实验环境：

被攻击系统：08\_r2\_dat\_zh-chs + phpstudy2018 + cmsms-2.2.9 + xdebug + vscode

攻击系统：kali2019\_x64\_en-us

cmsms官网地址：<https://www.cmsmadesimple.org/>

cmsms下载地址如下：http://s3.amazonaws.com/cmsms/downloads/14311/cmsms-2.2.9-install.expanded.zip，我这里选择的是扩展版本

被攻击系统环境搭建：

0：先安装phpstudy2018，一路下一步即可，安装目录为c:\phpStudy\，启动phpstudy

1：将 cmsms-2.2.9-install.expanded.zip解压后的目录移动到c:\phpStudy\PHPTutorial\WWW\下

2：浏览器访问http://127.0.0.1/cmsms-2.2.9-install.expanded/，依照提示操作，其中Destination Directory需要使用一个空的目录，我这里新建了一个目录，名为cmsms2.2.9，在数据库配置中

Database Hostname: localhost

Database Name: cmsms229（需要到数据库中创建，命令为create database cmsms229;）

User name: root

Password: root（这里没有密码不可以，更改root密码，命令为update mysql.user set password=password(‘root’) where user=’root’ and host=’localhost’;）

攻击系统环境准备：

0：更新kali系统，命令如下：

apt-get update && apt-get upgrade

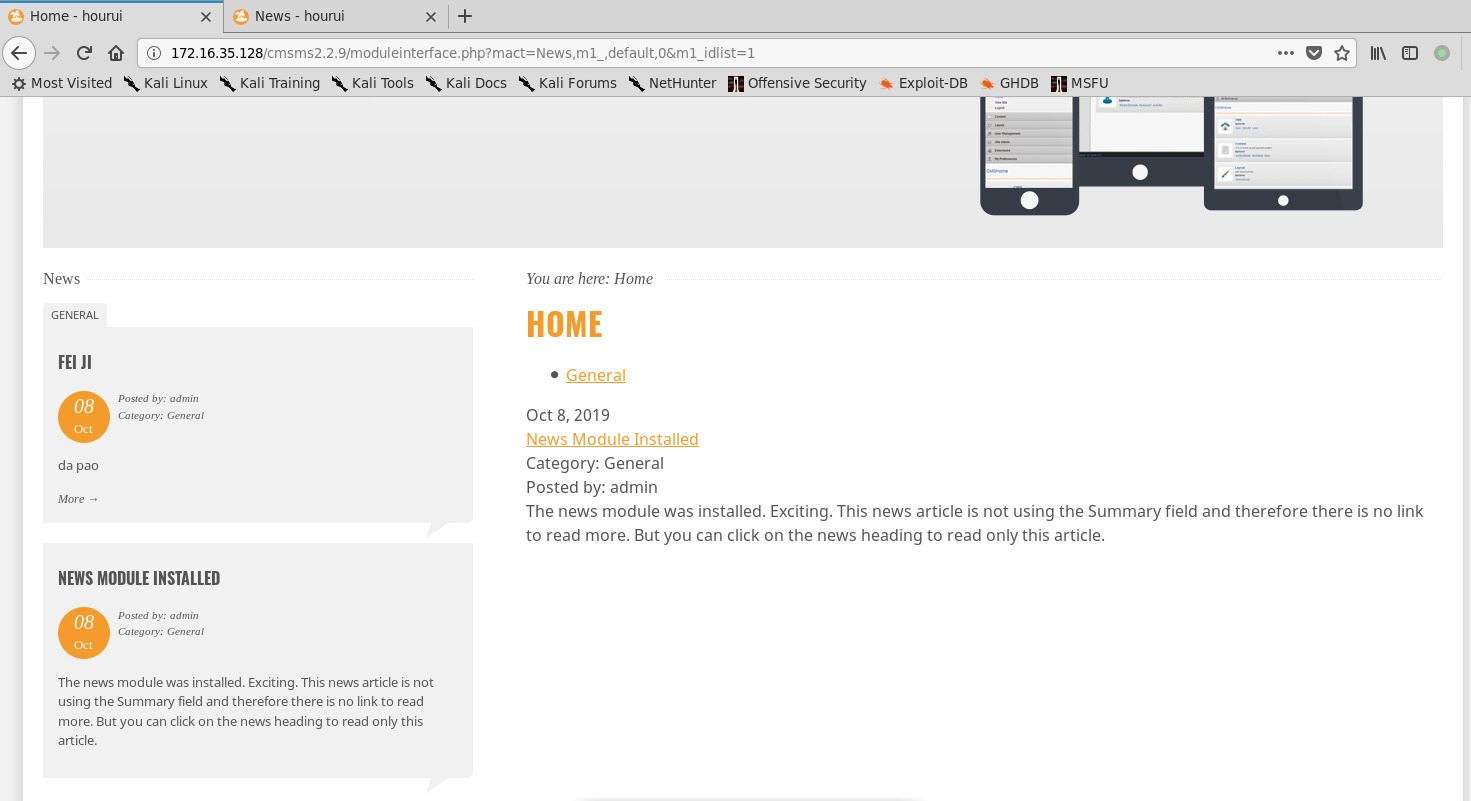
1：浏览器访问http://172.16.35.128/cmsms2.2.9/index.php，看到网站能正常访问

