

【HTML中隐写】Snow免安装、网站版

原创

[黑色地带\(崛起\)](#) 已于 2022-03-30 10:20:40 修改 121 收藏

文章标签: [安全](#)

于 2022-03-29 13:28:25 首次发布

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_53079406/article/details/123810053

版权

目录

Snow

准备阶段:

原理:

使用方法:

[Options \(选项\)](#)

[Examples \(例子\)](#)

使用:

对比:

[用浏览器打开瞅瞅](#)

[使用工具](#)

换网站:

[Decryption \(解密\)](#)

[Encryption \(加密\)](#)

[让我来浅试一下:](#)

[总结:](#)

(又是一个隐写细节, 更完所有隐写工具, 整合集)

以蝼蚁之行, 展鸿鹄之志



Snow

准备阶段:

下载地址（开源的）：

[The SNOW Home Page \(darkside.com.au\)](http://darkside.com.au)

使用Snow 的网络版：

[Snow web-page encryption/decryption \(misty.com\)](http://misty.com)

（里面有Windows可执行的，无需安装的，直接用）

选择适合自己的下

As of 16 June 2013, SNOW is available under an Apache 2.0 license. The usual conditions apply, but if you want to hear about it.

Recent changes

Prior to 22 November 1998 the DOS version, contained in *snowdos.zip*, had a bug affecting encryption. Files encrypted by this version could not be decrypted by the other versions, and vice versa. The bug was caused by bit-shifting of 16-bit

The source version, when compiled under Unix, also had a bug where it could not read data concealed by the DOS version. This has also been fixed as of 22 November 1998.

- Documentation
 - [How it works](#)
 - [Manual page](#)
 - [About the logo](#)
- Download source
 - [snow-20130616.tar.gz](#) (16210 bytes)
 - [snow.zip](#) (22071 bytes)
- Download DOS/Windows executable
 - 16-bit executable [snwdos16.zip](#) (27001 bytes)
 - 32-bit executable [snwdos32.zip](#) (30961 bytes)
- Download Java 1.1 version
 - Java source [jsnow.zip](#) (10691 bytes)
 - Java classes [jsnow.jar](#) (24039 bytes)
- Java 1.1 applet
 - Download source, classes, and doco [jsnowapp.zip](#) (35117 bytes)
 - Run the [applet](#) (Note - needs Java 1.1 browser)
- Examples
 - Dr Rick Perry's interactive [CGI script](#) for concealing/extracting messages in HTML pages.
- [About the author](#)

CSDN @黑色地带(崛起) PI

名称	修改日期	类型	大小
 SNOW.DOC	1998/11/22 15:56	Microsoft Word ...	
 SNOW.EXE	1998/11/16 15:05	应用程序	

原理：

Snow 的man 手册中讲到“通过在文本文件末尾追加由制表位隔开的空格可以实现数据隐藏，最多可以添加 7 个空格，这使得每 8 列可以嵌入 3 位”。

也就是说找到很多空格的地方说明隐写成功了

使用方法：

Options（选项）

-C

如果隐藏，则压缩数据，或者如果提取，则会解压缩。

-Q

静音模式。如果未设置，则程序报告统计信息，例如压缩百分比和可用存储空间的数量。

-S

报告文本文件中隐藏消息的近似空间量。考虑线长度，但忽略其他选项。

-p password

如果设置为此，则在隐藏期间将使用此密码加密数据，或在提取期间解密。

-l line-length

在附加空格时，Snow将始终产生比此值短的线条。默认情况下，它设置为80。

-f message-file

此文件的内容将隐藏在输入文本文件中。

-m message-string

此字符串的内容将被隐藏在输入文本文件中。请注意，除非在字符串中包含一个换行符，否则在提取邮件时，否则不会打印换行符。

Examples（例子）

以下命令将隐藏文件infile中的消息“I am lying”中，压缩，并使用密码“Hello World”加密。生成的文本将被存储在外档中。

```
snow -C -m "I am lying" -p "hello world" infile outfile
```

