Online Shopping Info (9)
  - Various Online Devices (202)
  - Vulnerable Files (54)
  - Vulnerable Servers (46)
    - "ftp://" "www.eastgame.net"
    - "html allowed" guestbook
    - "Powered by: vBulletin Version 1
    - "Select a database to view" intitl
    - "set up the administrator user" in
    - "There are no Administrators Acc
    - "Welcome to Administration" "Ge
    - "Welcome to Intranet"
    - "Welcome to PHP-Nuke" congra
    - "Welcome to the Prestige Web-E
    - "YaBB SE Dev Team"
    - "you can now password" | "this i
    - ("Indexed.By"|"Monitored.By") h
    - (inurl:/shop.cgi/page=) | (inurl:/sh
    - allinurl:"index.php" "site=sglinks"
    - allinurl:install/install.php
    - allinurl:intranet admin
    - filetype:cgi inurl:"fileman.cgi"
    - filetype:cgi inurl:"Web_Store.cgi"
    - filetype:php inurl:vAuthenticate
    - filetype:pl intitle:"Ultraboard Setu

Host: www.googlebig.com

Dork Info

"Select a database to view" intitle:"filemaker pro"
"Select a database to view" intitle:"filemaker pro"

An oldie but a goodie. This search locates servers which provides access to Filemaker pro databases via the web. The severity of this search varies wildly depending on the security of the database itself. Regardless, if Google can crawl it, it's potentially using cleartext authentication.

Results

Status	Dork	URL found
Clean	"2005 SugarCRM Inc. All Rights Reserved" "Powered By SugarCRM"	
Clean	"Copyright (c) Tektronix, Inc." "printer status"	
Clean	allinurl:intranet admin	
Clean	allinurl:install/install.php	
Clean	"ftp://" "www.eastgame.net"	

Console

```
Next page to request : 0
Scan returned no results.
FinalizeScanning()
```

Ready.

Lastly, There is lot more in the World Wide Web

We have presented only a glimpse.

Conclusion

- Information gathering is the prime key
- Unique signatures lead to detection
- Variation in http based network devices
- Bad design practices in use

Questions

Thanks

- OWASP Brazil
- SecNiche Security
- Bracktrack Brazil