2：浏览器访问http://172.16.35.128/cmsms2.2.9/admin/，输入刚才创建的用户，登录后台，在content-news中，添加一条记录

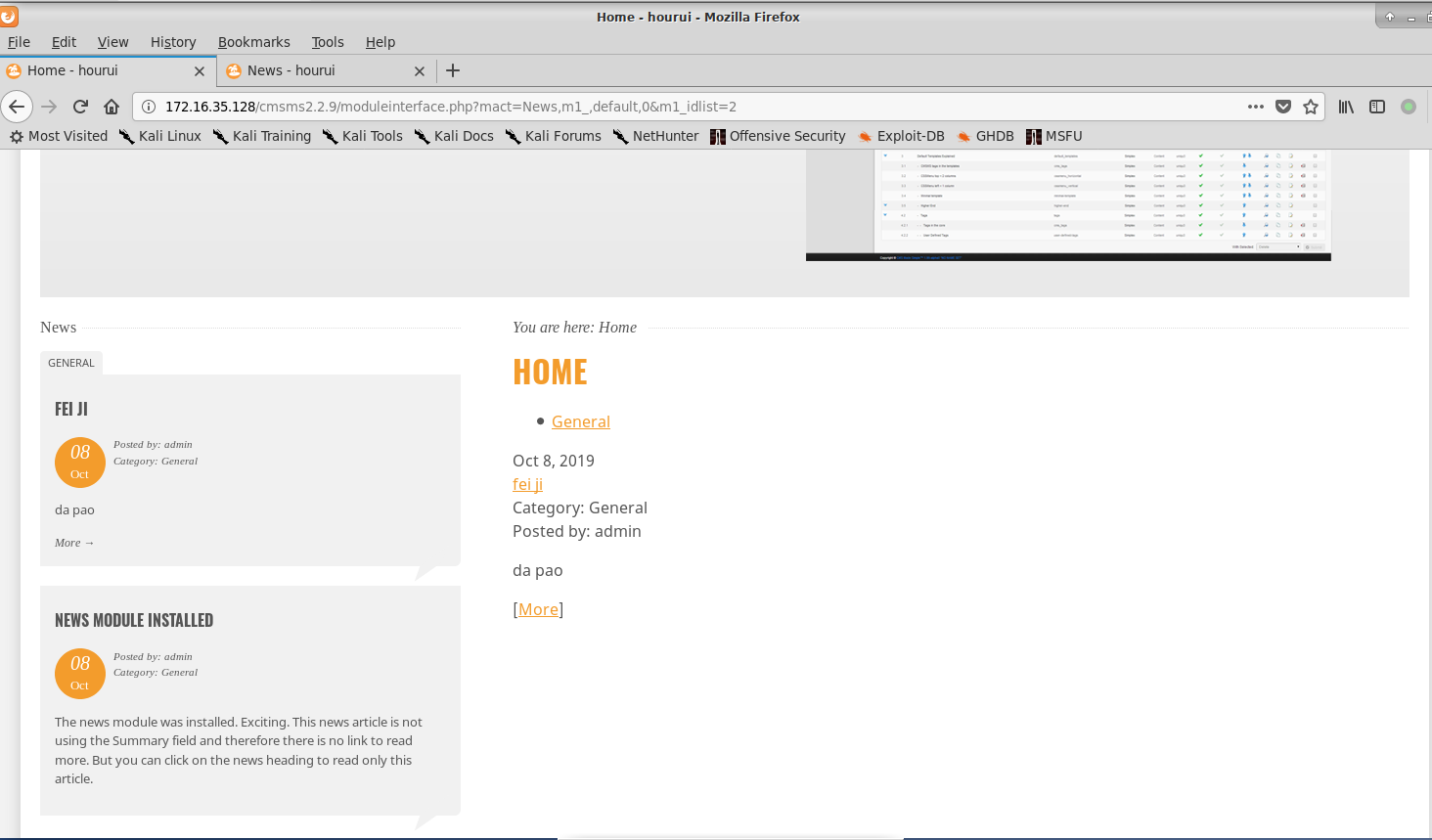
漏洞静态分析：

出现漏洞的url如下：

http://172.16.35.128/cmsms2.2.9/moduleinterface.php?mact=News,m1\_,default,0&m1\_idlist=1，如图：

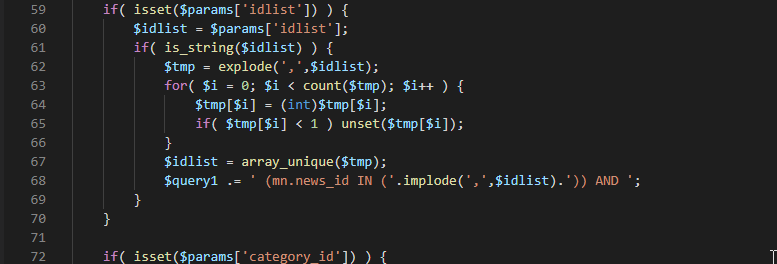


当改变id的值为2时，页面也会改变，如图：



使用vscode打开项目目录cmsms2.2.9（使用xdebug+vscode调试php的环境搭建，参见我的另为一篇博文[https://github.com/xuxuedong/YBDTBlog\_Security/blob/master/2019\_09\_24\_vscode%2Bxdebug%E8%B0%83%E8%AF%95php/2019\_09\_24\_vscode%2Bxdebug%E8%B0%83%E8%AF%95php.md](https://github.com/xuxuedong/YBDTBlog_Security/blob/master/2019_09_24_vscode%2Bxdebug调试php/2019_09_24_vscode%2Bxdebug调试php.md)）

出现漏洞的代码段如图：

逐行解释59-67：

59：判断是否设置了参数idlist，如果设置了，则进入循环

60：获取参数idlist的值

61：判断$idlist是否为字符串，如果是，则进入循环

62：将$idlist按照逗号分割，赋值给数组变量$tmp

63-66：问题就出在这个for循环中，假设数组有2个元素，当第一次循环时变量值小于1，则会被unset()，此时，数组的数量就少了一个，在下次循环时，元素数量减1，执行$i++，元素序号加1，所以下一个元素将被跳过，也就构成了过滤不严格

