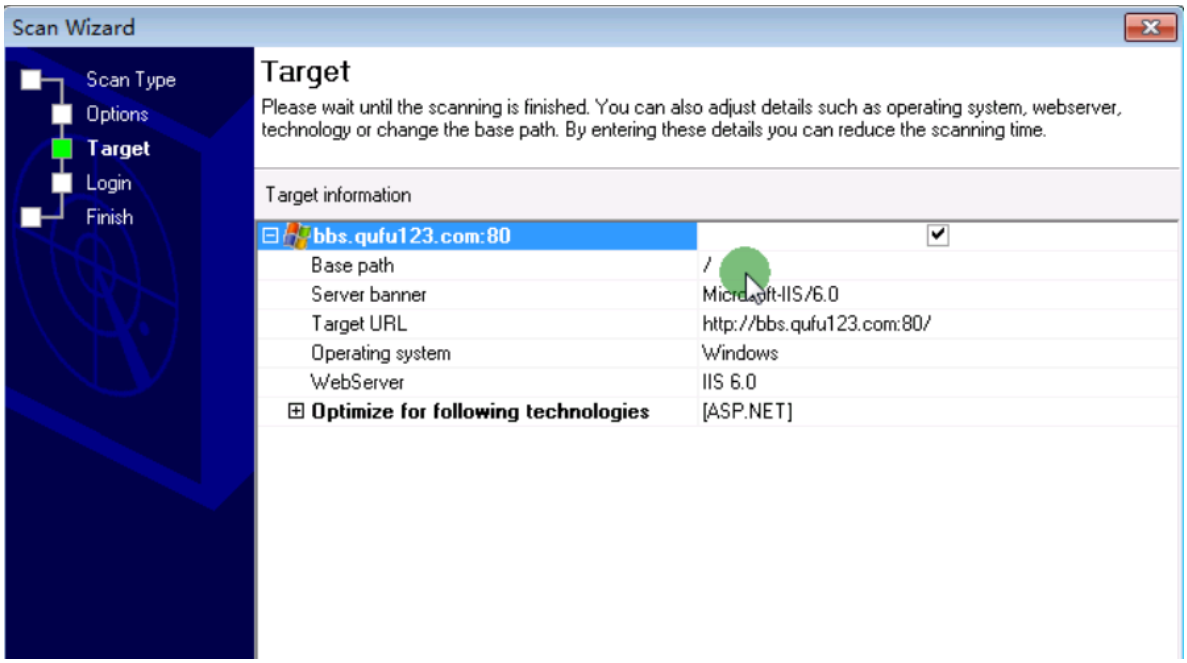
一、判断网站cms类型

cms就是网站使用的模板

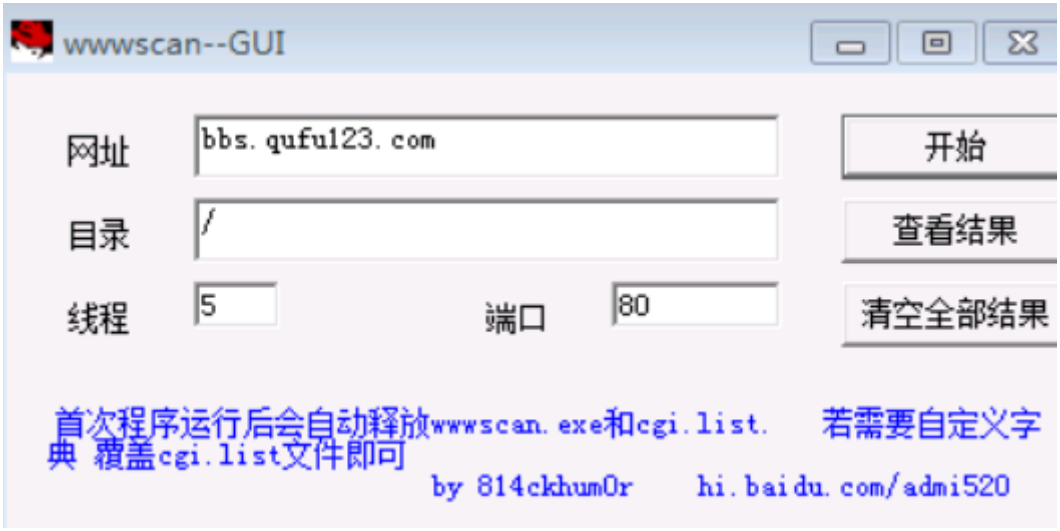
-判断目标：
-脚本语言：
-操作系统：
-搭建平台：
-cms厂商：
-使用工具：

