[Root-me]HTTP - Open redirect Writeup

原创

Vicl1fe 于 2019-12-29 10:18:58 发布 850 收藏

分类专栏： Rootme

本文链接：https://blog.csdn.net/qq_41918771/article/details/103751046

个人博客地址

```
http://www.darkerbox.com
```

欢迎大家学习交流

Root-me网址：

```
https://www.root-me.org/en/Challenges/Web-Server/HTTP-Open-redirect
```

知识点

- url重定向

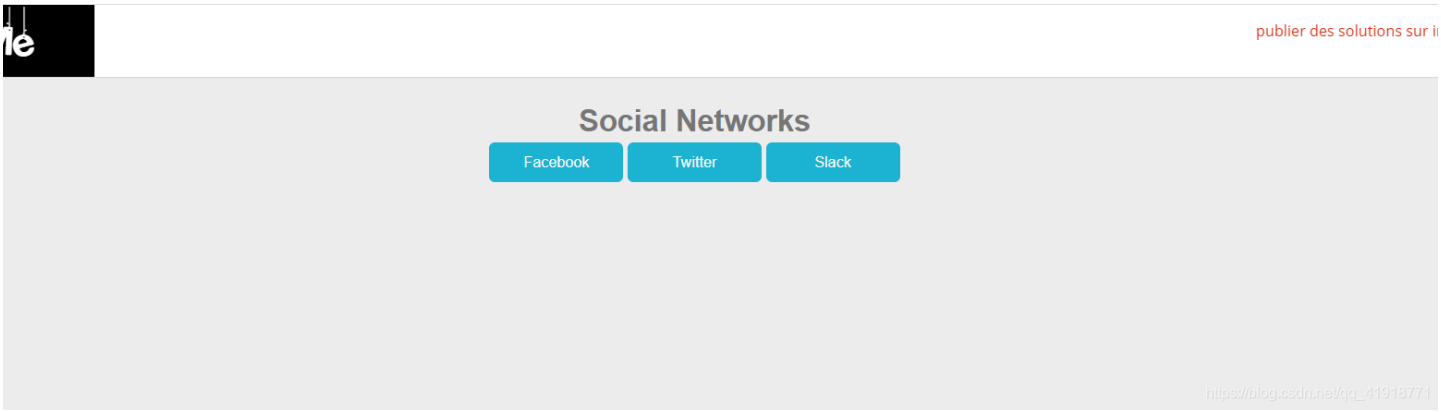
前言

自己以前做过一些，但没写wp。只能写一些还没做过的wp了

这个题考察的url重定向

漏洞利用

页面是这样的。

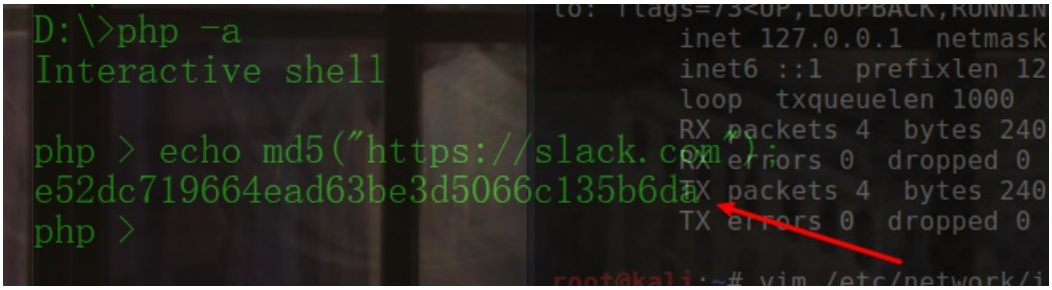


查看源码发现

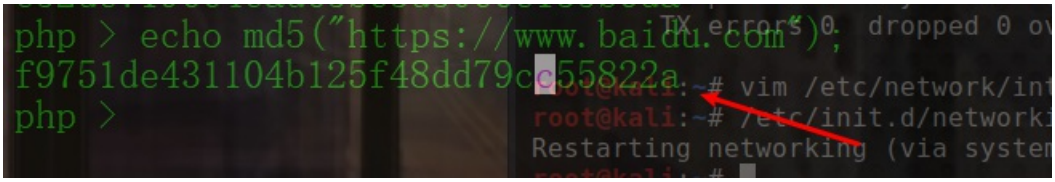
```
7
8  <body><link rel='stylesheet' property='stylesheet' id='s' type='text/css' href='/template/s.css' media='all' /
9          <h1>Social Networks</h1>
10 <a href='?url=https://facebook.com&h=a023cfbf5f1c39bdf8407f28b60cd134'>facebook</a>
11 <a href='?url=https://twitter.com&h=be8b09f7f1f66235a9c91986952483f0'>twitter</a>
12 <a href='?url=https://slack.com&h=e52dc719664ead63be3d5066c135b6da'>slack</a>
13 <style type="text/css">
14         body{
15                 text-align: center;
```

也不需要多解释，跟着url参数表明跳转到这个url。但是后面的这个h就不知道是干嘛的了，像是个md5加密后的值，会不会是前面url加密后的呢？实验一下。
我直接用php加密了，比较方便。
我在命令行直接输入php -a(需要提前设置环境变量)。进入php交互模式。好像只有php7才有。

和mysql一样，只有最后是分号才表示一行代码的结尾。看见`https://slack.com`加密后的值是`e52dc719664ead63be3d5066c135b6da`和后面`h`参数的值是相同的



说明就是md5加密后的。
我使用`https://www.baidu.com`



我们自己构造payload

```
url=https://www.baidu.com&h=f9751de431104b125f48dd79cc55822a
```

当你提交的时候，会将flag显示出来，但很快就跳转到www.baidu.com了

手速有点慢...

只能打开我们的神器了：`burpsuite`

bp抓包发送就可得到flag了。我这因为某些原因就不截图了。

欢迎大家一起学习交流，共同进步，欢迎加入信息安全小白群