



K8哥哥

(/)



【教程】Ladon迷你WEB服务器/一键内网HTTP服务器

<% Visit 116 %>

前言

你是否在为配置浏览器漏洞测试环境而烦恼，如配置Apache解析某种MIME测试某个漏洞又或者在为内网机器无WEB又无法通过其它协议传输文件到内网另一台不出网的主机烦恼还有些远程命令不支持多条语句，需要多次写入或HTTP一次性下载过去，显然都会选后者

应用场景

- 1.浏览器oday漏洞测试或VPS上一键部署，无需安装配置Apache
- 2.内网HTTP协议文件传输，如内网目标不出网不允许其它协议通过
- 3.Office/Word/Pdf等漏洞或远程下载SCT、HTA等格式的CS Payload
- 4.IP追踪，在邮件里放任意URL，当目标查阅邮件时，可记录访问IP
- 5.系统探测，无论用于XSS或IP追踪都会记录UA，确认目标操作系统
- 6.出网探测，内网命令行访问VPS-WEB，看到IP证明可通过HTTP出网
- 7.远控问题，内网可访问WEB，HTTP不上线，就不要甩锅网络或WAF
写个txt放CMD命令或结果，内网访问txt，若正常说明WAF根本不拦

PS：第7点做点修改就可以得到简单的HTTP马了类似CS，读取TXT获取CMD命令，然后执行。

WebSer启动

- 1 Ladon web 80
- 2 Ladon webser 80



运行权限

使用TCP SOCKET实现的HTTP服务器，任意权限下都可以，不像HTTPListen需管理员权限
很多人常说TCPListen和HTTPListen有什么区别，都可以实现一模一样的WEB服务器
但权限不一样，实现过程也不一样，就像不同快递，包装材料不一样，送达时间也不一样
直接使用HTTP不需要自己构造协议包，而使用TCP得自己构造HTTP包，这就是区别之一

文件下载

在Ladon同目录下放你想下载的文件，浏览器访问即可，命令行下载也可以

Linux: Wget、curl等

Windows: 10几20多种，自行去网上搜索

工具下载

最新版本: <https://k8gege.org/Download/Ladon.rar> (<https://k8gege.org/Download/Ladon.rar>)

历史版本: <https://github.com/k8gege/Ladon/releases> (<https://github.com/k8gege/Ladon/releases>)