

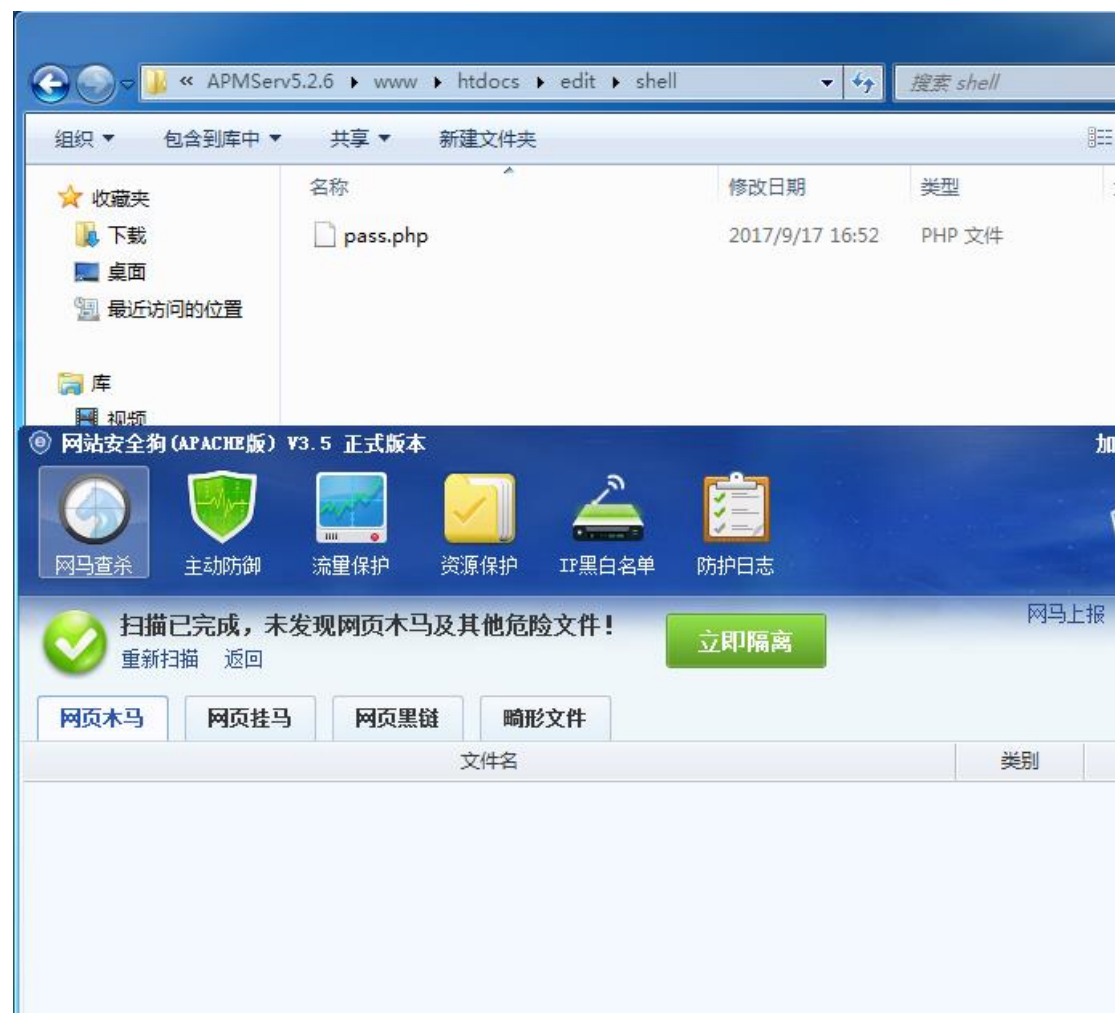
# Substr 函数助你免杀 php 脚本（异类思路）

本文原创作者：Laimooc(原名 xoanHn)，本文属 i 春秋原创奖励计划，未经许可禁止转载

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：

