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

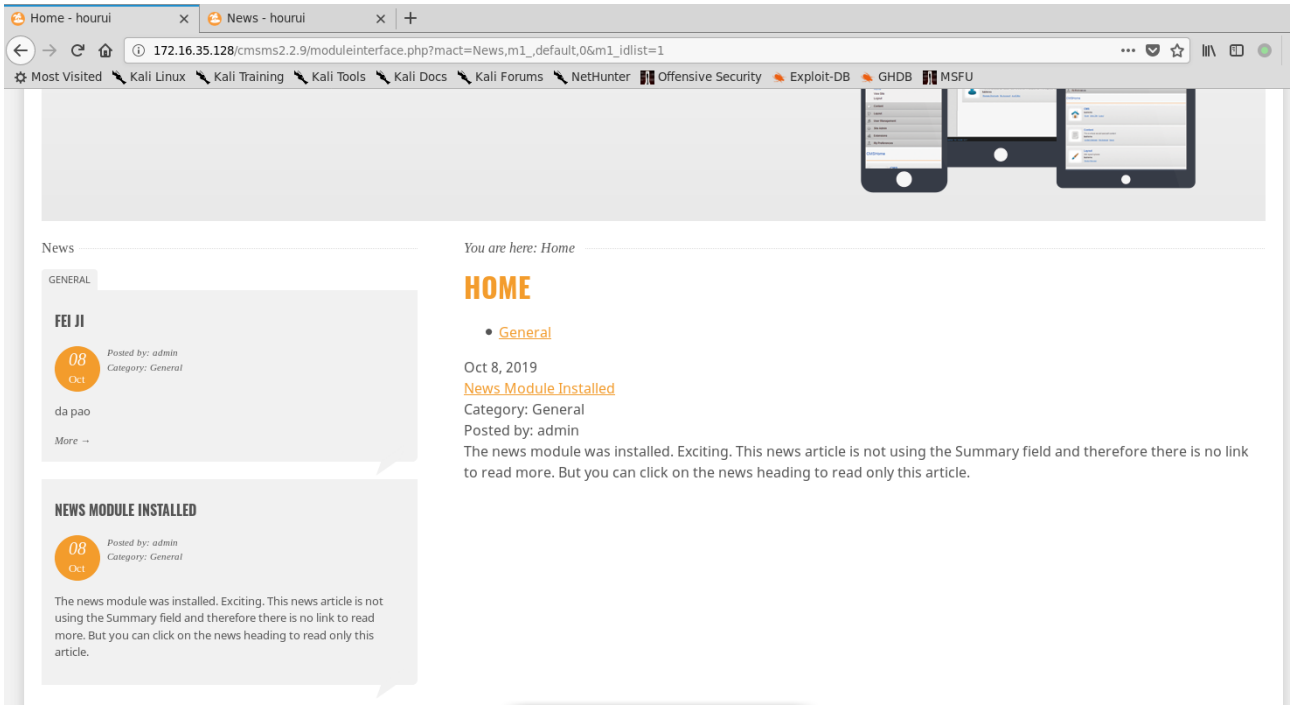
1：浏览器访问 http://172.16.35.128/cmsms2.2.9/index.php，看到网站能正常访问

