

# i春秋web-Test(海洋CMS漏洞)

原创

大千SS 于 2019-05-22 17:41:02 发布 1086 收藏 2

分类专栏: [web简单站练习 i春秋](#) 文章标签: [i春秋 海洋CMS](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/zz\\_Caleb/article/details/90448611](https://blog.csdn.net/zz_Caleb/article/details/90448611)

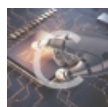
版权



[web简单站练习](#) 同时被 2 个专栏收录

4 篇文章 0 订阅

订阅专栏



[i春秋](#)

13 篇文章 0 订阅

订阅专栏

前面部分参考[https://blog.csdn.net/zz\\_Caleb/article/details/88244046](https://blog.csdn.net/zz_Caleb/article/details/88244046)

以前做过一个漏洞的复现, 下面只介绍连接上之后的操作。

这里用的是中国蚁剑进行的连接。

The screenshot shows a file manager interface with two panes. The left pane displays a directory tree for the path `/var/www/html/data/`. The right pane shows a list of files and folders in this directory. The file `common.inc.php` is highlighted in blue.

名称	日期	大小	属性
admin	2016-09-13 17:31:28	4 Kb	0555
backupdata	2016-09-13 17:31:28	4 Kb	0555
cache	2016-09-13 17:31:28	4 Kb	0555
mark	2016-09-13 17:31:28	4 Kb	0555
sessions	2016-09-13 17:31:28	4 Kb	0555
admin_d41d8cd98f00b204e9800998.php	2016-09-13 16:38:33	31 b	0555
<b>common.inc.php</b>	2016-09-13 17:06:50	198 b	0555
config.cache.bak.php	2016-09-13 16:38:34	2.73 Kb	0555
config.cache.inc.php	2016-09-13 16:38:34	2.65 Kb	0555
config.ftp.php	2016-09-13 16:38:34	247 b	0555
config.ucenter.php	2016-09-13 16:38:34	0 b	0555
config.user.inc.php	2016-09-13 16:38:34	482 b	0555
cron.cache.php	2016-09-13 16:38:34	149 b	0555

这里找到数据库的配置文件，其内容如下：

```
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/zz\\_Caleb](https://blog.csdn.net/zz_Caleb)

按照上面给出的数据库信息利用蚁剑来进行数据库的操作：



连接上之后执行查找命令即可：

