# 第一章 信息收集

## 一、信息收集的相关概念、作用、收集目标

渗透测试，是为了证明网络防御按照预期计划正常运行而提供的一种机制。不妨假设，你的公司定期更新安全策略和程序，时时给系统打补丁，并采用了[漏洞扫描器](https://baike.baidu.com/item/%E6%BC%8F%E6%B4%9E%E6%89%AB%E6%8F%8F%E5%99%A8)等工具，以确保所有补丁都已打上。如果你早已做到了这些，为什么还要请外方进行审查或渗透测试呢？因为，渗透测试能够独立地检查你的网络策略，换句话说，就是给你的系统安了一双眼睛。而且，进行这类测试的，都是寻找网络系统安全漏洞的专业人士。

### [渗透测试的8个步骤 展现一次完整的渗透测试过程及思路](http://toutiao.secjia.com/pentest-process)

发布时间：2017年10月25日 15:11    浏览量：1104

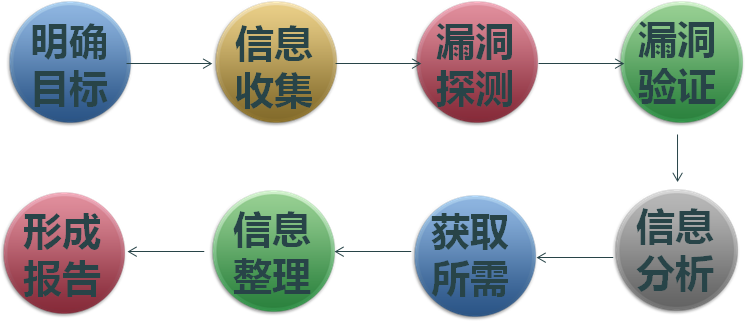
[渗透测试这个事情不是随便拿个工具就可以做了， 要了解业务还需要给出解决方案](http://toutiao.secjia.com/penetration-testing)。之前安全加介绍了金融行业 [实战微信银行渗透测试，](http://toutiao.secjia.com/weixin-bank-pentest)运营商 [渗透测试实战](http://toutiao.secjia.com/telecom-penetration-test)，今天让我们来说说 [渗透测试](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95.shtml)的流程及渗透测试相关概念。

**渗透测试流程**

**渗透测试与入侵的最大区别**

* 渗透测试：出于保护系统的目的，更全面地找出测试对象的安全隐患。
* 入侵：不择手段地（甚至是具有破坏性的）拿到系统权限。

**一般渗透测试流程**



流程并非万能，只是一个工具。思考与流程并用，结合自己经验。

**2.1 明确目标**

* 确定范围：测试目标的范围，ip，域名，内外网。
* 确定规则：能渗透到什么程度，时间？能否修改上传？能否提权等。
* 确定需求：web应用的漏洞(新上线程序)？业务逻辑漏洞（针对业务的）？人员权限管理漏洞（针对人员、权限）？等等。

（立体全方位）根据需求和自己技术能力来确定能不能做，能做多少。

**2.2 信息收集**

方式：主动扫描，开放搜索等

开放搜索：利用搜索引擎获得，后台，未授权页面，敏感url等。

* 基础信息：IP，网段，域名，端口
* 系统信息：操作系统版本
* 应用信息：各端口的应用，例如web应用，邮件应用等等
* 版本信息：所有这些探测到的东西的版本。
* 服务信息
* 人员信息：域名注册人员信息，web应用中网站发帖人的id，管理员姓名等。
* 防护信息：试着看能否探测到防护设备

**2.3 漏洞探索**

利用上一步中列出的各种系统，应用等使用相应的漏洞。方法：

* 1.漏扫，awvs，IBM appscan等。
* 2.结合漏洞去exploit-db等位置找利用。
* 3.在网上寻找验证poc。

**内容：**

* 系统漏洞：系统没有及时打补丁
* Websever漏洞：Websever配置问题
* Web应用漏洞：Web应用开发问题
* 其它端口服务漏洞：各种21/8080(st2)/7001/22/3389
* 通信安全：明文传输，token在cookie中传送等。

**2.4 漏洞验证**

将上一步中发现的有可能可以成功利用的全部漏洞都验证一遍。结合实际情况，搭建模拟环境进行试验。成功后再应用于目标中。

* 自动化验证：结合自动化扫描工具提供的结果
* 手工验证，根据公开资源进行验证
* 试验验证：自己搭建模拟环境进行验证
* 登陆猜解：有时可以尝试猜解一下登陆口的账号密码等信息
* 业务漏洞验证：如发现业务漏洞，要进行验证
* 公开资源的利用

-exploit-db/wooyun/

-google hacking

-渗透代码网站

-通用、缺省口令

-厂商的漏洞警告等等。

**2.5 信息分析**

为下一步实施渗透做准备。

* 精准打击：准备好上一步探测到的漏洞的exp，用来精准打击
* 绕过防御机制：是否有防火墙等设备，如何绕过
* 定制攻击路径：最佳工具路径，根据薄弱入口，高内网权限位置，最终目标
* 绕过检测机制：是否有检测机制，流量监控，杀毒软件，恶意代码检测等（免杀）
* 攻击代码：经过试验得来的代码，包括不限于xss代码，sql注入语句等

**2.6 获取所需**

* 实施攻击：根据前几步的结果，进行攻击
* 获取内部信息：基础设施（网络连接，vpn，路由，拓扑等）
* 进一步渗透：内网入侵，敏感目标
* 持续性存在：一般我们对客户做渗透不需要。rookit，后门，添加管理账号，驻扎手法等
* 清理痕迹：清理相关日志（访问，操作），上传文件等

**2.7 信息整理**

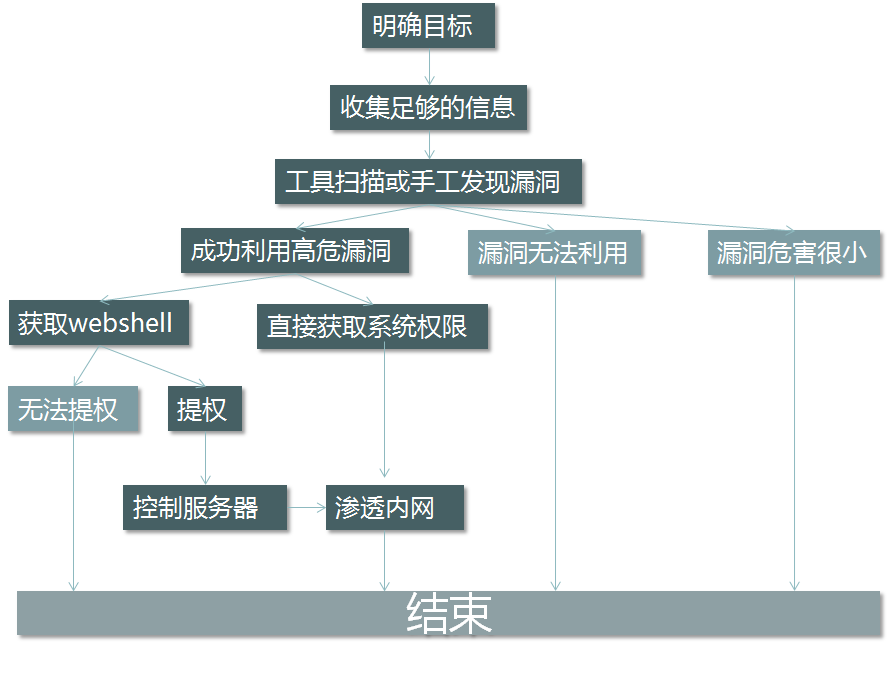
* 整理渗透工具：整理渗透过程中用到的代码，poc，exp等
* 整理收集信息：整理渗透过程中收集到的一切信息
* 整理漏洞信息：整理渗透过程中遇到的各种漏洞，各种脆弱位置信息

目的：为了最后形成报告，形成测试结果使用。

**2.8 形成报告**

* 按需整理：按照之前第一步跟客户确定好的范围，需求来整理资料，并将资料形成报告
* 补充介绍：要对漏洞成因，验证过程和带来危害进行分析
* 修补建议：当然要对所有产生的问题提出合理高效安全的解决办法

