[WriteUp]网络信息安全攻防平台-综合关3

原创

Fai7y 于 2021-03-11 20:17:18 发布 221 收藏

文章标签： 信息安全

本文链接：https://blog.csdn.net/m0_49800617/article/details/114661086

网络信息安全攻防平台-综合关3-美图闪亮亮交友平台

综合关传送门

□□注意：这是第三题的WP

需要的工具：一台部署好nginx的VPS(这里只要能用url访问就行，不一定需要nginx，nginx只是给不熟悉的提供一个参考)

正文开始

经典题目无用，tips先记着，直接进入环境

美图闪闪亮_让你快速找到男女朋友

美图上传区

为了保护您的个人隐私，请提交您的照片链接和说明，当您不希望别人看到您的照片时，您可以随时删除原始链接的图片内容！我们将进行人工审核，系统不会保存您的照片的任何信息。

姓　名：　例如：王小明

图片url：　例如：http://www.hackinglab.cn/meitu.jpg

照片描述：

例如：这是我在xx酒吧拍得噢，漂亮吧！

提交　重置

什么都不管，先正常传一次图片试试，这个滑稽我是从我图床里扒过来的

美图闪闪亮_让你快速找到男女朋友

管理员审核进度通知

您的审核申请已经发送到管理员邮箱，待审核通过后您的照片将自动推送到系统首页

美图闪闪亮，筑您找到心仪的她（他）

姓　名：123

描述：abc

我直接好家伙，居然有回显！

tip里提到没有xss，那就传马，多次尝试上传木马失败（这里走了不少弯路，文末另提）。

算了，仔细看看这个网页，UI丑得很，废话又多。众所周知，程序员都是很懒的，要我来我就懒得写那么多字，他又老提“管理员人工审核”，生怕我注意不到，掐指一算，八成是有用的信息，深究一下。

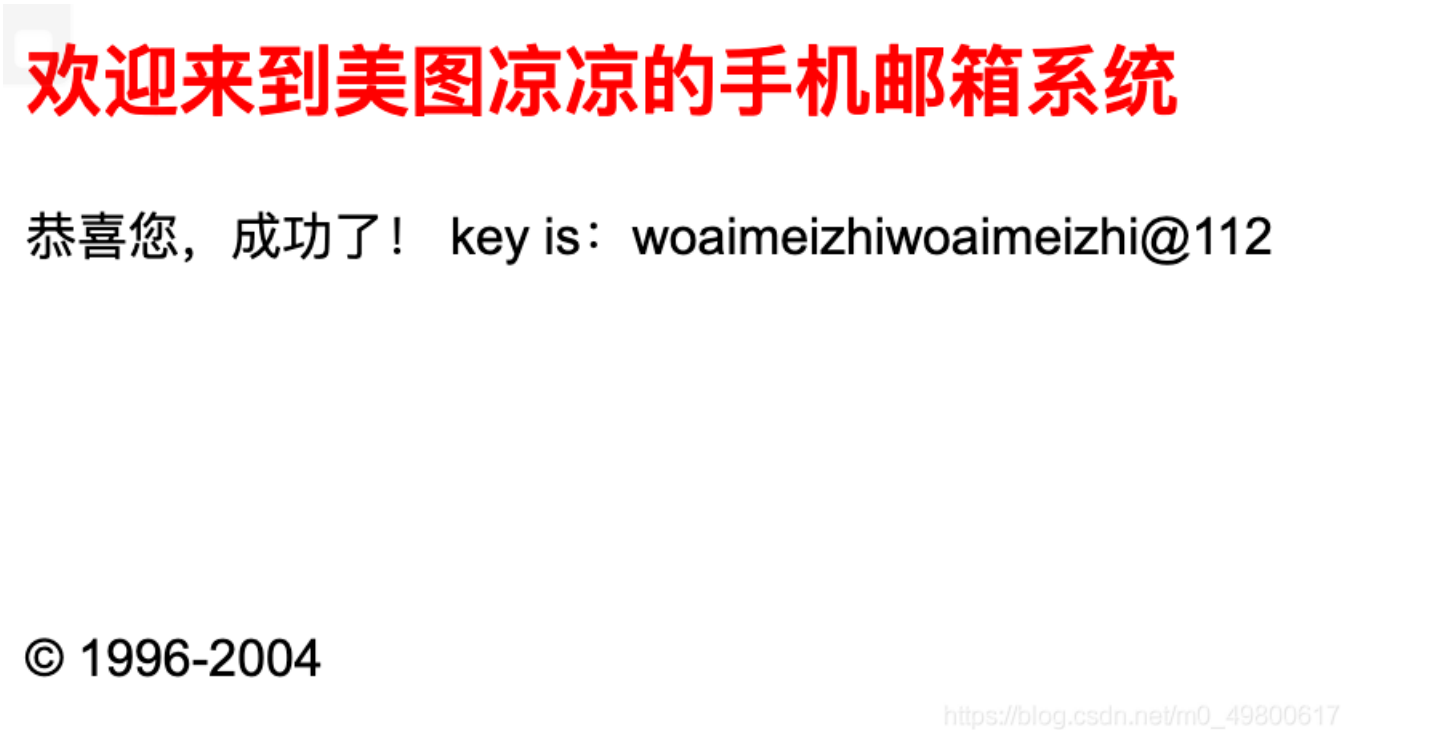
既然你本身不存储图片，那你管理员要审核自然也是要访问我的服务器的，那么有没有可能是管理员直接从后台访问呢？

刚好我url给的是自建网站里的，直接查看nginx日志

```
cat /var/log/nginx/access.log
```

瞧瞧我发现了什么:D

直接浏览器访问就出flag了，我以为还要绕个登录状态验证啥的



此处是弯路，但是多少带些东西，就保留了

我：？？？有回显？

我当场就动了歪心思啊，反手传个一句话木马，传马就肯定别用图床了，怎么办呢？用自己的VPS吧**(注意，在自己的服务器上放马就不是什么很安全的行为，用了立马删掉，以免出事。我自己的VPS只有一些学习资料，还有硬盘备份，所以胆子就很肥了)**

这里的前置过程我就不从盘古开天辟地开始说了，就提一嘴向VPS上传文件可以用rz这个命令，具体安装用法自己搜了，教程很多。
甚至于你无所谓一些问题的话，你租国内大厂的vps都可以一键部署的，上传也有图形界面

反正你现在已经搭好了一个简单的网站，万事俱备，只缺木马。

简单的一句话木马无非是`<?php eval($_POST[attack])?>`，由于此处上传使用的是url，首先尝试原型木马使用一些简单的后缀名绕过，如`shell.jpg.php`，访问发现404，没有上传成功。

那就花点时间做个图片马吧，在windows的cmd下（不包含“[]”）：

```
copy [原图片]/b+[原木马]/a [图片马]
```

上传后依然404，我木马直接就找不到，这让我非常的疑惑。几次无谓的尝试后发现我蠢了，不是有回显么，直接审查元素查回显所在路径不就完事了

得，上传了个寂寞。

假的，题目里什么上传都是假的，这根本就不是什么上传题。