让文件读取漏洞与shell环环相扣

原创 队员编号053 酒仙桥六号部队
2020-08-04原文

这是 **酒仙桥六号部队** 的第 **53** 篇文章。
全文共计1826个字，预计阅读时长7分钟。

前言

作为一个漏洞挖掘者，你会拿任意文件读取漏洞做些什么？

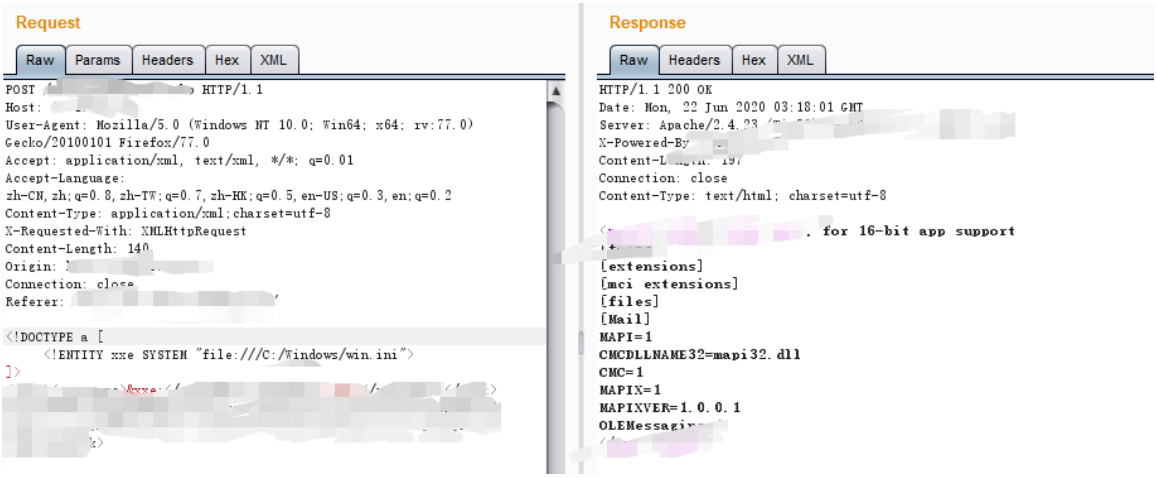
作为一个系统维护人员，你会在系统维护主机桌面保存什么重要信息？

背景

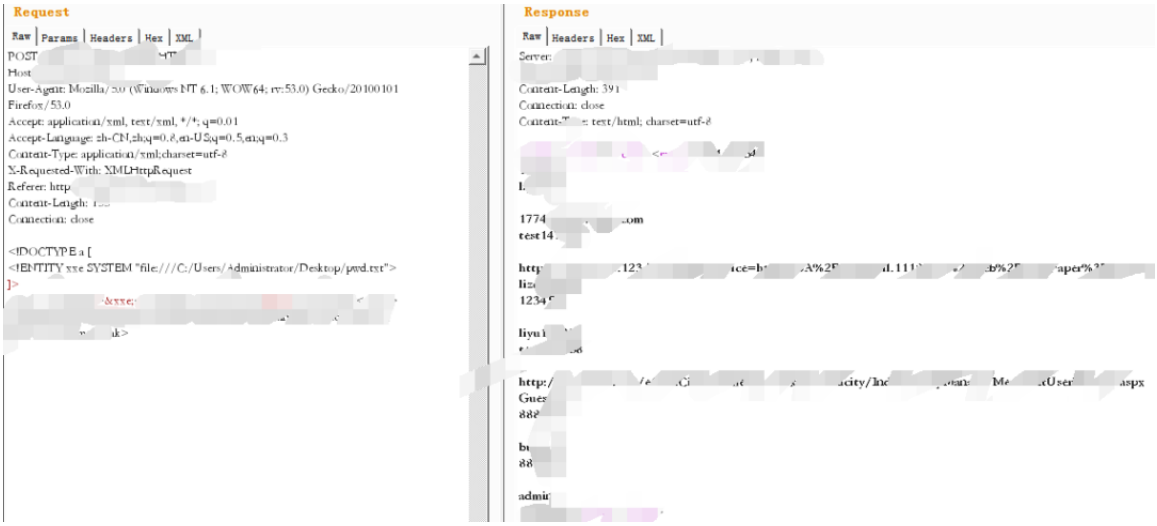
前不久，我接到一个渗透测试项目，一共8个域名。领导给的期限是2周。我总觉得一个人做项目缺少点激情。想起我的狗友-单身狗大强。我跟领导申请，我和大强共同完成这个渗透测试的项目。很快，在项目周期改为一周的前提下，我们两个开干了。客户只提供了多个用户系统的测试账号，未提供管理系统的测试账号，但是管理系统还在测试范围。经过四天的艰苦卓绝的努力下，不负所望，我和大强挖到了不少漏洞，细数战果，逻辑漏洞一大堆，系统漏洞也不少，可以愉快的交差了。但是，唯一缺少的就是一个shell，作为一个资深漏洞挖掘人员，知道渗透测试的目标是更多的发现问题，不以shell为终点。但没有拿到shell心里总觉得有一丝丝遗憾。就像将军拿下城池但未见敌军首领一般。

