moctf-writeup

原创

^BonnenuIt 于 2019-09-26 23:10:51 发布 177 收藏
分类专栏： CTF

目录

我想要钱

```
<?php
   include "flag.php";
   highlight_file(__FILE__);

   if (isset($_GET['money'])) {
       $money=$_GET['money'];
       if(strlen($money)<=4&&$money>time()&&!is_array($money))
       {
           echo $flag;
           echo "<!--By:daoyuan-->";
       }
       else echo "Wrong Answer!";
   }
   else echo "Wrong Answer!";
?>

Wrong Answer!
```

if(strlen($money)<=4&&$money>time()&&!is_array($money))长度小于等于4，money大于当前时间戳

```php
<?php
echo time();
```

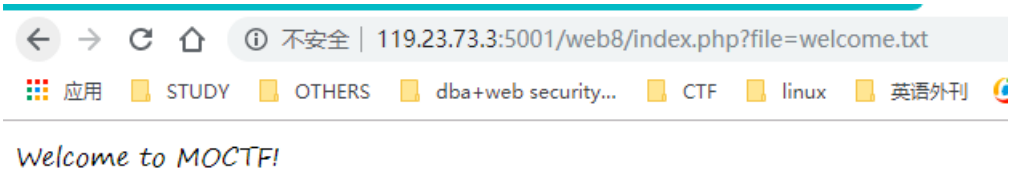
1569508657

尝试输出time(), 很大的数

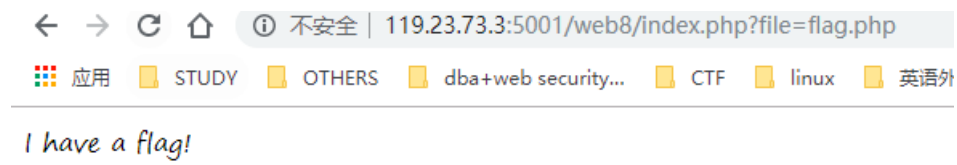
不能是数组，所以不能用数组大于任何数绕过

payload:用e绕过，科学记数法,9e10

文件包含



看到file=welcome.txt

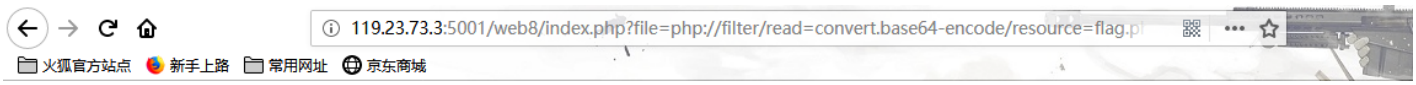


,

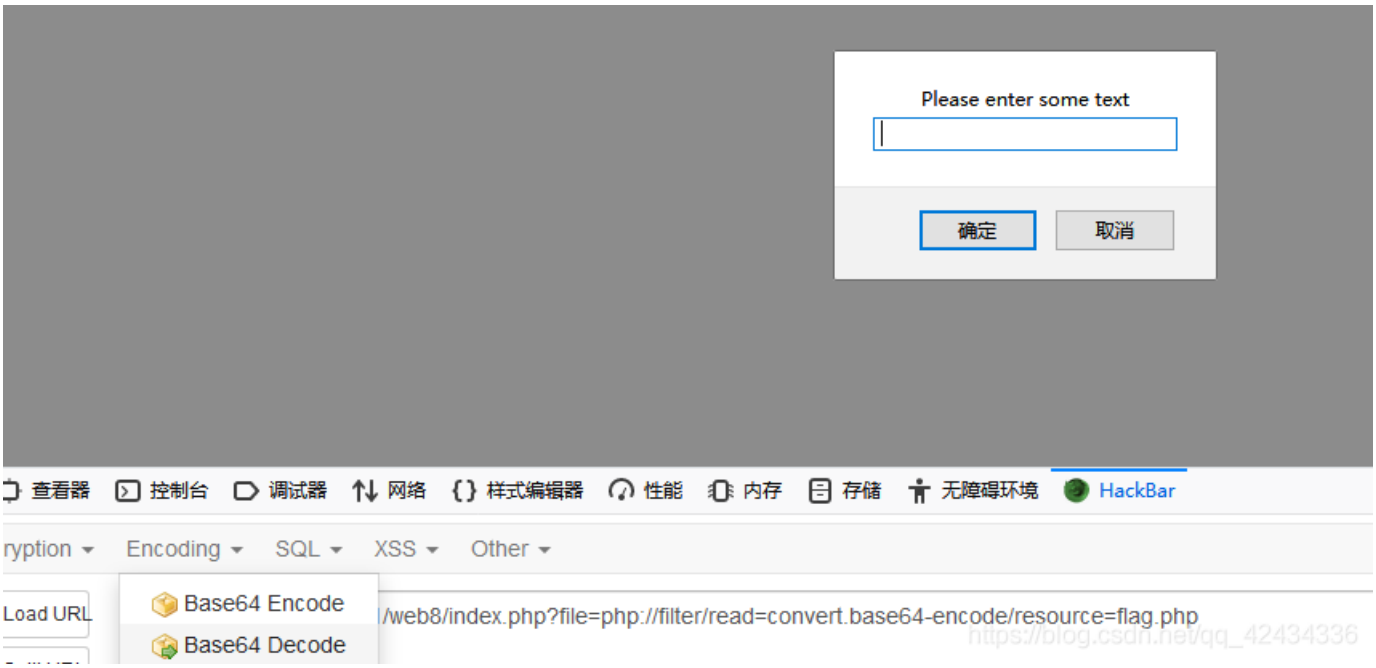
flag.php存在

题目提示文件包含，用php伪协议，首先尝试php://filter/resource=flag.php

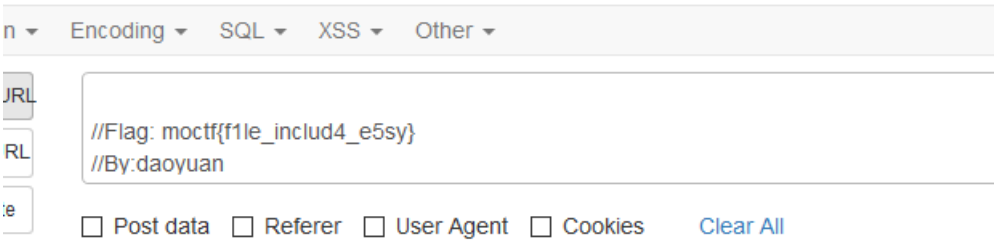
再尝试php://filter/read=convert.base64-encode/resource=flag.php