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

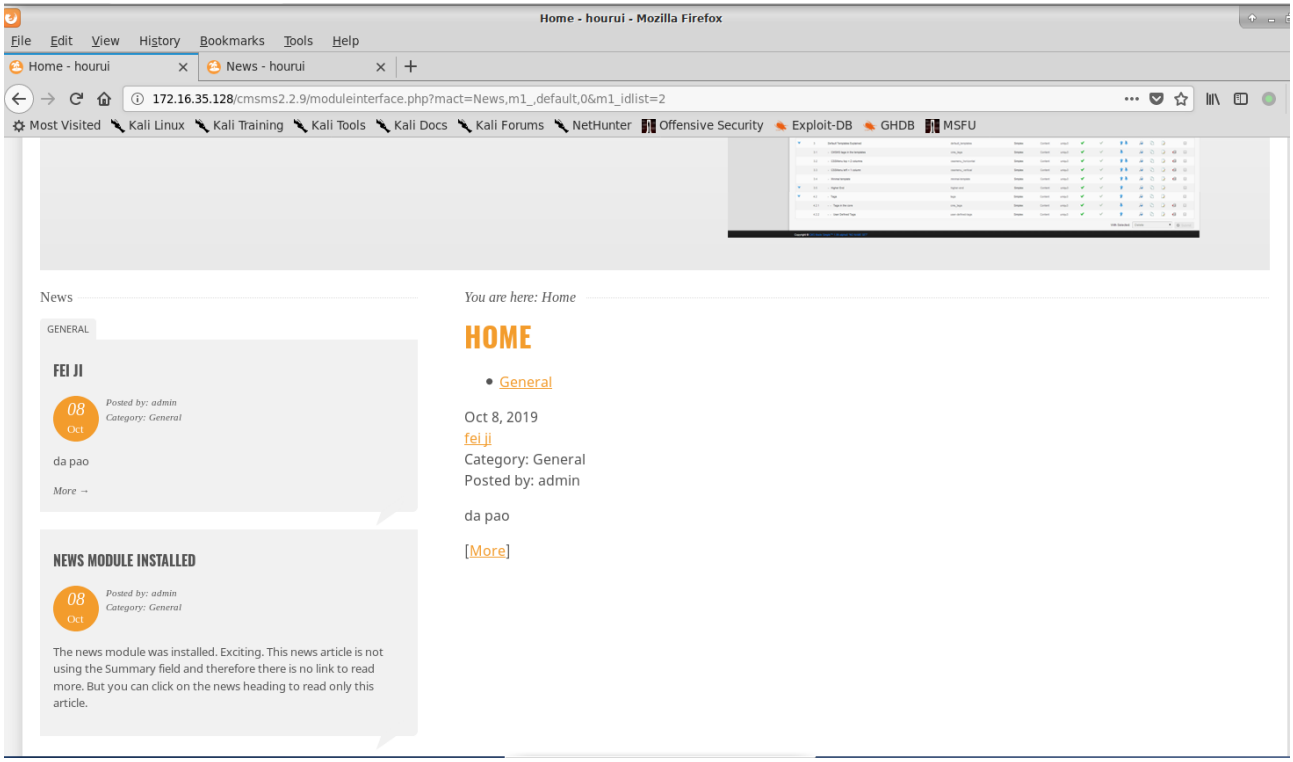
漏洞静态分析：

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 ）

出现漏洞的代码段如图：

```
59      if( isset($params['idlist']) ) {
60          $idlist = $params['idlist'];
61          if( is_string($idlist) ) {
62              $tmp = explode(',',$idlist);
63              for( $i = 0; $i < count($tmp); $i++ ) {
64                  $tmp[$i] = (int)$tmp[$i];
65                  if( $tmp[$i] < 1 ) unset($tmp[$i]);
66              }
67              $idlist = array_unique($tmp);
68              $query1 .= ' (mn.news_id IN ('.implode(',',$idlist).')) AND ';
69          }
70      }
71
72      if( isset($params['category_id']) ) {
```

