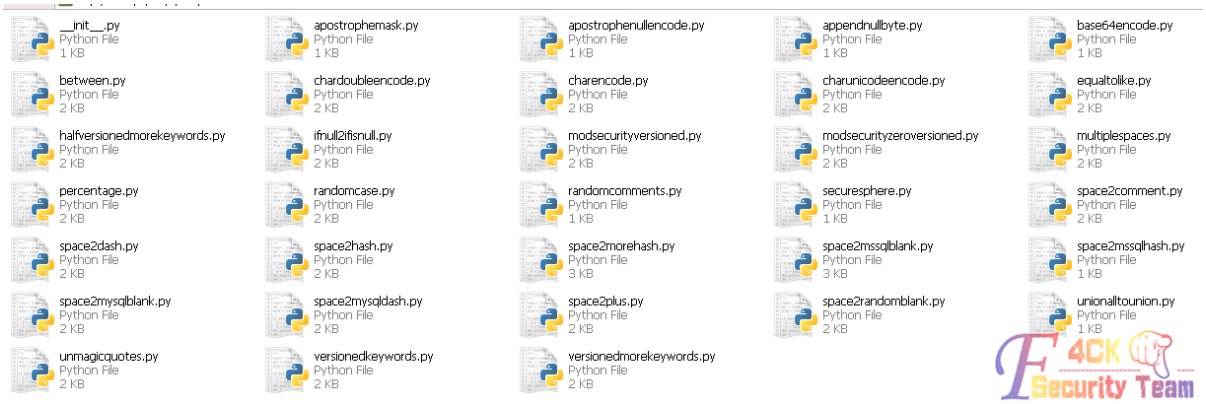
作品：使用 **sqlmap** 绕过过滤

作者：**arschloch**

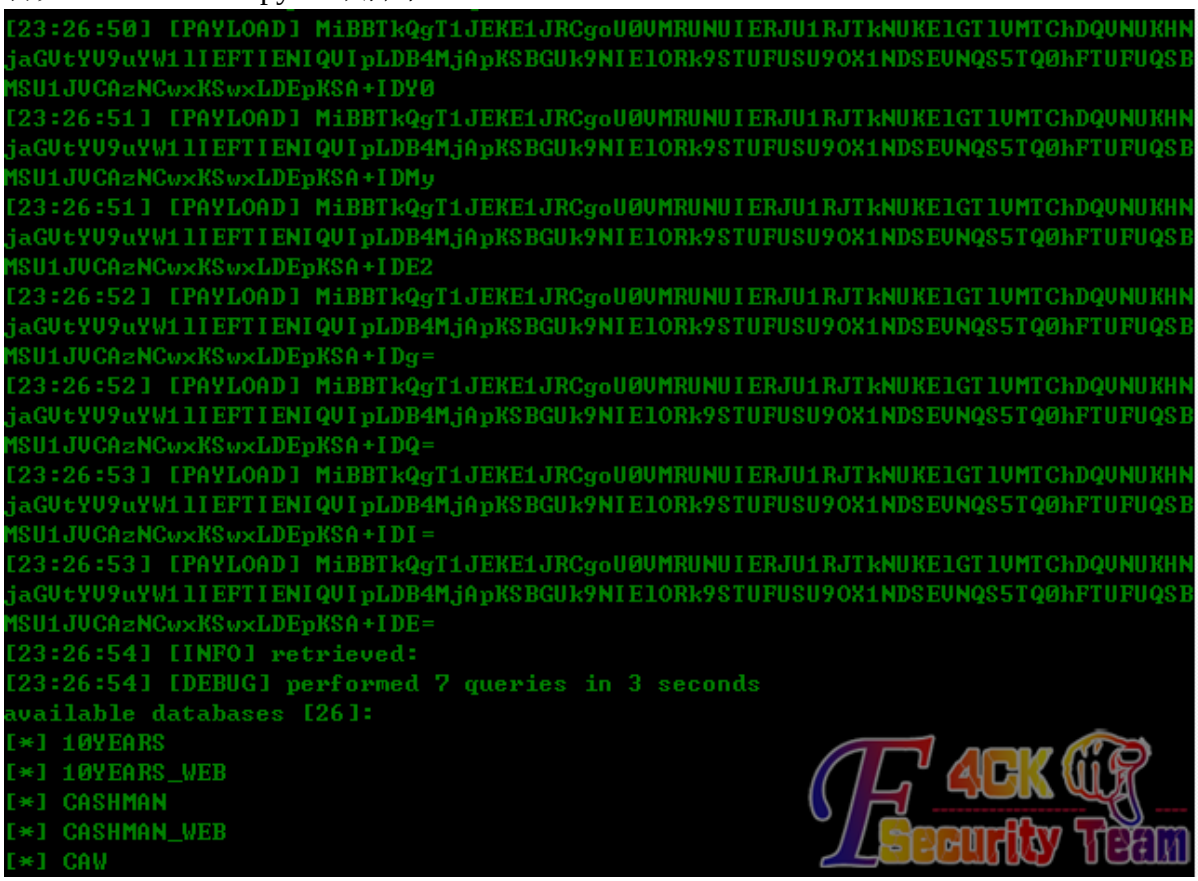
来自：法客论坛 **– F4ckTeam**

网址：**http://team.f4ck.net/**

大家都在积极的参加线上活动，那我也发个文章 O(∩_∩)O~
sqlmap 传说中的注入神器，一般的参数大家都用的灰常熟练了，那对于--tamper 这个参数大家了解多少？



这是 sqlmap 自带所有 tamper 脚本，当大家遇到注入被过滤关键字的时候是不是很惆怅，那么就到了 tamper 这个参数大发神威的时候了。
文章没有多少技术含量，算是普及贴，由于脚本较多，这里只说几个比较常用的，其他的大家自己动手去试一下就明白了。文章大多用图来说明。
首先 base64encode.py 这个脚本



上图可以看出，所有的注入语句已经都被转为 base64 的格式，对于以前那个《Base64 变形注入》貌似有着奇效！

上图：charencode.py（* mssql 2005 * MySQL 4, 5.0 and 5.5 * Oracle 10g* PostgreSQL 8.3, 8.4, 9.0）

chardoubleencode.py（ * mssql 2000 mssql 2005 MySQL 5.1.56 PostgreSQL 9.0.3）

两个脚本通过打乱编码来绕过关键字被过滤的情况

上图：为 space2mssqlblank.py（mssql 2000 和 05）和 space2mysqlblank.py（MySQL 5.1） mysql 允许空格被替换为 09，0A-0D，A0，

MSSQL 中允许 01-1F 替换为空格符

space2morehash.py 对应 mysql>= 5.1.13 和 MySQL 5.1.41，space2hash.py 对应 mysql 版本 4.0,5.0

上图可以发现空格符被替换为%23randomText%0A 这样的形式，而 CHAR(), USER()这样的函数被替换为% % 0 randomText 23()这样的形式，

啊？大家问为什么啊？为什么？这是规定，我也不知道为什么，想了解的就看这个 mysql 函数名称解析 这个破网站，我用这个脚本可以绕过去。so，这个很不错！

差不多就这个样子，虽然只说了几个，但是希望能起个抛砖引玉的作用，sqlmap 剩下的功能大家一起多多挖掘。O(∩_∩)O~

再加一句，额 ，哪位大牛能把 sqlmap 的-g 的 google 引擎替换为百度呢，或者把 google 的地址改为.com.hk.....