要提取消息，命令将是

```
snow -C -p "hello world" outfile
```

请注意，生成的消息不会被换行符终止。

为防止线包装，如果通过邮件或新闻读卡器缩进隐藏空间的文本，可以使用72或更小的线长度。

```
snow -C -l 72 -m "I am lying" infile outfile
```

可以使用-s选项确定文件的近似存储容量。

```
snow -S -l 72 infile
```

使用：

第一步：

先将文件都放在Snow文件夹中，再进行操作

原始文件也留一个做对比

名称	修改日期	类型	大小
index.html	2014/11/1 3:10	搜狗高速浏览器H...	
SNOW.DOC	1998/11/22 15:56	Microsoft Word ...	
SNOW.EXE	1998/11/16 15:05	应用程序	
test.html	2014/11/1 3:10	搜狗高速浏览器H...	

第二步：先进入到文件夹中

然后再执行隐写命令

```
snow.exe -C -m "flag" -p "123456" test.html
```

```
C:\Users\>
```

```
D:\>cd BaiduNetdiskDownload\snowdos32
```

```
D:\BaiduNetdiskDownload\snowdos32>snow.exe -C -m "flag" -p "123456" test.html
```

CSDN @黑色地带(崛起)

这里显示压缩了34.38%

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
Compressed by 34.38%
</head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Less-1 **Error Based- String**</title>
</head>
```

CSDN @黑色地带(崛起)

最后显示：消息使用大约1.60%的可用空间。

```
Message used approximately 1.60% of available space.
```

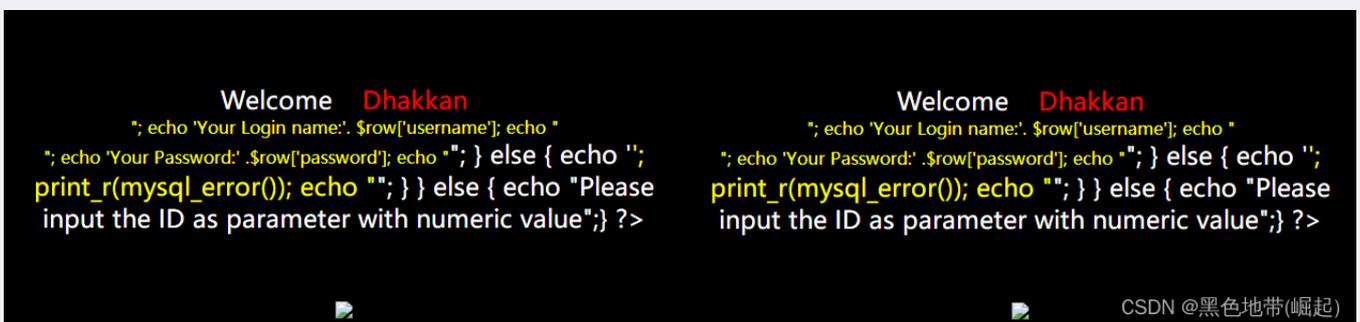
```
D:\BaiduNetdiskDownload\snowdos32>
```

CSDN @黑色地带(崛起)

对比：

用浏览器打开瞅瞅

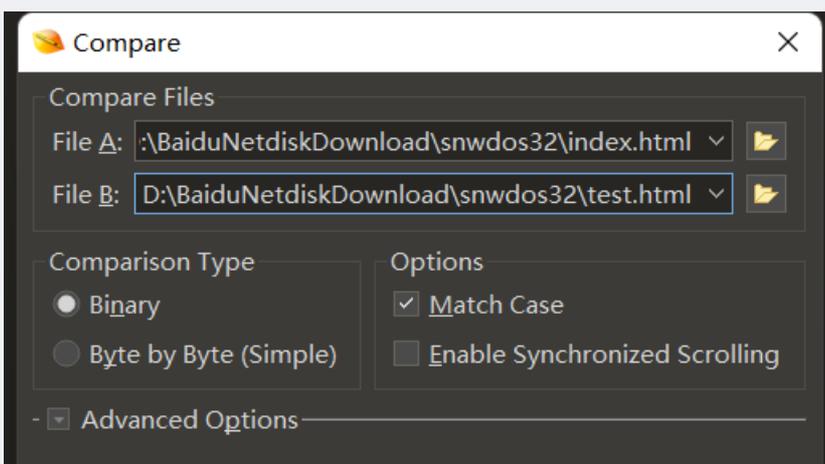
可以说看起来一模一样



CSDN @黑色地带(崛起)

使用工具

用Winhex（010 Editor 我更喜欢这个软件，看起来跟舒服）对比试试



Compare

Cancel

Help

CSDN @黑色地带(崛起)

对比结果是全部一样（大无语事件右发生了）

File Edit Search View Format Scripts Templates Debug Tools Window Help

Startup index.html x

