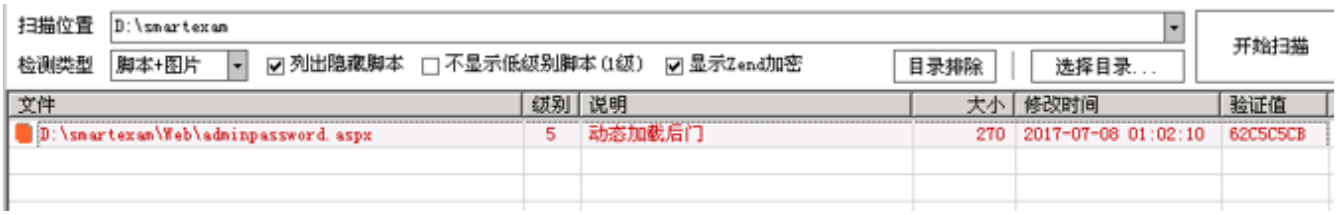
第1篇：网站被植入Webshell

网站被植入webshell，意味着网站存在可利用的高危漏洞，攻击者通过利用漏洞入侵网站，写入webshell接管网站的控制权。为了得到权限，常规的手段如：前后台任意文件上传，远程命令执行，Sql注入写入文件等。

现象描述

网站管理员在站点目录下发现存在webshell，于是开始了对入侵过程展开了分析。



Webshell查杀工具：

D盾_Web查杀 Window下webshell查杀：http://www.d99net.net/index.asp

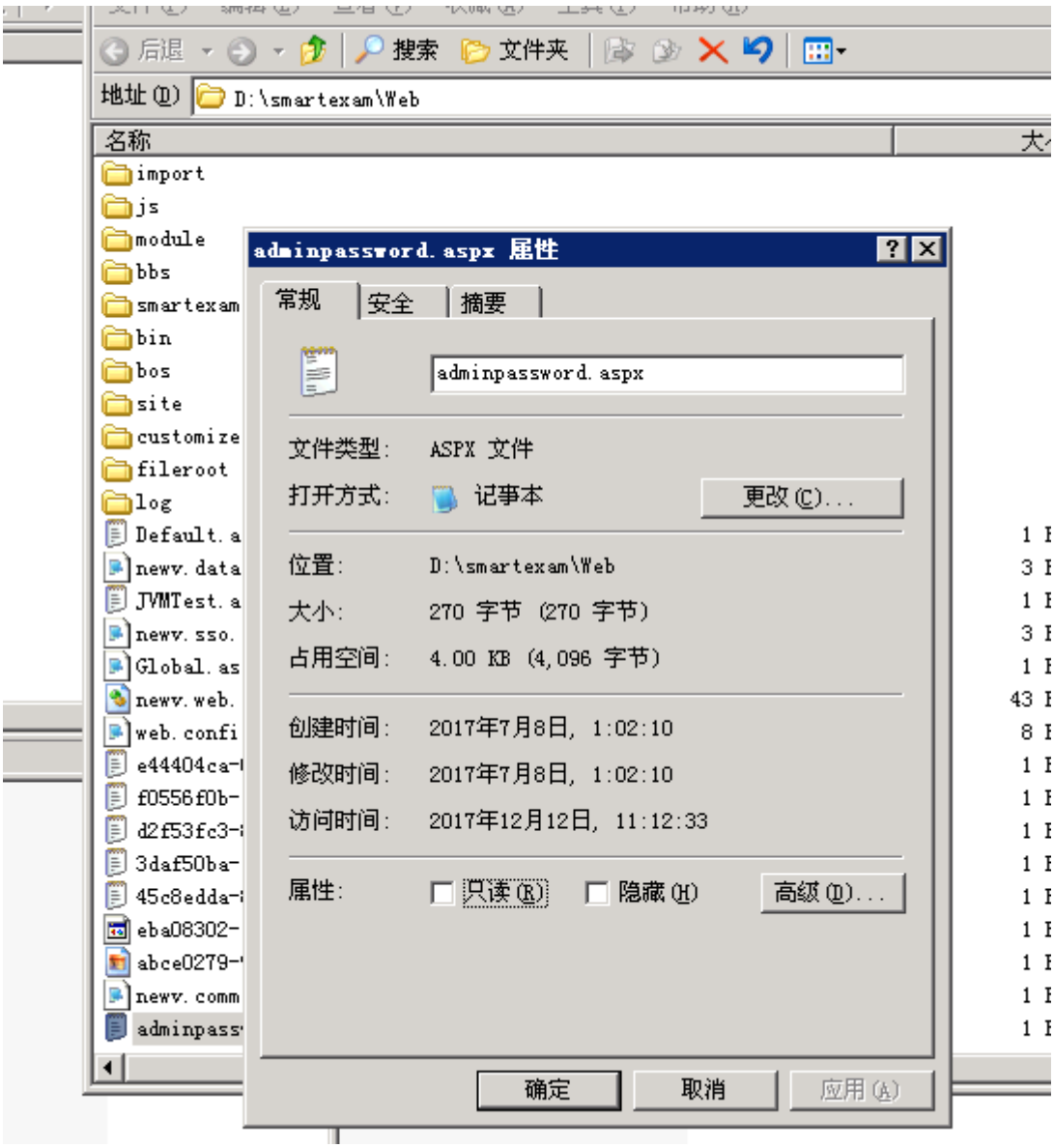
河马：支持多平台，但是需要联网环境。

使用方法: wget http://down.shellpub.com/hm/latest/hm-linux-amd64.tgz tar xvf hm-linux-amd64.tgz hm scan /www

