

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。

扫描位置	D:\smartercan					开始扫描
检测类型	脚本+图片	<input checked="" type="checkbox"/> 列出隐藏脚本	<input type="checkbox"/> 不显示低级别脚本(1级)	<input checked="" type="checkbox"/> 显示Zend加密	目录排除	选择目录...
文件	级别	说明	大小	修改时间	验证值	
D:\smartercan\Web\adminpassword.aspx	5	动态加载后门	270	2017-07-08 01:02:10	62C5C5CB	

Webshell查杀工具：

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

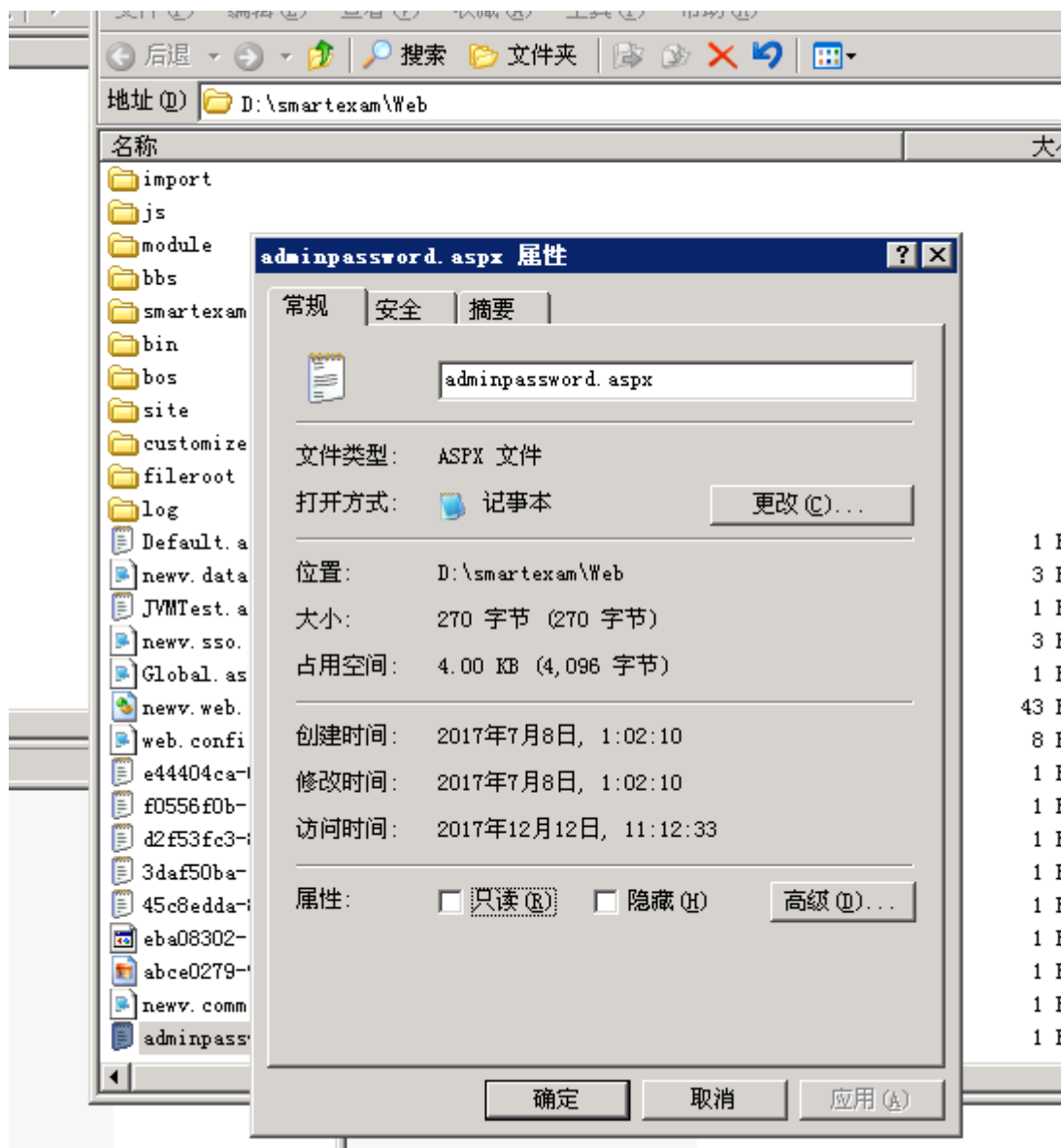
河马：支持多平台，但是需要联网环境。

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

WSDL Loader
Test Request
Plugin Configuration
Attack Overview
Log
Expert View
Configuration

