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

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

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

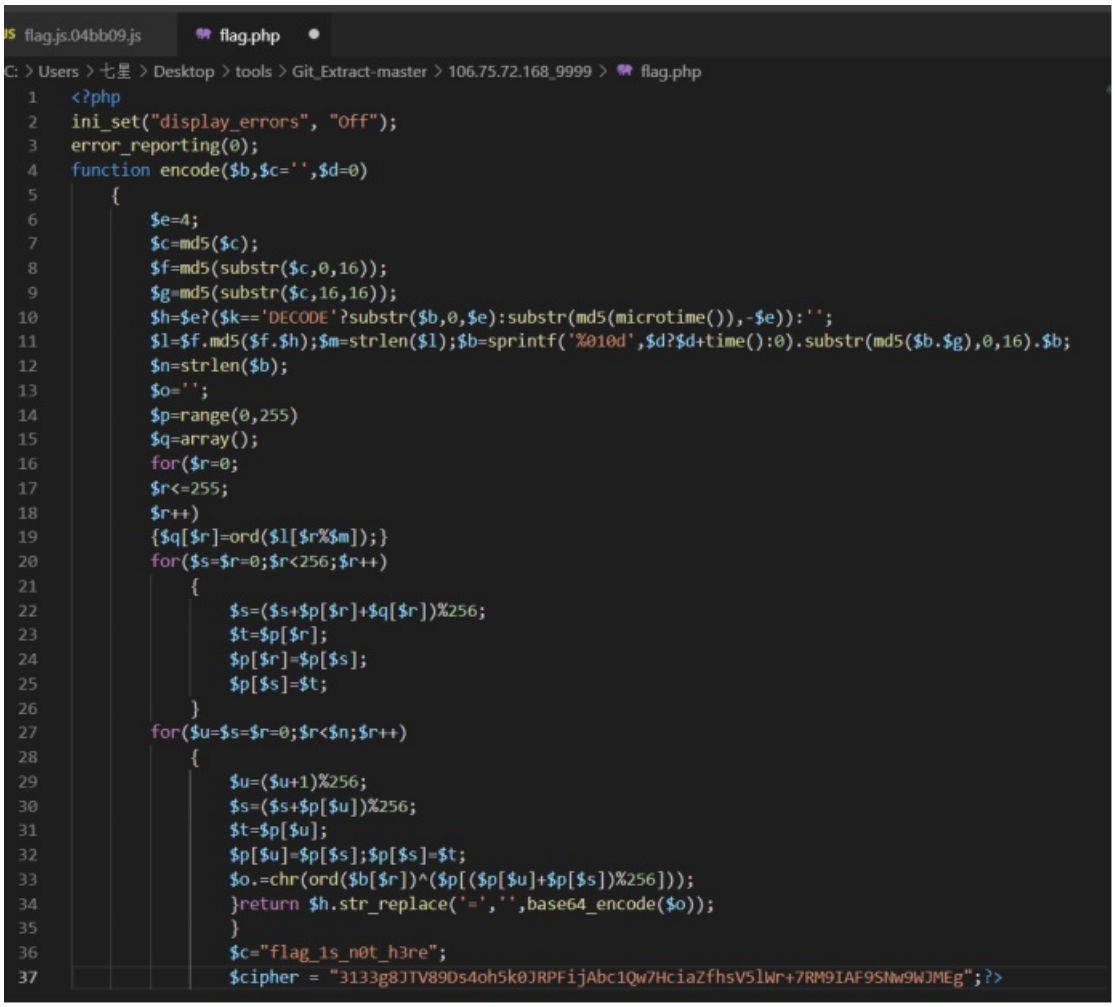
直接用githack去抓一下试试

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

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
