|  |
| --- |
| 文/图  作者：过河的卒  今天想拿一个大型的人才交流站，主站看了下，确实没有什么能利用的，于是旁注吧，旁站有好几百，肯定是虚拟机了。提权的可能性一下子就降低了，但是还是应该去试试。顺利看到一个熟悉的后台，也就是讯时的后台，怎么利用网上很详细，这里不做过多讲解。  111.jpg  看到很详细，如果也是如此好拿，今天我也没必要写这个文章。看了下上传文件，已经有前人传了asp的文件上去，但是我点开他的后门，出现了这样一幕。  222.jpg  不管是大马，小马，都不行，我用变形的一句话，就是如同汉字的那个uncode，不能正确解析。肯定是有第三方软件的，那么具体是什么，我猜想是一流。继续利用数据库备份吧。  333.jpg  看起来是成功了，那么我们来看看备份的大马。  可能有些朋友会说，你用大马容易被过滤，用小马，或者直传一句话。这些我都尝试了。后来我想，不然备份一句话吧，然后再上传大马，但是转念一想，如果真有第三方的过滤软件，这样也是不能上传的啊。算了，还是试试吧，事实胜于雄辩。  5555.jpg  备份成功，我们用一句话客户端连接。  666.jpg  依旧没有出现熟悉的hello，World。继续转换思路，利用图片木马备份。用到的工具有edjpgcom。用法很是简单，拖拽图片添加一句话。  777.jpg  是否出现了大家期待依旧的hello，world！那么话不多说，立刻利用一句话上传一个大马，这次大马上的很顺利，上了大马自然提权，其实大家刚才看我备份截图的网站路径也就看了个大概，这个是虚拟机。支持aspx，立即上传，看起来是成功了。  888.jpg  再次出现空白。怎么办，换马，还是不行，最后尝试直接写马，成功。  10000.jpg  其实到这一步，教程也结束了，因为这个提权实在是在我的能力范围之外，换了cmd名字，可以执行set，其他都不行，如果哪位大牛知道如何提权或者想尝试，都可以在下面写出，我放出shell。最后说一点，其实拿这个shell还可以尝试利用iis的解析漏洞，在备份数据库的那一步。也就是换掉databack同样出现让人激动的hello，world。（还是必须用图片马）  111111.jpg  最后揭秘到底是什么过滤软件  133333.jpg  看来先前的猜想是没有错了，最后就是把我们刚才上传的图片以及木马，还有我们备份的一句话全部删除，希望大家都能进行扫尾工作。此文仅做技术交流，如有疏漏，大牛莫笑。 |

[444.jpg](http://wwww.hake.cc/forum.php?mod=attachment&aid=MjM1OHwwMmUzZGViMnwxMzE5NzI1MDU5fDgxNTI%3D&nothumb=yes) (16.03 KB, 下载次数: 0)