```

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
04B0h: 6F 6C 6F 72 3D 20 22 23 46 46 46 46 30 30 22 3E 01or= "#FFFF00">
04C0h: 27 3B 0D 0A 09 70 72 69 6E 74 5F 72 28 6D 79 73 ';...print_r(mys
04D0h: 71 6C 5F 65 72 72 6F 72 28 29 29 3B 0D 0A 09 65 ql_error());...e
04E0h: 63 68 6F 20 22 3C 2F 66 6F 6E 74 3E 22 3B 20 20 cho "</font>";
04F0h: 0D 0A 09 7D 0D 0A 7D 0D 0A 09 65 6C 73 65 20 7B ...}...else {
0500h: 20 65 63 68 6F 20 22 50 6C 65 61 73 65 20 69 6E echo "Please in
0510h: 70 75 74 20 74 68 65 20 49 44 20 61 73 20 70 61 put the ID as pa
0520h: 72 61 6D 65 74 65 72 20 77 69 74 68 20 6E 75 6D ramer with num
0530h: 65 72 69 63 20 76 61 6C 75 65 22 3B 7D 0D 0A 0D eric value";}...
0540h: 0A 3F 3E 0D 0A 3C 2F 66 6F 6E 74 3E 20 3C 2F 64 .?>...</font> </d
0550h: 69 76 3E 3C 2F 62 72 3E 3C 2F 62 72 3E 3C 2F 62 iv></br></br></b
0560h: 72 3E 3C 63 65 6E 74 65 72 3E 0D 0A 3C 69 6D 67 r><center>...</
0590h: 63 65 6E 74 65 72 3E 0D 0A 3C 2F 62 6F 64 79 3E center>...</body>
05A0h: 0D 0A 3C 2F 68 74 6D 6C 3E 0D 0A 0D 0A 0D 0A 0D ..</html>.....
  
```

test.html x

```

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
04B0h: 6F 6C 6F 72 3D 20 22 23 46 46 46 46 30 30 22 3E 01or= "#FFFF00">
04C0h: 27 3B 0D 0A 09 70 72 69 6E 74 5F 72 28 6D 79 73 ';...print_r(mys
04D0h: 71 6C 5F 65 72 72 6F 72 28 29 29 3B 0D 0A 09 65 ql_error());...e
04E0h: 63 68 6F 20 22 3C 2F 66 6F 6E 74 3E 22 3B 20 20 cho "</font>";
04F0h: 0D 0A 09 7D 0D 0A 7D 0D 0A 09 65 6C 73 65 20 7B ...}...else {
0500h: 20 65 63 68 6F 20 22 50 6C 65 61 73 65 20 69 6E echo "Please in
0510h: 70 75 74 20 74 68 65 20 49 44 20 61 73 20 70 61 put the ID as pa
0520h: 72 61 6D 65 74 65 72 20 77 69 74 68 20 6E 75 6D ramer with num
0530h: 65 72 69 63 20 76 61 6C 75 65 22 3B 7D 0D 0A 0D eric value";}...
0540h: 0A 3F 3E 0D 0A 3C 2F 66 6F 6E 74 3E 20 3C 2F 64 .?>...</font> </d
0550h: 69 76 3E 3C 2F 62 72 3E 3C 2F 62 72 3E 3C 2F 62 iv></br></br></b
0560h: 72 3E 3C 63 65 6E 74 65 72 3E 0D 0A 3C 69 6D 67 r><center>...</
0590h: 63 65 6E 74 65 72 3E 0D 0A 3C 2F 62 6F 64 79 3E center>...</body>
05A0h: 0D 0A 3C 2F 68 74 6D 6C 3E 0D 0A 0D 0A 0D 0A 0D ..</html>.....
  
```

Compare

D:\BaiduNetdiskDownload\snowdos32\index.html vs.

Result	Address A	Size A	Address B	Size B
Match	0h	5B8h	0h	5B8h

CSDN @黑色地带(崛起)

File Edit Search View Format Scripts Templates Debug Tools Window Help

Startup index.html x