SSBoYXZlIGEgZmxhZyEKPD9waHAgCgovL0ZsYWc6IG1vY3Rme2YxbGVfaW5jbHVkNF9INXN5fQovL0J5OmRhb3I1YW4KCj8+Cg==



hackbar来decode一下



得到flag

Flag在哪？

有个follow redirection，重定向

一共重定向5次

```
flag.php
where_is_flag.php
I_have_a_flag.php
I_have_a_frog.php
no_flag.php
```

I have a pen,I have an apple. (Uhh~)Apple-pen! 歌词

结合得到flag

302重定向又称之为暂时性转移(Temporarily Moved)，英文名称：302 redirect。 也被认为是暂时重定向（temporary redirect），一条对网站浏览器的指令来显示浏览器被要求显示的不同的URL，当一个网页经历过短期的URL的变化时使用。一个暂时重定向是一种服务器端的重定向，能够被搜索引擎蜘蛛正确地处理。

php黑魔法

php源代码泄露

几种常见的格式：index.php.bak;index.php.swp;index.php~

```
<?php

   $flag="moctf{**************}";

   if (isset($_GET['a'])&&isset($_GET['b'])) {
      $a=$_GET['a'];
      $b=$_GET['b'];


      if($a==$b)
      {
         echo "<center>Wrong Answer!</center>";
      }
      else {
         if(md5($a)==md5($b))
         {
            echo "<center>".$flag."</center>";
            echo "By:daoyuan";
         }
         else echo "<center>Wrong Answer!</center>";
      }

   }
   else echo "<center>癞藉僭灏氈簡鑌逛粗涔</center>";
?>
```