```

依次打开检查

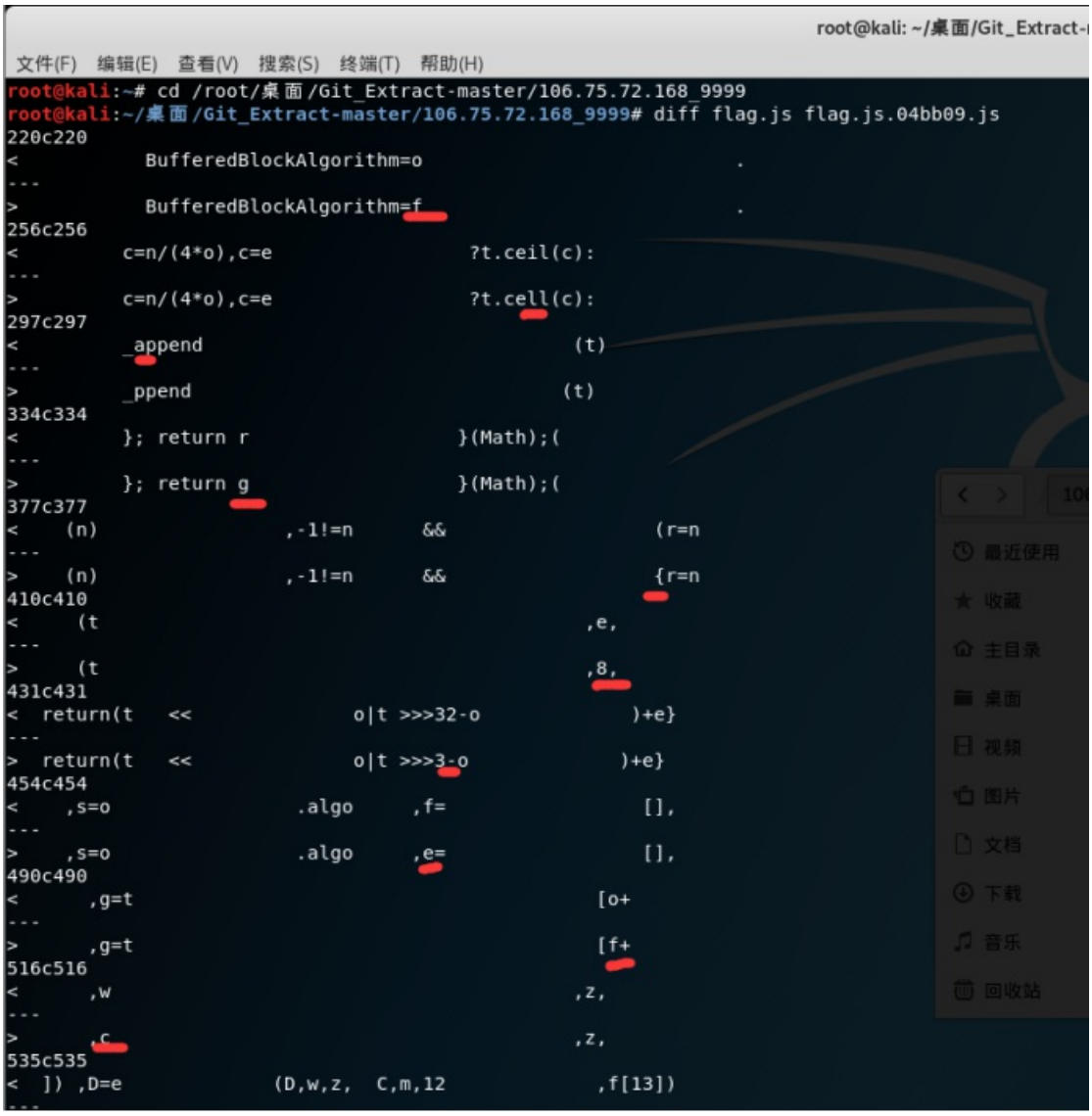


发现flag.php中似乎有蹊跷，最后一个cipher的值很奇怪，怀疑是加密的，试试解密，不成功，上面那个变量c提示我们flag不在这里。。。。。

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）（这里其实不用看那么多，直接diff就行了）


root@kali: ~/桌面/Git_Extract-
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
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= [],