**2.9 流程总结**



**渗透测试相关名词解析**

**1.1 一些前置知识（包含但不限于）**

* 脚本（asp、php、jsp）
* html（css、js、html）
* HTTP协议
* CMS（B/S）

**1.2 肉鸡**

被黑客入侵并被长期驻扎的计算机或服务器。可以随意控制，可以是任意系统的设备，对象可以是企业，个人，政府等等所有单位。

**1.3 抓鸡**

利用使用量大的程序的漏洞，使用自动化方式获取肉鸡的行为。

**1.4 Webshell**

通过Web入侵的一种脚本工具，可以据此对网站服务进行一定程度的控制。

**1.5 漏洞**

硬件、软件、协议等等的可利用安全缺陷，可能被攻击者利用，对数据进行篡改，控制等。

**1.6 木马**

通过向服务端提交一句简短的代码，配合本地客户端实现webshell功能的木马。

<%eval request("pass")%>

<%execute(request("pass"))%>

request("pass")接收客户端提交的数据，pass为执行命令的参数值。

eval/execute    函数执行客户端命令的内容

**1.7 提权**

操作系统低权限的账户将自己提升为管理员权限使用的方法。

**1.8 后门**

黑客为了对主机进行长期的控制，在机器上种植的一段程序或留下的一个"入口"。

**1.9 跳板**

使用肉鸡IP来实施攻击其他目标，以便更好的隐藏自己的身份信息。

**1.10 旁站入侵**

即同服务器下的网站入侵，入侵之后可以通过提权跨目录等手段拿到目标网站的权限。常见的旁站查询工具有：WebRobot、御剑、明小子和web在线查询等

**1.11 C段入侵**

即同C段下服务器入侵。如目标ip为192.168.180.253 入侵192.168.180.\*的任意一台机器，然后利用一些黑客工具嗅探获取在网络上传输的各种信息。常用的工具有：在windows下有Cain，在UNIX环境下有Sniffit, Snoop, Tcpdump, Dsniff 等。

**1.12 黑盒测试**

在未授权的情况下，模拟黑客的攻击方法和思维方式，来评估计算机网络系统可能存在的安全风险。

黑盒测试不同于黑客入侵，并不等于黑站。黑盒测试考验的是综合的能力（OS、Datebase、Script、code、思路、社工）。思路与经验积累往往决定成败。

**1.13 白盒测试**

相对黑盒测试，白盒测试基本是从内部发起。白盒测试与黑盒测试恰恰相反，测试者可以通过正常渠道向被测单位取得各种资料，包括网络拓扑、员工资料甚至网站或其它程序的代码片断，也能够与单位的其它员工（销售、程序员、管理者……）进行面对面的沟通。

**1.13 黑白盒的另一种说法**

知道源代码和不知道源代码的渗透测试。这时，黑盒测试还是传统的渗透测试，而白盒测试就偏向于代码审计。

**1.14 APT攻击**

Advanced Persistent Threat，高级可持续性攻击，是指组织(特别是政府)或者小团体利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。

* 1.极强的隐蔽性
* 2.潜伏期长，持续性强
* 3.目标性强

**渗透测试相关资源**

实战类：

[实战微信银行渗透测试 展示安全评估思路、工具及经验](http://toutiao.secjia.com/weixin-bank-pentest)

[某运营商渗透测试实战 展示渗透测试工具及业务系统中的常见问题](http://toutiao.secjia.com/telecom-penetration-test)

工具类：

[渗透测试人员入门 如何配置Kali Linux直接用于工作](http://toutiao.secjia.com/setup-kali-linux)

[下载 | Kali Linux2017.2新版发布 增加了一大批新网络渗透测试工具](http://toutiao.secjia.com/kali-linux-2017-2)

[安全工程师的福音 免费恶意软件分析工具FlareVM 还可进行逆向工程和渗透测试](http://toutiao.secjia.com/fireeye-releases-free-malware-analysis-toolbox)

[渗透测试工程师的17个常用工具 还有专家告诉你如何成为渗透测试人员](http://toutiao.secjia.com/17pen-testing-tools)

本文由：绿盟科技博客 发布，版权归属于原作者。   
如果转载，请注明出处及本文链接：   
<http://toutiao.secjia.com/pentest-process>  
如果此文章侵权，请留言，我们进行删除。

[全行业](http://toutiao.secjia.com/category/%E5%85%A8%E8%A1%8C%E4%B8%9A.shtml)[渗透测试](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95.shtml)[渗透测试服务](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95%E6%9C%8D%E5%8A%A1.shtml)[渗透测试工具](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95%E5%B7%A5%E5%85%B7.shtml)[渗透测试案例](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95%E6%A1%88%E4%BE%8B.shtml)[渗透测试方案](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95%E6%96%B9%E6%A1%88.shtml)[渗透测试步骤](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95%E6%AD%A5%E9%AA%A4.shtml)[渗透检测原理](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%A3%80%E6%B5%8B%E5%8E%9F%E7%90%86.shtml)[渗透测试概念](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95%E6%A6%82%E5%BF%B5.shtml)

### PTES渗透测试执行标准

2016年11月25日 14:59:22

阅读数：3093

渗透测试注意事项：

1：不要进行恶意攻击

2：不要做傻事

3：在没有获得书面授权时，不要攻击任何目标

4：考虑你的行为将会带来的后果

5：如果你干了非法的是，天网恢恢疏而不漏

渗透测试执行标准http://www.pentest-standard.org/

1：前期交互阶段

在前期交互（Pre-Engagement Interaction）阶段，渗透测试团队与客户组织进行交互讨论，最重要的是确定渗透测试的范围、目标、限制条件以及服务合同细节。

该阶段通常涉及收集客户需求、准备测试计划、定义测试范围与边界、定义业务目标、项目管理与规划等活动。

2：情报收集阶段

在目标范围确定之后，将进入情报搜集（Information Gathering）阶段，渗透测试团队可以利用各种信息来源与搜集技术方法，尝试获取更多关于目标组织网络拓扑、系统配置与安全防御措施的信息。

渗透测试者可以使用的情报搜集方法包括公开来源信息查询、Google Hacking、社会工程学、网络踩点、扫描探测、被动监听、服务查点等。而对目标系统的情报探查能力是渗透测试者一项非常重要的技能，情报搜集是否充分在很大程度上决定了渗透测试的成败，因为如果你遗漏关键的情报信息，你将可能在后面的阶段里一无所获。

3：威胁建模阶段

在搜集到充分的情报信息之后，渗透测试团队的成员们停下敲击键盘，大家聚到一起针对获取的信息进行威胁建模（Threat Modeling）与攻击规划。这是渗透测试过程中非常重要，但很容易被忽视的一个关键点。

通过团队共同的缜密情报分析与攻击思路头脑风暴，可以从大量的信息情报中理清头绪，确定出最可行的攻击通道。

4：漏洞分析阶段

在确定出最可行的攻击通道之后，接下来需要考虑该如何取得目标系统的访问控制权，即漏洞分析（Vulnerability Analysis）阶段。

在该阶段，渗透测试者需要综合分析前几个阶段获取并汇总的情报信息，特别是安全漏洞扫描结果、服务查点信息等，通过搜索可获取的渗透代码资源，找出可以实施渗透攻击的攻击点，并在实验环境中进行验证。在该阶段，高水平的渗透测试团队还会针对攻击通道上的一些关键系统与服务进行安全漏洞探测与挖掘，期望找出可被利用的未知安全漏洞，并开发出渗透代码，从而打开攻击通道上的关键路径。

5：渗透攻击阶段

渗透攻击（Exploitation）是渗透测试过程中最具有魅力的环节。在此环节中，渗透测试团队需要利用他们所找出的目标系统安全漏洞，来真正入侵系统当中，获得访问控制权。

渗透攻击可以利用公开渠道可获取的渗透代码，但一般在实际应用场景中，渗透测试者还需要充分地考虑目标系统特性来定制渗透攻击，并需要挫败目标网络与系统中实施的安全防御措施，才能成功达成渗透目的。在黑盒测试中，渗透测试者还需要考虑对目标系统检测机制的逃逸，从而避免造成目标组织安全响应团队的警觉和发现

6：后渗透攻击阶段

后渗透攻击（Post Exploitation）是整个渗透测试过程中最能够体现渗透测试团队创造力与技术能力的环节。前面的环节可以说都是在按部就班地完成非常普遍的目标，而在这个环节中，需要渗透测试团队根据目标组织的业务经营模式、保护资产形式与安全防御计划的不同特点，自主设计出攻击目标，识别关键基础设施，并寻找客户组织最具价值和尝试安全保护的信息和资产，最终达成能够对客户组织造成最重要业务影响的攻击途径。