考察的是弱类型，md5无法加密数组，都返回false，因此构造?a=[]=1&b[]=2，得到flag

QNKCDZO————————————s878926199a

登录就对了

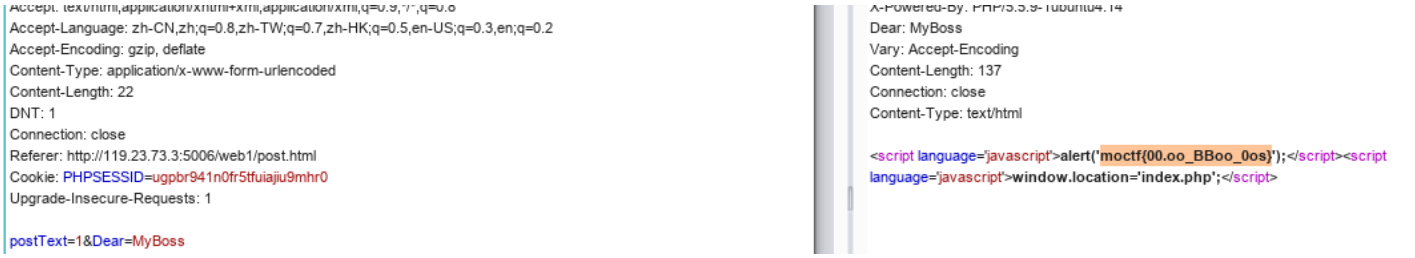
页面标题是SQLi LOGIN

万能密码 构造用户名:`' or '1'='1'#`，密码随意，成功登录

暴跳老板

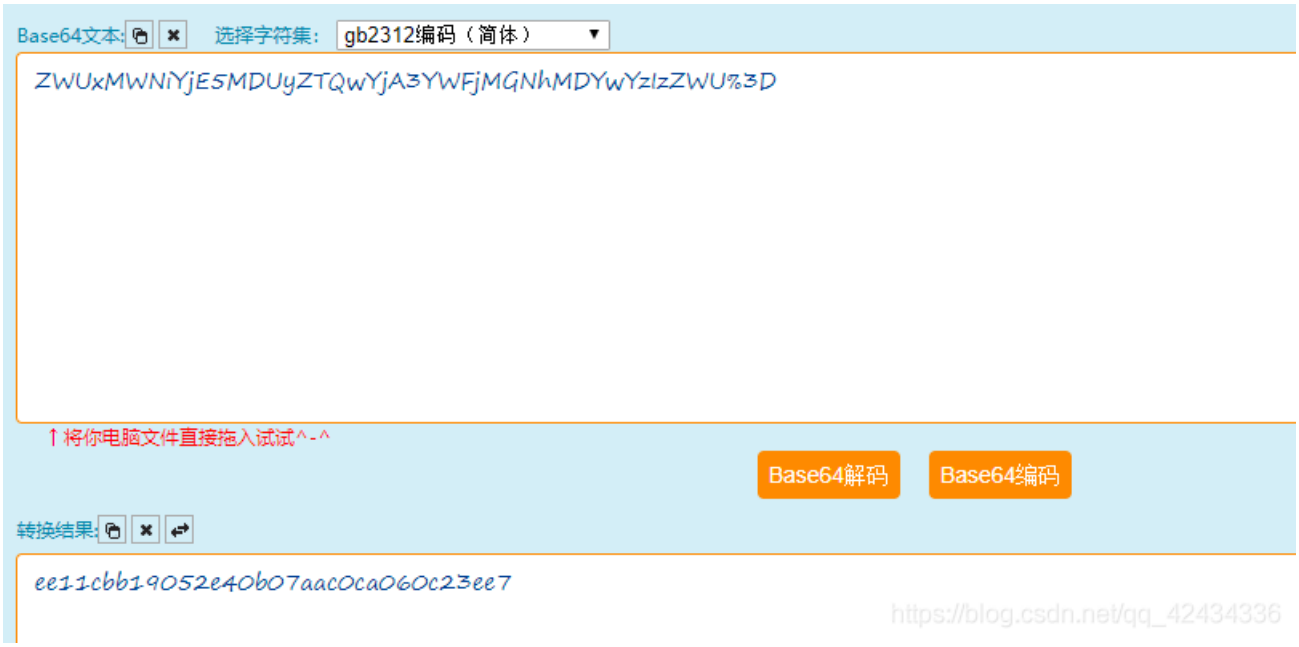
发邮件的时候抓个包，然后发送出去看看返回了什么

发现返回包中有一条`Dear： MyBoss` 构造url:postText=1&Dear=MyBoss