```

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0350h: 76 69 74 79 20 0D 0A 0D 0A 0D 0A 24 73 71 6C 3D vity.....$sql=
0360h: 22 53 45 4C 45 43 54 20 2A 20 46 52 4F 4D 20 75 "SELECT * FROM u
0370h: 73 65 72 73 20 57 48 45 52 45 20 69 64 3D 27 24 sers WHERE id=$
0380h: 69 64 27 20 4C 49 4D 49 54 20 30 2C 31 22 3B 0D id' LIMIT 0,1";.
0390h: 0A 24 72 65 73 75 6C 74 3D 6D 79 73 71 6C 5F 71 .$result=mysql_q
03A0h: 75 65 72 79 28 24 73 71 6C 29 3B 0D 0A 24 72 6F uery($sql);..$ro
03B0h: 77 20 3D 20 6D 79 73 71 6C 5F 66 65 74 63 68 5F w= mysql_fetch_
03C0h: 61 72 72 61 79 28 24 72 65 73 75 6C 74 29 3B 0D array($result);.
03D0h: 0A 0D 0A 09 69 66 28 24 72 6F 77 29 0D 0A 09 7B ....if($row)...{
03E0h: 0D 0A 20 20 09 65 63 68 6F 20 22 3C 66 6F 6E 74 .. echo "<font
03F0h: 20 73 69 7A 65 3D 27 35 27 20 63 6F 6C 6F 72 3D size='5' color=
0400h: 20 27 23 39 39 46 46 30 30 27 3E 22 3B 0D 0A 20 '#99FF00'>";...
0410h: 20 09 65 63 68 6F 20 27 59 6F 75 72 20 4C 6F 67 .echo 'Your Log
0420h: 69 6E 20 6E 61 6D 65 3A 27 2E 20 24 72 6F 77 5B in name:'. $row[
0430h: 27 75 73 65 72 6E 61 6D 65 27 5D 3B 0D 0A 20 20 'username'];...
0440h: 09 65 63 68 6F 20 22 3C 62 72 3E 22 3B 0D 0A 20 .echo "<br>";...
  
```

test.html x

```

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0350h: 76 69 74 79 20 0D 0A 0D 0A 0D 0A 24 73 71 6C 3D vity.....$sql=
0360h: 22 53 45 4C 45 43 54 20 2A 20 46 52 4F 4D 20 75 "SELECT * FROM u
  
```

