**0x01 Web**[**漏洞扫描**](https://cloud.tencent.com/product/vds?from_column=20065&from=20065)**器**

国内：

绿盟（WVSS）：

https://www.nsfocus.com.cn/html/2019/206\_0911/8.html

安恒（明鉴）：

https://www.dbappsecurity.com.cn/show-63-38-1.html

知道创宇（websoc）：

https://scanv.yunaq.com/websoc/index.html

启明星辰（天镜）：

https://www.venustech.com.cn/article/type/1/253.html

奇安信（网神SecVSS 3600）：

https://www.qianxin.com/product/detail/pid/1

天融信：

http://www.topsec.com.cn/product/63.html

长亭：

https://www.chaitin.cn/zh/xray

复制

国外：

AWVS：

http://wvs.evsino.com/

Nessus：

https://www.tenable.com/downloads/nessus

Appscan：

https://ibm-security-appscan-standard.software.informer.com/8.7/

Netsparker：

https://www.netsparker.com/

Webinspect：

https://www.microfocus.com/en-us/products/webinspect-dynamic-analysis-dast/download?utm\_campaign=00173365&utm\_content=Search-NB-DSA-ESP-Fortify-X-APJ-X-GGL&gclid=EAIaIQobChMIrLqP4-P86QIVg2kqCh2\_tApXEAAYASAAEgJzqvD\_BwE

WebReaver：

https://webreaver.com/

复制

综合：

Nexpose：

Windows/Linux版本：

https://www.rapid7.com/info/nexpose-trial/

虚拟机版本：

https://www.rapid7.com/info/nexpose-virtual-appliance/

社区版本：( 免费试用一年 )

https://www.rapid7.com/info/nexpose-community/

复制

注：以上WEB漏洞扫描器产品中，有收费的，也有免费的，国内的大部分都是收费的，除了长亭的X-ray，但是长亭的Xray高级版一样是收费的，其开放的是社区版，而我们日常渗透中常用的WEB漏洞扫描器可能就是AWVS、Nessus、APPScan这三款。接下来会针对主流的扫描器进行优缺点分析以及其指纹特征分析。

**0x02 扫描器优缺点分析**

WEB漏洞扫描器的好坏取决于爬行页面数、漏洞库数量、扫描效率、误报率等等，漏洞扫描还分主动式扫描和被动式扫描，Xray、w13scan就是利用被动式扫描，AWVS利用的是主动式扫描。通常在企业，如果企业内部有自己的漏洞扫描器，则用企业内部提供的，如果没有，我们都是选用两款比较好用、主流的WEB漏洞扫描器进行漏洞扫描，完成扫描后生成报告对比并合并，系统也一样。

**0x03 扫描器特征分析**

1) AWVS

AWVS扫描器在请求的URL，Headers, Body三项里随机包含了能代表自己的特征信息

<1> Url:

acunetix-wvs-test-for-some-inexistent-file

by\_wvs

acunetix\_wvs\_security\_testacunetix

acunetix\_wvs

acunetix\_test

复制

<2> Headers:

Acunetix-Aspect-Password:

Cookie: acunetixCookie

Location: acunetix\_wvs\_security\_testX-Forwarded-Host: acunetix\_wvs\_security\_testX-Forwarded-For: acunetix\_wvs\_security\_testHost: acunetix\_wvs\_security\_testCookie: acunetix\_wvs\_security\_testCookie: acunetix

Accept: acunetix/wvs

Origin: acunetix\_wvs\_security\_testReferer: acunetix\_wvs\_security\_testVia: acunetix\_wvs\_security\_testAccept-Language: acunetix\_wvs\_security\_testClient-IP: acunetix\_wvs\_security\_testHTTP\_AUTH\_PASSWD: acunetix