在不同的渗透测试场景中，这些攻击目标与途径可能是千变万化的，而设置是否准确并且可行，也取决于团队自身的创新意识、知识范畴、实际经验和技术能力。

7：报告阶段

渗透测试过程最终向客户组织提交，取得认可并成功获得合同付款的就是一份渗透测试报告（Reporting）。这份报告凝聚了之前所有阶段之中渗透测试团队所获取的关键情报信息、探测和发掘出的系统安全漏洞、成功渗透攻击的过程，以及造成业务影响后果的攻击途径，同时还要站在防御者的角度上，帮助他们分析安全防御体系中的薄弱环节、存在的问题，以及修补与升级技术方案。

渗透术语

渗透攻击（Exploit）

攻击者利用安全漏洞，所进行的攻击行为；常见的渗透攻击技术包括缓冲区溢出、web应用程序漏洞攻击（SQL注入）、利用配置错误等

攻击载荷（Payload）

目标系统在被渗透攻击之后执行的代码

shellcode

在渗透攻击时作为攻击载荷运行的一组机器指令，通常用汇编语言编写

模块（Module）

一段软件代码组件

监听器（Listener）

用来等待连入网络连接的组件

## 二、利用搜索引擎搜索信息

GoogleHacking：利用搜索引擎（如：Google，百度）有针对的搜索信息来进行网络入侵的技术和行为。搜索引擎对于搜索的关键字提供了多种语法，构造出特殊的关键字，GoogleHacking技术能够快速全面的让攻击者挖掘到有价值的信息。利用搜索引擎的搜集目标主要有一下几种：

1. 敏感信息
2. 具备特殊url关键字的目标地址
3. 搜索已有的攻击结果
4. 指定格式文件
5. 其他与某个站点相关的信息

特别提示：利用网页快照功能， 有时候可以发现很多有价值的信息

可能有人会说Google和 Google的使用方法很简单呀，写入信息，点击搜索就可以了。但实际上只是如此么？很多的以为已经被互联网删除了的文件都可以再google上面找到（快照）。

例如：在谷歌中输入 site：microsoft.com filetype：pdf，就能得到microsoft.com网站上的所有pdf文档（但是因为每个人刚学习google hacking时都是搜索这个词条，microsoft.com早已经解决了这个漏洞，所以，现在可以试试site：baidu.com filetype：pdf）

Google hacking使用的通配符：

1、加号（“+”）

“+”号是强迫包含的意思，也就是说搜索的结果中要包含后面的内容，这里需要注意的是，在“+”号前面要有一个空格，比如说我们搜索“天津 +天津特产”，搜索出的结果，一共搜索到7,750,000 条，并且都是和特产有关的。

2、减号（“—”）

减号和加号相反，就是取出的意思，他会在我们搜索结果中去除我们写入的内容、例如“天津 —特产”。

3、波浪号(“~”)

波浪号“~”的意思是搜索同义词，这样的搜索结果会更多，例如“天津 ~天津”

4、点号（“.”）

点号的作用是取代一个字符，例如“war .3”，就会搜索到4070000个结果，但是我们如果输入 war 3 则会有1310000000项结果

5、星号（“\*”）

星号的意思是取代所有字符，例如搜索“war\*”，可以搜索到1070000000项结果。

6、双引号（""）

双引号是强调的意思，例如搜索“"视界The world"”，就会搜索到93500项结果，但如果我们直接搜索“视界The world”,则时能搜索到5710项结果，就比不加双引号少了很多。

搜索引擎使用高级语法：

1、allintext

allintext的意思是以网页正文内容中的冒个字符作为搜索条件，例如“allintext：我爱你”

2、allintitle

allintitle的意思是在网页标题中搜索我们要查找的字符，例如“allintitle：视界”

3、cache

cache的意思是缓存，例如“cache：www.stuhack.com”。

4、define

define的意思是词语的定义，例如：“define：中国”

5、filetype

filetype的意思是搜索指定格式的文件，例如“filetype：MDB”，

类似于这样的搜索通常都可以直接下载，我们这样搜索很可能搜索到别人的数据口哦！

6、info

info的意思是查找指定的网站基本信息，例如：“info：www.baidu.com”。

7、link

link的意思是查看连接的网站。例如“link：www.baidu.com”

8、related

related的意思是返回主页上连接的内容，例如“related：www.baidu.com”

9、site

site的作用非常的好，它可以制定一个特定的区域进行搜索，也就是说如果site后面是一个网站，那么我们得到的内容就是关于这个网站的，例如：“site：www.baidu.com”

10、inurl

inurl的作用是搜索得到你搜索内容的网址，例如：“inurl：[www.baidu.com](http://www.baidu.com)”

11. intext(仅正对Google有效)

把网页中的正文内容的某个字符作为搜索条件

12. intitle

把网页标题中的某个字符作为搜索条件

13. inurl

搜索包含指定字符的URL

典型用法：

1. 找管理后台地址

Site:xxx.com intext: 管理|后台|登陆|用户名|密码|系统|账号

Site:xxx.com inurl:login|admin|manage|manager|admin\_login|system

Site:xxx.com intitle:管理|后台|登陆

1. 找上传类漏洞的地址：

Site:xxx.com inurl:file

Site:xxx.com inurl:upload

1. 找注入页面：

Site:xxx.com inurl:php?id=

1. 找编辑页面：

Site:xxx.com inurl:ewebeditor

上面就是在GOOGLE搜索中最常用的，希望大家能够牢记。到这里，Google hacking这节也就基本结束了，干货很多，用处也很大，但是小编还是希望大家学会这些之后多做一些有益的事情。人在做，天在看。谨记！

## 三、 通过目标站点搜集信息

参透初期最常见的是只有一个网站或ip。进行有效渗透的第一步，就是从已知的网站名称地址中，尽可能多的挖掘 信息。由于目标网站或系统的配置都是未知的，为了避免对防火墙等安全软件硬件的触发。推荐首先使用被动方式的信息收集方法，也就是目标站点的页面中寻找信息，使用第三方的站在工具进行搜集信息等。

主要的搜集目标：

1. 目标站点使用的技术（页面，数据库等）
2. 目标站点的whois信息，是否可能存在旁站等
3. 挖掘目标站点可能使用的网络安全配置
4. 挖掘目标企业机构可能存在的管理架构
5. 使用站长工具初步扫描
6. 其他与目标站点相关信息

目标企业机构网站是信息的重要来源，网站内容常可以帮助渗透人员了解目标网站的基本情况：

1. 目标是做什么的
2. 目标提供什么产品和服务
3. 地址位置和联系方式
4. 招聘信息和行政架构
5. 管理成员简介
6. 支持论坛和电子邮件茂名规则（灵查注册，可查看邮箱注册了哪些网站）
7. 可能用于密码分析的特殊字符或短语

**使用站长工具搜集信息：**

1. Ip查询
2. 同ip网站查询
3. Whois查询和反查
4. 子域名查询
5. 识别服务器类型，页面类型
6. DNS信息查询
7. 网站安全检测
8. 端口扫描

## 四、漏洞信息搜集

**常用的漏洞平台如下：**

1. 乌云漏洞平台
2. 360补天漏洞平台
3. Exploit-DB
4. GHDB
5. CVE中文漏洞信息
6. 中国国家信息安全漏洞库
7. 国家信息安全漏洞共享平台

**漏洞库搜索方式：**

搜索对应的厂商

搜索定义软件平台

**信息搜集的目标：**

已有的渗透过程

目标的技术架构

目标使用架构的公开漏洞

目标可能进行的修复

**使用搜索引擎搜索漏洞：**

上传类

注入类

敏感信息类

## 五、使用工具搜集信息

Windows平台下常用的几种工具和方法：

1. DOS
2. 扫描工具
3. 浏览器内置功能和插件

**常用的DOS命令：**

Ping:网络连通测试

Arp：显示和修改地址解析协议

Tracert:显示路由

Nslookup：域名系统查询

Telnet：测试是否开启远程连接

Netstat：查看本机所有开发的端口

Nbtstat：获取NetBIOS信息

FTP：测试开放的ftp的远程主机

Net：最后要的命令，需要透彻掌握每一个命令

**常用的扫描工具：**

AWVS

APPScan

Zenmap

Dirbuster

Wwwscan

御剑系列扫描工具

Layer子域名挖掘机

Maltego

**使用浏览器内置功能和插件：**

以fireFox浏览器为例，几种实用的插件如下：

ShowIP插件 HttpFox插件 Cookie Watcher插件 Header Spy插件 Wappalyzer插件 FlagFox插件 Domain Details插件 浏览器内置开发者工具