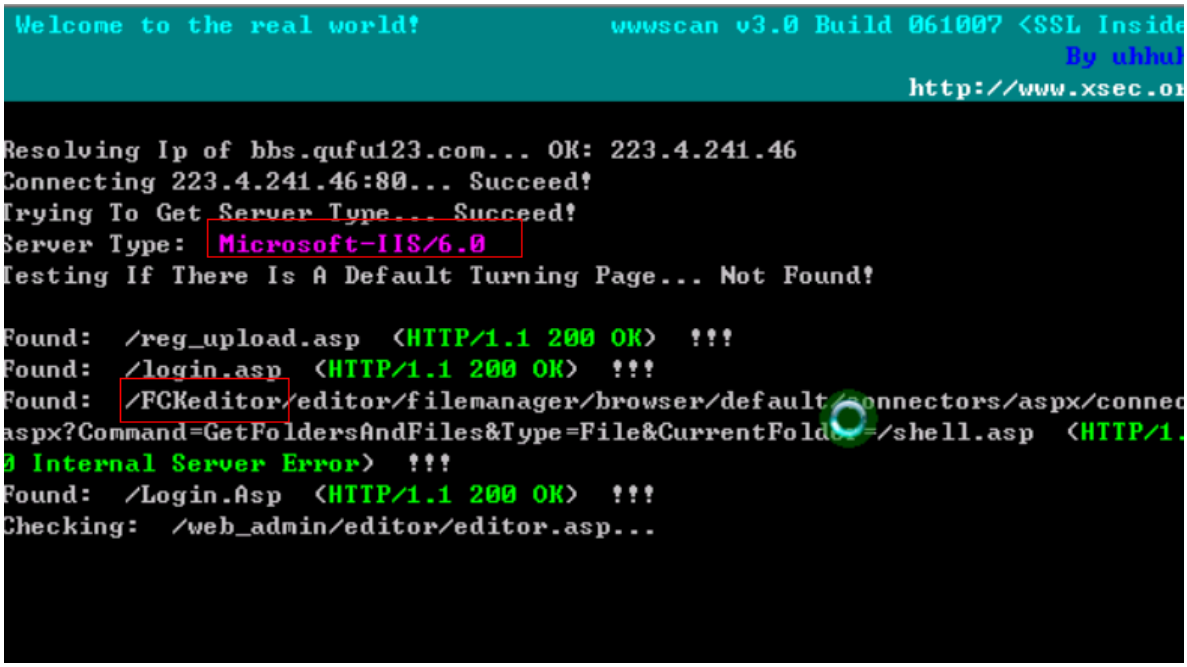
1.**wvs**



2.wwwscan

直接输入网站后点击开始





站长工具

whatweb、googlehack

补充:

打开一个网页后自动跳转到其他网站:

添加一个html标签

<meta http-equiv="refresh" content="5"; url="想要跳转到的网站" />

二、网站暴库漏洞

简介

暴库，就是通过一些技术手段或者程序漏洞得到数据库的地址，并将数据非法下载到本地。黑客非常乐意于这种工作，为什么呢？因为黑客在得到网站数据库后，就能得到网站管理账号，对网站进行破坏与管理，黑客也能通过数据库得到网站用户的隐私信息，甚至得到服务器的最高权限。

实例

http://xxx.com/database/%23data.mdb

其中%23= # ，网站管理员为了防止直接下载，在这里需要添加一个#才行.