User-Agent: acunetix\_wvs\_security\_testAcunetix-Aspect-Queries:任意值

Acunetix-Aspect:任意值

复制

<3> Body （请求的post信息）

acunetix\_wvs\_security\_testacunetix

复制

2) Nessus

Nessus扫描器的特征信息同样在请求的URL，Headers，Body三项里

<1> Url

nessus

Nessus

复制

<2> Headers

x\_forwarded\_for: nessus

referer: nessus

host: nessus

复制

<3> Body

nessus

Nessus

复制

3) APPScan

Appscan依然在请求的URL，Headers，Body三项里随机包含了能代表自己的特征信息

<1>Url

Appscan

复制

<2> Headers

Content-Type: Appscan

Content-Type: AppScanHeader

Accept: Appscan

User-Agent:Appscan

复制

<3> Body

Appscan

**awvs**

1. url

acunetix-wvs-test-for-some-inexistent-file

by\_wvs

acunetix\_wvs\_security\_test

acunetix

acunetix\_wvs

acunetix\_test

1. headers

Acunetix-Aspect-Password:

Cookie: acunetixCookie

Location: acunetix\_wvs\_security\_test

X-Forwarded-Host: acunetix\_wvs\_security\_test

X-Forwarded-For: acunetix\_wvs\_security\_test

Host: acunetix\_wvs\_security\_test

Cookie: acunetix\_wvs\_security\_test

Cookie: acunetix

Accept: acunetix/wvs

Origin: acunetix\_wvs\_security\_test

Referer: acunetix\_wvs\_security\_test

Via: acunetix\_wvs\_security\_test

Accept-Language: acunetix\_wvs\_security\_test

Client-IP: acunetix\_wvs\_security\_test

HTTP\_AUTH\_PASSWD: acunetix

User-Agent: acunetix\_wvs\_security\_test

Acunetix-Aspect-Queries:任意值

Acunetix-Aspect:任意值

1. body

acunetix\_wvs\_security\_test

acunetix

**nessus**

1. url

nessus

Nessus

1. headers

x\_forwarded\_for: nessus

referer: nessus

host: nessus

1. body