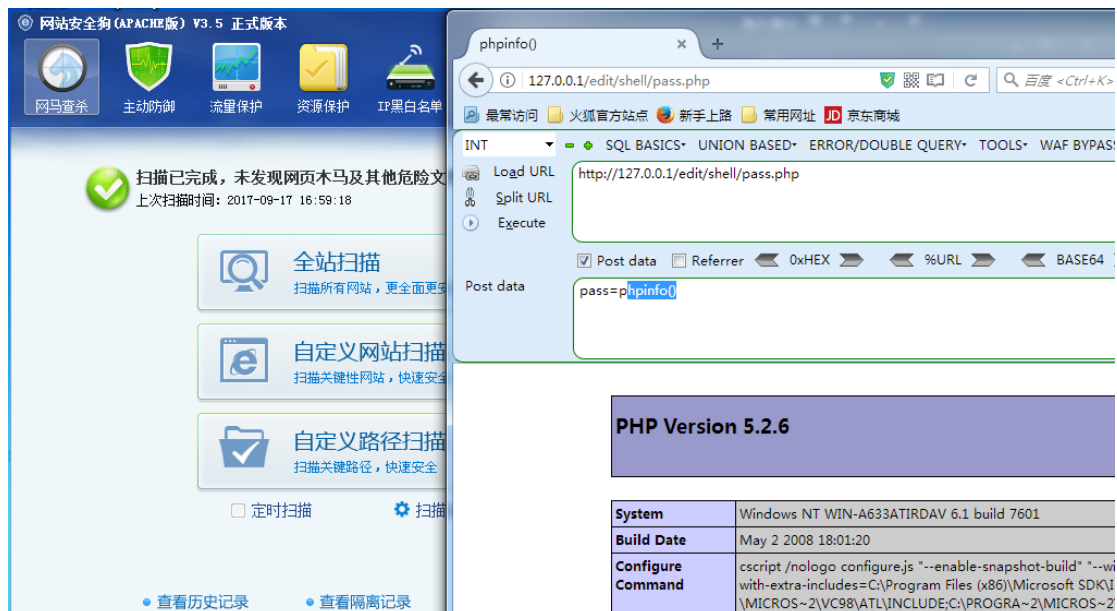


成功看到：扫描已完成，未发现网页木马以及其他威胁（开心吗，战友们~）

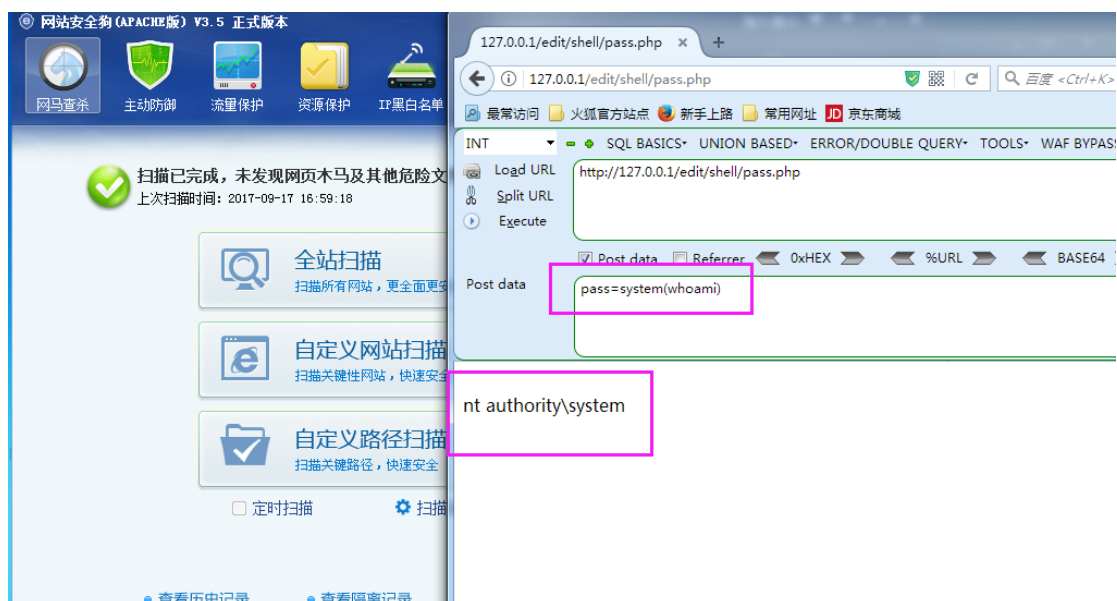
最新版安全狗信息：