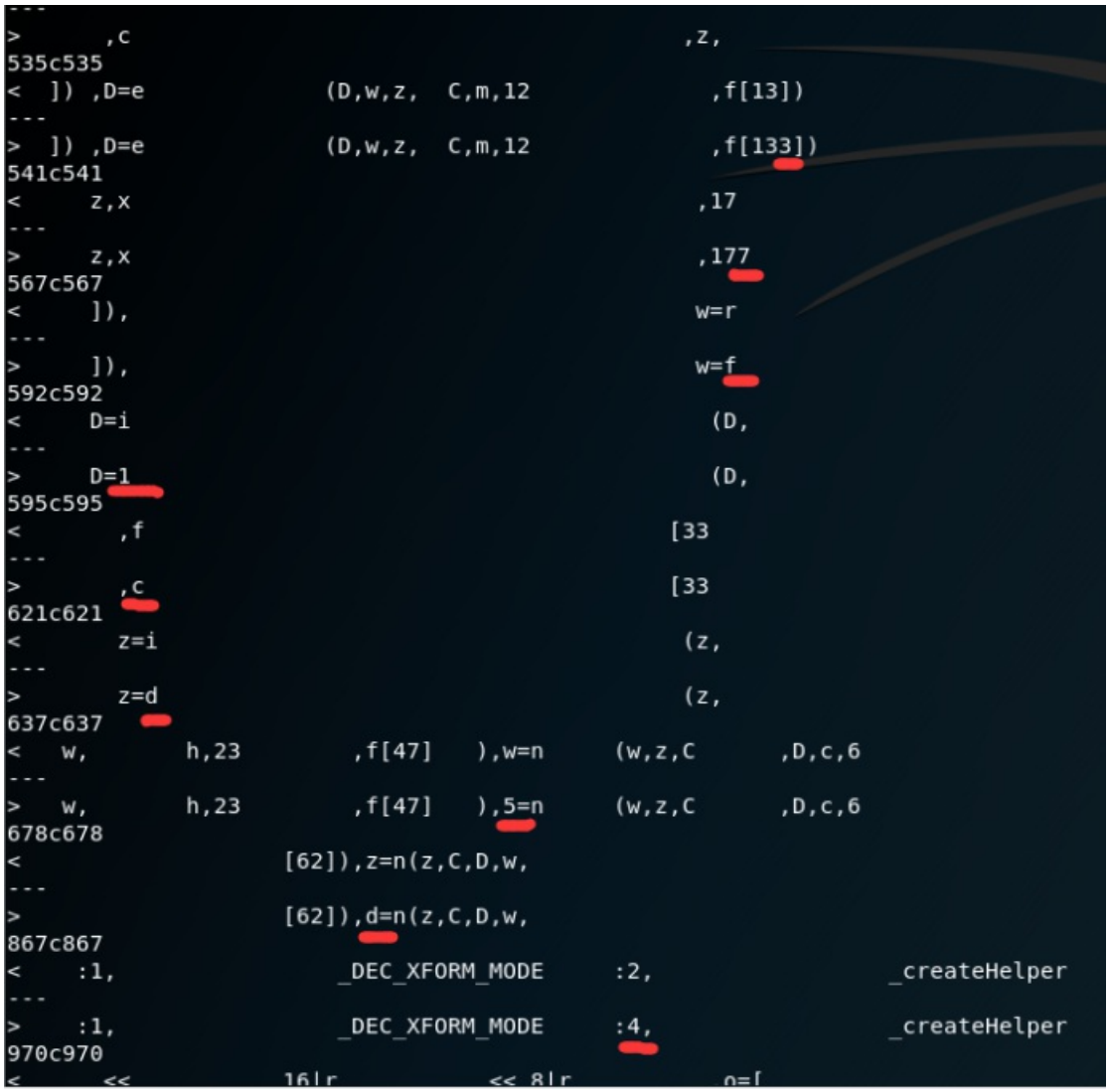
> ,s=o .algo ,e= [],
490c490
< ,g=t [o+

> ,g=t [f+
516c516
< ,w ,z,

> ,c ,z,
535c535
<]) ,D=e (D,w,z, C,m,12 ,f[13])

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=1 (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 o=[

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[_