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

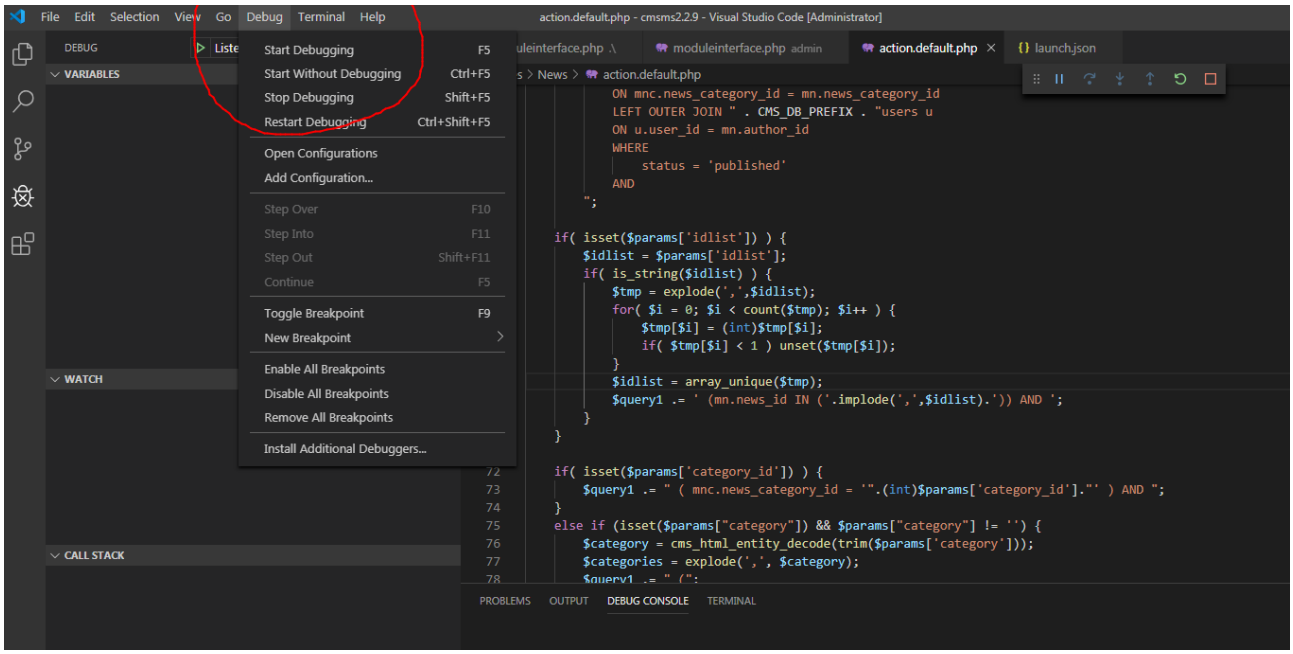
67：对数组去重