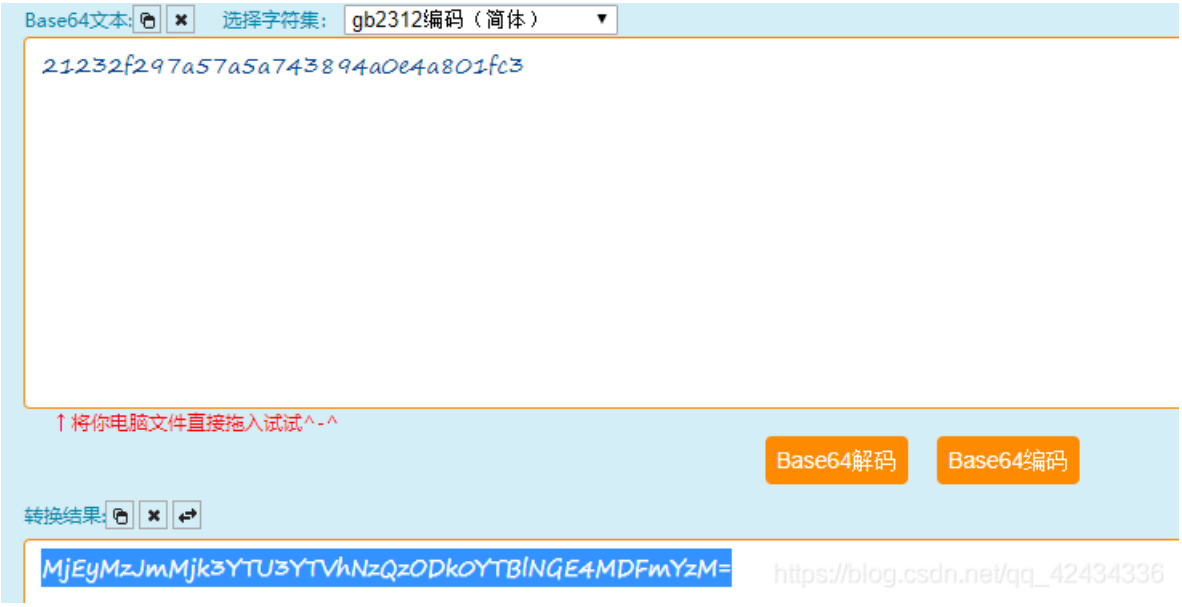
美味的饼干

饼干指cookie,解密cookie，先用base64解密http://web.chacuo.net/charsetbase64

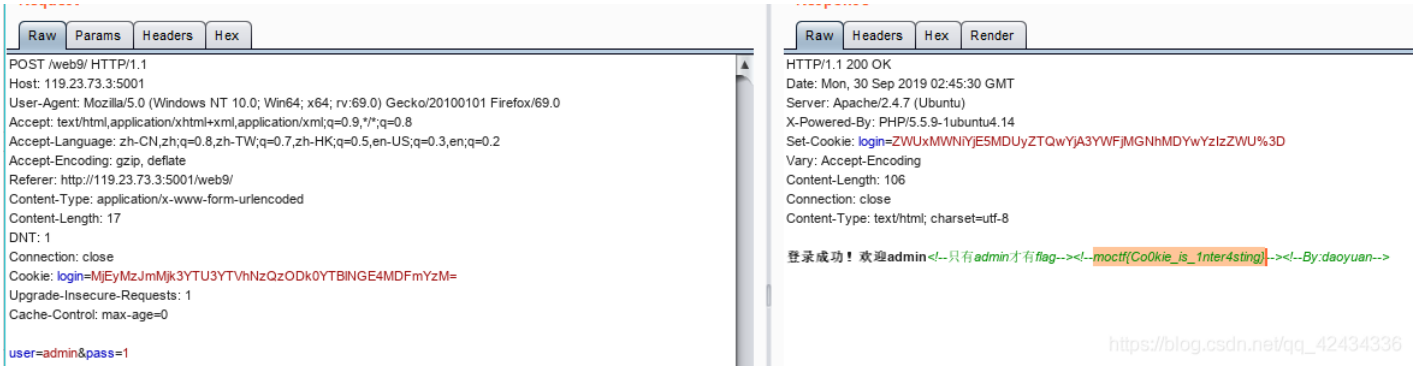


然后用md5解密https://www.somd5.com/

解出的是user，但注释提示用admin登陆，所以反过来对admin加密得出cookie登陆

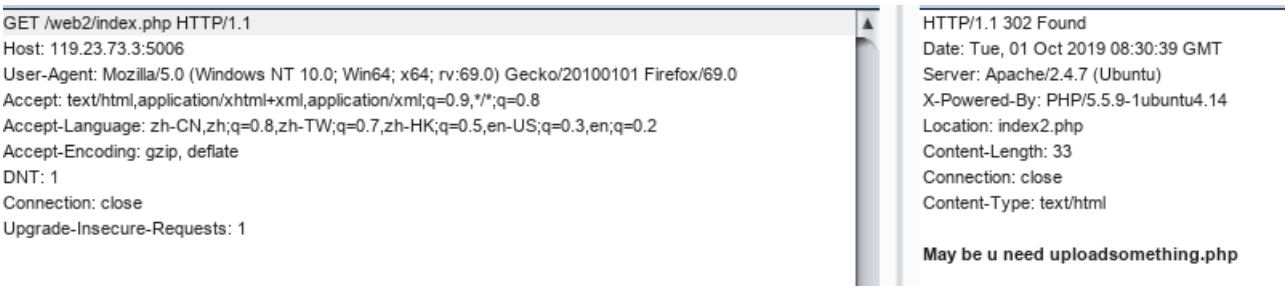


抓取登陆之后的网站才有cookie

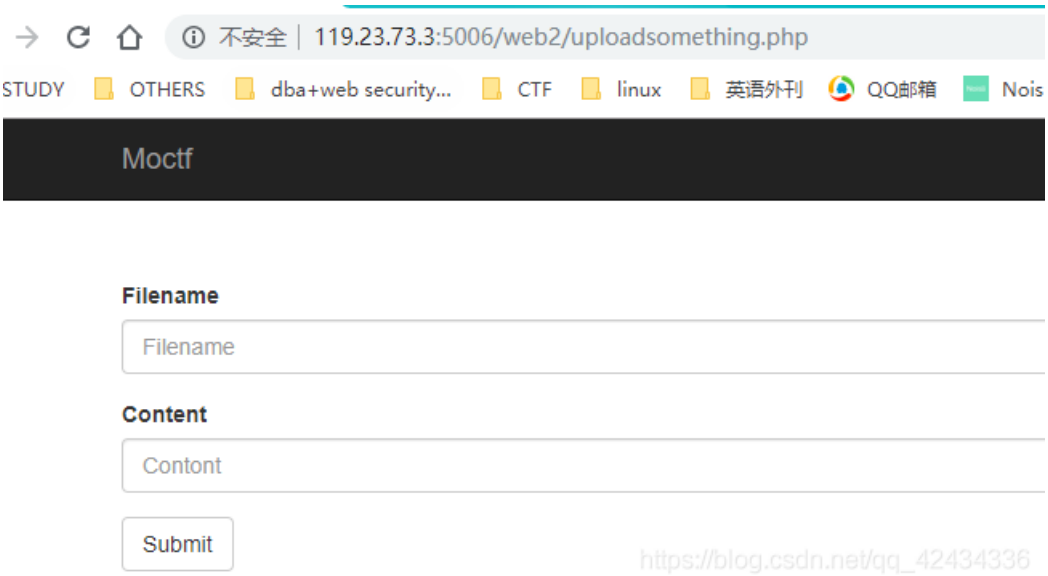


