Metinfo5.3审计思考

niexinming / 2018-03-05 16:50:36 / 浏览数 11226 技术文章 技术文章 顶(0) 踩(0)

---

metinfo这个cms很有趣，我觉得可以玩的点也有很多，分享给大家来看
这里主要分析metinfo5.3，首先解压看文件结构

首先要梳理这个cms的结构，先要打开index.php去看入口文件的结构

```
<?php
# MetInfo Enterprise Content Management System
# Copyright (C) MetInfo Co.,Ltd (http://www.metinfo.cn). All rights reserved.
$url=$_SERVER['PHP_SELF'];
$turnurl=dirname('http://'.$_SERVER['HTTP_HOST'].$_SERVER["REQUEST_URI"]);
$resstr=strstr($url,'index.php/');
if($resstr){
 $turnurl=str_replace('index.php','404.html',$turnurl);
 header("location:".$turnurl);
}
if(!file_exists('./config/install.lock')){
   if(file_exists('./install/index.php')){
       header("location:./install/index.php");exit;
   }
   else{
       header("Content-type: text/html;charset=utf-8");
       echo "■■■■■■■■■■■■■■■■■■■■■■■■■config/install.lock■■■";
       die();
   }
}
if(file_exists('./update')&&!file_exists('./update/install.lock')){
   header("location:./update/index.php");exit;
}
$index="index";
require_once 'include/common.inc.php';
require_once 'include/head.php';
$index=array();
$index[index]='index';
$index[content]=$met_index_content;
$index[lang]=$lang;
$index[news_no]=$index_news_no;
$index[product_no]=$index_product_no;
$index[download_no]=$index_download_no;
$index[img_no]=$index_img_no;
$index[job_no]=$index_job_no;
$index[link_ok]=$index_link_ok;
$index[link_img]=$index_link_img;
$index[link_text]=$index_link_text;
$show['description']=$met_description;
$show['keywords']=$met_keywords;
require_once 'public/php/methtml.inc.php';
if($met_indexskin=="" or (!file_exists("templates/".$met_skin_user."/".$met_indexskin.".".$dataoptimize_html)))$met_indexskin=
if($map&&$met_mobileok&&is_numeric($uid)) {
   if($wap_skin_user != 'wap001' && $wap_skin_user != 'mobile_001' && $wap_skin_user != 'mobile_002' && $wap_skin_user != 'mob
       $met_indexskin = 'map';
   }
}
include template($met_indexskin);
footer();
```

1-20行判断cms是否是安装状态，后面是初始化各个各个变量
其中注意25行的

```
require_once 'include/common.inc.php';
```

我们打开这个文件common.inc.php
注意36到42行这个代码

```
foreach(array('_COOKIE', '_POST', '_GET') as $_request) {
   foreach($$_request as $_key => $_value) {
       $_key{0} != '_' && $$_key = daddslashes($_value,0,0,1);
       $_M['form'][$_key] = daddslashes($_value,0,0,1);
   }
}
```

如果玩代码审计比较多人应该知道这里有个任意变量覆盖的风险，具体例子可以参考我的一个漏洞分析：http://blog.csdn.net/niexinming/article/details/53153629
可以通过一个简单的小栗子来演示这段代码

```
<?php
$a="a";
$b;
global $c;
$c="555";
require_once 'include/common.inc.php';
global $e;
$d;
var_dump($a);
echo "</br>";
var_dump($b);
echo "</br>";
var_dump($c);
echo "</br>";
var_dump($d);
echo "</br>";
var_dump($e);
```

可以看到在require_once 'include/common.inc.php';这段代码上面的变量都被覆盖了无论是否被初始化都被传递进来的参数给覆盖掉了，这段代码下面的变量只要没有被赋值就会被传递进来的
举个不是安全的问题的例子供大家玩耍一下
大家可以看的index.php中有这样的一段代码

```
$index="index";
require_once 'include/common.inc.php';
require_once 'include/head.php';
$index=array();
```

可以给index.php传递index=2333，看一下效果

可以看的代码逻辑被改变了，造成了页面的混乱，而metinfo5.3里面引用到这个代码require_once 'include/common.inc.php';的地方有很多

所以可以玩的点有很多，比如可以找到一些任意文件删除的地方，删除一些关键文件来使得一些变量变成未初始化的变量，从而控制整个代码流程

现在metifo最新版的是6.0,他们已经意识到这样的问题，所以对框架做了许多改善，逐渐减少了通过require_once 'include/common.inc.php';引入参数的做法，使得metifo6.0的安全性更强了一些

上一篇：如何清除window上的RDP连接记录 下一篇：渗透技巧——获取Windows系统...
1. 0 条回复

- 动动手指，沙发就是你的了！