nessus

Nessus

**appscan**

1. url

Appscan

1. headers

Content-Type: Appscan

Content-Type: AppScanHeader

Accept: Appscan

User-Agent:Appscan

1. body

Appscan

**Rsas (绿盟极光)**

1. url

nsfocus

1. headers

User-Agent: Rsas

**sqlmap**

1. url

sqlmap

1. headers

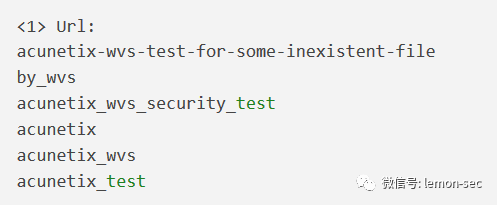
User-Agent: sqlmap（后接版本号，跟当前版本有关系）

1. body

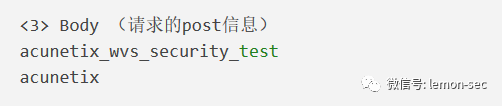
sqlmap

### 1. Awvs（Acunetix Web Vulnerability Scanner ）版本10.5和11

Awvs在请求的Url，Headers, Body三项里随机包含了能代表自己的特征信息

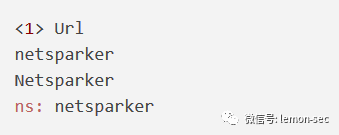


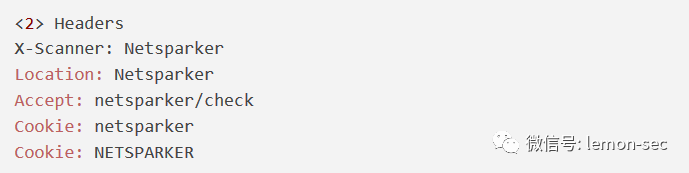


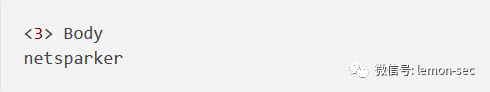


### 2. Netsparker

Netsparker依然在请求的Url，Headers, Body三项里随机包含了能代表自己的特征信息

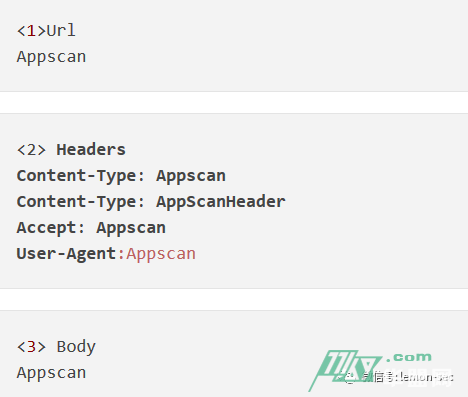






### 3. Appscan

Appscan依然在请求的Url，Headers, Body三项里随机包含了能代表自己的特征信息



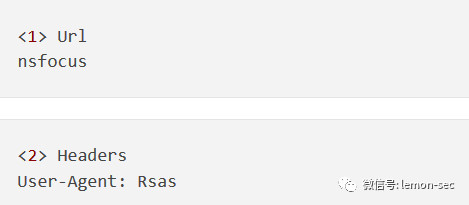
### 4. Webinspect

Webinspect依然在请求的Url，Headers, Body三项里随机包含了能代表自己的特征信息



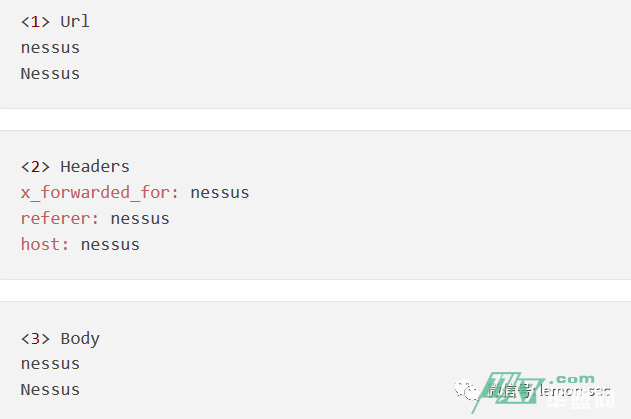
### 5.Rsas (绿盟极光)

Rsas 的主要的特征在Url和Headers中



### 6. Nessus

Nessus的特征主要在Url，Headers，Body中



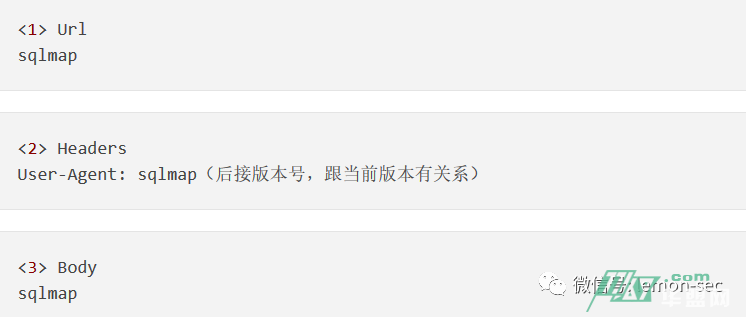
### 7. WebReaver

WebReaver的特征只在Headers中的UA中



### 8.Sqlmap

Sqlmap在Url，Headers，Body中都含有特征值



### 扫描器指纹

1.awvs:acunetix

2.netsparker:netsparker

3.appscan:Appscan

4.nessus:nessus

5.sqlmap:sqlmap

### 常见后台地址

1.admin

2.manager

3.login

4.system

Disallow

一般情况下，大多数网站创建者或管理员都会在网站的根目录放置一个名为robots.txt的文本文件，用来控制自己的网站哪些目录允许SE搜索引擎，爬行并收录，哪些目录禁止搜索引擎收录，Disallow，正是robots.txt文件中设置禁止搜索引擎收录哪些目录的一个词语。