```

0370h: 73 65 72 73 20 57 48 45 52 45 20 69 64 3D 27 24 sers WHERE id='$
0380h: 69 64 27 20 4C 49 4D 49 54 20 30 2C 31 22 3B 0D id' LIMIT 0,1";.
0390h: 0A 24 72 65 73 75 6C 74 3D 6D 79 73 71 6C 5F 71 .$result=mysql_q
03A0h: 75 65 72 79 28 24 73 71 6C 29 3B 0D 0A 24 72 6F uery($sql);..$ro
03B0h: 77 20 3D 20 6D 79 73 71 6C 5F 66 65 74 63 68 5F w=mysql_fetch_
03C0h: 61 72 72 61 79 28 24 72 65 73 75 6C 74 29 3B 0D array($result);.
03D0h: 0A 0D 0A 09 69 66 28 24 72 6F 77 29 0D 0A 09 7B ...if($row)...{
03E0h: 0D 0A 20 20 09 65 63 68 6F 20 22 3C 66 6F 6E 74 ..echo "<font
03F0h: 20 73 69 7A 65 3D 27 35 27 20 63 6F 6C 6F 72 3D size='5' color=
0400h: 20 27 23 39 39 46 46 30 30 27 3E 22 3B 0D 0A 20 '#99FF00'>";..
0410h: 20 09 65 63 68 6F 20 27 59 6F 75 72 20 4C 6F 67 .echo 'Your Log
0420h: 69 6E 20 6E 61 6D 65 3A 27 2E 20 24 72 6F 77 5B in name:'. $row[
0430h: 27 75 73 65 72 6E 61 6D 65 27 5D 3B 0D 0A 20 20 'username'];..
0440h: 09 65 63 68 6F 20 22 3C 62 72 3E 22 3B 0D 0A 20 .echo "<br>";..

```

Find Results

Address	Value
Found 99 occurrences of '20'.	
9h	20
Eh	20

CSDN @黑色地带(崛起)

File Edit Search View Format Scripts Templates Debug Tools Window Help

Startup index.html x

```

0450h: 20 09 65 63 68 6F 20 27 59 6F 75 72 20 50 61 73 .echo 'Your Pas
0460h: 73 77 6F 72 64 3A 27 20 2E 24 72 6F 77 5B 27 70 sword:'. $row['p
0470h: 61 73 73 77 6F 72 64 27 5D 3B 0D 0A 20 20 09 65 assword'];.. .e
0480h: 63 68 6F 20 22 3C 2F 66 6F 6E 74 3E 22 3B 0D 0A cho "</font>";..
0490h: 20 20 09 7D 0D 0A 09 65 6C 73 65 20 0D 0A 09 7B }...else {...{
04A0h: 0D 0A 09 65 63 68 6F 20 27 3C 66 6F 6E 74 20 63 ..echo '<font c
04B0h: 6F 6C 6F 72 3D 20 22 23 46 46 46 46 30 30 22 3E olor= "#FFFF00">
04C0h: 27 3B 0D 0A 09 70 72 69 6E 74 5F 72 28 6D 79 73 ';...print_r(mys
04D0h: 71 6C 5F 65 72 72 6F 72 28 29 29 3B 0D 0A 09 65 ql_error());...e
04E0h: 63 68 6F 20 22 3C 2F 66 6F 6E 74 3E 22 3B 20 20 cho "</font>";
04F0h: 0D 0A 09 7D 0D 0A 7D 0D 0A 09 65 6C 73 65 20 7B }...}...else {
0500h: 20 65 63 68 6F 20 22 50 6C 65 61 73 65 20 69 6E echo "Please in
0510h: 70 75 74 20 74 68 65 20 49 44 20 61 73 20 70 61 put the ID as pa
0520h: 72 61 6D 65 74 65 72 20 77 69 74 68 20 6E 75 6D ramer with num
0530h: 65 72 69 63 20 76 61 6C 75 65 22 3B 7D 0D 0A 0D eric value";}...
0540h: 0A 3F 3E 0D 0A 3C 2F 66 6F 6E 74 3E 20 3C 2F 64 .?>..</font> </d

```

test.html x