打开**辅臣数据库浏览器 / 破障access数据查看器**等等一类的工具。

只要是打开就行。

常见的暴库利用方法

```
inurl:/inc/conn.asp inurl:/inc+conn.asp to parent directory intext:
inurl:/inc/conn.asp
inurl:/inc+conn.asp
```

目录遍历

百度/google搜： to parent directory或者 转到父目录

而利用google来搜索目录浏览的google语法主要有：intitle　intext inurl　site filetype等等

搜索域名后缀，常见的后缀名有com net mil org info gov edu biz coop areo pro int arpa

实例

直接下载复旦大学官网的数据库

intext:to parent directory+intext:mdb site:fudan.edu.cn

该漏洞已打好补丁，只是说下思路

暴库绕过防下载

#sdsf.mdb　　加个#号或者%23

高级暴库语句

```
inurl:./..admin../..add..
inurl:./..admin../..del..
inurl:/.asp<id=<% <%< %
intext:<%eval
intitle:<%eval
```

下载漏洞

正常的下载地址是访问根目录下接收路径进行下载

url/shida/uploadfiles/indentattfile/2012061222041778.doc

如果通过参数进行下载文件的话，就可能存在下载漏洞

url/down.asp?fileup=shida/uploadfiles/indentattfile/2012061222041778.doc

通过动态参数进行引用传递的话，也可能存在下载漏洞

url/ggjs/news/down.asp?filename=doc/2012-5/2012053010329973.doc

关键词查找该漏洞

```
inurl:down.asp?FileName=
inurl:down.php?File=
```

查看某网站是否有该漏洞　inurl:down.asp?FileName= site:xxx.com

下载漏洞利用

通过蜘蛛爬行

找到该url

下载conn.asp　config.php config.asp

db.mdb

三、网站后台查找

1.默认后台：admin，admin/login.asp，admin/admin_login.asp，admin/admini.asp，manage，login.asp

2.查看网页链接：一般来说，网站的主页有管理登陆类似的东西，有些有可能被管理员删掉

3.查看网站图片的属性

有些图片有可能上传到管理员目录，右击图片属性，有可能看到目录

4.查看网站使用的管理系统，从而确定后台

通过下载该类型网站cms源码进行分析，从而确定网站的后台

常见的cms管理系统有：

织梦、discuz、帝国、phpweb、wordpress、aspcms、科讯、南方、良精、ecshop等

常见的默认管理页面：

cms	默认后台
织梦	dede
discuz	admin.php
帝国	e/admin
phpweb	admin.php
wordpress	wp-admin
科讯	admin
南方	admin
良精	admin
ecshop	admin

当然也可能是manager、login_admin、login_manage、login.asp、houtai、denglu等等

5.用工具查找：wwwscan，intellitamper，御剑，啊d

目录爆破扫描

6.查看robots,txt的帮助：rebots.txt文件告诉蜘蛛程序在服务器上什么样的文件可以被查看

7.Googlehack

intitle:后台管理

特定网站： site:xxx.com intitle:后台管理

inurl:xxx.com

site:xx.com 后台管理

site:xx.com 后台登陆/录

site:xx.com 管理员登陆

8.查看网站使用的**编辑器**是否有默认后台，密码

9.蜘蛛爬行：robots、burpsuite、wvs、netpark

10.社会工程

四、网站管理员密码猜解

为了管理员方便管理网站，cms系统通常有管理员后台管理接口，该接口需要出示管理员账号密码，正确验证后方可登录

一般都是爆破弱口令

猜解工具：hydra、PKAV HTTP Fuzzer(这是针对有验证码的)、Discuz批量用户密码暴力破解器

爆破工具：burpsuite、一些python密码破解脚本、或者其他针对性的破解工具

五、网站漏洞的利用

EXP利用

EXP是exploit（漏洞利用的缩写），当cms出现漏洞的时候针对漏洞原理可以写出针对该漏洞的exploit，有的exp可以直接添加管理员、或者getshell、爆出管理员账号密码、数据库账号密码等等。

主流的网站基本上都有漏洞和exp。

最经典的是注入exp

EXP收集

百度搜集、与朋友交流探讨、利用工具直接exp

批量检测站点

通常用于某一类型漏洞站点的安全检测

> 关键字：
>
> 有限公司--Powered by ASPCMS V2.0
>
> Powered by AspCMS V2
>
> Powered by AspCMS V2.0
>
> AspCms
>
> Powere

实例

关键字：

```
inurl:netgoods.asp?action_key_order=news
```

利用方法：admin_shopxp/upload_bm.asp

漏洞名称：phpwen漏洞

关键字：

```
inurl:/class/?1.html
inurl:/class/index/php?catid=0
inurl:/page/html/?1.html
inurl:news/html/?411.html(推荐)
```