漏洞动态分析：

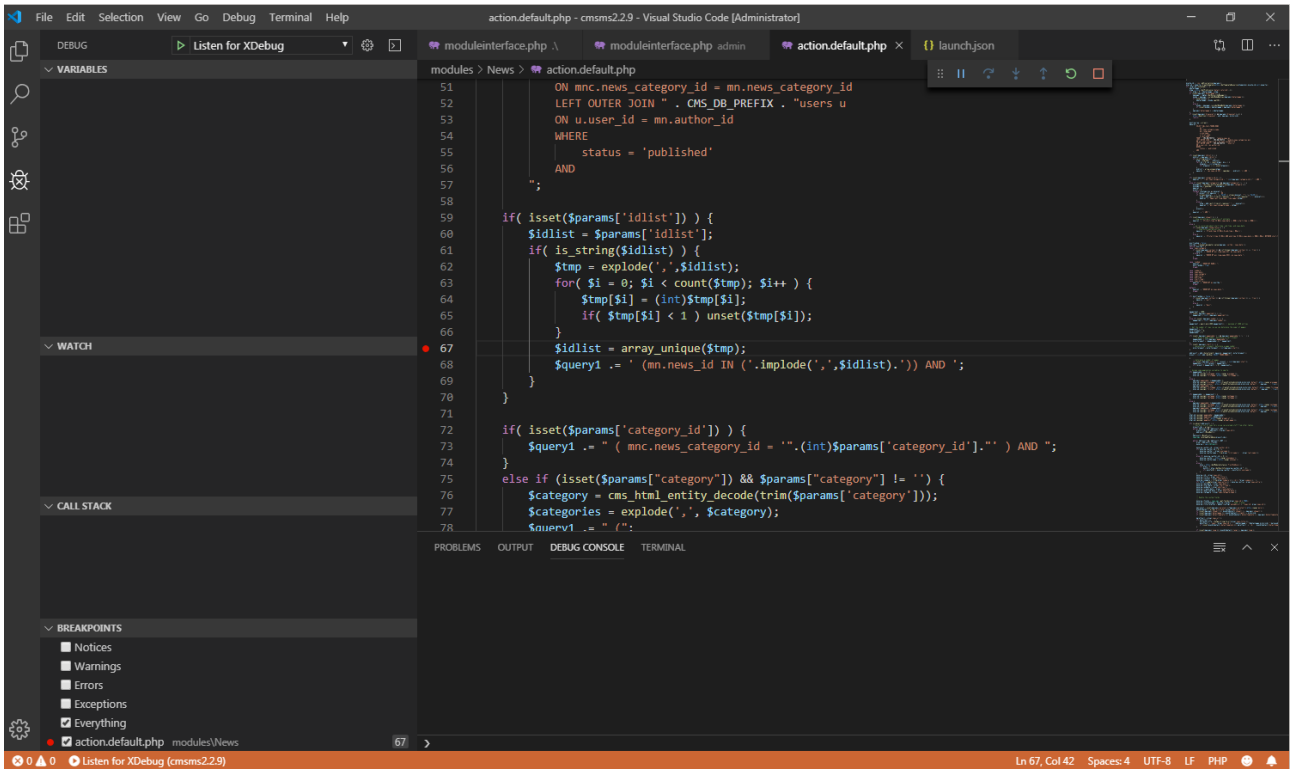
代码段位于文件\modules\news\action.default.php，我们随便选一行下断点