WSDL
Load

Interface
FileManage Soap12
Operation
UploadFile
New

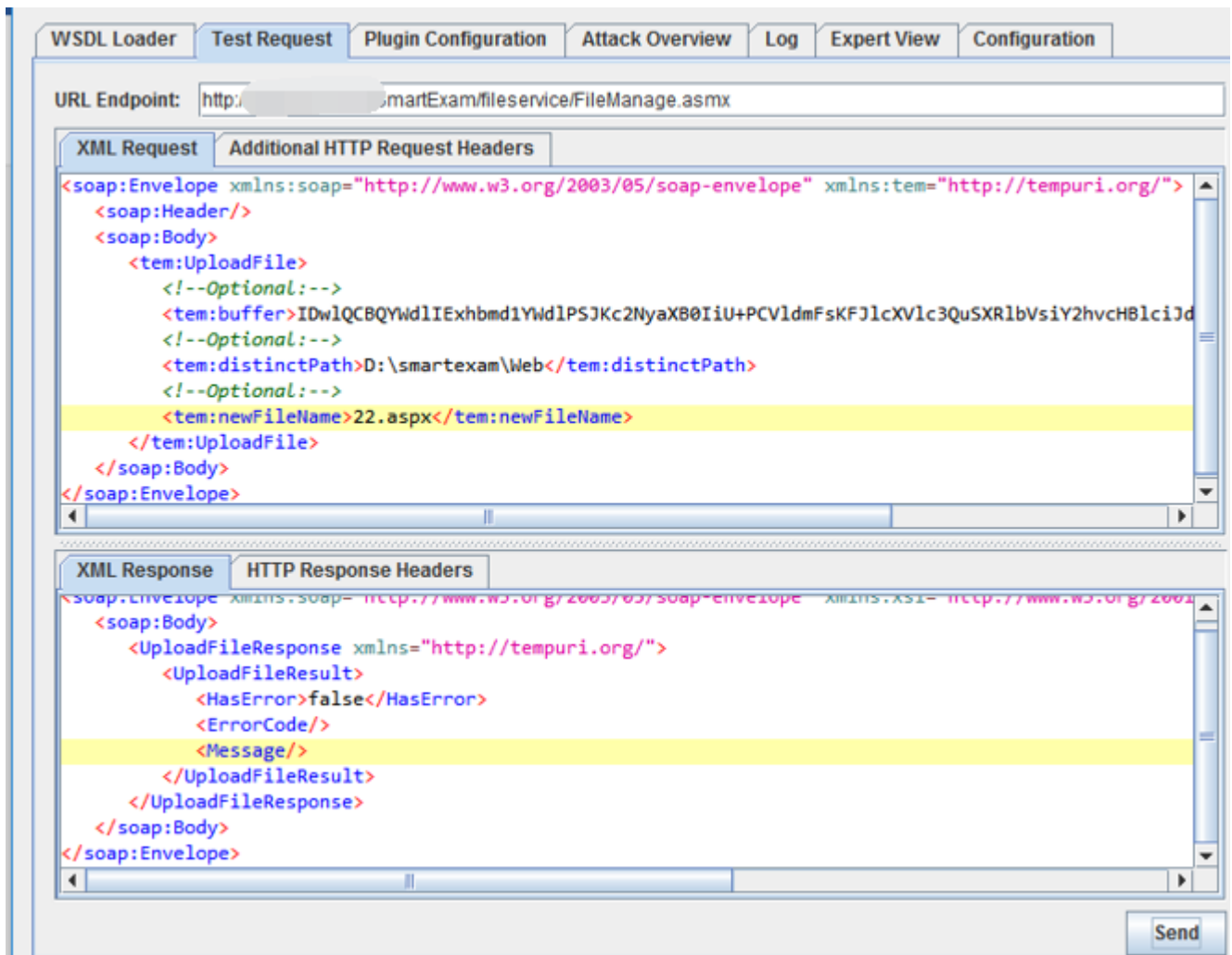
Prefix	Uri
soap	http://www.w3.org/2003/05/soap-envelope
tem	http://tempuri.org/

Request Input Table
Request Expert View

Name	Parents	Value
tem:buffer	soap:Envelope -> soap:Body -> tem:UploadFile	IDwIQCBQYWdIIExhbmd1YWdlP...
tem:distinctPath	soap:Envelope -> soap:Body -> tem:UploadFile	D:\smartexam\Web
tem:newFileName	soap:Envelope -> soap:Body -> tem:UploadFile	22.aspx

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



smartexam	App_Browsers	2012-04-27 08:23:42	0	-
aspnet_client	App_Code	2011-12-30 09:48:51	0	-
Web	App_Themes	2012-03-22 10:59:38	0	-
App_Browsers	aspnet_client	2011-09-14 10:47:50	0	-
App_Code	bbs	2012-12-29 23:18:59	0	-
App_Themes	bin	2017-12-12 13:06:20	0	-
aspnet_client	bos	2016-07-14 15:54:21	0	-
bbs	customize	2017-12-12 14:07:47	0	-
bin	dist	2012-03-22 10:59:40	0	-
bos	exam	2017-12-12 13:07:37	0	-
customize	fileroot	2017-09-21 14:44:10	0	-
dist	fileservice	2012-04-27 08:23:59	0	-
exam	framework	2012-04-27 08:24:00	0	-
fileroot	import	2012-04-27 08:24:00	0	-
fileservice	js	2012-04-27 08:24:00	0	-
framework	log	2017-12-12 10:30:48	0	-
import	module	2012-04-27 08:24:00	0	-
js	site	2016-07-14 15:54:21	0	-
log	smartexam	2016-07-14 10:17:17	0	-
module	style	2012-03-22 11:01:05	0	-
site				
smartexam				
style				
trn				
user				
SmartExam2009				

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。