**Kali Linux**

1. 枚举服务

DNS枚举工具DNSenum

DNS枚举工具firece

SNMP枚举工具Snmpwalk

1. 测试网络范围

域名查询工具Dmitry

跟踪路由工具Scapy

1. 识别活跃的主机，查看打开的端口，系统指纹识别，服务的指纹识别

Nmap

Hping3

1. 其他信息收集手段

ARP侦查工具Netdiscover

1. 使用Maltego收集信息

**社交网络中进行数据挖掘**

社交网络特点：

清晰暴露个人关系网络

包含大量个人信息

具备多种工作、生活服务功能

身份认证机制并非完美

记录大量个人行为特征

**养小号**

## 六、渗透测试中的信息搜集经验分享

更新时间：2018-08-06 11:21:48•点击：95 • 网络安全

**每天对着目标站点进行渗透测试。渗透测试的第一步是信息搜集，那么你的信息搜集完整性决定了你渗透测试的结果，”知己知彼，百战不殆”，在此，我分享下我信息搜集的一些经验。**

### 01 前言

信息搜集分为主动信息搜集和被动信息搜集，主动信息搜集是与目标主机进行直接交互，从而拿到我们的目标信息，而被动信息搜集恰恰与主动信息搜集相反，不与目标主机进行直接交互，通过搜索引擎或者社交等方式间接的获取目标主机的信息。当我们拿到一个目标进行渗透测试的时候，我们关注目标主机的whois信息，子域名，目标IP，旁站C段查询，邮箱搜集，CMS类型，敏感目录，端口信息，服务器与中间件信息。针对上边的信息，网上有很多工具，但是，我们可以自己写一个工具得到所有的信息，方便渗透测试。

### 02 whois信息

whois信息可以获取关键注册人的信息，包括注册公司、注册邮箱、管理员邮箱、管理员联系手机等,对后期社工很有用。同时该工具还可以查询同一注册人注册的其他的域名，域名对应的NS记录、MX记录，自动识别国内常见的托管商（万网、新网等）。常用的工具有：chinaz,kali下的whois命令。

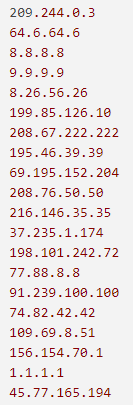


### 03 子域名

在渗透测试的时候，往往主站的防御会很强，常常无从下手，那么子站就是一个重要的突破口，因此子域名是渗透测试的主要关注对象，子域名搜集的越完整，那么挖到的漏洞就可能更多，甚至漏洞的级别也会更高。常用的工具有：搜索引擎（google，baidu，bing）,DNS区域传送漏洞，子域名挖掘机Layer,subDomainsBrute,[phpinfo.me](https://phpinfo.me/domain/),定制字典暴力破解。

### 04 目标IP

现在大部分网站都加了CDN,CDN的虚假IP干扰了我们的渗透测试，如何绕过CDN查找到目标的真实IP，对我们来说非常重要。首先，我们需要判断下是否存在CDN,方法很简单，只要在不同地区进行ping检测就可以知道。不同地区ping同一个网址，得到不同的IP地址，那么该网站开启了CDN加速，相反如果得到的是同一个IP地址，那么极大可能不存在cdn，但是不绝对。常用的工具有[多个地点ping服务器-网站测速-站长工具](http://ping.chinaz.com/)。其次，绕过CDN获取真实IP的方法互联网上有很多，我常用的有**二级域名法**，目标长得一般不会把所有的二级域名放在cdn上，伤钱呐，确定了没有使用CDN的二级域名后，本地将目标域名绑定到同ip，能访问就说明目标站与二级域名在同一服务器叶可能在同C段，扫描C段所有开80端口的ip，挨个尝试。**nslookup法**，大部分CDN提供商只针对国内市场，而对国外市场几乎是不做CDN，所以有很大的几率直接解析到真实IP，不过需要国外的冷门的DNS，如下：



### 05 旁站C段查询

旁站是和目标网站在同一台服务器上的其它的网站；如果从目标站本身找不到好的入手点，这时候，如果想快速拿下目标的话，一般都会先找个目标站点所在服务器上其他的比较好搞的站下手，然后再想办法跨到真正目标的站点目录中。C段是和目标机器ip处在同一个C段的其它机器；通过目标所在C段的其他任一台机器，想办法跨到我们的目标机器上。常用的工具有webscancc，Nmap，Zenmap。

### 06 邮箱收集

首先确定目标的邮件服务器所在的真实位置，看看邮件服务器自身有没有什么错误配置，比如，没有禁用VREY或者EXPN命令导致用户信息泄露。然后从whois中获取域名的注册人、管理员邮箱，利用搜索引擎或者社工库查看有木有泄露的密码，然后尝试泄露的密码进行登录，最后从目标站点上搜集邮箱，例如网站上的联系我们,我们发发邮件钓鱼什么的。常用的工具有kali下的theharester。

### 07 CMS（内容管理系统）类型

对目标渗透测试过程中，目标CMS是十分重要的信息，有了目标的CMS，就可以利用相关的bug进行测试，进行代码审计。CMS识别方式有**网站特有文件**，例如/templets/default/style/dedecms.css — dedecms；**网站独有文件的md5**，例如favicon.ico，但是该文件可以被修改导致不准确；**网站命名规则**；**返回头的关键字**；**网页关键字**；**URL特征**；**Meta特征**；**Script特征**；**robots.txt**；**网站路径特征**；**网站静态资源**；**爬取网站目录信息**；常用的工具有 [云悉](http://www.yunsee.cn/)，[工具1](http://www.iguoli.cn/cms.php)，[BugScaner](http://whatweb.bugscaner.com/look/)。

### 08 敏感目录/文件

用扫描器扫描目录，这时候你需要一本强大的字典，重在平时积累。字典越强扫描处的结果可能越多，这一步主要扫出网站的管理员入口，一些敏感文件（.mdb,.excel,.word,.zip,.rar）,查看是否存在源代码泄露。常见有.git文件泄露，.svn文件泄露，.DB\_store文件泄露，WEB-INF/web.xml泄露。目录扫描有两种方式，使用目录字典进行暴力才接存在该目录或文件返回200或者403；使用爬虫爬行主页上的所有链接，对每个链接进行再次爬行，收集这个域名下的所有链接，然后总结出需要的信息。常用的工具有：御剑，kali下的dirb，DirBrute。

### 09 端口信息

服务和安全是相对应的，每开启一个端口，那么攻击面就大了一点，开启的端口越多，也就意味着服务器面临的威胁越大。开始扫描之前不妨使用telnet先简单探测下某些端口是否开放，避免使用扫描器而被封IP，扫描全端口一般使用Nmap，masscan进行扫描探测，尽可能多的搜集开启的端口好已经对应的服务版本，得到确切的服务版本后可以搜索有没有对应版本的漏洞。常见的端口信息及渗透方法。

端口号 端口服务/协议简要说明 关于端口可能的一些渗透用途

tcp 20,21 ftp 默认的数据和命令传输端口[可明文亦可加密传输] 允许匿名的上传下载,爆破,嗅探,win提权,远程执行(proftpd 1.3.5),各类后门(proftpd,vsftp 2.3.4)

tcp 22 ssh[数据ssl加密传输] 可根据已搜集到的信息尝试爆破,v1版本可中间人,ssh隧道及内网代理转发,文件传输,等等…常用于linux远程管理…

tcp 23 telnet[明文传输] 爆破,嗅探,一般常用于路由,交换登陆,可尝试弱口令,也许会有意想不到的收获

tcp 25 smtp[简单邮件传输协议,多数linux发行版可能会默认开启此服务] 邮件伪造,vrfy/expn 查询邮件用户信息,可使用smtp-user-**enum**工具来自动跑

tcp/udp 53 dns[域名解析] 允许区域传送,dns劫持,缓存投毒,欺骗以及各种基于dns隧道的远控

tcp/udp 69 tftp[简单文件传输协议,无认证] 尝试下载目标及其的各类重要配置文件

tcp 80-89,443,8440-8450,8080-8089 web[各种常用的web服务端口] 各种常用web服务端口,可尝试经典的top n,vpn,owa,webmail,目标oa,各类java控制台,各类服务器web管理面板,各类web中间件漏洞利用,各类web框架漏洞利用等等……

tcp 110 [邮局协议,可明文可密文] 可尝试爆破,嗅探

tcp 137,139,445 samba[smb实现windows和linux间文件共享,明文] 可尝试爆破以及smb自身的各种远程执行类漏洞利用,如,ms08-067,ms17-010,嗅探等……

