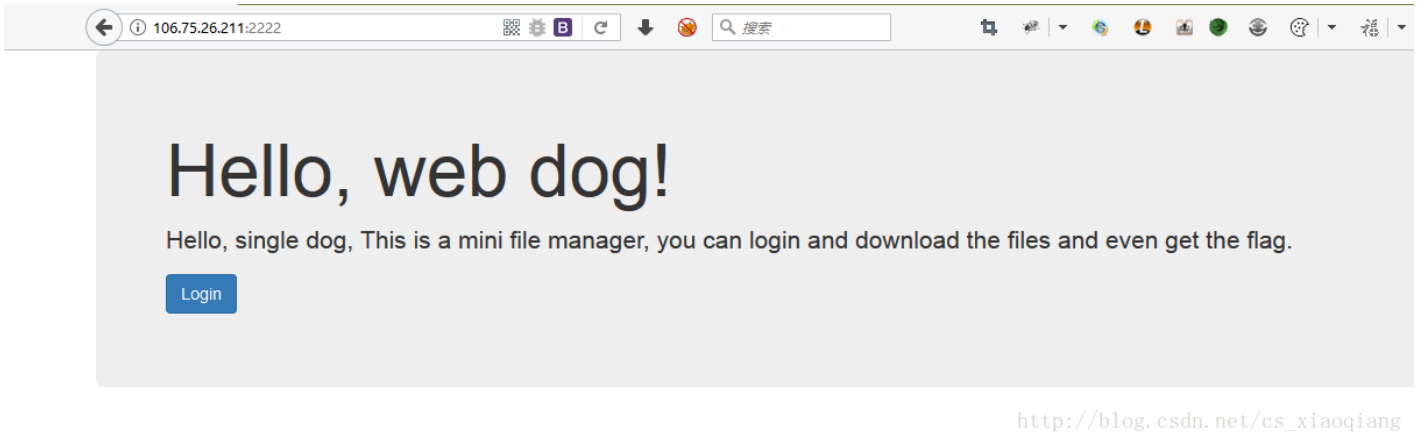
ctf GetFlag

原创

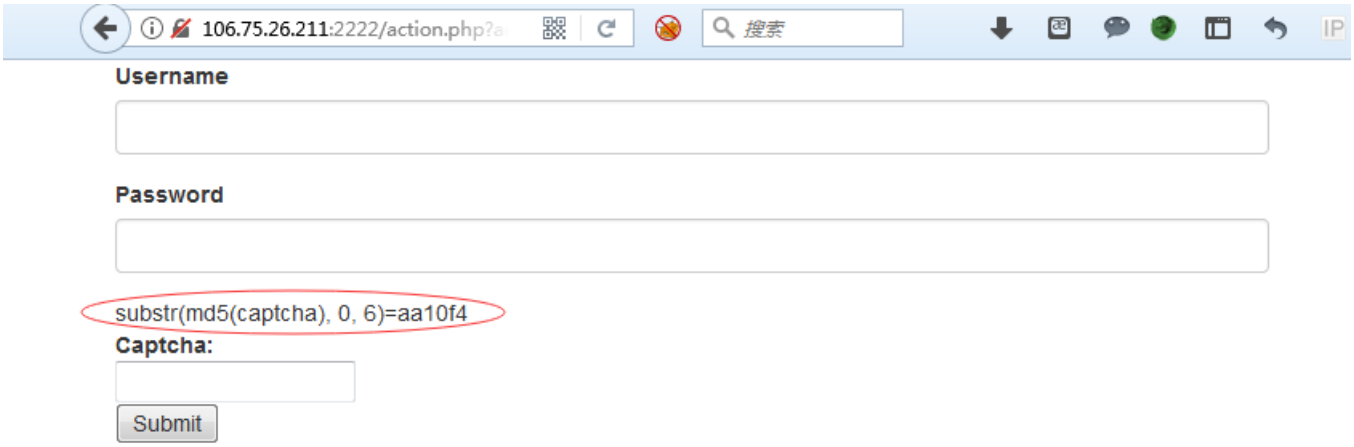
cs_xiaoqiang 于 2018-01-18 18:29:57 发布 4672 收藏 3
分类专栏： 安全 ctf 文章标签： ctf

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



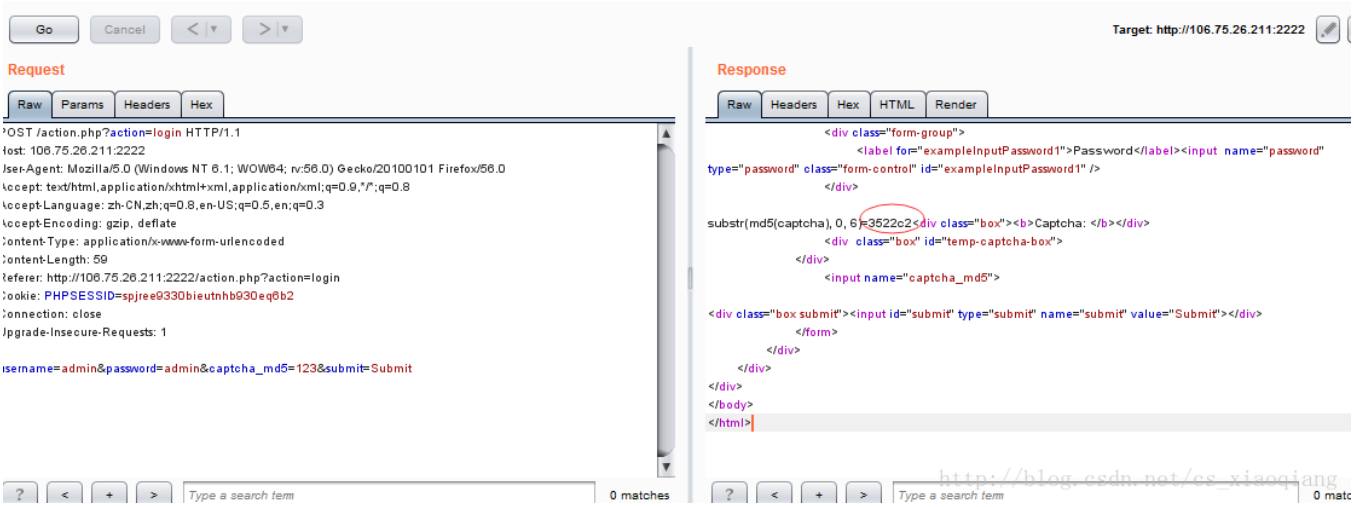
先查看源码，没有任何发现。但是在页面上发现一个登陆窗口，跳转到登陆窗口。



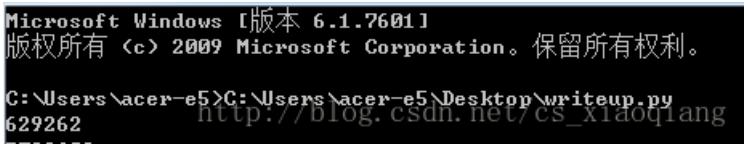
并且发现验证码是纯数字的md5的值取最前面的6位，那么可以自己写一个脚本来跑