过程

在整理报告的时候，我发现大强的漏洞报告里有一个XXE漏洞，并且还是回显的。仔细的研究后发现，这个接口是整个系统登录后的的统一参数入口。系统解析到xml里的方法后，再根据对应的方法执行响应的逻辑。按耐不住内心的躁动，我和大强开始了通过fuzz找各种敏感文件。

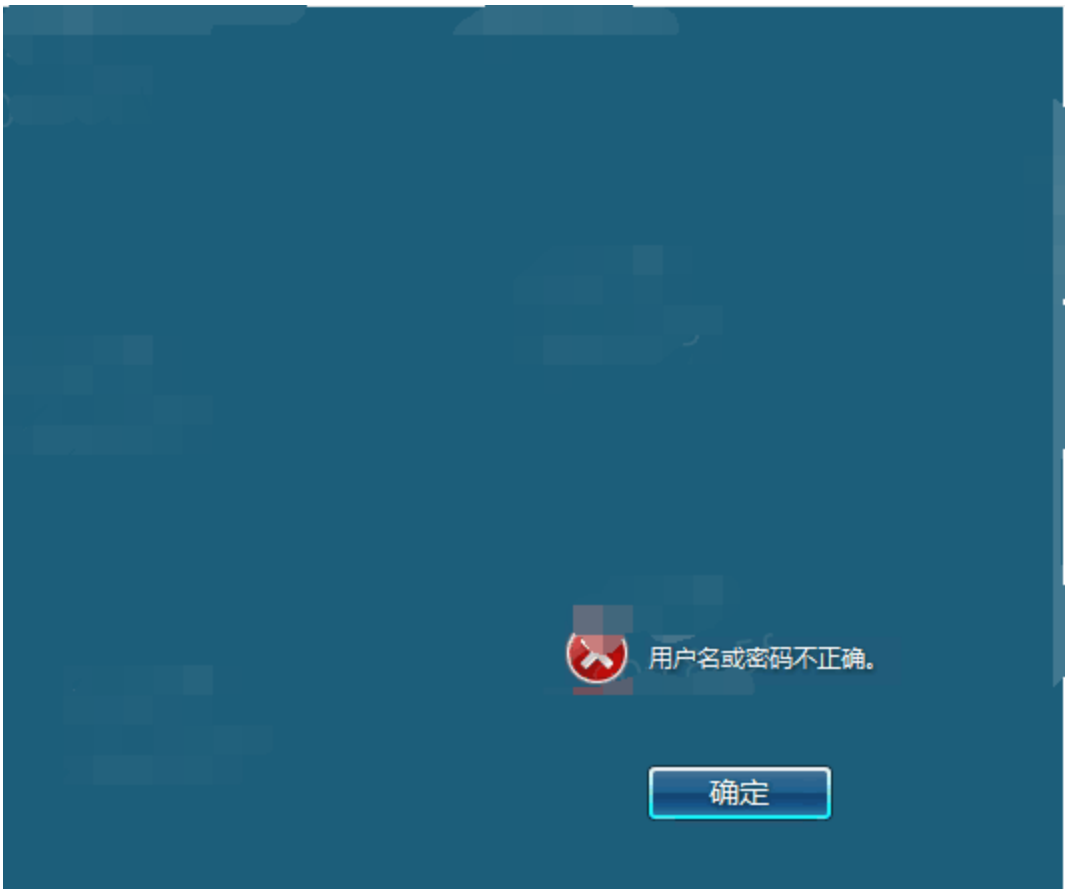


经过各种尝试，读取了大量系统敏感信息。但是对Getshell几乎无任何帮助。大强几乎要放弃了。此时，我盯着大强的电脑屏幕、发现他桌面放着1.txt、2.txt等等文件。真巧，我桌面也使用简单命名，放着一些重要的临时文件。灵机一动、是不是有不少人也为了图方便，在桌面存储一些不易记录的敏感信息。