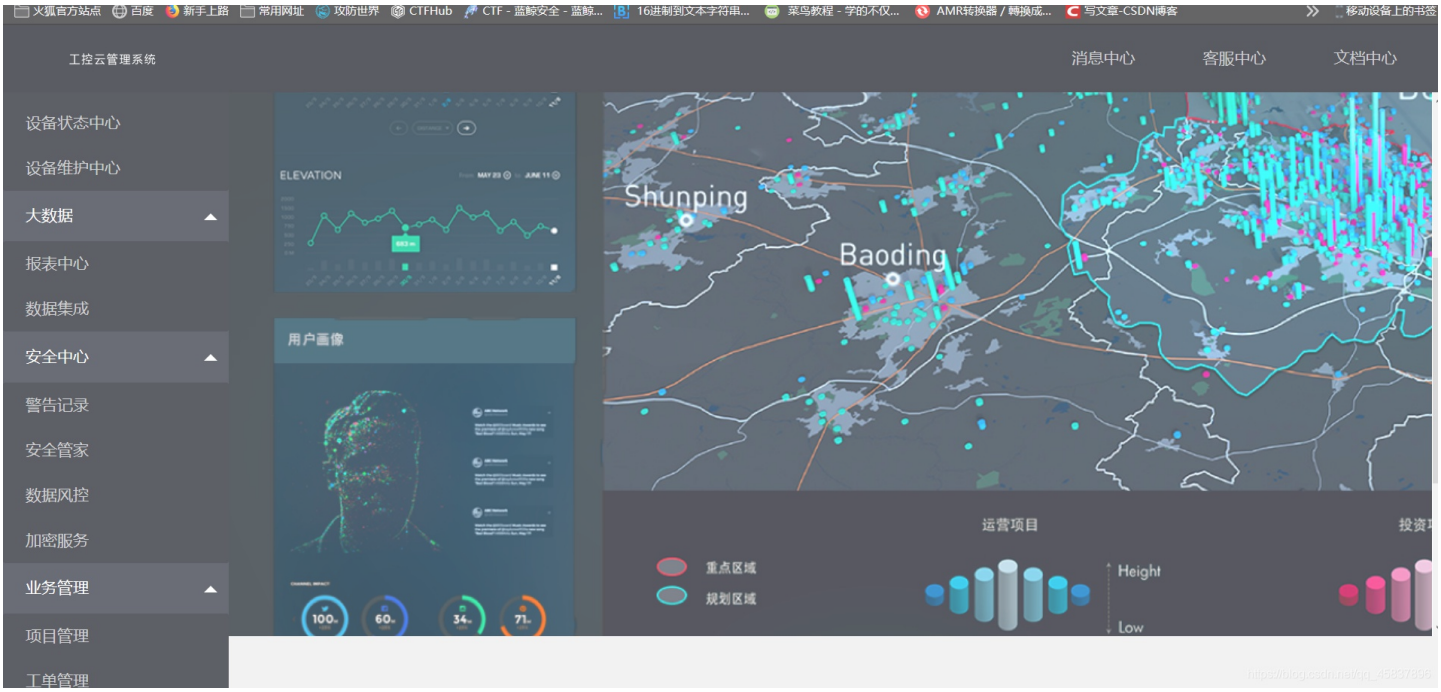
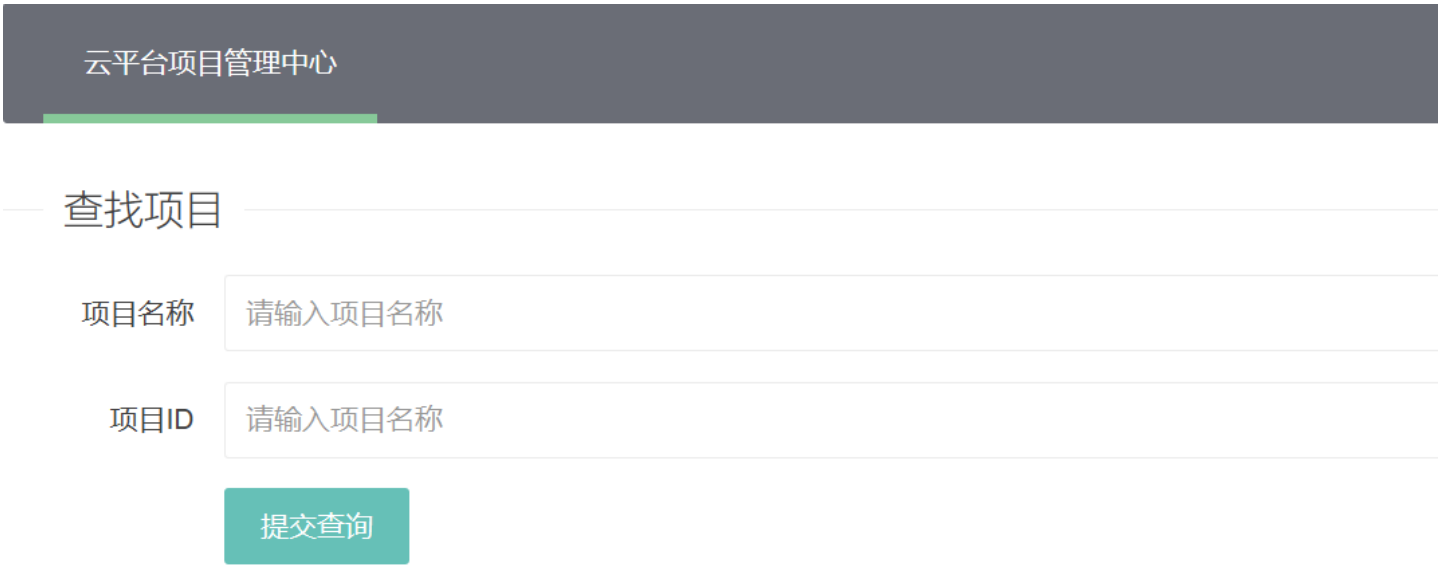
攻防世界web ics-07 writeup