tcp 143 imap[可明文可密文] 可尝试爆破

udp 161 snmp[明文] 爆破默认团队字符串,搜集目标内网信息

tcp 389 ldap[轻量级目录访问协议] ldap注入,允许匿名访问,弱口令

tcp 512,513,514 linux rexec 可爆破,rlogin登陆

tcp 873 rsync备份服务 匿名访问,文件上传

tcp 1194 openvpn 想办法钓vpn账号,进内网

tcp 1352 Lotus domino邮件服务 弱口令,信息泄漏,爆破

tcp 1433 mssql数据库 注入,提权,sa弱口令,爆破

tcp 1521 oracle数据库 tns爆破,注入,弹shell…

tcp 1500 ispmanager 主机控制面板 弱口令

tcp 1025,111,2049 nfs 权限配置不当

tcp 1723 pptp 爆破,想办法钓vpn账号,进内网

tcp 2082,2083 cpanel主机管理面板登录 弱口令

tcp 2181 zookeeper 未授权访问

tcp 2601,2604 zebra路由 默认密码zerbra

tcp 3128 squid代理服务 弱口令

tcp 3312,3311 kangle主机管理登录 弱口令

tcp 3306 mysql数据库 注入,提权,爆破

tcp 3389 windows rdp远程桌面 shift后门[需要03以下的系统],爆破,ms12-020[蓝屏exp]

tcp 4848 glassfish控制台 弱口令

tcp 4899 radmin远程桌面管理工具,现在已经非常非常少了 抓密码拓展机器

tcp 5000 sybase/DB2数据库 爆破,注入

tcp 5432 postgresql数据库 爆破,注入,弱口令

tcp 5632 pcanywhere远程桌面管理工具 抓密码,代码执行,已经快退出历史舞台了

tcp 5900,5901,5902 vnc远程桌面管理工具 弱口令爆破,如果信息搜集不到位,成功几率很小

tcp 5984 CouchDB 未授权导致的任意指令执行

tcp 6379 redis未授权 可尝试未授权访问,弱口令爆破

tcp 7001,7002 weblogic控制台 java反序列化,弱口令

tcp 7778 kloxo 主机面板登录

tcp 8000 Ajenti主机控制面板 弱口令

tcp 8443 plesk主机控制面板 弱口令

tcp 8069 zabbix 远程执行,sql注入

tcp 8080-8089 Jenkins,jboss 反序列化,控制台弱口令

tcp 9080-9081,9090 websphere控制台 java反序列化/弱口令

tcp 9200,9300 elasticsearch 远程执行

tcp 10000 webmin linux主机web控制面板入口 弱口令

tcp 11211 memcached 未授权访问

tcp 27017,27018 mongodb 爆破,未授权访问

tcp 3690 svn服务 svn泄露,未授权访问

tcp 50000 SAP Management Console 远程执行

tcp 50070,50030 hadoop 默认端口未授权访问

### 10 服务器与中间件信息

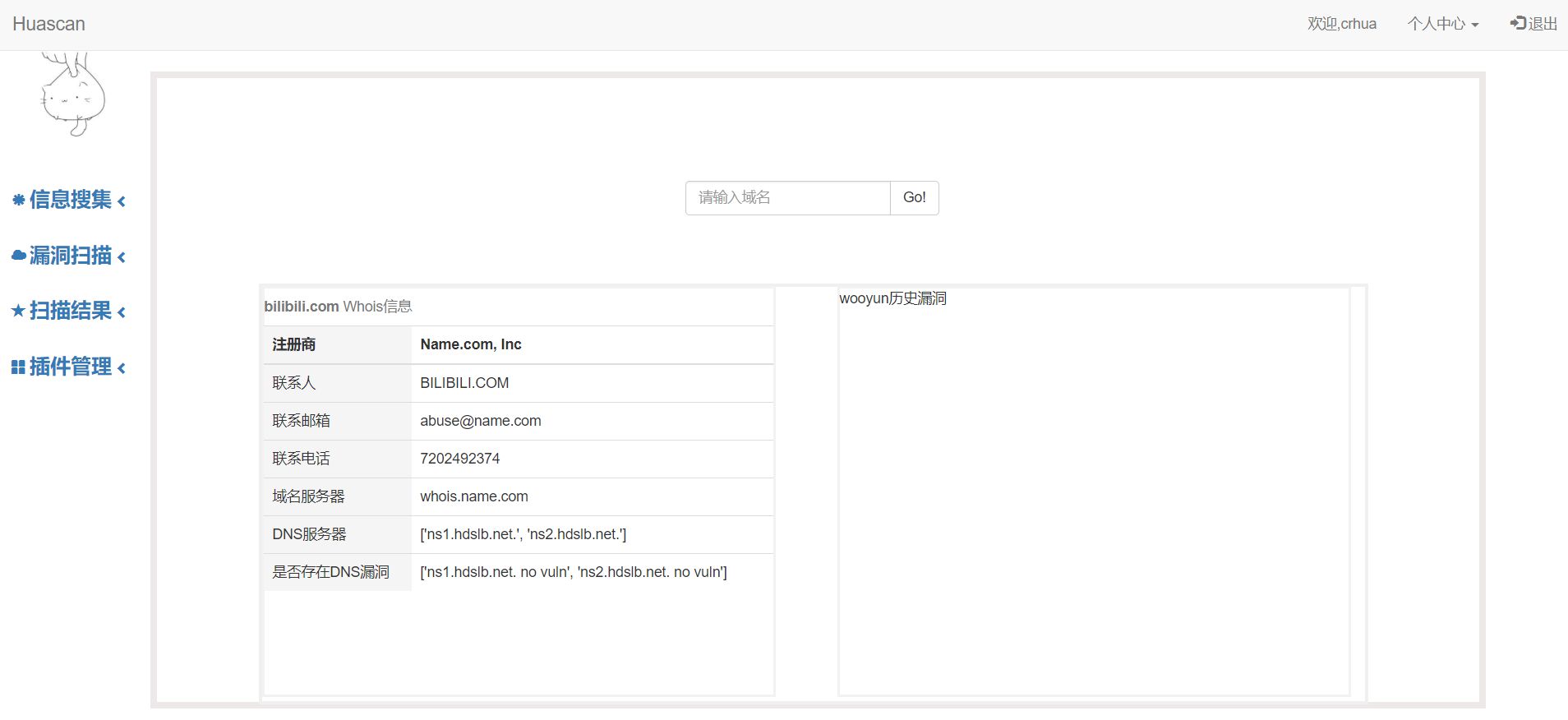
通过Nmap、Zmap等端口和指纹识别功能搜集，也可以使用nc和telnet获取Banner信息进行识别，常用工具有whatweb

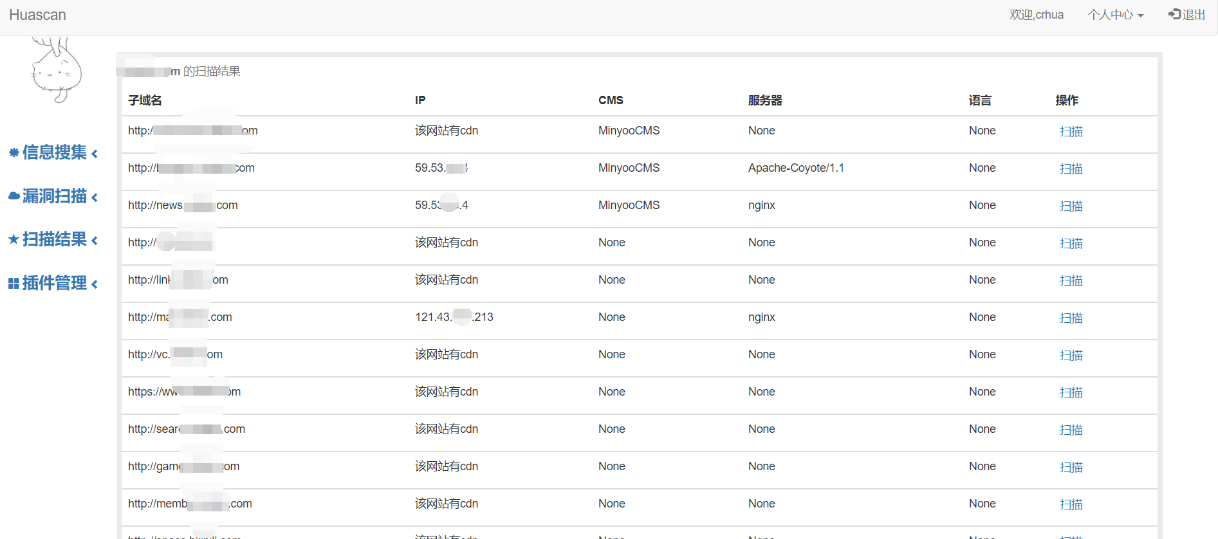


### 11 其他

探测目标是否存在WAF，WAF识别一般是基于headers头信息，例如，Mod\_Security是为Apache设计的开源Web防护模块，一个恶意的请求Mod\_Security会在响应头返回“406 Not acceptable”的信息。waf00f是kali下的识别WAF的老工具，[whatwaf](https://github.com/Ekultek/WhatWaf)不仅可以识别WAF类型还会给出一些bypass 方法；另外从乌云镜像站、CNVD搜集网站历史漏洞对渗透测试也是有很大帮助的。12 自己写的小脚本