接着，我们直接对管理员桌面文件进行了fuzz。在一番尝试下，我们找到了111.txt、123.txt、pwd.txt临时文件。其中发现pwd.txt文件中存储着一些网址及对应的账号密码，以及一些零散的字符串，貌似像密码。此时我和大强笑出了鹅叫声，他叫嚣着要教管理员如何做人。

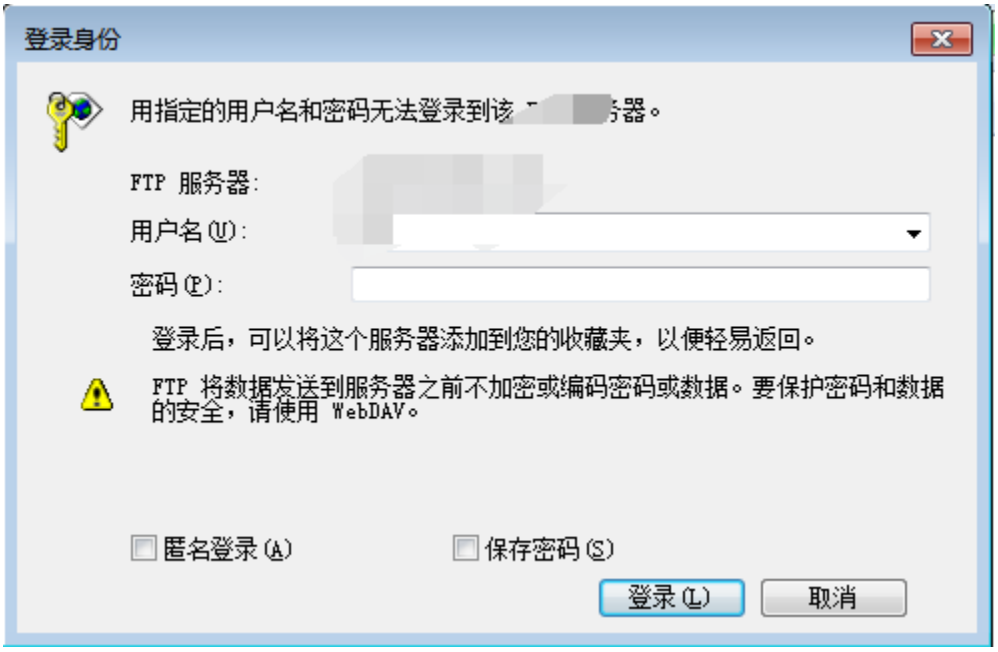


我和大强立即对这个目标主机进行了全端口服务扫描。发现这个主机开放着21、80、443、3389、6379、8080、8085、8086服务。我和大强盘算着，利用读到的6对账号密码中的某一个直接登入3389。怀着激动的心情，进行了一次又一次的尝试。然而画风是这样的：