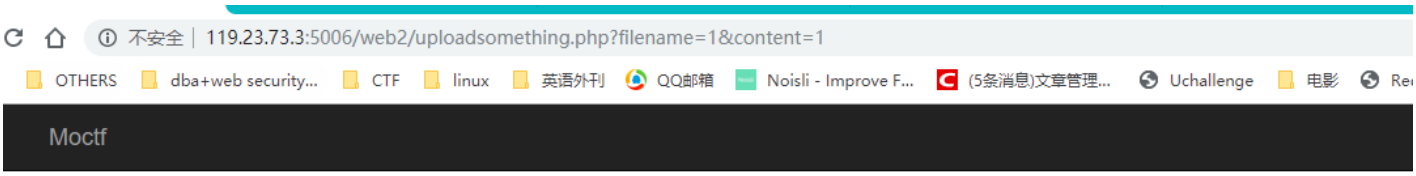
没时间解释了

题目访问的是index2.php,改成index.php访问，必须用burp抓包，否则跳回Index2.php界面

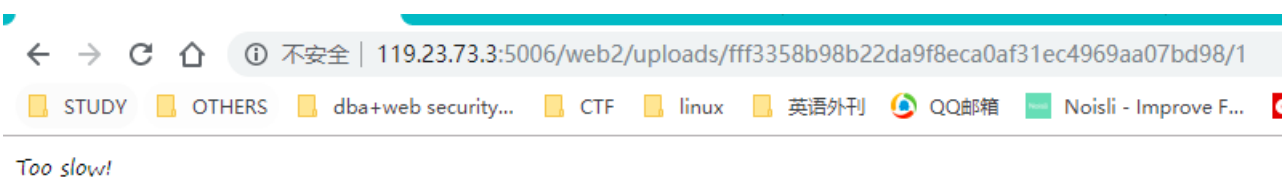


访问uploadsomething.php





Flag is here,come on~ http://119.23.73.3:5006/web2/uploads/fff3358b98b22da9f8eca0af31ec4969aa07bd98/1



条件竞争

条件竞争漏洞是一种服务器端的漏洞，由于服务器端在处理不同用户的请求时是并发进行的，因此，如果并发处理不当或相关操作逻辑顺序设计的不合理时，将会导致此类问题的发生。

https://blog.csdn.net/u011377996/article/details/79511160

http://wiki.secbug.net/web_race-condtion.html

先抓取输入filename和content的下一个页面，即

Flag is here,come on~ http://119.23.73.3:5006/web2/uploads/fff3358b98b22da9f8eca0af31ec4969aa07bd98/1

然后再打开flag网页，因为burp在抓取中，所以都是在加载中，这时候intercept off就出现了flag