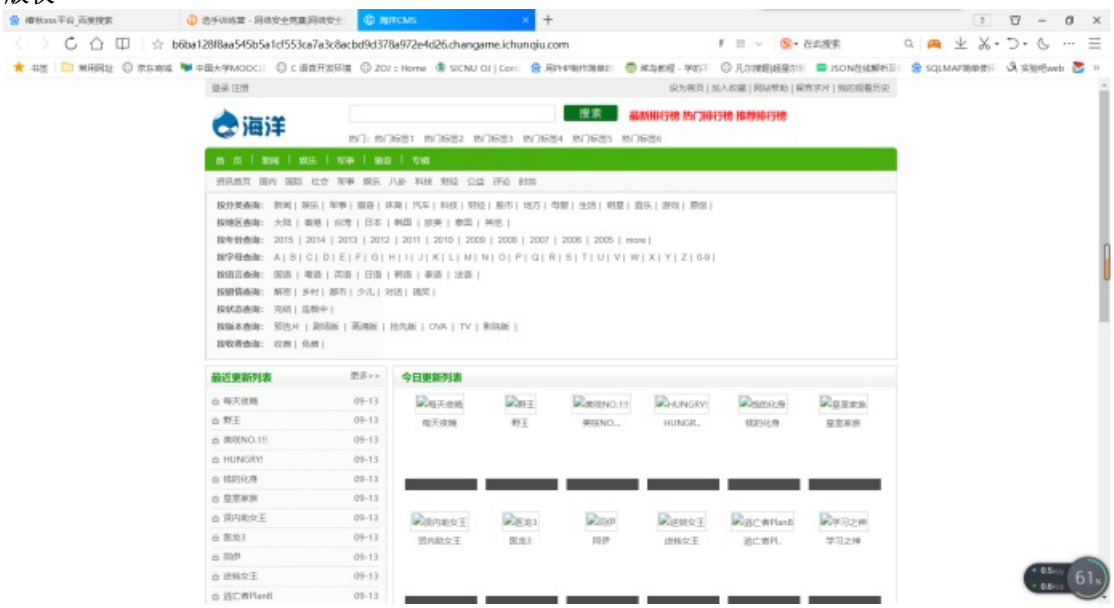
i春秋Test

转载

weixin_30555515 于 2019-08-05 18:55:00 发布 119 收藏
原文链接：http://www.cnblogs.com/wosun/p/11304895.html
版权



点开是个莫名其妙的网站。。。看看源码，

第一排好像有点东西

最后也有点东西，所以我们直接百度海洋CMS漏洞（https://www.freebuf.com/vuls/150042.html）

海洋CMS（SEACMS）几个老漏洞及其修补方法

在2017年2月，海洋CMS 6.45版本曾爆出一个前台getshell漏洞，漏洞具体内容参见：
http://blog.csdn.net/qq_35078631/article/details/76595817。该漏洞成因在于search.php没有对用户输入内容进行过滤，导致攻击者提交的order参数可进入parself函数中执行eval。

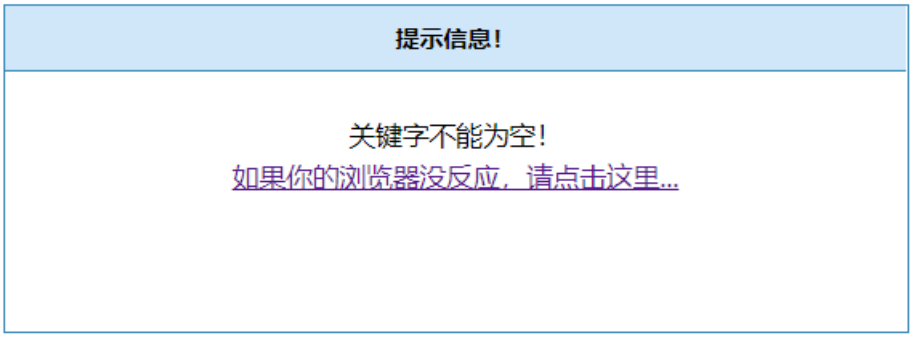
官方在6.46版中修复了该漏洞，修复方法是对用户输入的参数进行过滤并限制长度为20个字符。但这种修复方法并没有完全修复漏洞，因为在替换操作过程中用户输入的几个参数可以进行组合，因此补丁被绕过。

随后官方又在8月7日发布了6.54版本再次修复漏洞，这次修复增加了一句：

```
$order = ($order == "commend" || $order == "time" || $order == "hit") ? $order : "";
```

