curl命令以及浏览器对文件路径遍历的阻断与保护

卡尔 / 2017-03-11 09:57:30 / 浏览数 2576 安全技术 技术讨论 顶(0) 踩(0)

---

一 .现象
在渗透测试过程中常有 http://www.xxx.com/../../../../../../etc/passwd 常有这种类型的攻击方式，但是在偶尔需要单独测试的时候使用浏览器或者curl命令并不能达到我们想要的效果，因为curl 还有浏览器从安全方面考虑 将这种url已经过滤了。
例如：

http://192.168.146.13:3001/../../../../../../../../../etc/passwd
就变成
http://192.168.146.13:3001/etc/passwd

比如文件遍历的漏洞确实存在

这时候使用curl命令

关键的../被截取了

使用浏览器

也是相同的现象

二 . 分析
不用多说，肯定是被curl和浏览器帮你做了安全过滤，防止你发出恶意请求
先来看curl的源码

curl 后期的版本 认为这种../ 是恶意的，根据/切割后检测具体路径的内容判别合法性。将其直接过滤掉了（详情可以比较7.29 和 7.54，7.29是可以使用的而 7.54 不行）

在来看浏览器，这里以chrome为例，将可以接受的字符都列在
const unsigned char kPathCharLookup[0x100] 这样一个数组中，最后对入参进行判断，符合合法输入字符。
对满足../类型的路径进行push，不会加入到发包的url value中，详情

因此chrome的话，如果输入http://www.xxx.com/../../../../../../../../../etc/passwd，然后copy，再粘贴(url)出来就会发现已经被过滤掉了

三 .总结
因此在自测或者初步测试的时候不建议通过浏览器或者curl，尤其是使用curl的时候一定要注意版本，如果版本较高的话很可能导致本应该发现的问题遗漏。
建议保持用python发送request,尽可能减少麻烦

点击收藏 | 0 关注 | 0
上一篇：域渗透基础简单信息收集（基础篇） 下一篇：60字节无文件渗透测试实验
1. 1 条回复

 紫霞仙子 2017-03-11 11:21:16

擦 ，我之前一直遇到这个问题，就是没研究过是啥原因，666.

0 回复Ta

---

登录 后跟帖

先知社区

---

现在登录

热门节点

技术文章

社区小黑板

目录