基于以上内容写个一个蹩脚的脚本，大佬勿喷。





### 13 总结

信息搜集在渗透测试中的作用不言而喻，脚本基于以上文章的内容的编写，笔者还会继续完善，若读者有什么建议可以留言。菜鸡一定虚心接受。最后，信息搜集很重要，信息搜集很重要，信息搜集很重要。

# 第二章 安全工具

## 1. APPSCAN

IBM出的web安全漏洞扫描工具

**建议的学习方法：**

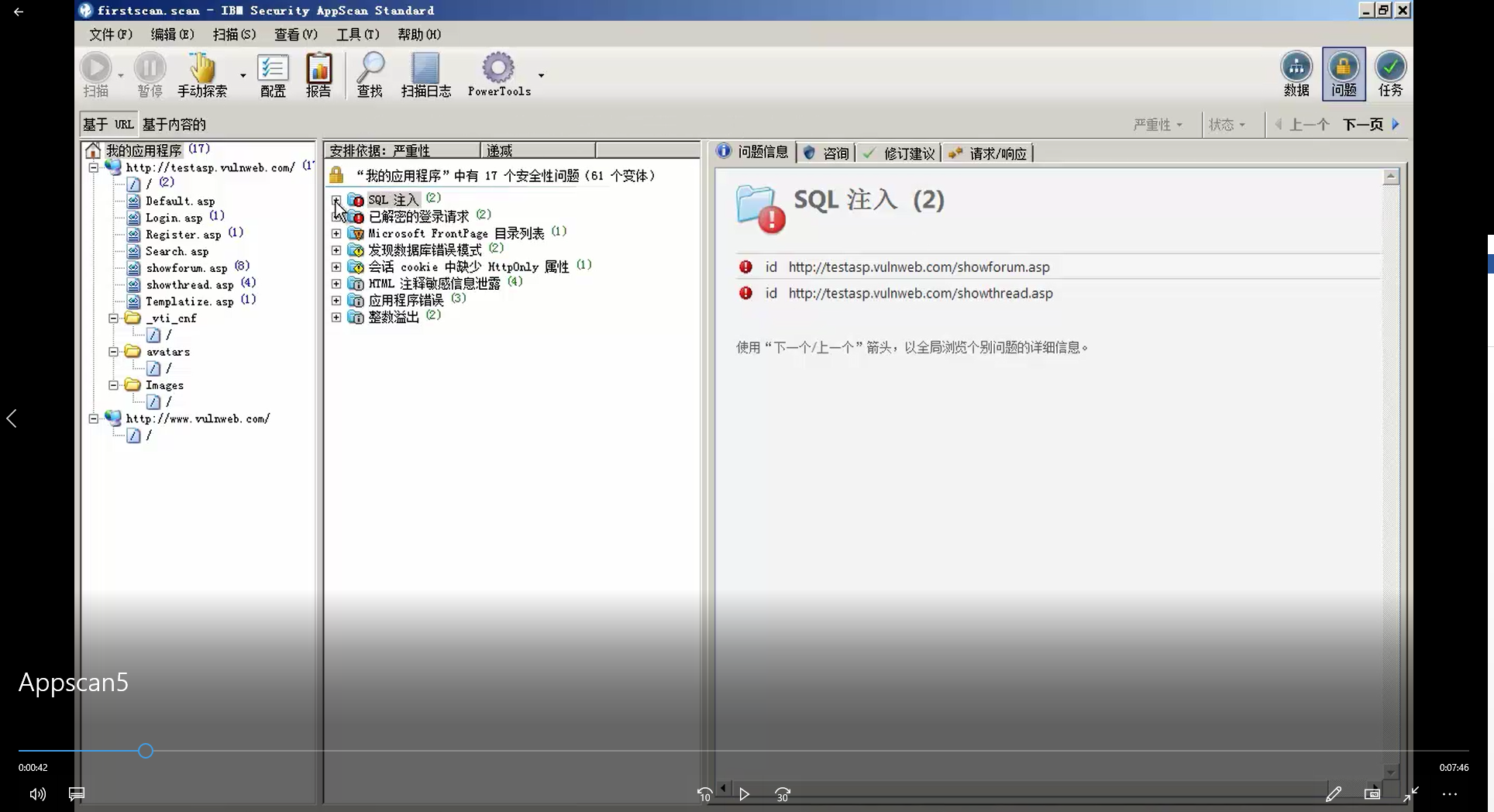
1.尽可能多的尝试使用不同的单项功能进行扫描

2.对扫描结果的每一项都仔细的查询相关的技术内容

**新建扫描**

测试地址：http://testasp.vulnweb.com/

文件—新建—常规扫描—AppSan---起始URL—登录方法---测试策略（缺省值【默认】）--启动全面自动扫描---启动扫描专家—保存—运行—问题—报告



**完全扫描配置**

**其他功能：**

Web service 扫描

Glass box扫描技术

记录代理功能

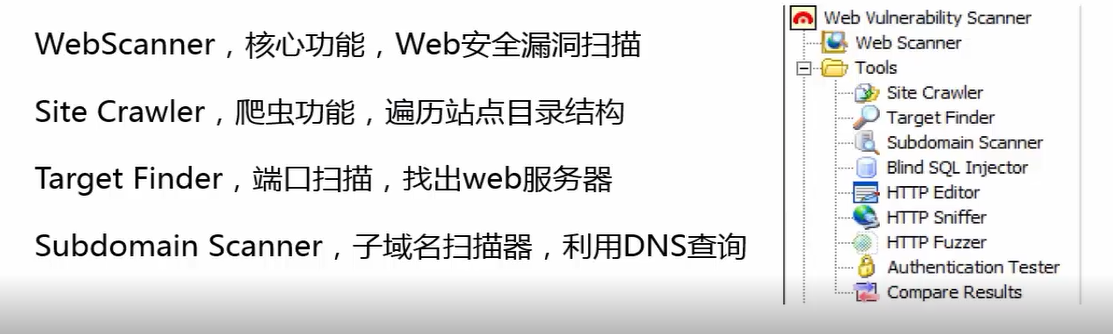
## AWVS

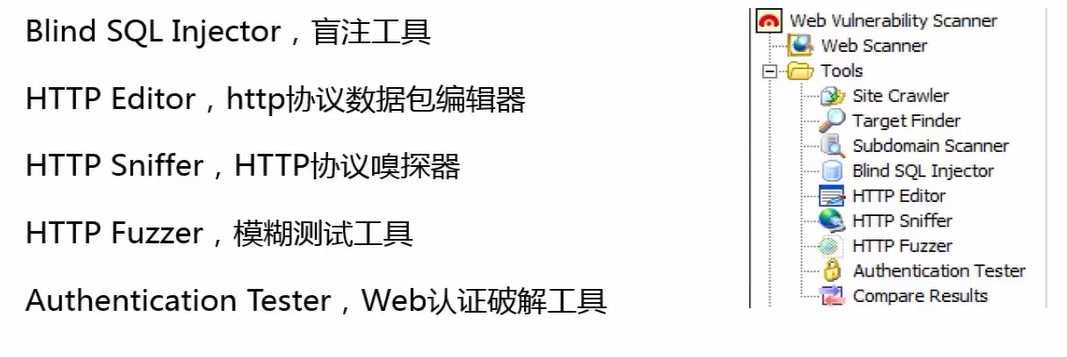
Awvs是一款自动化的web安全测试工具。

Awvs可以扫描任何通过web浏览器访问和遵循http/https规则的web站点