进入3389失败。。。



进入ftp失败。。。

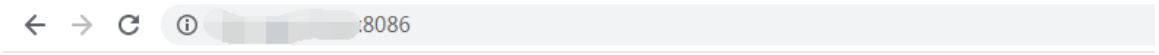


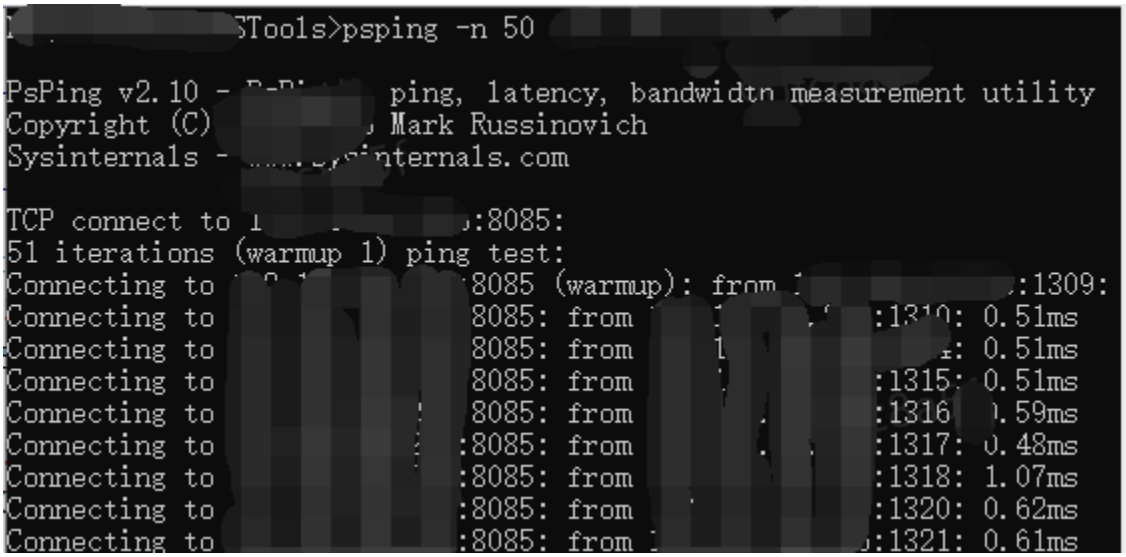
进入redis失败。。。

由于读取到的链接地址是内网系统，根本没有进入的机会。

.....

各种服务进入失败后，我们尝试进行了对3389、ftp等服务的爆破。仍然没有结果。我们对目标地址的8085和8086端口直接访问时，也没有任何服务直接展示。但是发现8085和8086服务连通性很不错。





