Substr 函数助你免杀 php 脚本（异类思路）

主旨：主要利用 substr 函数和 url 编解码

1】安全狗：

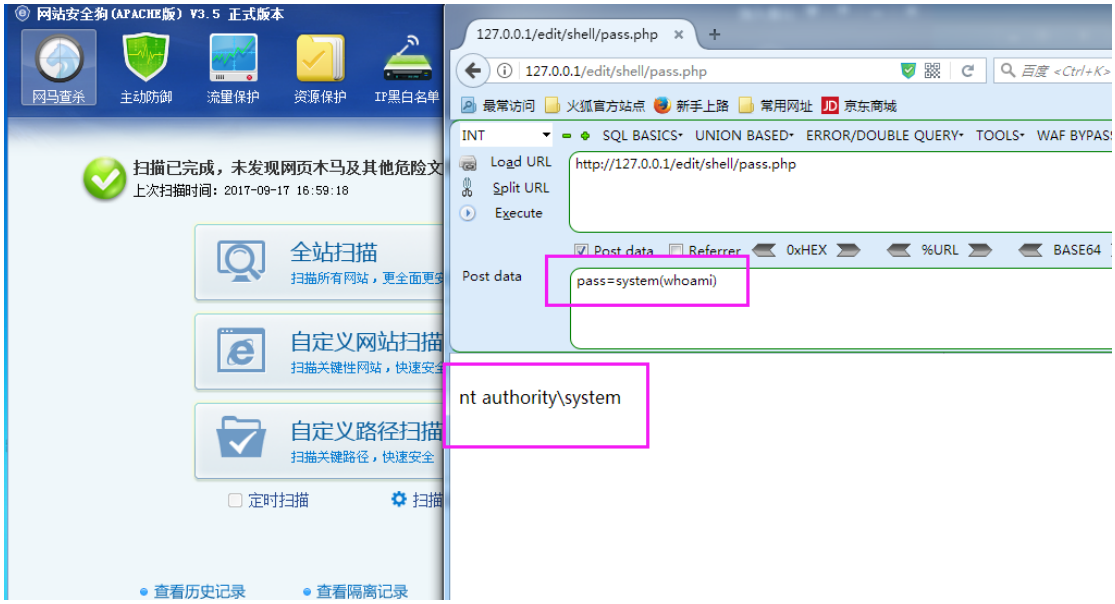
新研究的 php 脚本木马：最新版安全狗扫描如下：

成功看到：扫描已完成，未发现网页木马以及其他威胁（开心吗，战友们~）

最新版安全狗信息：

使用截图：来一个 phpinfo()试试效果>>

刺激吧。再试试 whoami >>

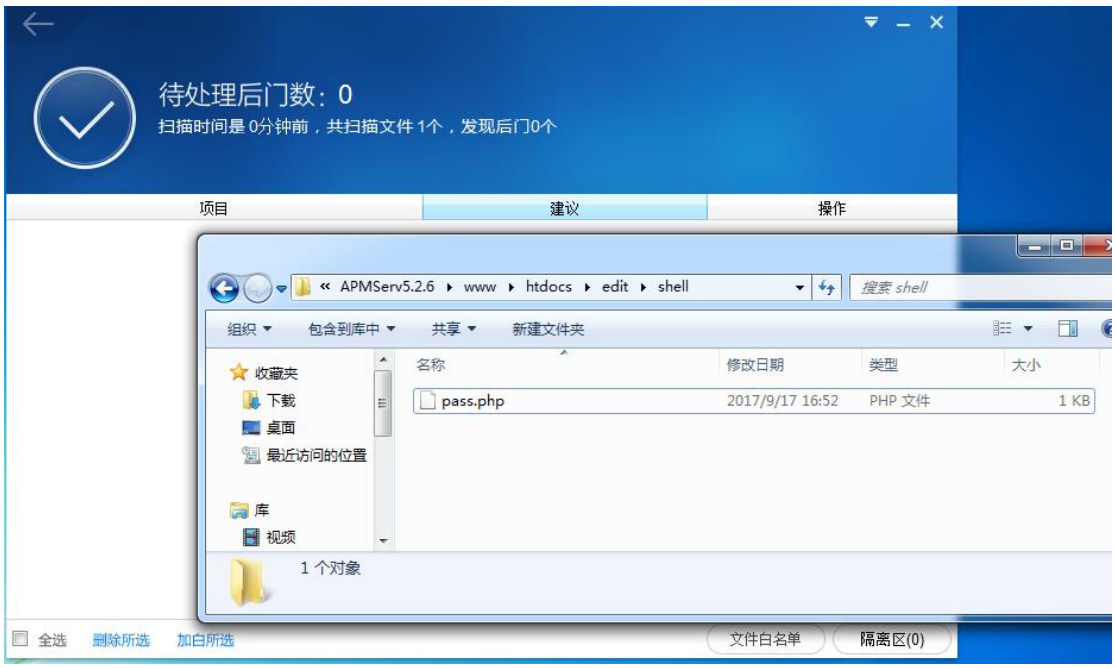


那么 ipconfig 更是可以了>>

别太开心了，战友们，下面还有更刺激的，用 360 网站卫士走一波：

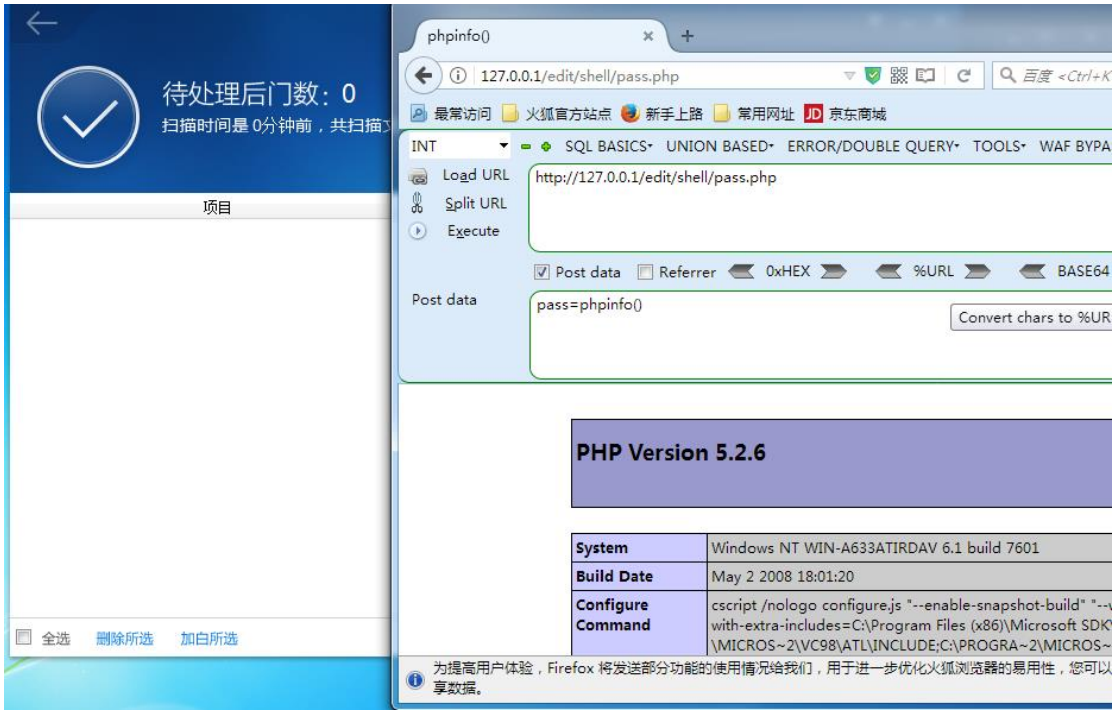
2】360 网站卫士：

直接打开 360 网站卫士，后门查杀扫描一下：