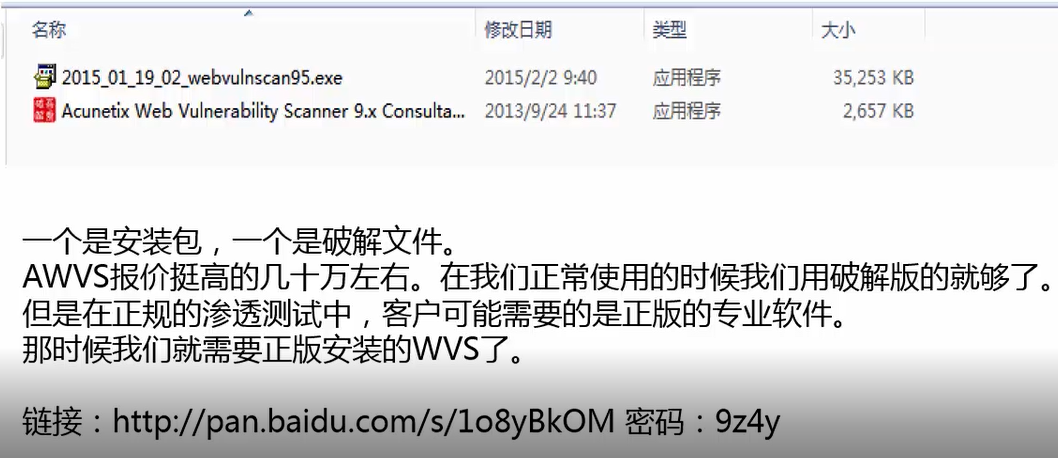
可以通过扫描漏洞，比如：sql注入，XSS。适用于任何企业的内网，外网，面向客户，厂商和其他人员的web网站

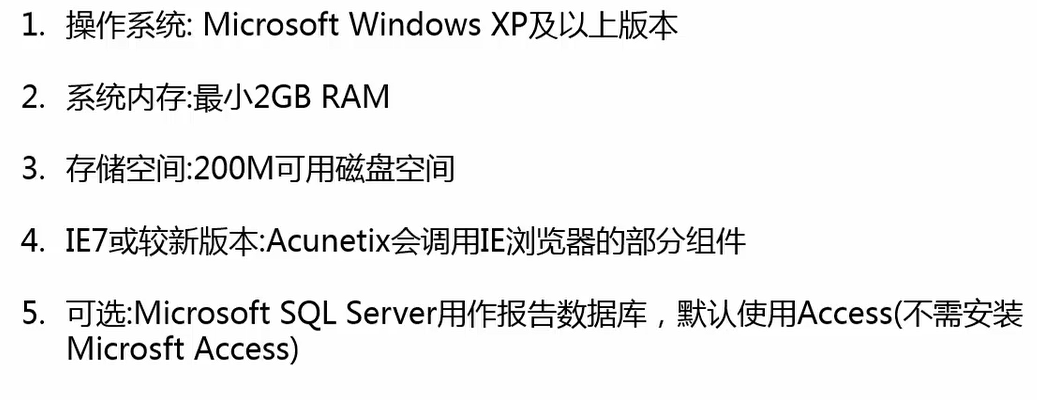
**功能介绍：**





**安装：**



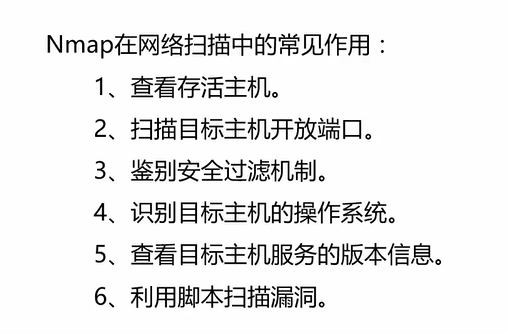
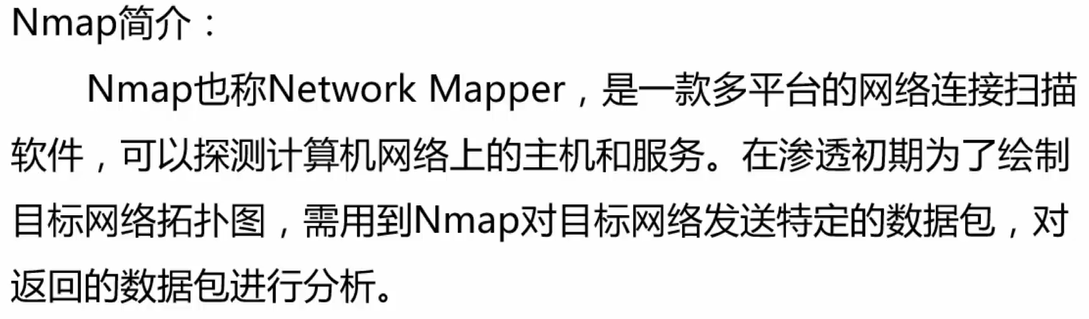


**实战：**

**New Scan---Scan single website/scan using saved crawling resutls---下一步---scanning profile（default）----scanning settings ---**

## Nessus

## Nmap



## SqlMap

基于Python编写，需要Python（2.x）环境。最好的sql注入工具。

# 第三章 漏洞专题

## 1. sql注入

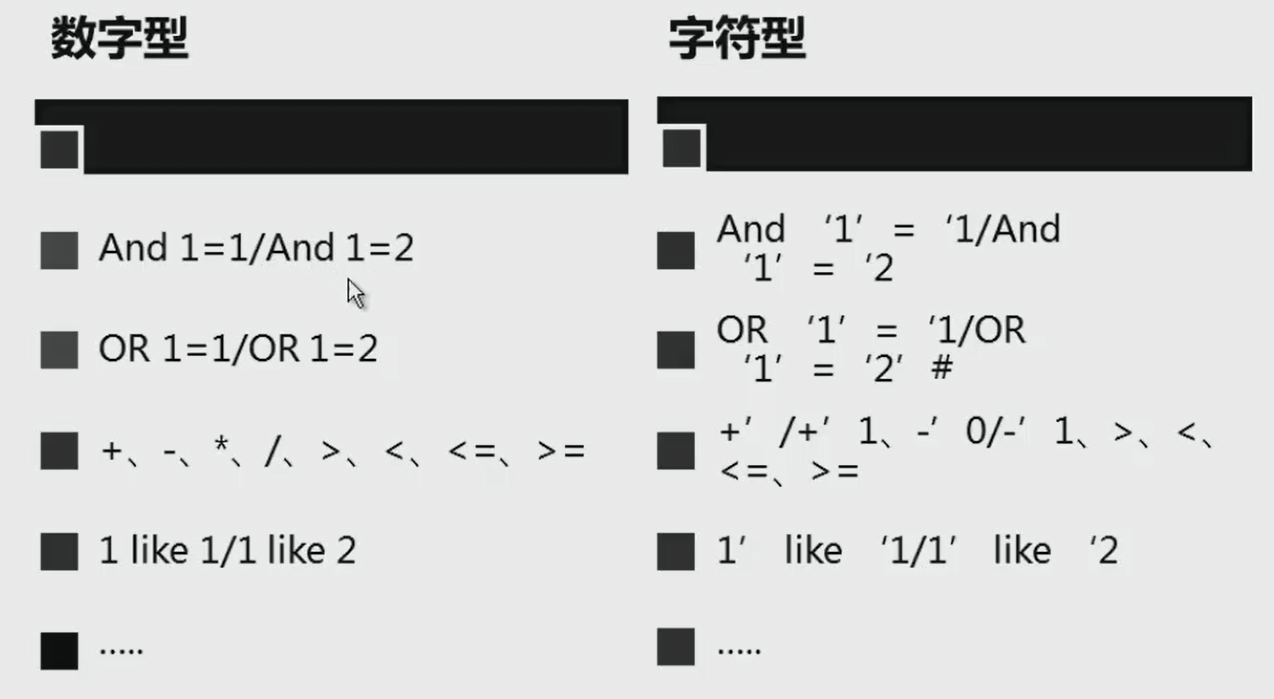
所谓SQL注入，就是通过把SQL命令插入到 Web表单提交 或 URL 或 页面请求等的查询字符串中，最终达到欺骗服务器执行恶意的SQL命令。