使用截图：来一个 phpinfo()试试效果>>



刺激吧。再试试 whoami >>



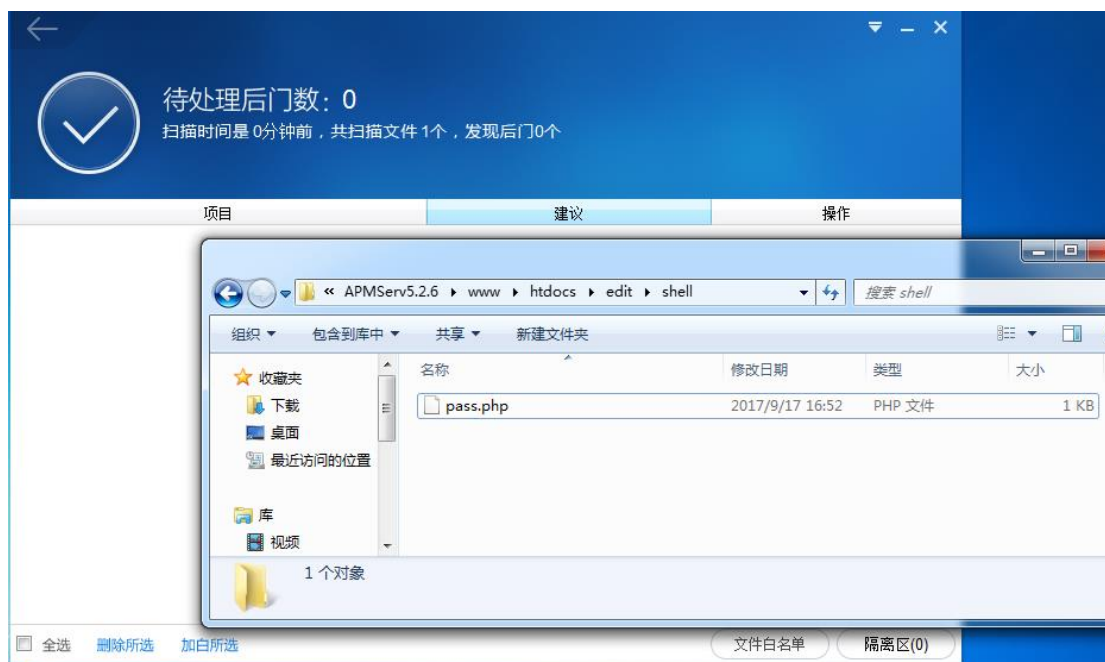
那么 ipconfig 更是可以了>>



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：