我们通过度娘努力寻找着可能存在8085和8086默认端口的服务信息。但依然无所获。

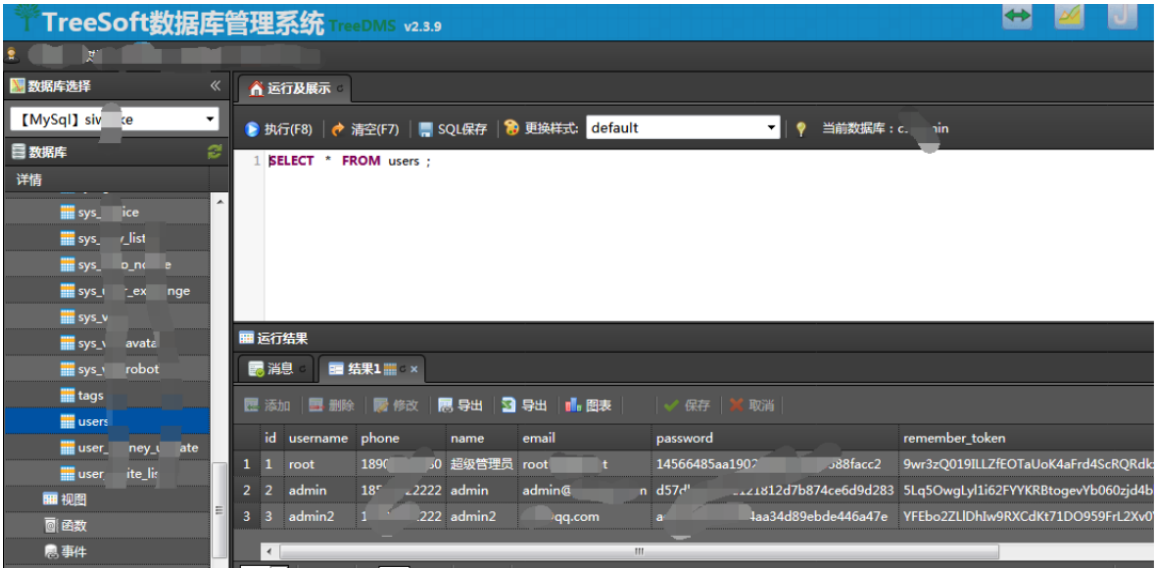
此刻，大强教管理员做人的叫嚣声也消失了。

等等，这不是结束，这样结束太草率了。我闭上眼，隐隐约约~仿佛好像在哪见过把这两个端口做默认端口的服务。经过大脑高速运转，以及一些残余的记忆。想起了多年以前遇到的treeNMS和treeDMS两个管理系统，默认端口就是8086和8085。经过验证，这次没让我和大强失望，就是这一对兄弟系统。我们利用通过XXE任意文件读取漏洞读取到的admin账号密码组合。首先成功的进入了treeNMS系统。

登录到treeNMS：

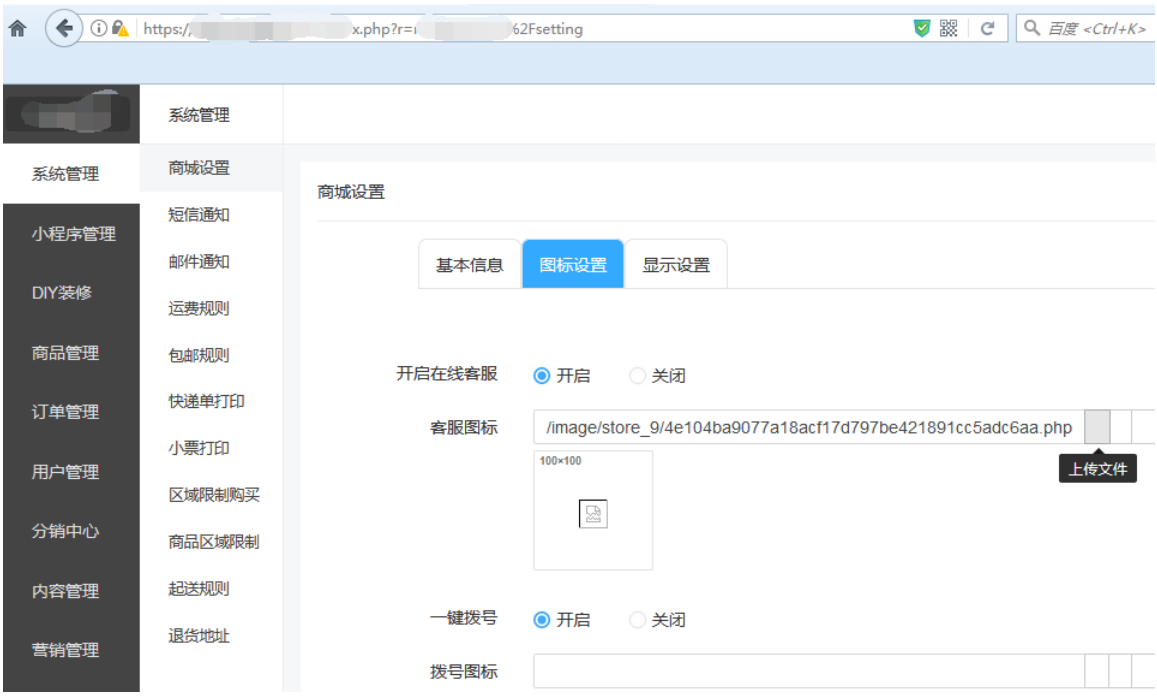
查看系统数据，What F**K,这个管理端是空的。Redis没有任何的信息。莫慌莫慌，还有DMS系统呢。怀着忐忑的心里继续尝试登入下一个。