Oh，No，没有检测出来，不过这很正常，完美与性能不能同时具备。

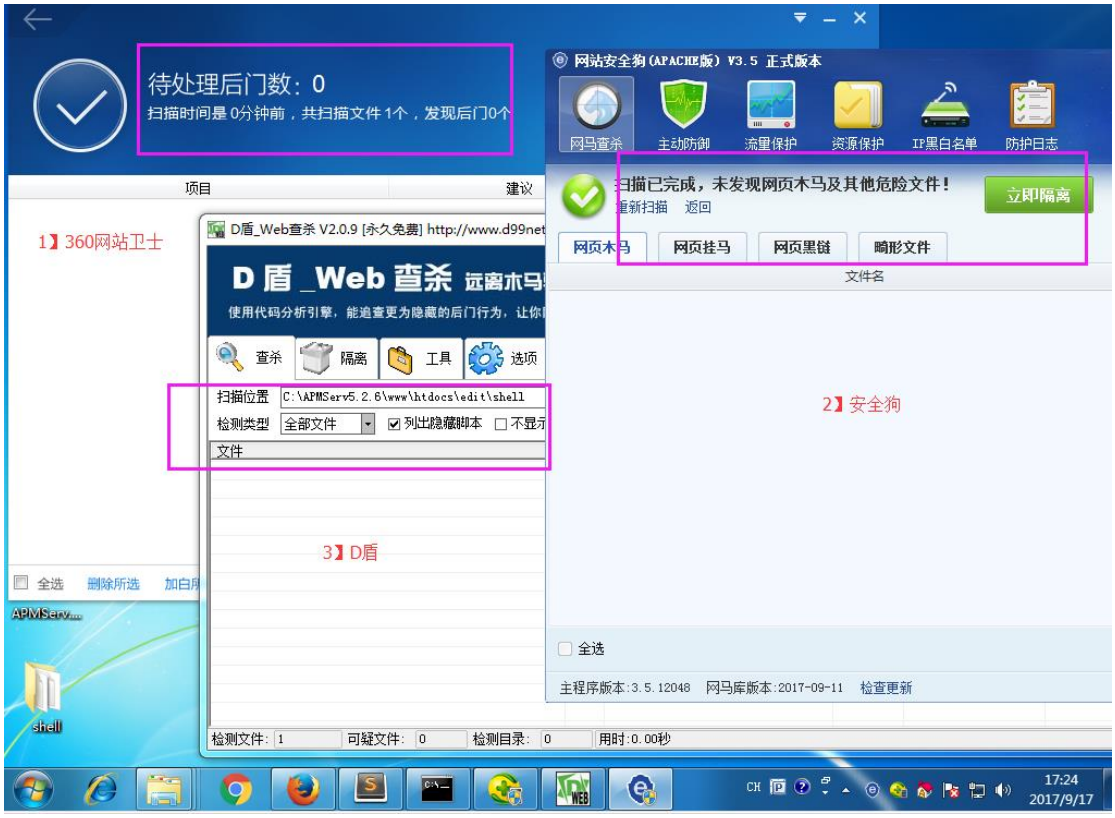
使用看：



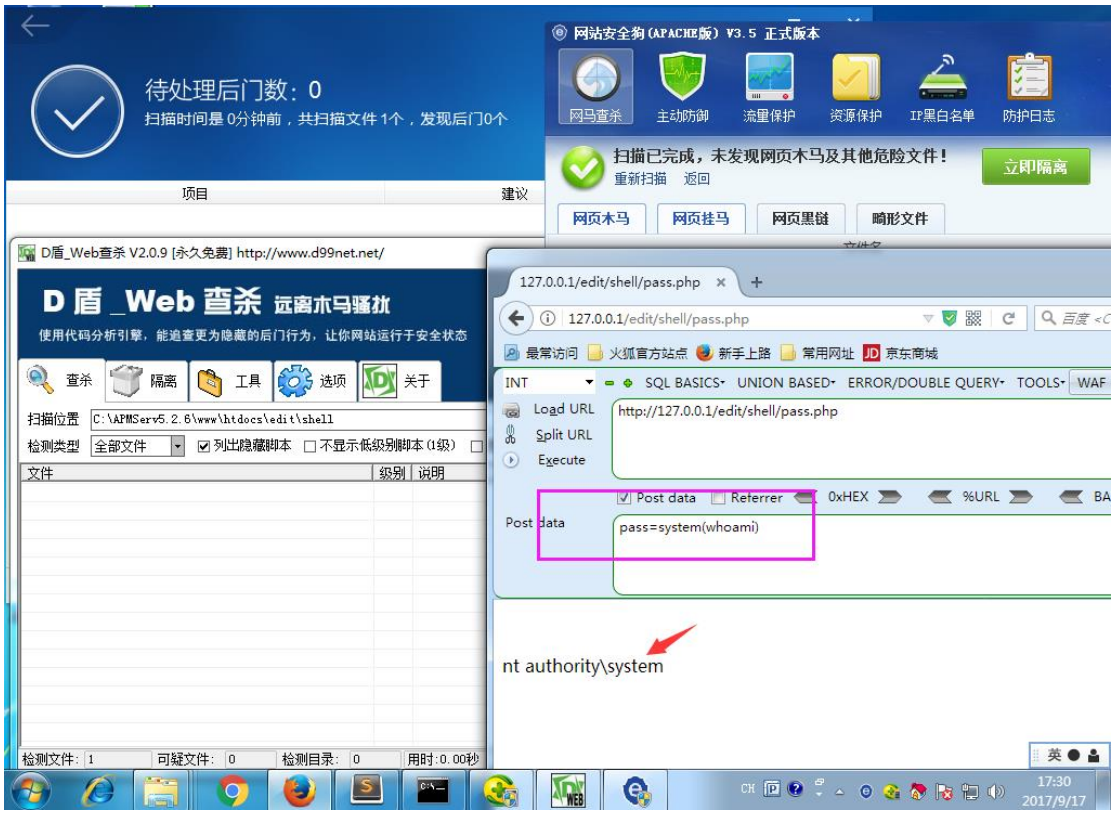
正常使用。

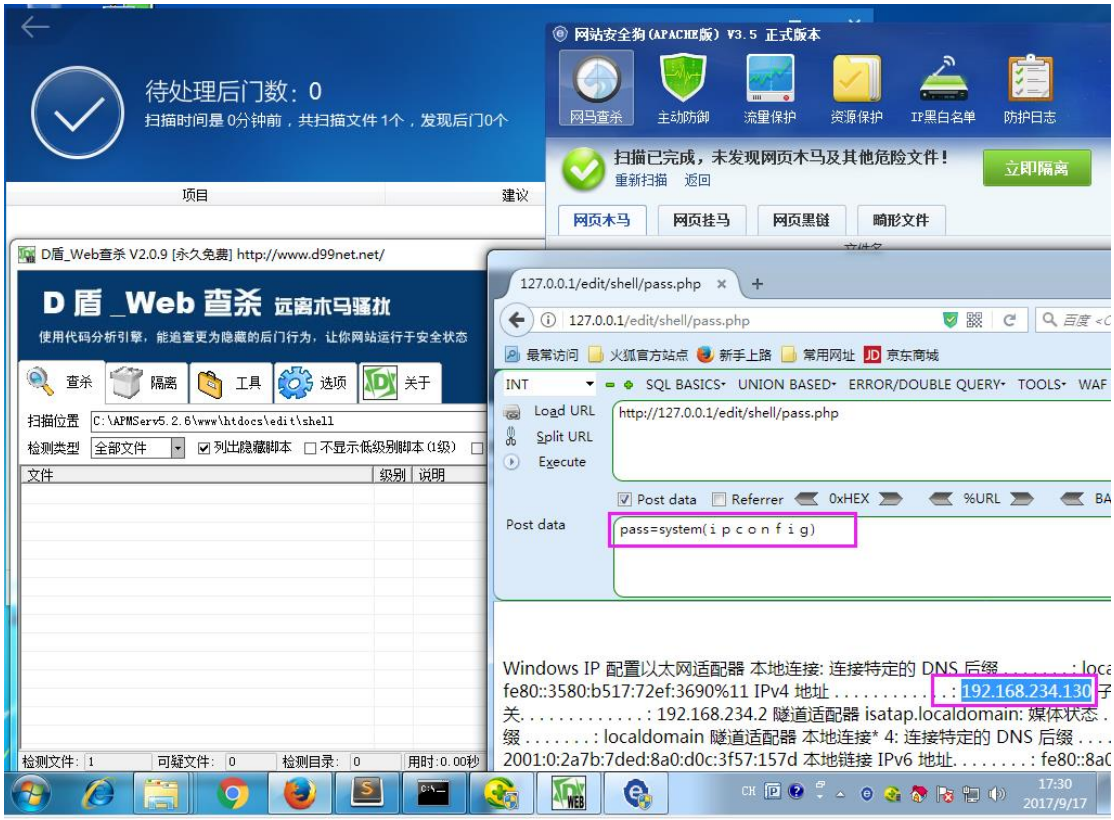
不说太多客套话了，直接上重点吧，是讲重点，大家都爱听。

上一张图：**360 网站卫士、安全狗、D 盾同时安装在服务器上，都扫描一下网站目录，均没有报警！！**

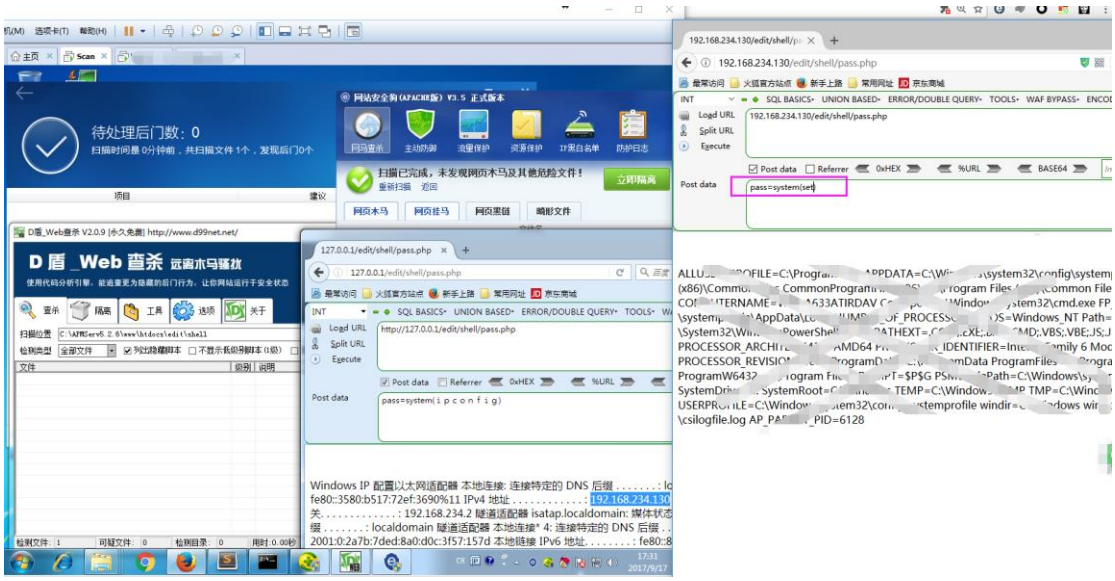

待处理后门数：0
扫描时间是 0分钟前，共扫描文件 1个，发现后门0个
网站安全狗（APACHE版）V3.5 正式版本
网马查杀
主动防御
流量保护
资源保护
IP黑白名单