事件分析

1、 定位时间范围

通过发现的webshell文件创建时间点，去翻看相关日期的访问日志。



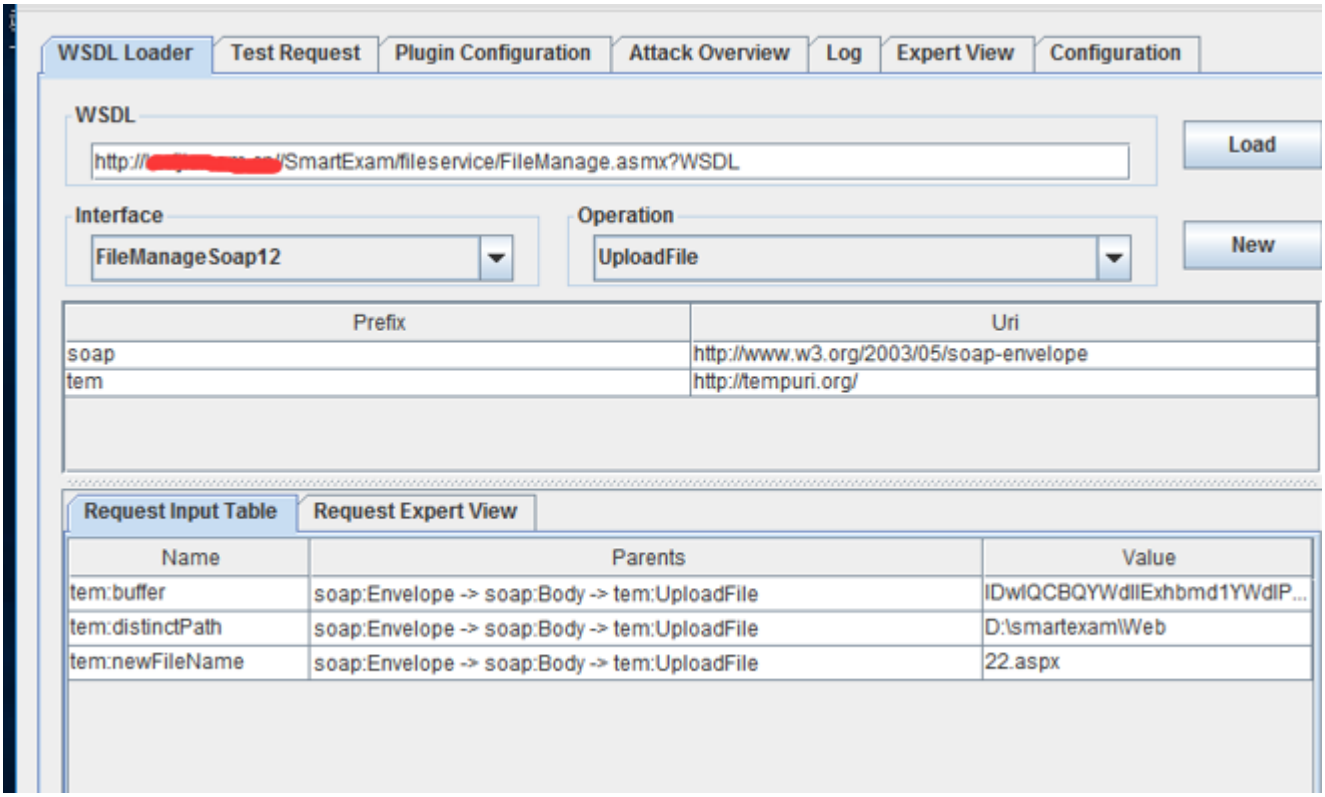
2、Web 日志分析

经过日志分析，在文件创建的时间节点并未发现可疑的上传，但发现存在可疑的webservice接口

```
2017-07-07 17:01:49 210.[redacted].53 POST /SmartExam/fileservice/FileManage.asmx - 80 - 10.16.65.4 Mozilla/4.0+(compa
2017-07-07 17:01:57 210.[redacted].53 POST /SmartExam/fileservice/FileManage.asmx - 80 - 10.16.65.4 Mozilla/4.0+(compa
2017-07-07 17:02:05 210.[redacted].53 POST /SmartExam/fileservice/FileManage.asmx - 80 - 10.16.65.4 Mozilla/4.0+(compa
```

