随着信息技术的发展，网络应用越来越广泛，很多企业单位都依靠网站来运营，正因为业务的不断提升和应用，致使网站的安全性显得越来越重要。另一 方面，网络上的黑客也越来越多，而且在利益驱使下，很多黑客对网站发起攻击，并以此谋利。作为网站的管理人员，应该在黑客入侵之前发现网站的安全问题，使 网站能更好的发挥作用。那么究竟如何检查网站的安全隐患和漏洞呢?

下面我们介绍一款开放源代码的 Web 漏洞扫描软件，网站管理员可以用它对 WEB 站点进行安全审计，尽早发现网站中存在的安全漏洞。

Nikto 是一款开放源代码的、功能强大的 WEB 扫描评估软件，能对 web 服务器多种安全项目进行测试的扫描软件，能在 230 多种服务器上扫描出 2600 多种有潜在危险的文件、CGI 及其他问题，它可以扫描指定主机的 WEB 类型、主机名、特定目录、COOKIE、特定 CGI 漏洞、返回主机允许的 http 模式等等。它也使用 LibWhiske 库，但通常比 Whisker 更新的更为频繁。Nikto 是网管安全人员必备的 WEB 审计工具之一。

Nikto 最新版本为 2.0 版，官方下载网站：[url]http://www.cirt.net/[/url]

Nikto 是基于 PERL 开发的程序，所以需要 PERL 环境。Nikto 支持 Windows（使用 ActiveState Perl 环境)、Mac OSX、多种 Linux 或 Unix 系统。Nikto 使用 SSL 需要 Net::SSLeay PERL 模式，则必须在 Unix 平台上安装 OpenSSL。具体的可以参考 nikto 的帮助文档。

从官方网站上下载 nikto-current.tar.gz 文件，在 Linux 系统解压操作：

tar -xvf nikto-current.tar.gz

gzip -d nikto-current.tar

解压后的结果如下所示：

Config.txt、docs、kbase、nikto.pl、plugins、 templates

Nikto 的使用说明：

Nikto 扫描需要主机目标 IP、主机端口。默认扫描的是 80 端口。扫描主机目标 IP 地址可以使用选项-h(host)。下面将扫描 IP 为 192.168.0.1 的 TCP 80 端口，如下所示：

perl nkito.pl –h 192.168.0.1

也可以自定义扫描的端口，可以使用选项-p(port)，下面将扫描 IP 为 192.168.0.1 的 TCP 443 端口，如下所示：

perl nikto.pl –h 192.168.0.1 –p 443

Nikto 也可以同时扫描多个端口，使用选项-p(port)，可以扫描一段范围（比如：80-90)，也可以扫描多个端口（比如：80,88,90)。下面扫描主机的 80/88/443 端口，如下所示：

Perl nikto.pl –h 192.168.0.1 –p 80,88,443

如果运行 Nikto 的主机是通过 HTTP proxy 来访问互联网的，也可以使用代理来扫描，使用选项-u(useproxy)。下面将通过 HTTP proxy 来扫描，如下所示：

Perl nikto.ph –h 192.168.0.1 –p 80 –u

Nikto 的更新：

Nikto 的升级可以通过-update 的命令来更新插件和数据库，如下所示：

Perl nikto.ph –update

也可以通过从网站下载来更新插件和数据库：[url]http://updates.cirt.net/[/url]

Nikto 的选项说明：

-Cgidirs

扫描 CGI 目录。

-config

使用指定的 config 文件来替代安装在本地的 config.txt 文件

-dbcheck

选择语法错误的扫描数据库。

-evasion

使用 LibWhisker 中对 IDS 的躲避技术，可使用以下几种类型：

1．随机 URL 编码（非 UTF-8 方式）

2．自选择路径（/./）

3．虚假的请求结束

4．长的 URL 请求

5．参数隐藏

6．使用 TAB 作为命令的分隔符

7．大小写敏感

8．使用 Windows 路径分隔符\替换/

9．会话重组

-findonly

仅用来发现 HTTP 和 HTTPS 端口，而不执行检测规则

-Format

指定检测报告输出文件的格式，默认是 txt 文件格式（csv/txt/htm）

-host

目标主机，主机名、IP 地址、主机列表文件。

-id

ID 和密码对于授权的 HTTP 认证。格式：id:password

-mutate

变化猜测技术

1.使用所有的 root 目录测试所有文件

2.猜测密码文件名字

3.列举 Apache 的用户名字(/~user)

4.列举 cgiwrap 的用户名字(/cgi-bin/cgiwrap/~user)

-nolookup

不执行主机名查找

-output

报告输出指定地点

-port

扫描端口指定，默认为 80 端口。

-Pause

每次操作之间的延迟时间

- Display

控制 Nikto 输出的显示

1.直接显示信息

2.显示的 cookies 信息

3.显示所有 200/OK 的反应

4.显示认证请求的 URLs

5.Debug 输出

-ssl

强制在端口上使用 SSL 模式

-Single

执行单个对目标服务的请求操作。

-timeout

每个请求的超时时间，默认为 10 秒

-Tuning

Tuning 选项控制 Nikto 使用不同的方式来扫描目标。

0.文件上传

1.日志文件

2.默认的文件

3.信息泄漏

4.注射（XSS/Script/HTML）

5.远程文件检索（Web 目录中）

6.拒绝服务

7.远程文件检索（服务器）

8.代码执行 - 远程 shell

9.SQL 注入

a.认证绕过

b.软件关联

g.属性（不要依懒 banner 的信息）

x.反向连接选项

-useproxy

使用指定代理扫描

-update

更新插件和数据库

例子：使用 Nikto 扫描目标主机 10.0.0.12 的 phpwind 论坛网站。

Perl nikto.pl –h 10.0.0.12 –o test.txt