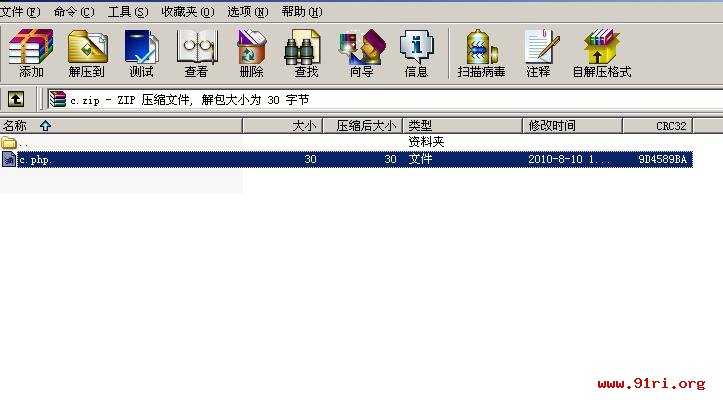
本来是搞一个站，linux+php+Sybaser。进后台后有上传，正常的在上传图片哪我是想尽了各种办法也没有突破，不过该站还有一种上传，看图1



但是把c.php放在压缩包里后它还会给你自动变成c.php.txt。这时我们可以用到rar的特性了。正常情况下，我们是没有办法在win下把c.php改名成”c.php.”,但是在压缩包里我们是可以这样改名的。看图2



改成这个名字后上传，该站php程序解压后自动就解压成了正常的c.php。

这个方法的意义在于，如果是这种方式上传， win下当然会自动去掉最后一个点，从而绕过系统的过滤。但是这个站是linux的，所以不知是系统的解压问题还是php的解压程序问题。

这种方法类似于抓包上传，在发包里的数据中将文件后缀加个点。但是在这个站上这个方法是不灵的，因为它是linux系统，linux可以把”c.php.”当成合格文件名。

至于这种上传解压的站，不知是否对zip包里的这种文件后缀加点的办法有防范呢？是系统的问题还是解压程序的问题，我是不深究了，反正是webshell上成功上传了。

本文来自: 网络安全攻防研究室(www.91ri.org) 请尊重作者，转载时带上版权信息。 详细内容请参考：http://www.91ri.org/3360.html