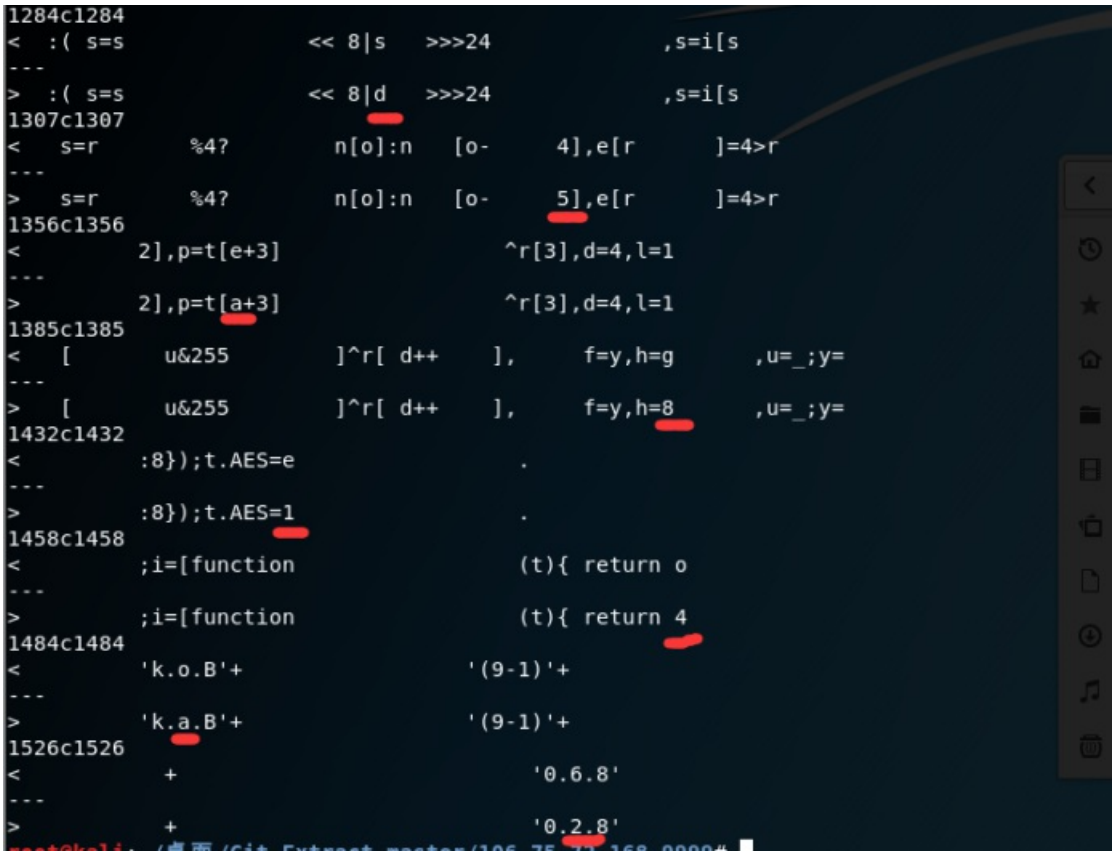
> [v],B=c [S], m=257 *d[_
1239c1239
< _]=m <<

> _]=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
最近使用
收藏
主目录
桌面
视频
图片
文档
下载
音乐
回收站

636ea7cadc



d5a814a2

发现flag

flag{82efc37f1cd5d4636ea7cadcd5a814a2}

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