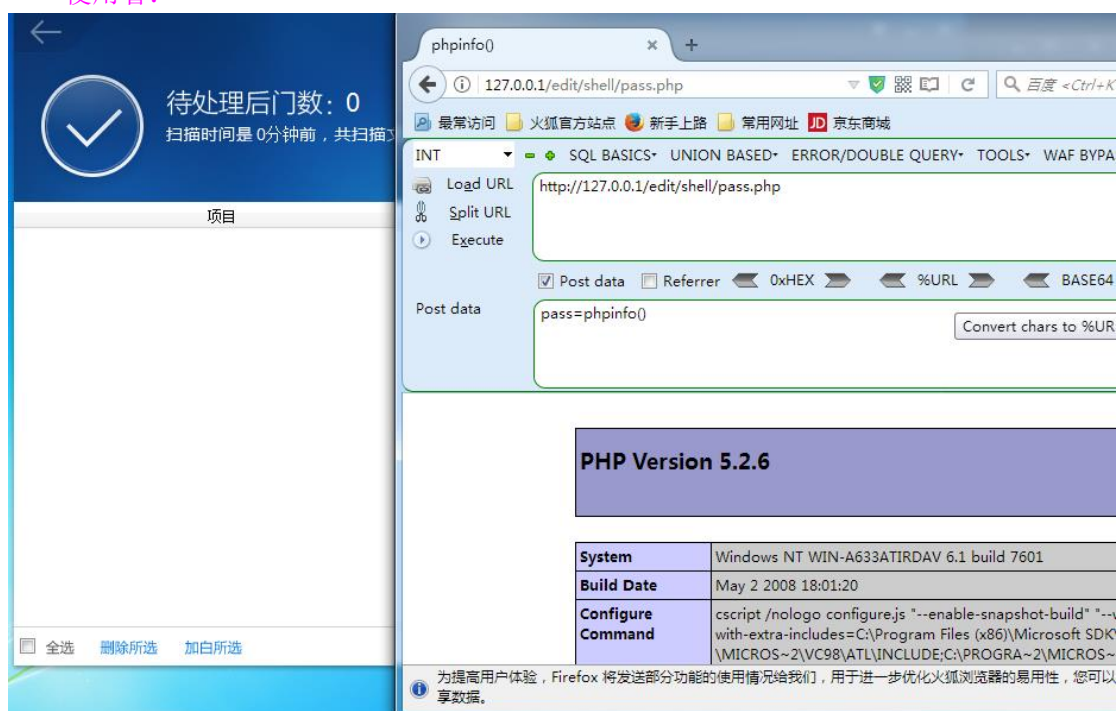
## 2】360 网站卫士：

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。

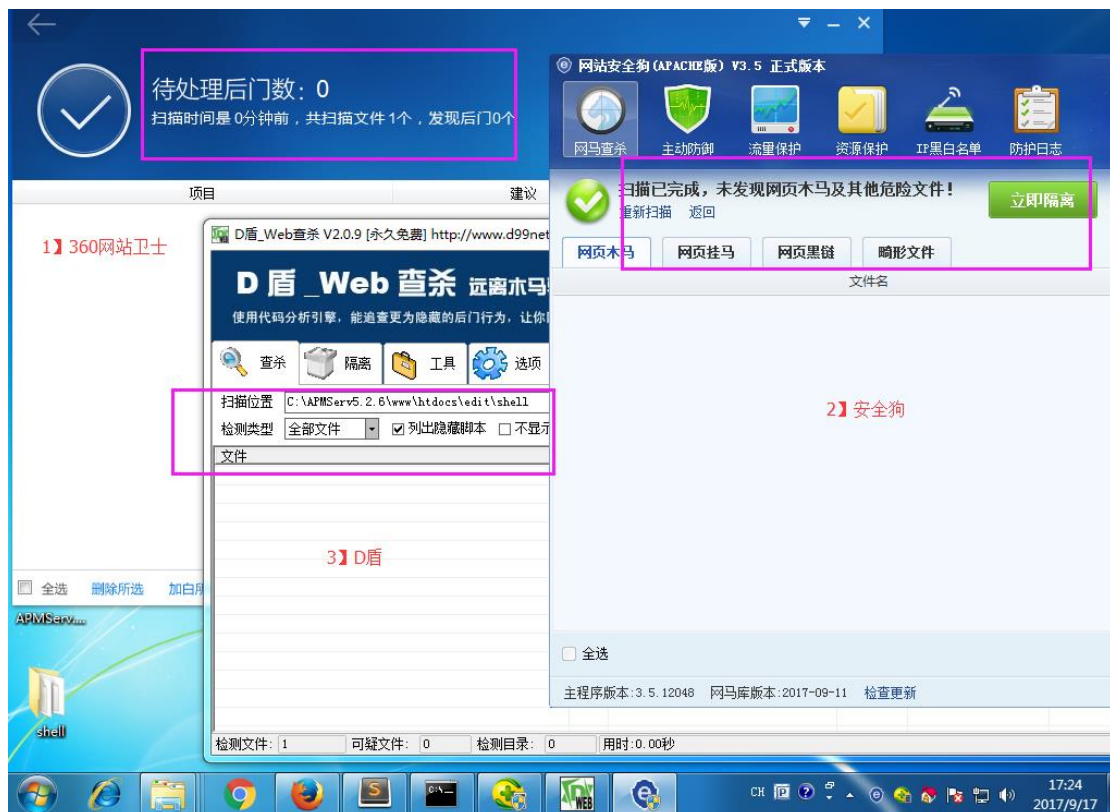
使用看:



