Metinfo5.3.10版本Getshell

笑然 / 2016-12-05 11:03:00 / 浏览数 2910 安全技术 漏洞分析 顶(0) 踩(0)

■■■■■http://www.venenof.com/index.php/archives/179/

好久没代码审计了，今早上cheery师傅跟我说了一下这个洞，尽管这个洞已经被修复了，但是还是比较新的，看了下没那么难，就简单写下步骤：

0x01

首先看一下配置的文件include/common.inc.php

发现Metinfo采用了伪全局变量的这样一个设置，那么是否会有变量覆盖之类的漏洞，grep下：

0x02

觉得login那里应该会发生点什么故事XD
既然这样的话，看了下后台登录的地方：

1. login.php
2. login_check.php
3. login_out.php

0x03

一共三个文件，看一下check，既然包含了common.inc.php，那么就意味着里面存在一些可控的变量：

果不其然，对于参数并没有初始赋值，比较开心XD

研究了下发现有两种做法：
0x01：知道路径的话：
既然可以require，那么我们需要一个文件就可以执行，so，注册一下会员，看看有没有什么惊喜的东西XD
发现可以上传图片logo：

既然这样的话，我们可以上传一个利用phar或者zip打包的文件，从而达到RCE的目的：

然后file_put_contents或者一开始就用file_put_contents拿到一个shell。
0x02不知道路径
貌似是不能用../去代替的，如果有师傅成功的话，求交流。
在这种情况下，我们可以用php的伪协议去达到一些我们想达到的目的，不过allow_url_include默认是不开启的，所以也算有点鸡肋，不过CTF比赛可以用一下。
如果allow_url_include = on，那么我们可以利用base64让后面的../失效，从而达到RCE，具体可以自己试一下:)

上一篇：面对勒索软件，除了交赎金，还能怎么办？ 下一篇：某云PC客户端命令执行挖掘过程

1. 0 条回复
   - 动动手指，沙发就是你的了！