登入treeDMS：

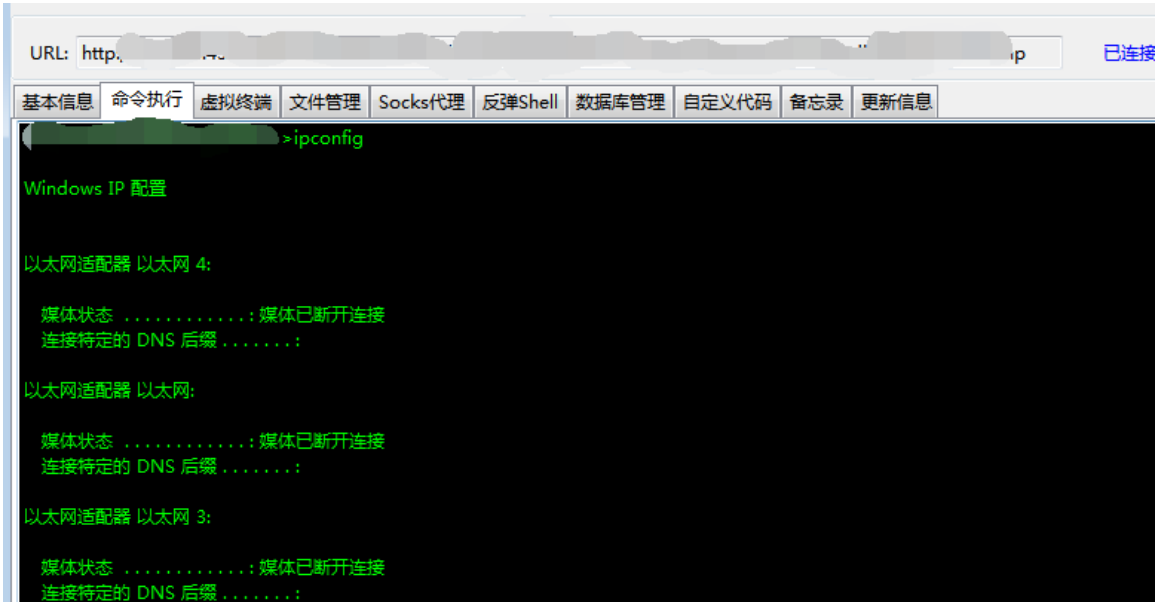


此刻心情是无比激动的，大强的叫嚣声又回来了。管理端一共有三个账户，密码是通过MD5存储的。经过反查，成功查到两个账号的密码。直接登入。看看能不能有所收获。

登入后台：



果然不出所料。这个商品管理后台系统还是比较脆弱的。对上传类型的文件没有做限制，我们通过图标设置模块，进行文件上传直接拿到了shell。当然内心的那份遗憾已经得到了很好的弥补。



本着一颗红心，既然进到了后台，并且在测试范围，我们在客户的授权下，对这个后台系统做了全面的漏洞挖掘。也挖到了不少的漏洞。我们在项目截止时间的最后一刻，完成了所有目标的测试工作

。交了一份比较完美的成果，也没有留下什么遗憾。虽然过程没有多么跌宕起伏，但还是值得我们总结。

总结

漏洞挖掘与利用的过程，不仅仅是挖到一个漏洞，就简单的利用该漏洞可能带来的直接效果。而是通过某一漏洞不断寻找，突破思维限制，在任何可以关联的事件中，寻找最大化的利用程度。为什么在漏洞挖掘与利用的过程中，你总是觉得别人都够能找到一些你找不到的突破口。这个问题可能是你知识面比较窄，但也可能是你的思维受到限制。所以，不要让惯性思维限制了你能力的进步。所以漏洞挖掘就是先拼技术能力，再拼思维。在技术达到某一程度后，思维决定了发展的高度。

精选留言

用户设置不下载评论