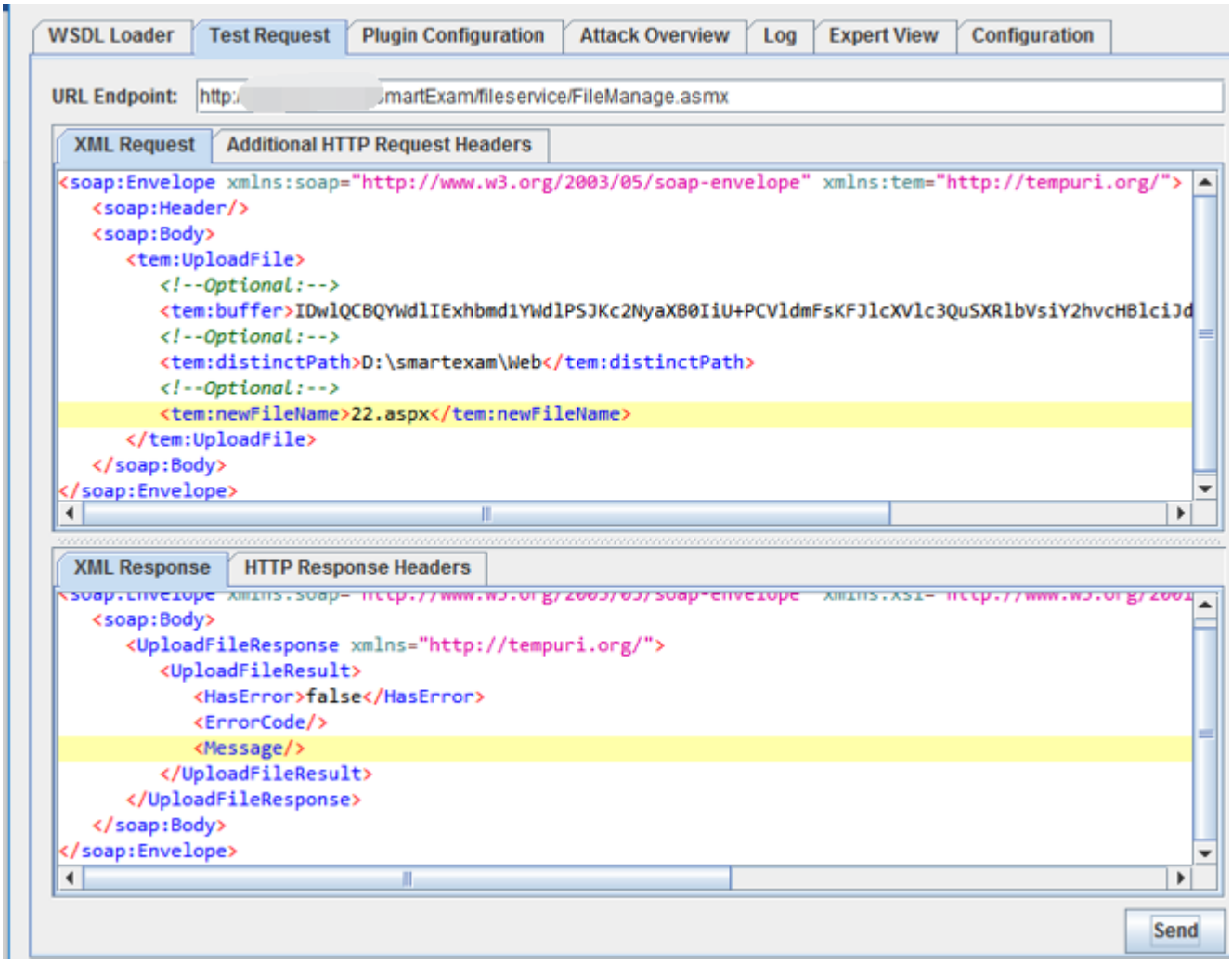
3、漏洞分析

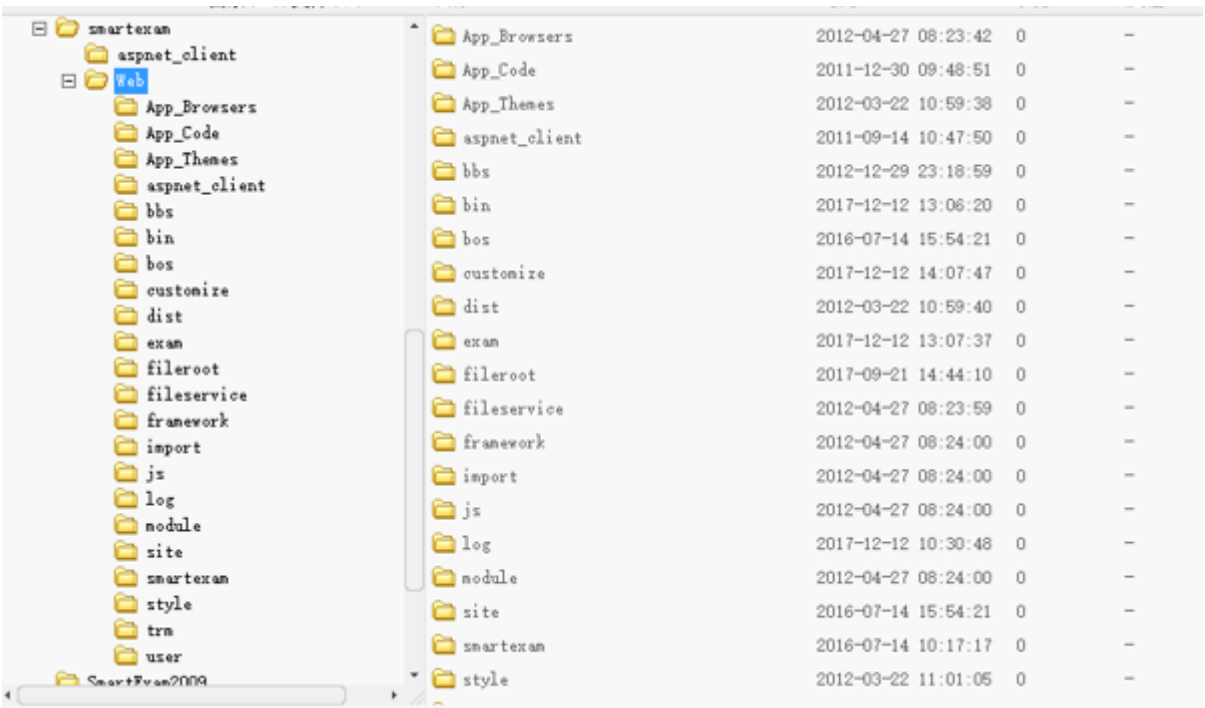
访问webservice接口，发现变量：buffer、distinctpach、newfilename可以在客户端自定义



4、漏洞复现

尝试对漏洞进行复现，可成功上传webshell，控制网站服务器





5、漏洞修复

清除webshell并对webservice接口进行代码修复。

从发现webshell到日志分析，再到漏洞复现和修复，本文暂不涉及溯源取证方面。

后续持续更新内容，将发布在公众号Bypass--，同时公众号提供了该项目的PDF版本，关注后回复"应急响应" 即可下载。