```

0450h: 20 09 65 63 68 6F 20 27 59 6F 75 72 20 50 61 73 .echo 'Your Pas
0460h: 73 77 6F 72 64 3A 27 20 2E 24 72 6F 77 5B 27 70 sword:'. $row['p
0470h: 61 73 73 77 6F 72 64 27 5D 3B 0D 0A 20 20 09 65 assword'];.. .e
0480h: 63 68 6F 20 22 3C 2F 66 6F 6E 74 3E 22 3B 0D 0A cho "</font>";..
0490h: 20 20 09 7D 0D 0A 09 65 6C 73 65 20 0D 0A 09 7B }...else {...{
04A0h: 0D 0A 09 65 63 68 6F 20 27 3C 66 6F 6E 74 20 63 ..echo '<font c
04B0h: 6F 6C 6F 72 3D 20 22 23 46 46 46 46 30 30 22 3E olor= "#FFFF00">
04C0h: 27 3B 0D 0A 09 70 72 69 6E 74 5F 72 28 6D 79 73 ';...print_r(mys
04D0h: 71 6C 5F 65 72 72 6F 72 28 29 29 3B 0D 0A 09 65 ql_error());...e
04E0h: 63 68 6F 20 22 3C 2F 66 6F 6E 74 3E 22 3B 20 20 cho "</font>";
04F0h: 0D 0A 09 7D 0D 0A 7D 0D 0A 09 65 6C 73 65 20 7B }...}...else {
0500h: 20 65 63 68 6F 20 22 50 6C 65 61 73 65 20 69 6E echo "Please in
0510h: 70 75 74 20 74 68 65 20 49 44 20 61 73 20 70 61 put the ID as pa
0520h: 72 61 6D 65 74 65 72 20 77 69 74 68 20 6E 75 6D ramer with num
0530h: 65 72 69 63 20 76 61 6C 75 65 22 3B 7D 0D 0A 0D eric value";}...
0540h: 0A 3F 3E 0D 0A 3C 2F 66 6F 6E 74 3E 20 3C 2F 64 .?>..</font> </d

```

Find Results

Address	Value
---------	-------

(隐写成功，也没见你写进去，感觉是在坑孩子)



换网站：

Snow 的网络版:

[Snow web-page encryption/decryption \(misty.com\)](#)

Snow网页加密/解密

另请参阅applet版本jsnowapp，它可以使用本地文件而不是URL

以下使用的URL必须是直接的，即，它们不得生成重定向，否则它将无法正常工作。

Snow web-page encryption/decryption

Also see the applet version [jsnowapp](#) which can work with local files instead of URL's.

URLs used below must be direct, i.e. they must not generate a redirect, otherwise it won't work.

Decryption

URL containing concealed message:

Password:

Encryption

URL to conceal message in:

Message to encrypt:

Password:

After selecting Encrypt, save the resulting page as HTML source (i.e. type "Web Page, HTML only", NOT "Web Page, complete") and put it on your web site. You can decrypt the message using the Decryption section above, or using the command-line version of snow: `snow -C -p password filename`

CSDN @黑色地带(崛起)

Decryption (解密)

包含隐藏消息的URL:

Encryption (加密)

隐藏消息的URL:

要加密的消息:

让我来浅试一下:

在本地搭建的好的靶场中新建一个进行测试

Encryption

URL to conceal message in:

Message to encrypt:

Password: 123456

Encrypt

After selecting Encrypt, save the resulting page as HTML source (i.e. type "Web Page, HTML only", NOT "Web Page, Text Only" in the

CSDN @黑色地带(崛起)



您要提交的信息不安全

由于正在提交的表单使用的连接不安全，其他人可以看到你的信息。

仍然发送

返回

CSDN @黑色地带(崛起)

脚本失败 脚本失败：未找到主机：localhost：8080

← → ↻ 🏠 ⚠ 不安全 | fog.misty.com/cgi/snow

Script Failed

Script failed: host not found: localhost:8080

CSDN @黑色地带(崛起)

但实际上我自己

是能访问的

localhost:8080/sqli-labs-master/test/

百度 火狐官方网站 常用网址 商业计划书PPT模板下...

移动设备上的书签

```
Welcome Dhakkan
"; echo 'Your Login name:'. $row['username']; echo "
"; echo 'Your Password:'. $row['password']; echo "; } else { echo "; print_r(mysql_error()); echo "; } }
else { echo "Please input the ID as parameter with numeric value"; } ?>
```

SOLDIER DIVER SERIES

总结:

虽然失败告终，但是还是搞清楚了他的写入原理

(放话：每一步都有它特殊的意义)



推荐:

【数据隐藏】一起入门隐写吧，宝? word、图像、移动设备、文件压缩数据隐藏