vscode 中下断点方式如下：

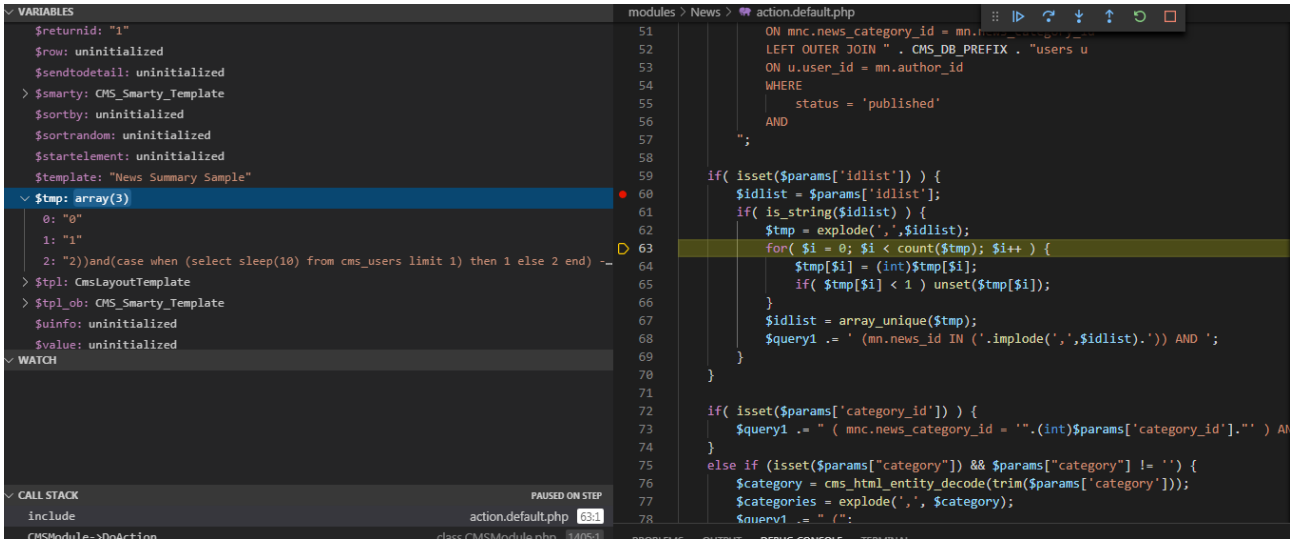
点击 debug->start debuging，如图：



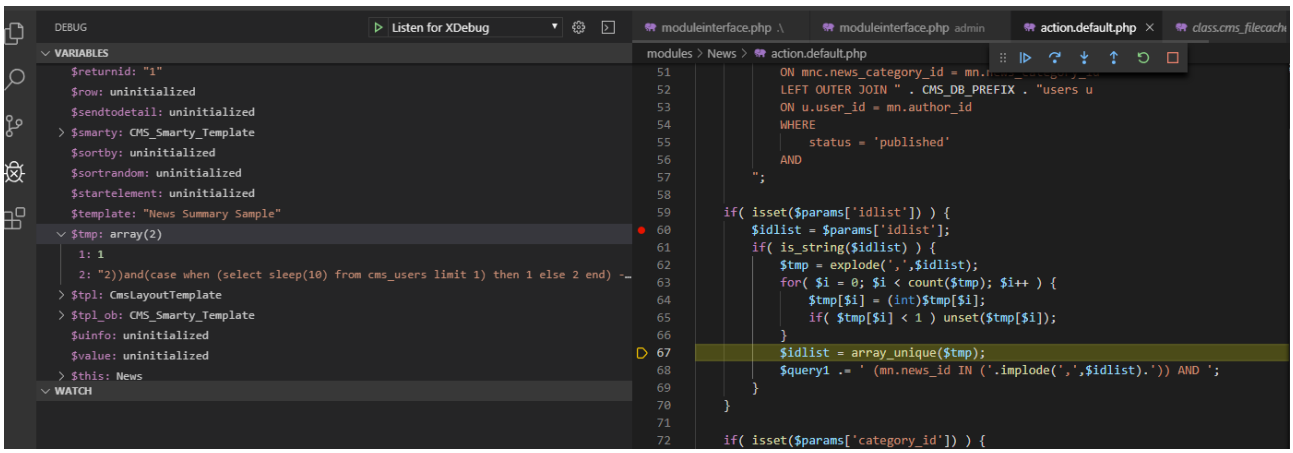
当底部出现黄色条行时，表示已经启动调试功能，如图：



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


DEBUG
Listen for XDebug
VARIABLES
$returnid: "1"
$row: uninitialized
$sendtodetail: uninitialized
$smarty: CMS_Smarty_Template
$sortby: uninitialized
$sortrandom: uninitialized
$startelement: uninitialized
$template: "News Summary Sample"
$tmp: array(2)
1: 1
2: "2))and(case when (select sleep(10) from cms_users limit 1) then 1 else 2 end) -
$tpl: CmsLayoutTemplate
$tpl_ob: CMS_Smarty_Template
$uinfo: uninitialized
$value: uninitialized
$this: News
WATCH
moduleinterface.php
moduleinterface.php admin
action.default.php
modules > News > action.default.php
ON mnc.news_category_id = mn.
LEFT OUTER JOIN " . CMS_DB_PREFIX . "users u
ON u.user_id = mn.author_id
WHERE
status = 'published'
AND
";
if(isset($params['idlist'])) {
$idlist = $params['idlist'];
if(is_string($idlist)) {
$tmp = explode(',',$idlist);
for($i = 0; $i < count($tmp); $i++) {
$tmp[$i] = (int)$tmp[$i];
if($tmp[$i] < 1) unset($tmp[$i]);
}
$idlist = array_unique($tmp);
$query1 .= ' (mn.news_id IN ('.implode(',',$idlist).')) AND ';
}
}
if(isset($params['category_id'])) {