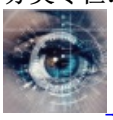
三个白帽挑战赛第二期的writeup(详细记录一系列的坑) [代码审计]

转载

qq_28247467 于 2016-03-30 12:57:11 发布 1164 收藏
分类专栏： CTF


CTF 专栏收录该内容
1 篇文章 0 订阅
订阅专栏

post by answer / 2016-3-25 20:41 Friday

首先想说这是我见过的最绕的题目了，不得不说出题人的思路太猥琐。

首先在访问http://8ed0a7d1a5ed5b5ac.jie.sangebaimao.com/sangebaomao.zip得到源码。根据tips是二次注入还要getshell。看着就带劲。

一、先看看文件吧

其中include.php做了伪全局，而且GET、POST、COOKIE 用了addslashes转义，所以基本不能通过一次注入来获得shell，,因为在利用select语句写shell的时候，路径是必须被单引号包裹起来的。

看看main.php有个25行

其中的limit后面的$num是来自 $_SESSION['limit']，追溯$_SESSION['limit']最终来自的是用户注册，因为limit之后是可以执行into outfile的。这也算是一个知识点吧。所以我们能够通过注册的limit来控制写入的路径，那怎么控制写入的内容呢。很明显。我们只有从name 和 message字段下手。追溯这两个字段的来源。

name字段是由注册的时候nickname参数的先存入数据库，然后再查询出来的。追溯到注册的代码才发现$name被htmlspecialchars()实体化了，所以name是不能直接引入<符号的。$message也被实体化了。但是要写入php代码是必须带着<符号的，此处我懵逼了。

后来玉林嘎大牛提醒，用0x, 他一说0x，我马上反应过来再找个二次注入，让message字段入库的时候以16进制写进数据库，只要是没有单引号包裹的16进制最后入库都会还原成原本的字符串。

解开这个结的就是main.php中的18行的sql语句。

在这个inster语句中，$name是注册的时候可控的。所以我们如果注册的时候，我把name注册成这样aa',0x3c3f706870204065766 16c28245f504f53545b615d293b3f3e)#

其中16进制是一句话的hex编码。这样的话 我们执行 insert into guestbook(`uid`,`name`, `message`) values('".$uid."','".$name."','".$message."')的时候真正的数据库代码是如下图的

#之后的被注释，0x3c3f706870204065766 16c28245f504f53545b615d293b3f3e就是字段message的值，而且是没有单引号包裹的。所以当我们执行了insert操作之后。message字段的值就是<?php eval($_POST[a]);?>了，那么当执行select操作语句的时候,message是从数据库查询出来的所以不会被实体化，因此就可以getshell啦。听着是不是觉得好绕啊。

具体过程由于官方的原因，就不贴出来啦。懂得人自会做。

看看执行的sql语句，就懂啦

来看看写入的文件，完美写入网站根目录

三、

到这里这里你觉得就oK了吗，然而并不是，最好玩的才刚开始。我在三个白帽的服务器上测试的时候怎么也写不进，然后去问了出题人是不是web目录不可写然后得到了答案不可写。

而且还提示要利用代码里面的_autoload函数的特性。后来去搜了搜特性，发现这是一个注册类的函数，在没有给定处理用函数数的情况下当你去实例化类的时候，就会直接包含目录下的与类名相同的.php文件或者是.inc文件。其实说简单点，就是这个函数可以包含文件。

然后我就去看了看题目的源代码，看在哪里调用了_autoload这个函数，这个函数是写在include.php中的，然后被ini.php包含,int.php再然后被main.phph包含 在main.php中有一个类的实例化的操作

可以看到类名是$action，而$action是我们控的。看到这里，我的思路就明了啦。我们往一个可写目录写一个php文件，然后我们再把这个文件的完整目录和文件名传给$action,那么当php去实例化这个$action这个类的时候。就会自动包含我们穿上去的文件，那么我们就通过文件包含getshell啦。因为是linux的服务器，所以/tmp 目录应该是可写的。

看下面截图你就知道怎么利用啦，具体过程不便放出。

此处有一个坑，就是必须在登录情况下才能访问到shell。如果你用菜刀的话，还要想办法带着session。所以我就直接写成了<?php system($_POST[a]);?>，用火狐去发包。

然后成功翻到flag

后记：只能说出题人太猥琐，而且确实太绕啦。不过确实很有趣，二次注入写shell加上利用特性，简直是极致。