注入方法：手工、工具（sqlmap）

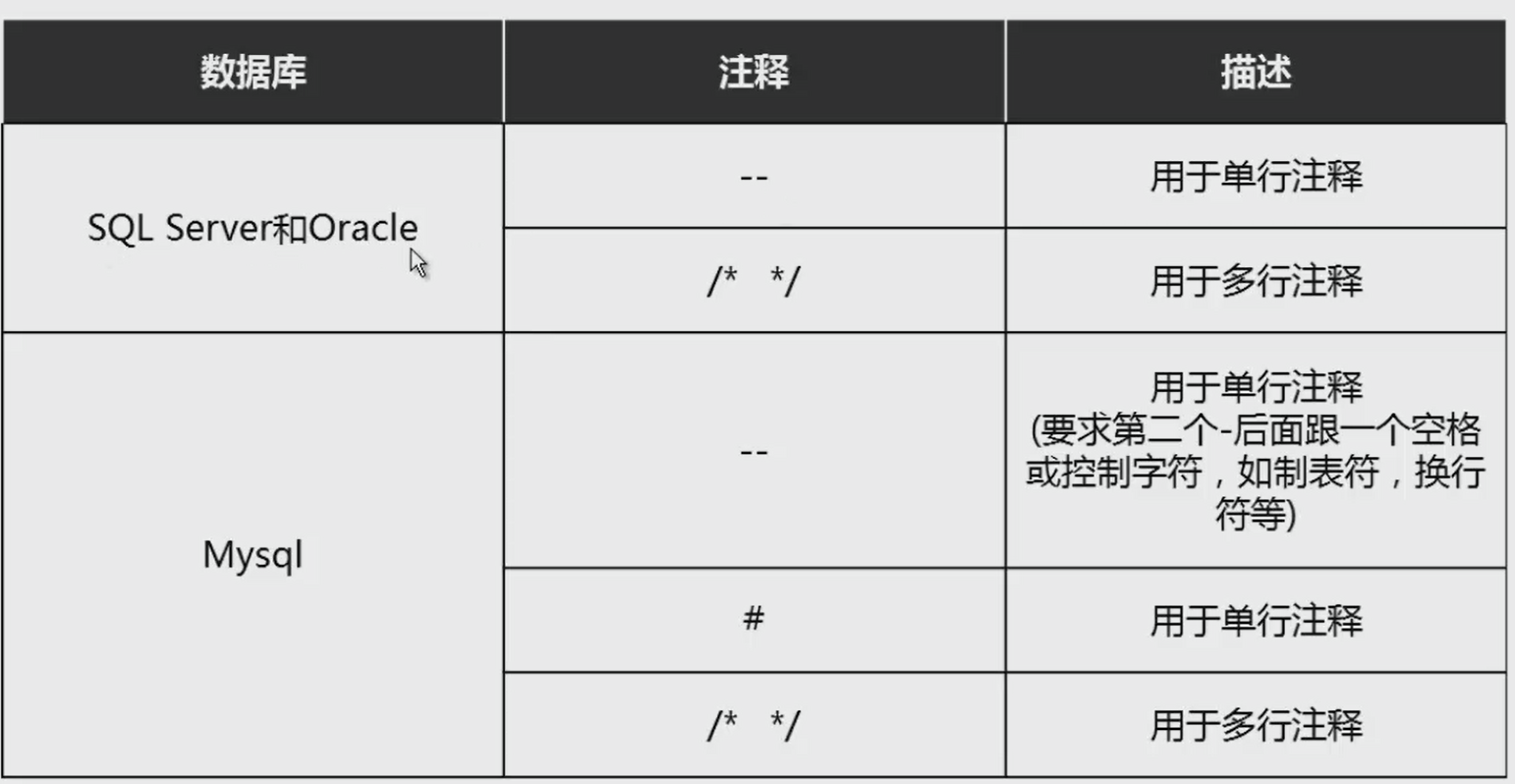
Sql注入漏洞，常见出现的地方：

URL 参数，http 包头，搜索框，目录名，文件名等等未经检查和过滤即被带入到sql语句中执行。最普遍的注入漏洞是由于参数值过滤不严导致的。

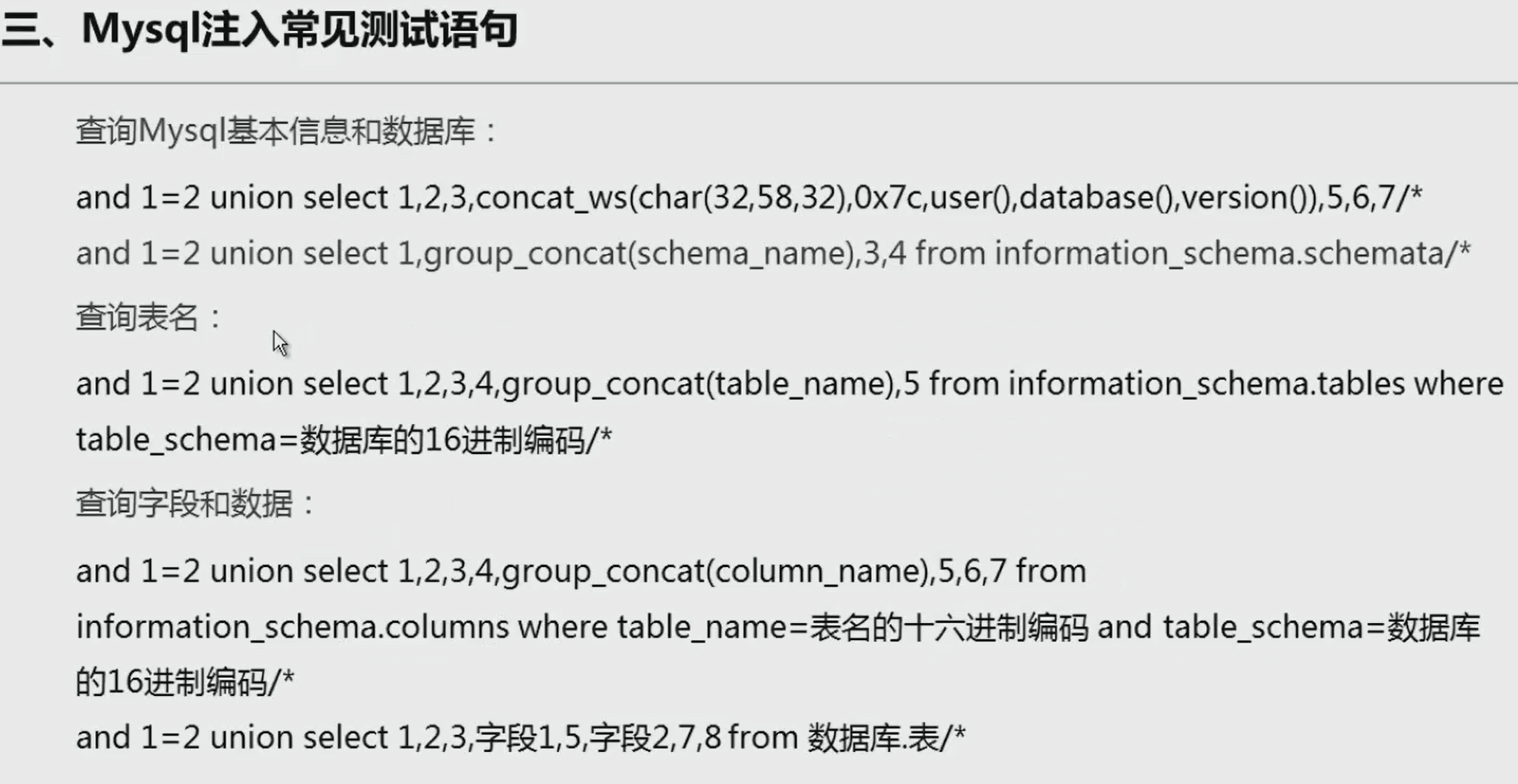
常见的sql测试语句



MySQL注入实例







Msyql注入实例：

测试URL：<https://192.168.0.1/sql.php?id=1>

测试是否存在sql注入：

<https://192.168.0.1/sql.php?id=1> and1=1

<https://192.168.0.1/sql.php?id=1> and1=2

<https://192.168.0.1/sql.php?id=1-1>

<https://192.168.0.1/sql.php?id=1>’

确认可注入，注入过程：

<https://192.168.0.1/sql.php?id=1> order by 6#

# 号代表注入

在6开始报错说明这个表有5个字段

接下里查看表结构

<https://192.168.0.1/sql.php?id=1>-1 union select 1,2,3,4,5#

查看数据库的一些信息：

<https://192.168.0.1/sql.php?id=1-1> union select user(),@@version(),database(),@@basedir,laod\_file(‘c:/win.ini’)#