防护日志
扫描已完成，未发现网页木马及其他危险文件！
重新扫描
返回
立即隔离
网页木马
网页挂马
网页黑链
畸形文件
文件名
项目
建议
1】360网站卫士
D盾_Web查杀 V2.0.9 [永久免费] http://www.d99net
D 盾 _Web 查杀
使用代码分析引擎，能追查更为隐藏的后门行为，让你
查杀
隔离
工具
选项
扫描位置
C:\APMServ5.2.6\www\htdocs\edit\shell
检测类型
全部文件
列出隐藏脚本
文件
2】安全狗
3】D盾
全选
删除所选
主程序版本:3.5.12048
网马库版本:2017-09-11
检查更新
检测文件: 1
可疑文件: 0
检测目录: 0
用时:0.00秒
shell
17:24
2017/9/17

访问脚本：


待处理后门数：0
扫描时间是 0分钟前，共扫描文件 1个，发现后门0个
网站安全狗（APACHE版）V3.5 正式版本
扫描已完成，未发现网页木马及其他危险文件！
重新扫描
返回
立即隔离
网页木马
网页挂马
网页黑链
畸形文件
项目
建议
D盾_Web查杀 V2.0.9 [永久免费] http://www.d99net.net/
D 盾 _Web 查杀 远离木马骚扰
使用代码分析引擎，能追查更为隐藏的后门行为，让你网站运行于安全状态
查杀
隔离
工具
选项
关于
扫描位置
C:\APMServ5.2.6\www\htdocs\edit\shell
检测类型
全部文件
列出隐藏脚本
不显示低级别脚本(1级)
文件
级别
说明
127.0.0.1/edit/shell/pass.php
最常访问
火狐官方站点
新手上路
常用网址
京东商城
INT
SQL BASICS
UNION BASED
ERROR/DOUBLE QUERY
TOOLS
WAF
Load URL
Split URL
Execute
http://127.0.0.1/edit/shell/pass.php
Post data
Referrer
0xHEX
%URL
Post data
pass=system(whoami)
nt authority\system
检测文件: 1
可疑文件: 0
检测目录: 0
用时:0.00秒
17:30
2017/9/17



在外面访问试试：



好了，本次研究到此结束，大家改动需要谨慎，放大你的脑洞。

参考文章：

http://blog.csdn.net/shaobingj126/article/details/6318749

其他思路：

可考虑 url 多次编码解码、chr()、base64_encode()和 base64_decode()、rawurlencode()与 rawurldecode();等