

# i春秋Hello World

转载

[weixin\\_30701575](#) 于 2019-09-16 15:58:00 发布 457 收藏 1

文章标签: [数据结构与算法](#)

原文链接: <http://www.cnblogs.com/wosun/p/11527770.html>

版权

< > ↻ 🏠 📖 | ☆ 106.75.72.168:9999

★ 书签 | 📁 常用网址 🌐 京东商城 📖 中国大学MOOC(中) 🌐 C 语言开发环境 🌐

## Hello, World!

📄 106.75.72[1] - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<html>
<head>
<title>
</title>
</head>
<script src="flag.xmas.js"> </script>
<h1>Hello, World!</h1>
</html>
```

打开只有一句hello world, 直接查看源码, 发现一个flag.xmas.js文件

试试直接访问<http://106.75.72.168:9999/flag.xmas.js> <http://106.75.72.168:9999/flag.xmas> 访问不了

再试试<http://106.75.72.168:9999/flag.js>发现下载下来这个js文件了

```
JS flag.js x
C: > Users > 七星 > Desktop > JS flag.js > ...
1
2
3
4
5
6
7     var CryptoJS=CryptoJS
8     || function (t,e) {var
9     r= {},i=r .lib= {},
10    n=function (){ },o=i. Base= {extend :
11    function (t){ n. prototype=this ;var e=new n;t &&
12    e .mixIn (t);e. hasOwnProperty ("init"
13    ) ) ||
14
15
16
17    ( e.
18    init=function ()
19    {e
20    $super .init
21    . apply
22    (this ,
23    arguments )))
24    ;e. init
25    .prototype=e;e.
26
27
28
29
30
31
32
33    $super=this ; return e
34    }, create : function
35    (){ var t=this .
36    extend (); t.init . apply( t,
```

是一个打乱了的js文件。。。。没有耐心去看这么多打乱的js代码

可能是.git文件泄露

直接用githack去抓一下试试

```
C:\Users\七星\Desktop\tools\Git_Extract-master>python git_extract.py http://106.75.72.168:9999/.git/

Git Extract
Author: gakki429

[*] Start Extract
[*] Target Git: http://106.75.72.168:9999/.git/
[*] Analyze .git/HEAD
[*] Extract Ref refs/heads/master 887746
[*] Clone Commit 887746
[*] Parse Tree ../ b5dfb5
[+] Save ../flag.js
[+] Save ../flag.php
[+] Save ../index.php
[*] Analyze .git/logs/HEAD
[*] Clone Commit 09e053
[*] Parse Tree ../ 9ee4dc
[+] Save ../flag.js.04bb09
[*] Detect .git/index
[*] Extract Done
```

> tools > Git\_Extract-master > 106.75.72.168\_9999 >

名称	修改日期	类型	大小
.git	2019/9/16 14:16	文件夹	
flag.js	2019/9/16 14:16	JetBrains PhpSto...	88 KB
flag.js.04bb09	2019/9/16 14:16	04BB09 文件	88 KB
flag.php	2019/9/16 14:16	JetBrains PhpSto...	1 KB
index.php	2019/9/16 14:16	JetBrains PhpSto...	1 KB

依次打开检查

```
flag.js.04bb09.js  flag.php
C: > Users > 七星 > Desktop > tools > Git_Extract-master > 106.75.72.168_9999 > flag.php
1  <?php
2  ini_set("display_errors", "Off");
3  error_reporting(0);
4  function encode($b,$c='', $d=0)
5  {
6      $e=4;
7      $c=md5($c);
8      $f=md5(substr($c,0,16));
9      $g=md5(substr($c,16,16));
10     $h=$e?($k=='DECODE'?substr($b,0,$e):substr(md5(microtime()),-$e)):'';
11     $l=$f.md5($f.$h);$m=strlen($l);$b=sprintf('%010d',$d?$d+time():0).substr(md5($b.$g),0,16).$b;
12     $n=strlen($b);
13     $o='';
14     $p=range(0,255)
15     $q=array();
16     for($r=0;
17     $r<=255;
18     $r++)
19     {$q[$r]=ord($l[$r%$m]);}
20     for($s=$r=0;$r<256;$r++)
21     {
22         $s=($s+$p[$r]+$q[$r])%256;
23         $t=$p[$r];
24         $p[$r]=$p[$s];
25         $p[$s]=$t;
26     }
27     for($u=$s=$r=0;$r<$n;$r++)
28     {
29         $u=($u+1)%256;
30         $s=($s+$p[$u])%256;
31         $t=$p[$u];
32         $p[$u]=$p[$s];$p[$s]=$t;
33         $o.=chr(ord($b[$r])^($p[(($p[$u]+$p[$s])%256)]));
34     }return $h.str_replace('=',' ',base64_encode($o));
35     }
36     $c="flag_1s_n0t_h3re";
37     $cipher = "3133g8JTV89Ds4oh5k0JRPfijAbc1Qw7HciaZfhsV5lWr+7RM9IAF9SNw9WJMEg";?>
```

发现flag.php中似乎有蹊跷，最后一个cipher的值很奇怪，怀疑是加密的，试试解密，不成功，上面那个变量c提示我们flag不在此处。。。。。

根据其他wp得知，flag在js的修改处

我们在kali linux上使用diff来对比两个文件

diff的用法（[https://blog.csdn.net/zhangmeimei\\_pku/article/details/79483324](https://blog.csdn.net/zhangmeimei_pku/article/details/79483324)）（这里其实不用看那么多，直接diff就行了）