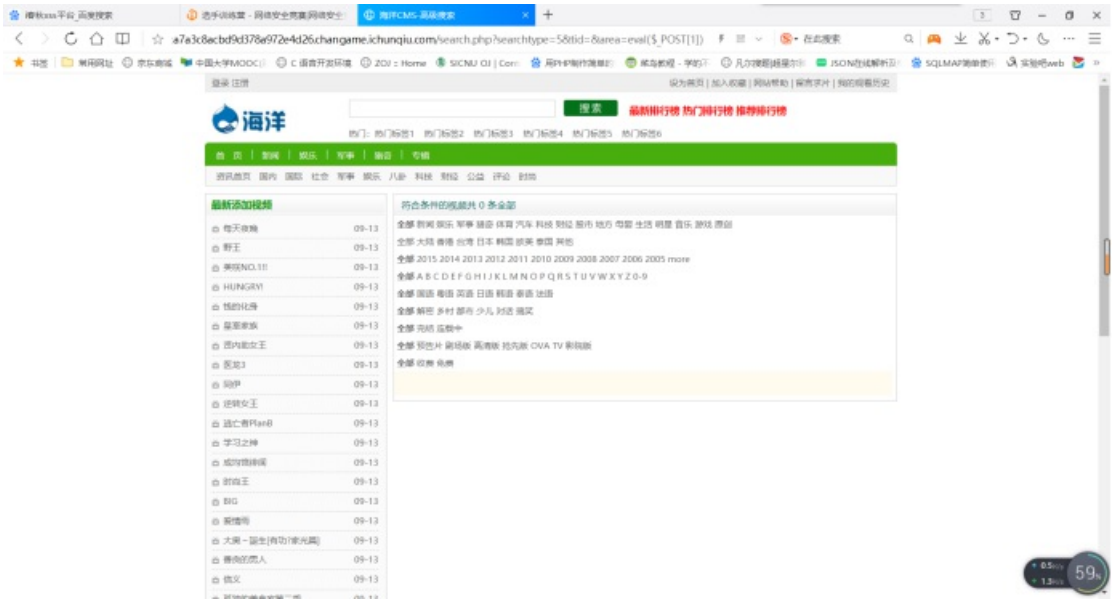
即限制了order参数只能是固定内容，这样虽然避免了通过order参数进行的攻击，但是却没有解决其他参数进入parself函数的问题。

所以这里直接在url中试试search.php

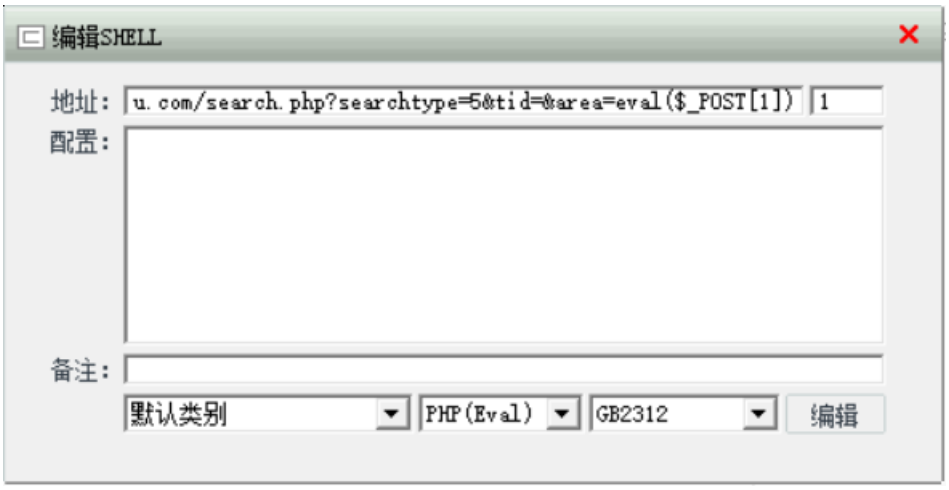


告诉我们需要有关键字，原来这里是进行关键字攻击的

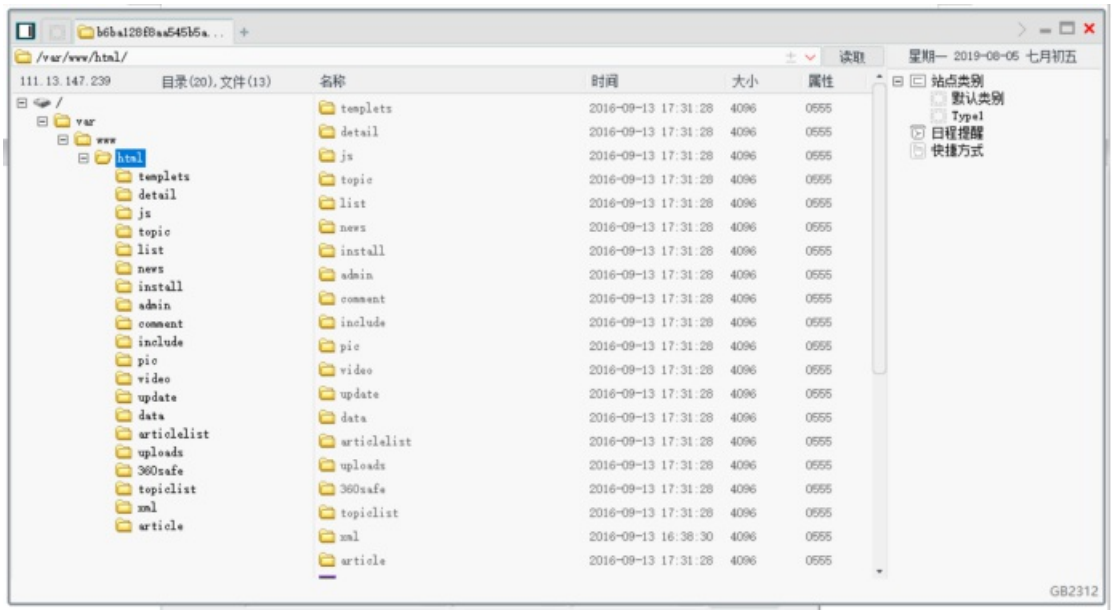
构造url后缀：/search.php?searchtype=5&tid=&area=eval($_POST[1])