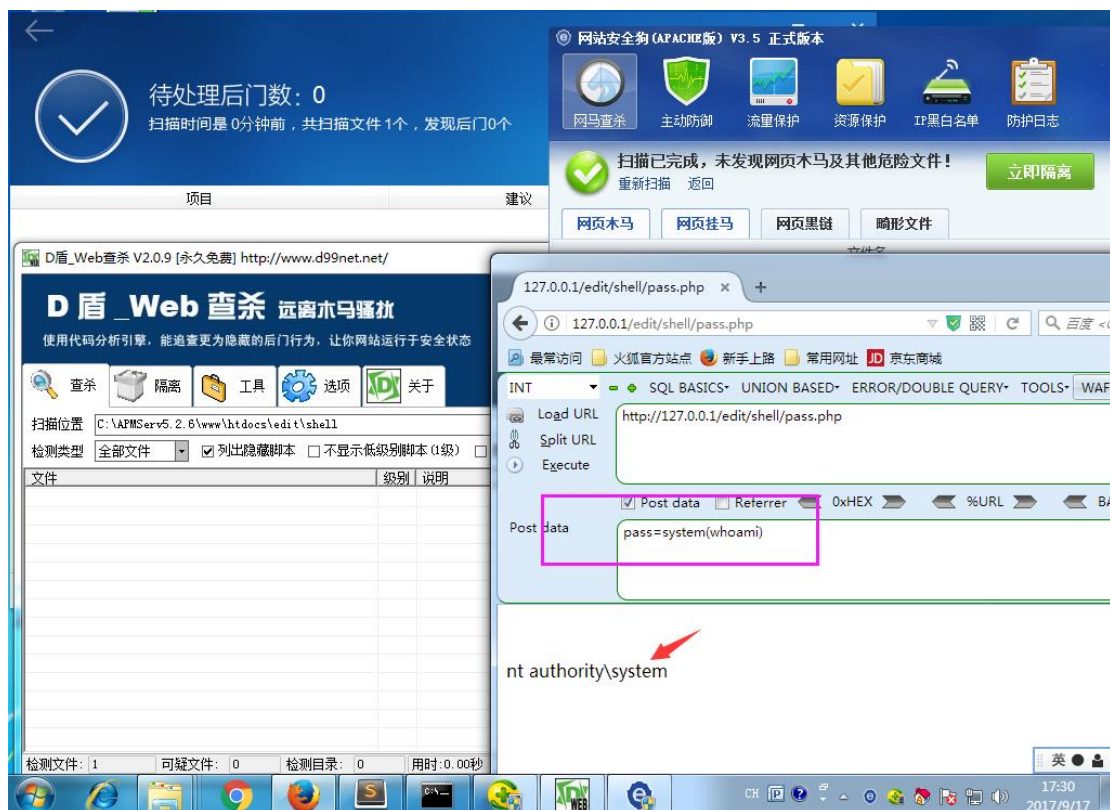
正常使用。

不说太多客套话了, 直接上重点吧, 是讲重点, 大家都爱听。

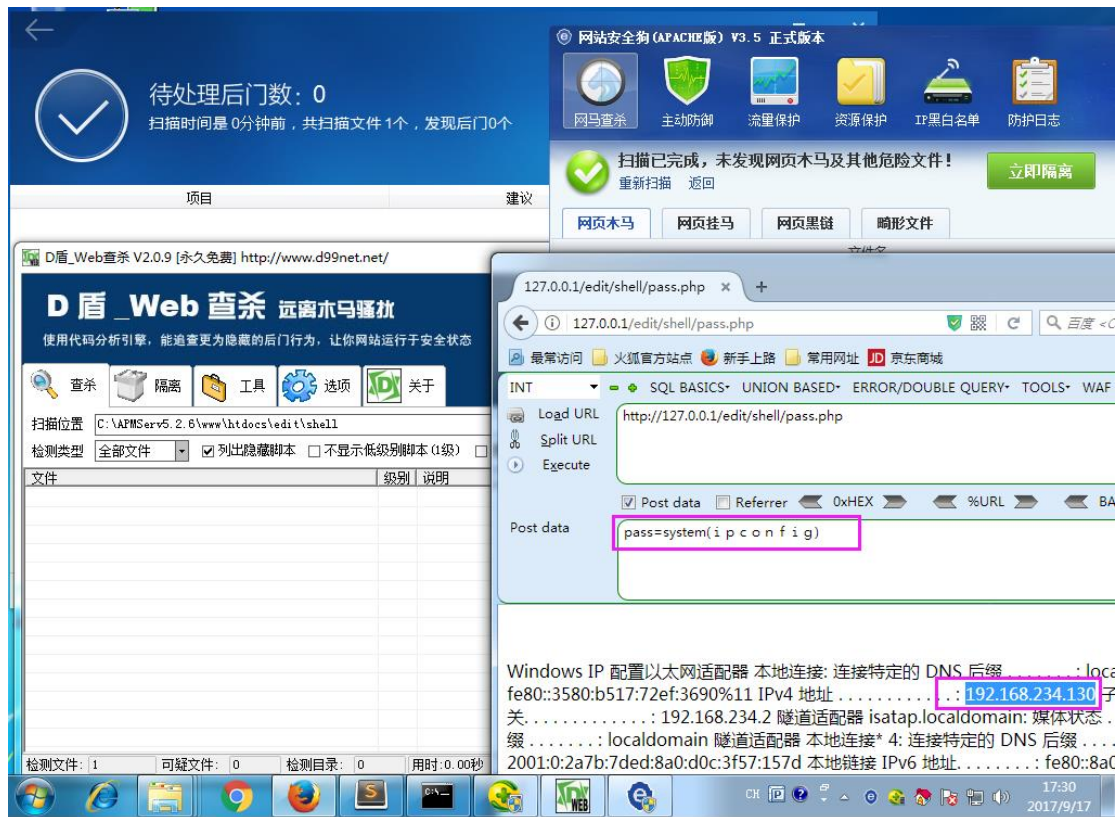
上一张图: 360 网站卫士、安全狗、D 盾同时安装在服务器上, 都扫描一下网站目录, 均没有报警!!



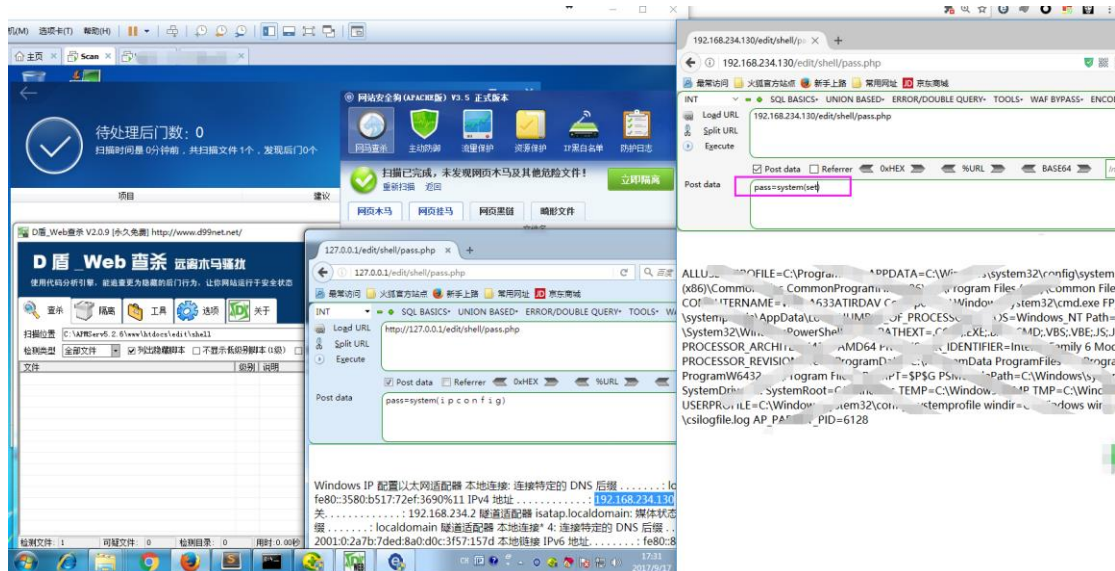
访问脚本:







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/shaobing126/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

I 春秋地址: <https://bbs.ichunqiu.com/thread-27138-1-1.html>