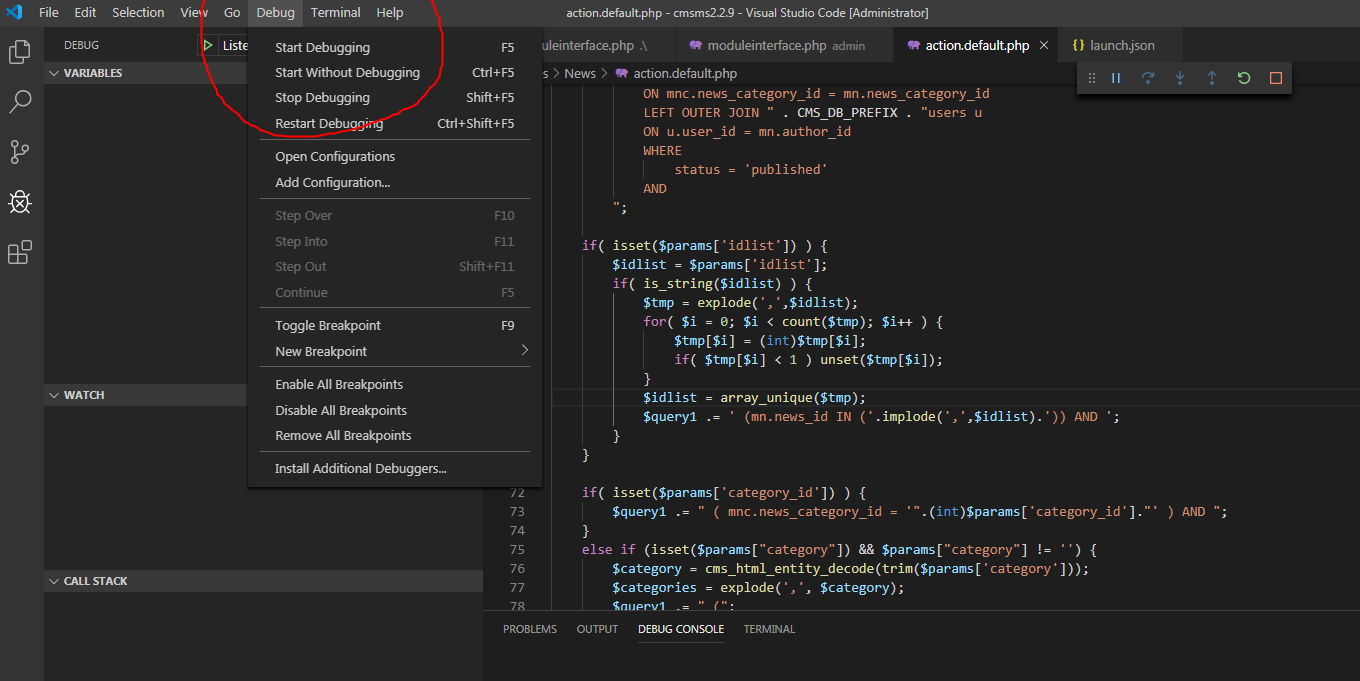
67：对数组去重

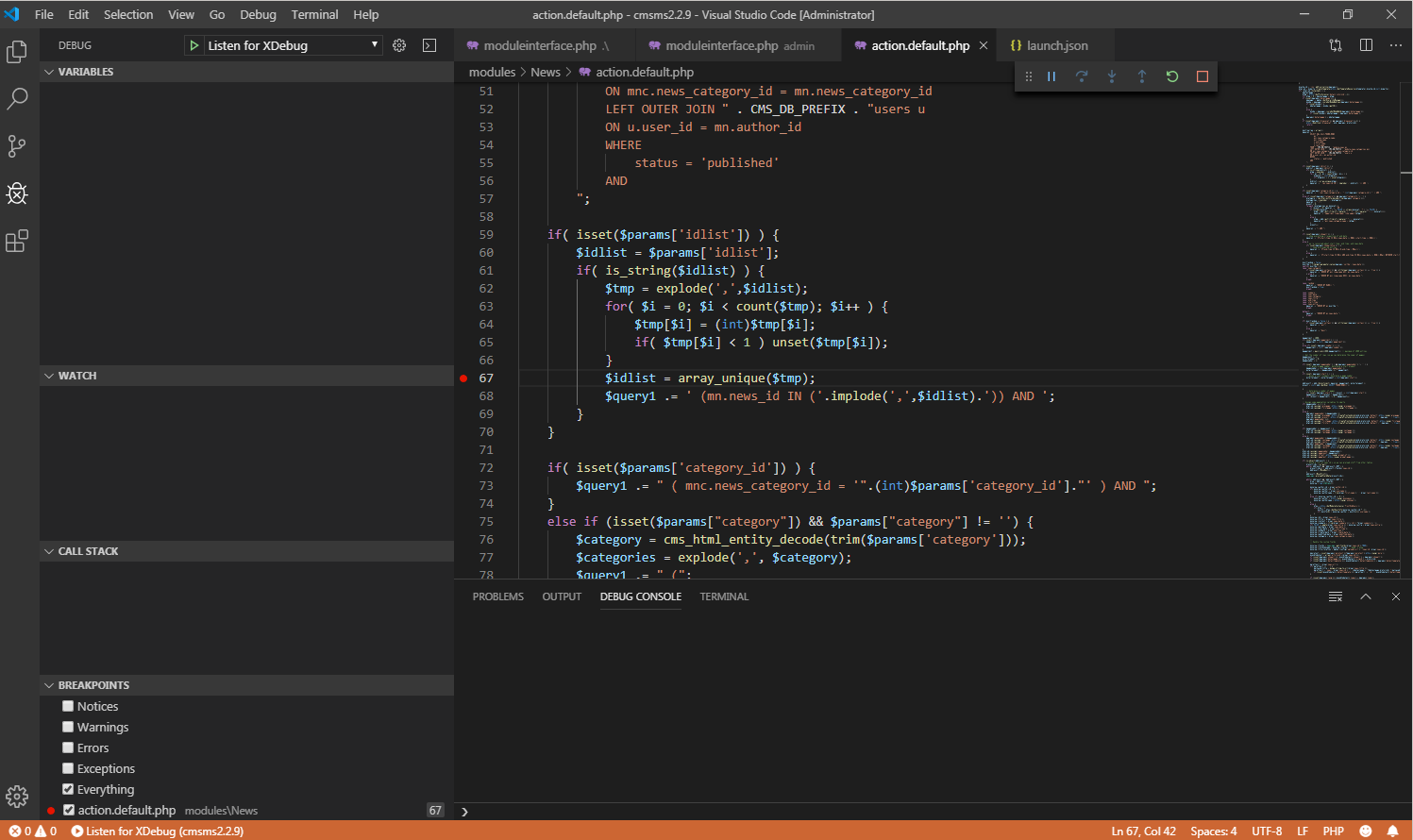
漏洞动态分析：

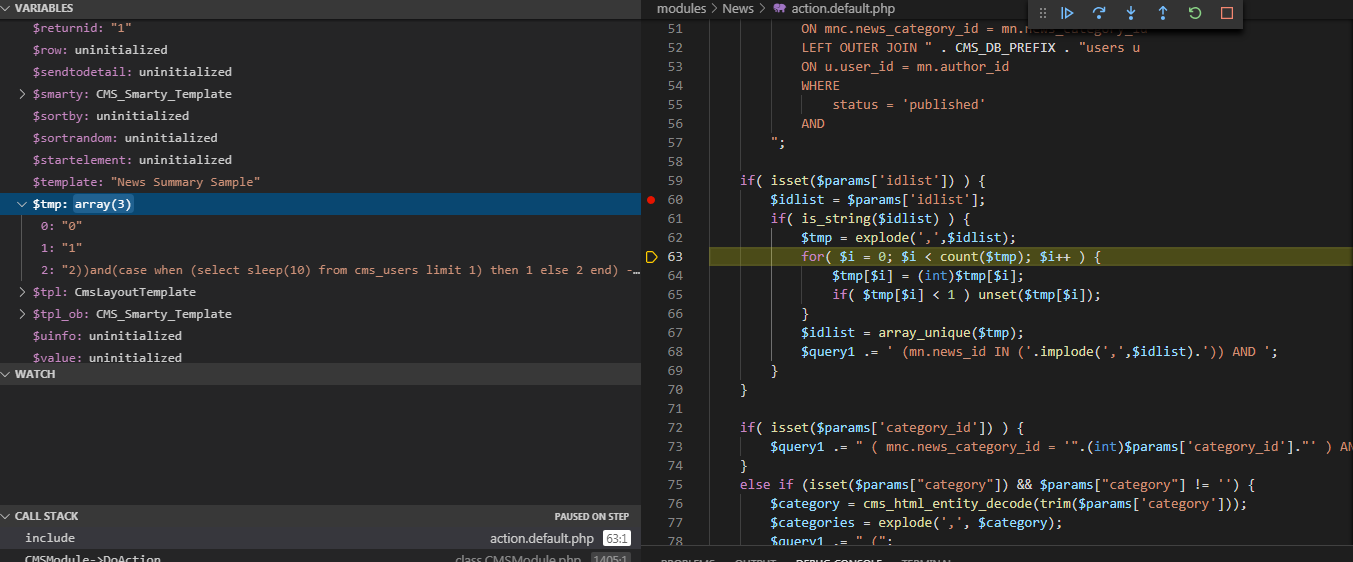
代码段位于文件\modules\news\action.default.php，我们随便选一行下断点

vscode中下断点方式如下：

点击debug->start debuging，如图：

当底部出现黄色条行时，表示已经启动调试功能，如图：

改为在第60行下断点，然后浏览器访问有漏洞的url，当代码执行到第63行时，此时变量$tmp的值如图中左侧

执行完循环后，当代码执行到第67行时，此时变量$tmp的值如图中左侧，表明字符串“2)))...”跳出了过滤

