Write up

----wuerror

Web

(1)谁吃了我的flag

根据hint，推测是未正常关闭的vim备份文件泄露

访问:http://118.25.111.31:10086/.index.html.swp

下载该文件，使用vim -r .index.html.swp恢复

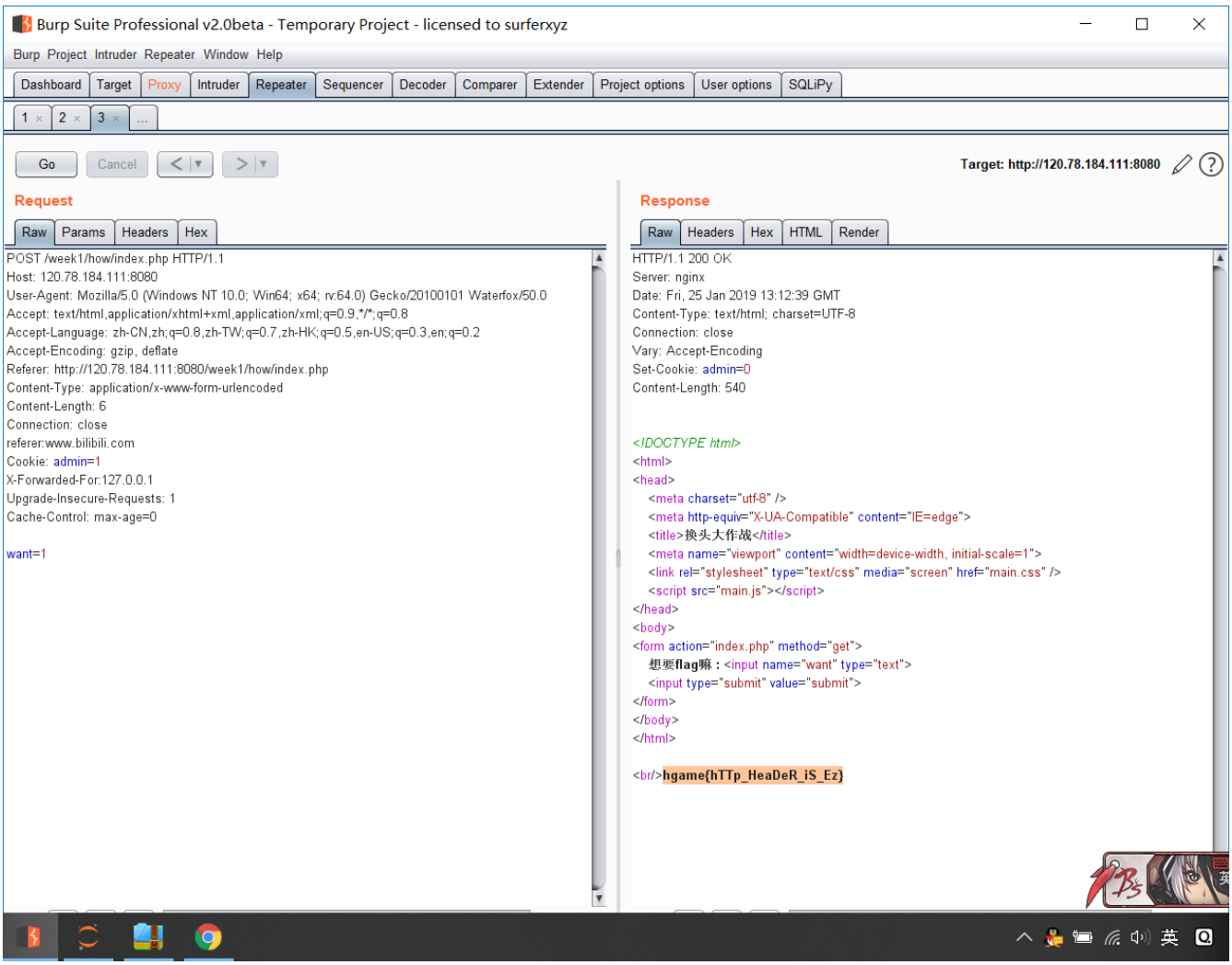
得到flag

(2)换头大作战

随便输入一个值，回显：request method is error.I think POST is better

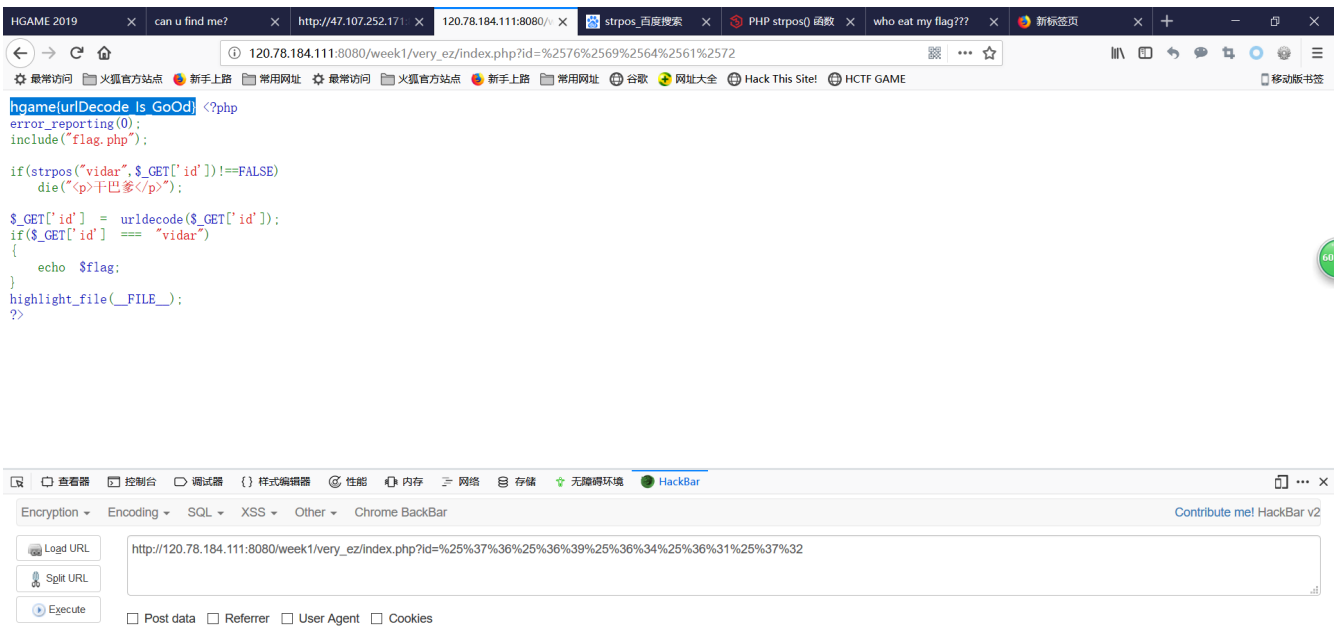
打开burpsuite使用post方法，在reapeater中在来一次，回显提示要local host

在头部加入X-Forwarded-for:127.0.0.1字段，接下来根据提示改头部就行



(3)very easy web

这代码审计就很简单了，用get方式传参id=vidar，当然vidar要两次URLencode



(4)can u find me

F12查看页面源代码，发现一个f12.php.点开。要求postpassword给它

打开burpsuite抓包，随便post一个password值,在response包头发现password: woyaoflag

Ok，post这个值再来一次。没记错的话，成功之后，还会有一个显示你太慢了的页面。在返回包列表里找一下，另一个包有flag。

Re

(1)hellore

IDA打开，一行注释就是flag

Misc

(1)hidden image in lsb

Stegsolve打开图片，调rgb就能找到

(2)brokenchest

这是一个损坏的zip文件，用winhex打开，修改文件头为正常zip文件的头部50 4B 03 04

保存，打开zip文件。提示需要密码，在右边框里就能看见密码。打开flag.txt获取flag.