原创

Sprint#51264 于 2020-07-18 18:44:55 发布 115 收藏



熟悉的界面，仍旧是点哪个哪个不能开的选项，只有项目管理能进入



那个view source是可以点的，不是让F12

开始代码审计

```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');
}

?>
```


page选其它页

面直接绕过...
第二段要求admin为true，所以先看第三段

```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;
    }
?>
```


要求传id值，其浮点数不能为1且该字符串最后一位为9.

于是使用1-9或者1/9（此处有疑惑）

进行传值有

view-source
id: 1
name:admin

admin为true，再次看源码

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


传file文件名，还有con（文件写入的数据）。

后面进行正则判断，题要从/.开始判断，要想绕过我们可以给文件起名为j.php/.

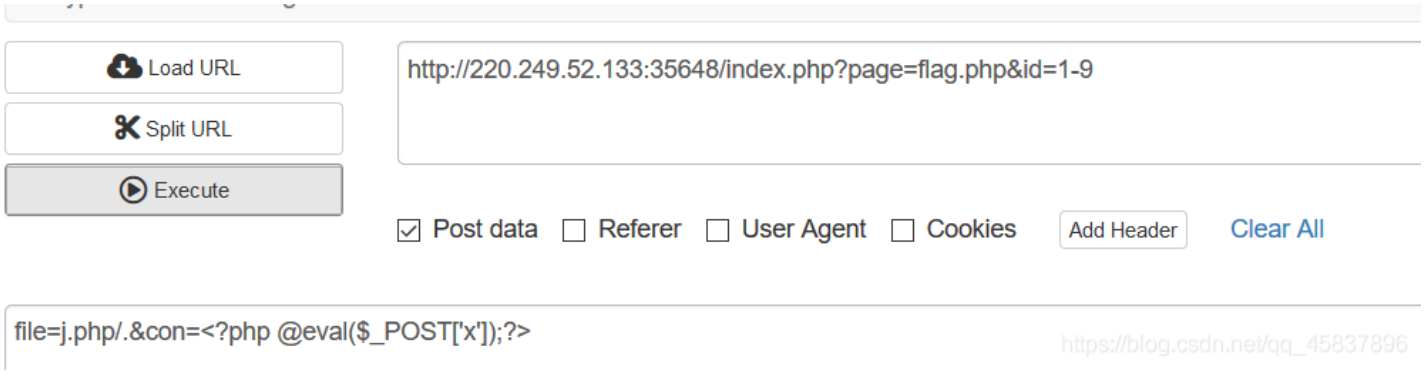
也就是说在文件名目录下加了个空目录，相当于没加，但是绕过了正则判断，这里还有一个chdir()函数

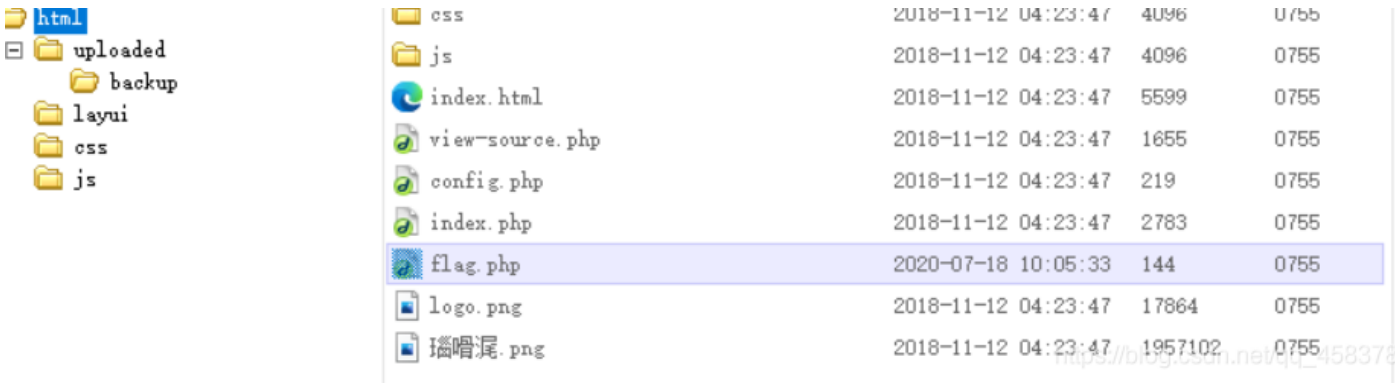
chdir(xxx) 函数改变当前的目录到所给值xxx

于是乎文件最后被存在了uploaded/backup/j.php

后面对文件写入con值

我们用hackbar工具进行POST传值，并在con中写php一句话准备用菜刀连接





找到flag.php并打开

```
<html>
<head>
  <meta charset="utf-8" />
</head>
<body>
  <?php
    $flag="cyberpeace{9419d2a17f31474c552edeedbf8404b3}";
   ?>
</body>
</html>
```

(我好无知，继续学习)