```

root@kali:~# cd /root/桌面/Git_Extract-master/106.75.72.168_9999
root@kali:~/桌面/Git_Extract-master/106.75.72.168_9999# diff flag.js flag.js.04bb09.js
220c220
<     BufferedBlockAlgorithm=o
< ---
>     BufferedBlockAlgorithm=f
256c256
<     c=n/(4*o),c=e           ?t.ceil(c):
< ---
>     c=n/(4*o),c=e           ?t.cell(c):
297c297
<     _append                 (t)
< ---
>     _ppend                  (t)
334c334
<     }; return r             }(Math);(
< ---
>     }; return g             }(Math);(
377c377
<     (n)                     ,-1!=n    &&           (r=n
< ---
>     (n)                     ,-1!=n    &&           {r=n
410c410
<     (t                       ,e,
< ---
>     (t                       ,8,
431c431
<     return(t <<              o|t >>>32-o           )+e}
< ---
>     return(t <<              o|t >>>3-o           )+e}
454c454
<     ,s=o                     .algo    ,f=           [],
< ---
>     ,s=o                     .algo    ,e=           [],
490c490
<     ,g=t                     [o+
< ---
>     ,g=t                     [f+
516c516
<     ,w                       ,z,
< ---
>     ,c                       ,z,
535c535
<     ]) ,D=e                  (D,w,z,  C,m,12         ,f[13])

```

< > 10

- 最近使用
- ★ 收藏
- 主目录
- 桌面
- 视频
- 图片
- 文档
- 下载
- 音乐
- 回收站

flag{82efc

```
> ,c ,z,
535c535
< ]) ,D=e (D,w,z, C,m,12 ,f[13])
---
> ]) ,D=e (D,w,z, C,m,12 ,f[133])
541c541
< z,x ,17
---
> z,x ,177
567c567
< ]), w=r
---
> ]), w=f
592c592
< D=i (D,
---
> D=l (D,
595c595
< ,f [33
---
> ,c [33
621c621
< z=i (z,
---
> z=d (z,
637c637
< w, h,23 ,f[47] ),w=n (w,z,C ,D,c,6
---
> w, h,23 ,f[47] ),5=n (w,z,C ,D,c,6
678c678
< [62]),z=n(z,C,D,w,
---
> [62]),d=n(z,C,D,w,
867c867
< :1, _DEC_XFORM_MODE :2, _createHelper
---
> :1, _DEC_XFORM_MODE :4, _createHelper
970c970
< << 16|r << 8|r n=[
```

37f1cd5d4

```
> :1, _DEC_XFORM_MODE :4, _createHelper
970c970
< << 16|r << 8|r ,o=[
...
> << 1|r << 8|r ,o=[
1026c1026
< _process (!0) ,t.unpad (e); return e
...
> _process (!3) ,t.unpad (e); return e
1051c1051
< function (t){ var e=t. ciphertext ;t=t .salt;
...
> function (t){ var e=t. ciphertext ;t=6 .salt;
1102c1102
< ; return p.create ({ ciphertext :e,key :r,iv:
...
> ; return p.create ({ eiphertext :e,key :r,iv:
1181c1181
< extend (i); e=this._parse (e ,i. format);r=i.
...
> extend (i); a=this._parse (e ,i. format);r=i.
1209c1209
< ,l=0 ;256
...
> ,l=0 ;257
1229c1229
< [v],B=d [S], m=257 *d[_
...
> [v],B=c [S], m=257 *d[_
1239c1239
< _]=m <<
...
> _]=a <<
1244c1244
< 16|m >>>16 ;u[_
...
> 16|d >>>16 ;u[_
1258c1258
< (var t=this._key,e=t .words,
...
> (var t=this._key,e=c .words,
1284c1284
< / s=s << 8|s >>>24 s=i|s
```

Navigation menu with icons and text: 最近使用, 收藏, 主目录, 桌面, 视频, 图片, 文档, 下载, 音乐, 回收站

636ea7cad

```
1284c1284
< :( s=s      << 8|s  >>>24      ,s=i[s
...
v :( s=s      << 8|d  >>>24      ,s=i[s
1307c1307
< s=r      %4?      n[o]:n  [o- 4],e[r  ]=4>r
...
v s=r      %4?      n[o]:n  [o- 5],e[r  ]=4>r
1356c1356
<      2],p=t[e+3]      ^r[3],d=4,l=1
...
v      2],p=t[a+3]      ^r[3],d=4,l=1
1385c1385
< [      u&255      ]^r[ d++  ],      f=y,h=g      ,u=_;y=
...
v [      u&255      ]^r[ d++  ],      f=y,h=8      ,u=_;y=
1432c1432
<      :8});t.AES=e      .
...
v      :8});t.AES=1      .
1458c1458
< ;i=[function      (t){ return o
...
v ;i=[function      (t){ return 4
1484c1484
< 'k.o.B'+      '(9-1)'+
...
v 'k.a.B'+      '(9-1)'+
1526c1526
< +      '0.6.8'
...
v +      '0.2.8'
```

d5a814a2

发现flag

flag{82efc37f1cd5d4636ea7cadcd5a814a2}

转载于:<https://www.cnblogs.com/wosun/p/11527770.html>