```
import hashlib

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

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

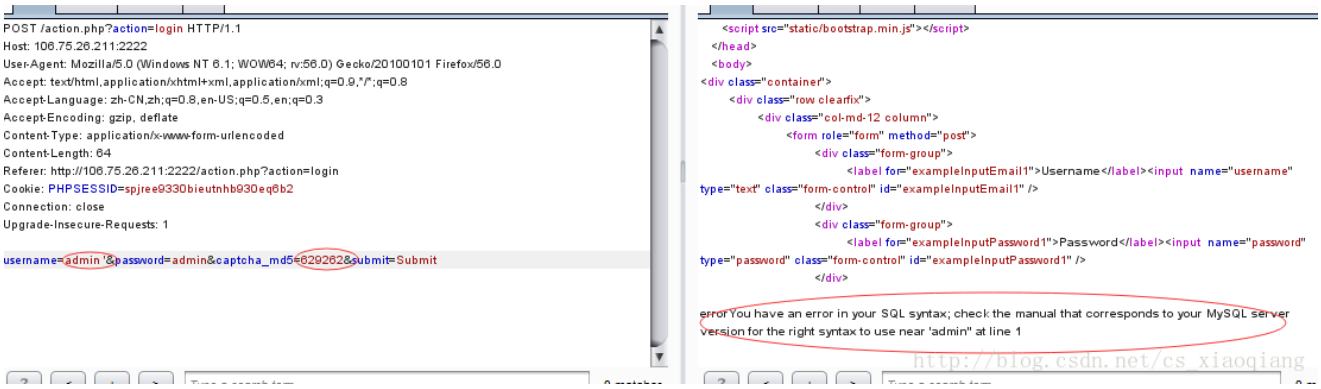

有了验证码之后，本来是准备尝试爆破的。可是发现每访问一次验证码都会改变，所以这条路明显行不通。经过多次的尝试之后发现登陆窗口存在注入，直接使用万能密码登陆。



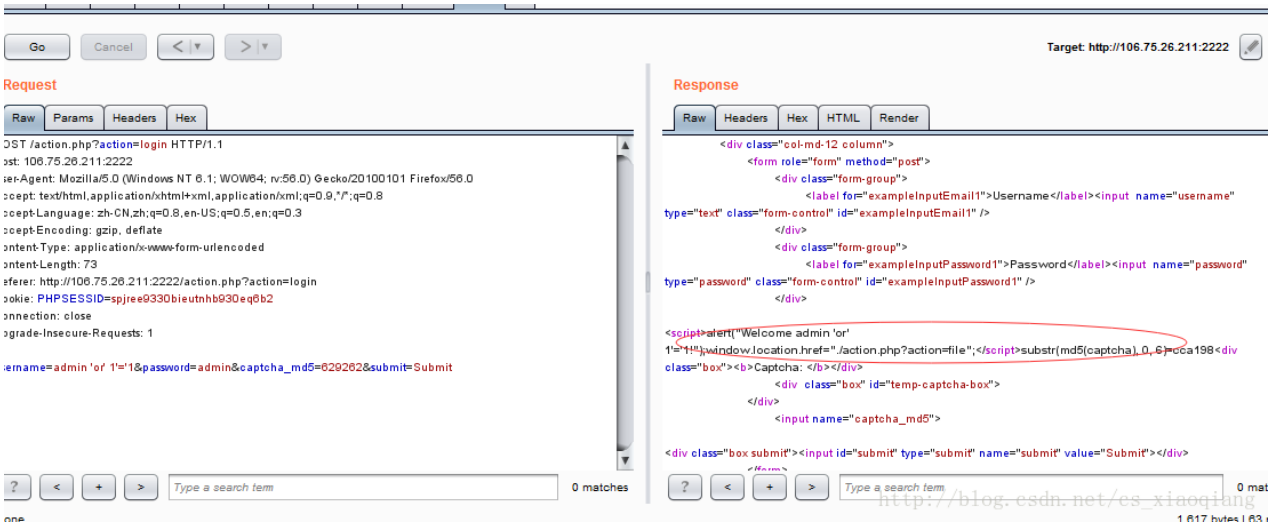
抓包，将验证码写入到刚刚写的脚本中，运行。



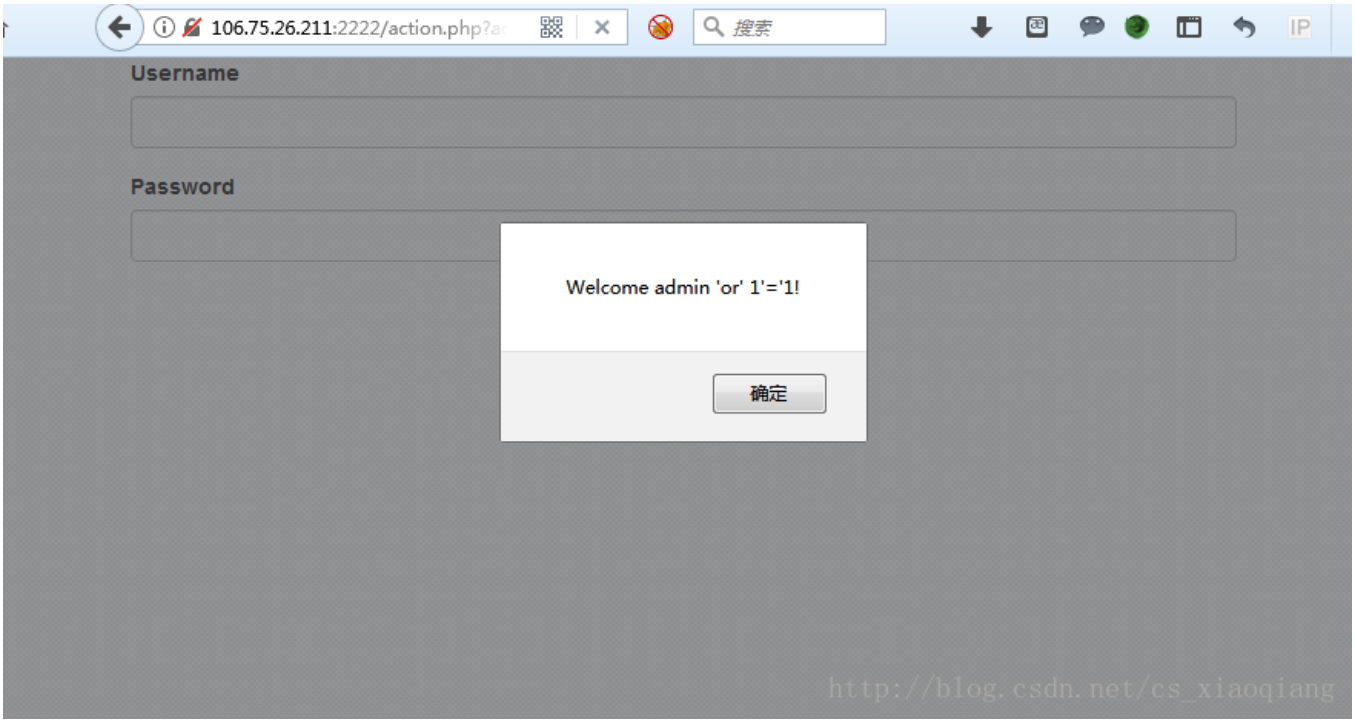