上传成功，然后使用菜刀连接



就打开了

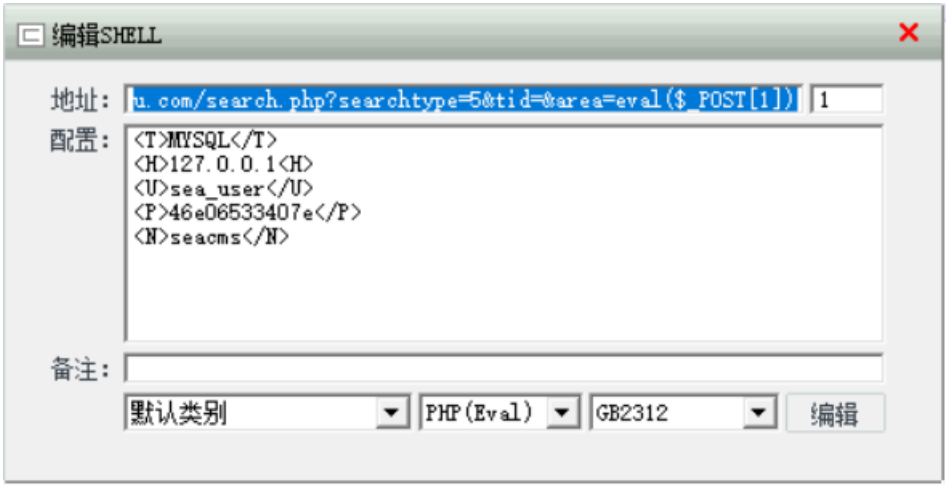


翻了翻，并没有flag文件。。。可能在数据库里面

在文件中找到数据库配置文件

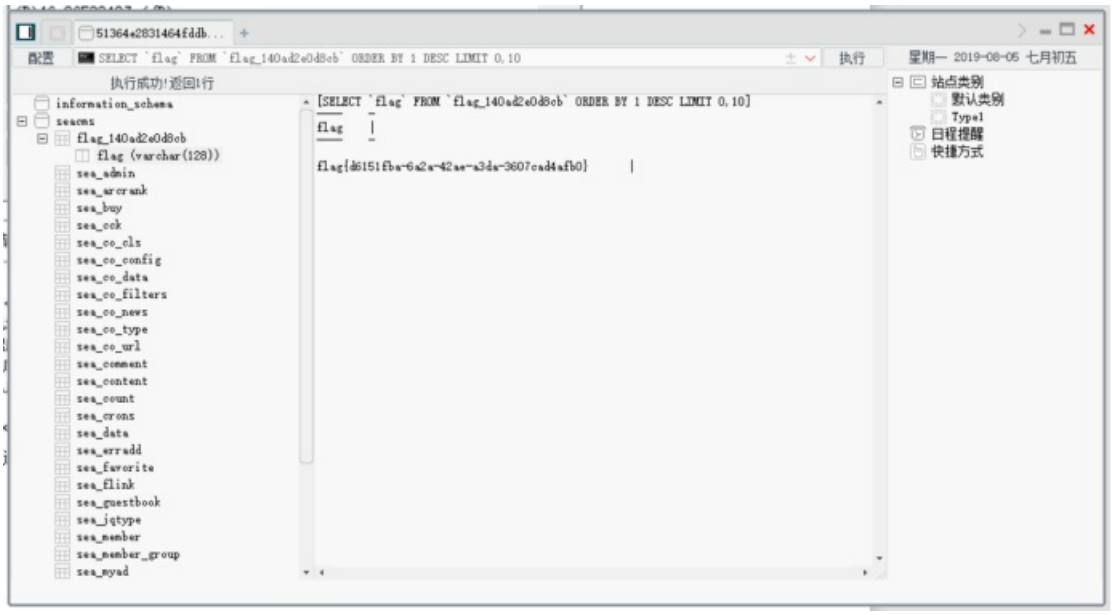
得到username和password

然后使用连接编辑，输入数据库全称，ip地址，用户名，密码，数据库名字



然后右键连接点数据库管理就可以进入数据库了

找到flag



转载于:https://www.cnblogs.com/wosun/p/11304895.html