

Week • 1 Writeup

——一名一无所知的同学的做题过程

第一周，只做出两道题。我很.....

WEB

1. 谁吃了我的 flag。

题目：`http://118.25.111.31:10086/index.html`

做题过程：

刚开始一无所知，后来题目中有了提示“vim”，“忘记保存直接关机”，便百度了“vim文件恢复”问题，自己试验了一下：

(1) `.vim hello.html`

(2) 编辑一段，：`sav hello.html` 再输入一些内容，关机。

(3) 打开，运行 `vim hello.html`，失败，告诉我这个 `.hello.html.swp` 存在。于是照搬代码 `vim -r hello.html`，成功复原。

Woo，这么神奇？

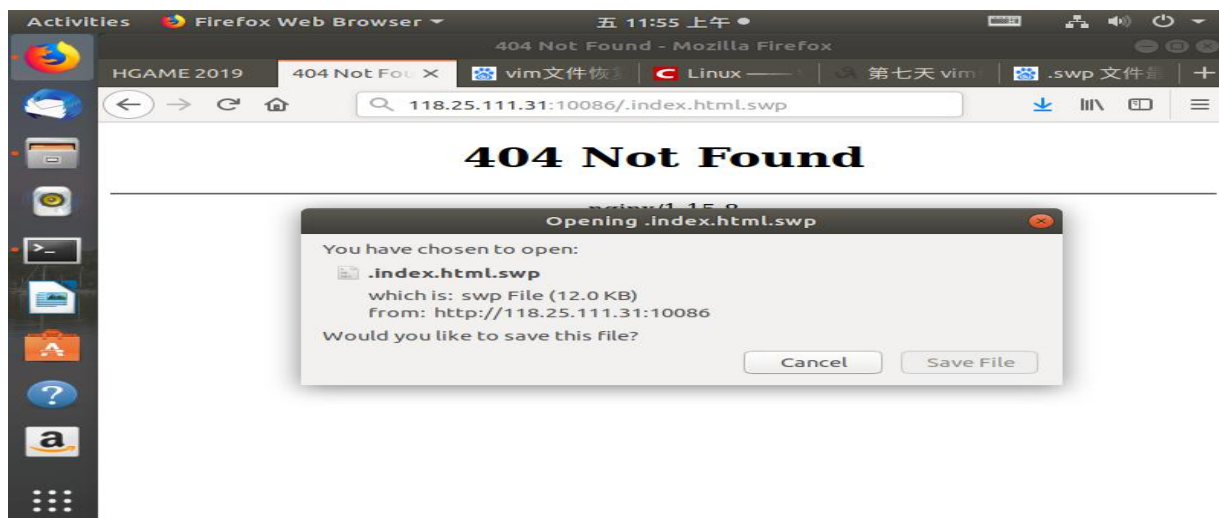
但是题目中并没有附带什么文件。大胆猜测，在题目网页所在的

上一级文件夹中，有%80 记几率存在 `.swp` 文件

(刚看 HTML 时，书上介绍服务器，了解到网页都是从服务器上请求的 HTML 文件，在浏览器展示，并且服务器上的文件所存位置就是域名后面的 `XXX\XXX\XXX\`)

所以，更改，访问：

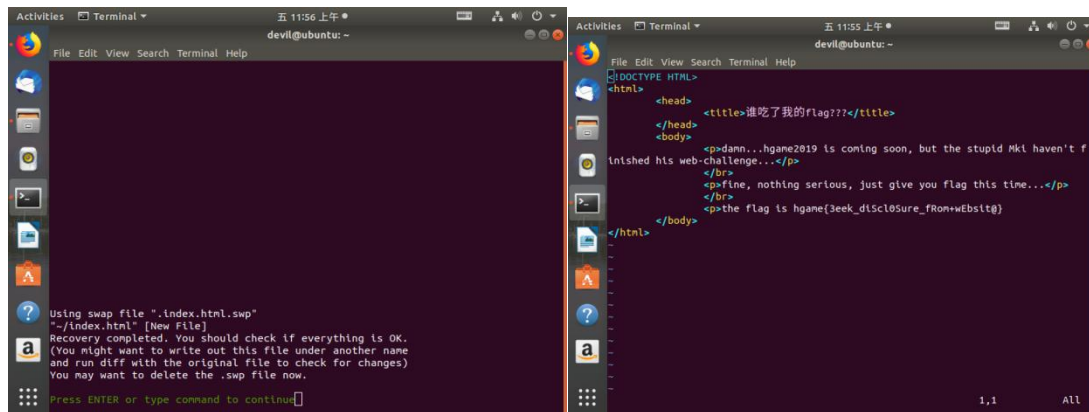
`http://118.25.111.31:10086/.index.html.swp`



果然有文件 `index.html.swp` 下载（特激动）。

下载，拖到 `home` 文件夹，在原来文件名前面加“.”发现这个文件竟然隐藏了。

运行 `vim -r index.html`



看到 flag

`ctrl C` `Ctrl V`.

2 代码审计：

题目：

解题过程：120.78.184.111:8080/week1/very_ez/index.php

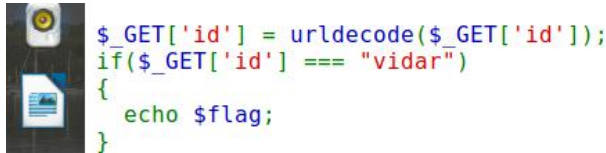
参考了类似题型与解答，得知只要在原网址后面加“?Id=xxxxx”，提交即可。
(后来知道这叫“GET”)

看代码，先得到字符串 id，运行 strpos() 函数且结果为 FALSE 才可以继续程序；百度函数 strpos(a, b)，作用是输出 a 在 b 中首次出现的位置，那么字符串 id 一定不能有“vidar”。



```
if(strpos("vidar", $_GET['id'])!==FALSE)
    die("<p>干巴爹</p>");
```

下一个条件，Urldecode 得到 id==vidar，再次百度 URL 解码规则：字母数字不变，符号等“%转义十六进制”；

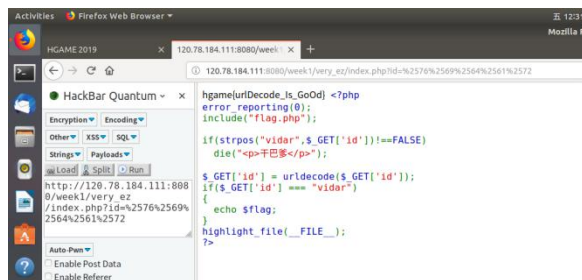


```
$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] === "vidar")
{
    echo $flag;
}
```

于是尝试为“vidar”的每一个字符‘%’加 ASCII 码
得到 %76%69%64%61%72，访问，结果出现“<干爹巴>”，也就是输入后就有 vidar 了，明白了程序直接当做“vidar”处理。

想到再次转义，找 URL 转码网站，转后得到%2576%2569%2564%2561%2572

，访问，OK。



仅此两题。

ID : i know nothing.