修改数据包里面的验证码，在admin的后面加上一个单引号（admin '），可以看到报错信息。证明的却存在注入。



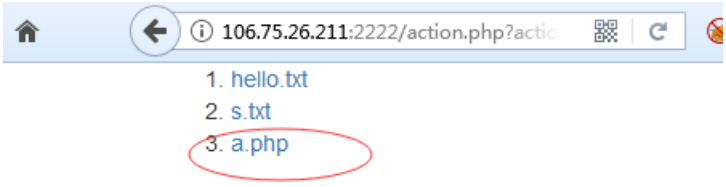
输入万能密码进行登录。（注意：进行登录要重新获取验证码。继续用脚本来获取新的验证码）



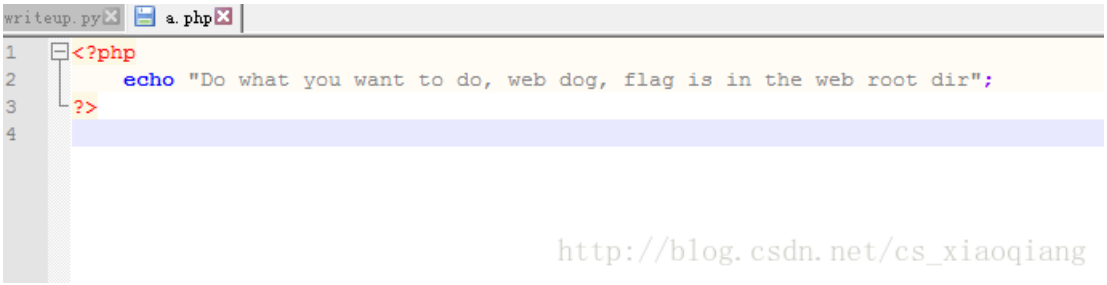
看到登陆成功，返回页面进行登录



发现有几个可下载的文件



全部下载下来之后，只有a.php里面有提示信息



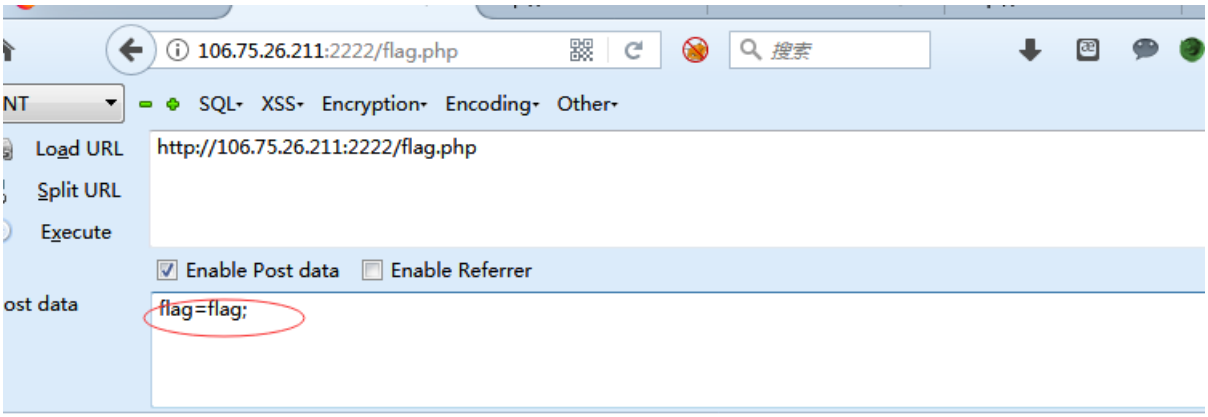
根据提示，可以知道flag在网站根目录下。直接推回到根目录，确实发现有一个flag的目录，但是什么东西也没有。查找无果之后，继续返回登录之后的页面。抓包看一下有什么发现。果然发现了一下载点的完整路径。

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）。

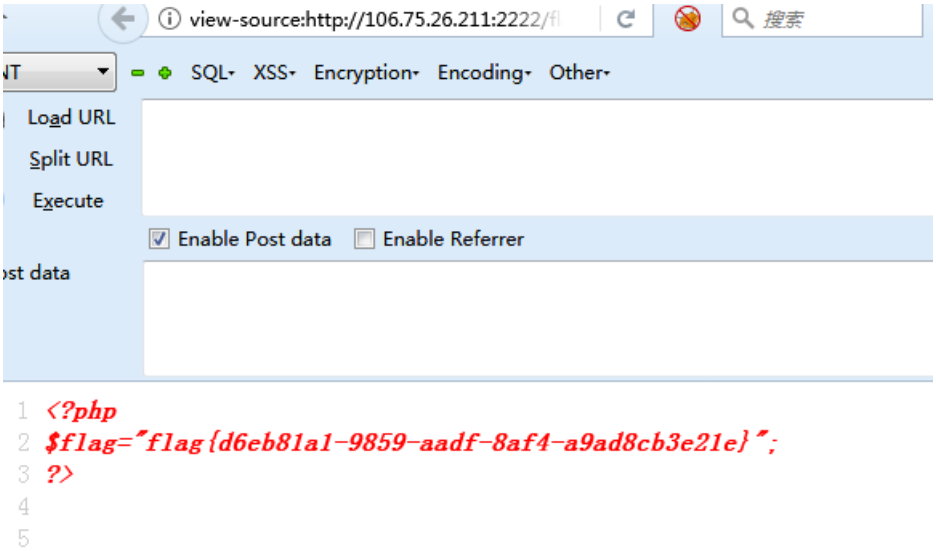
打开之后，查看源码。

```php
<?php
$f = $_POST['flag'];
$f = str_replace(array('`', '$', '*', '#', ':', '\\', '"', "'", '(', ')', '.', '>'), '', $f);
if((strlen($f) > 13) || (false !== stripos($f, 'return')))
{
    die('wowwwwwwwwwwwwwwwwwwwwwwwww');
}
try
{
    eval("\$spaceone = $f");
}
catch (Exception $e)
{
    return false;
}
if ($spaceone === 'flag'){
    echo file_get_contents("helloctf.php");
}

?>
```


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）



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




```
<?php
$flag="flag{d6eb81a1-9859-aadf-8af4-a9ad8cb3e21e}";
?>
```


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。