Admin MySQL Auxiliary Modules a11y.text Admin MySQL Auxiliary Modules mysql_enum a11y.text mysql_enum The mysql_enum module will connect to a remote MySQL database server with a given set of credentials and perform some basic enumeration on it.

```
msf > use auxiliary/admin/mysql/mysql_enum
msf auxiliary(mysql_enum) > show options

Module options (auxiliary/admin/mysql/mysql_enum):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOST                      yes       The target address
   RPORT     3306             yes       The target port
   USERNAME                   no        The username to authenticate as
```

To configure the module, we provide values for PASSWORD, RHOST, and USERNAME then let it run against the target.

```
msf auxiliary(mysql_enum) > set PASSWORD s3cr3t
PASSWORD => s3cr3t
msf auxiliary(mysql_enum) > set RHOST 192.168.1.201
RHOST => 192.168.1.201
msf auxiliary(mysql_enum) > set USERNAME root
USERNAME => root
msf auxiliary(mysql_enum) > run

[*] Running MySQL Enumerator...
[*] Enumerating Parameters
[*]  MySQL Version: 5.1.41
[*]  Compiled for the following OS: Win32
[*]  Architecture: ia32
[*]  Server Hostname: xen-xp-sploit
[*]  Data Directory: C:\xampp\mysql\data\
[*]  Logging of queries and logins: OFF
[*]  Old Password Hashing Algorithm OFF
[*]  Loading of local files: ON
[*]  Logins with old Pre-4.1 Passwords: OFF
[*]  Allow Use of symlinks for Database Files: YES
[*]  Allow Table Merge:
[*]  SSL Connection: DISABLED
[*] Enumerating Accounts:
[*]  List of Accounts with Password Hashes:
[*]   User: root Host: localhost Password Hash:
*58C036CDA51D8E8BBBBF2F9EA5ABF111ADA444F0
[*]   User: pma Host: localhost Password Hash:
*602F8827EA283047036AFA836359E3688401F6CF
[*]   User: root Host: % Password Hash: *58C036CDA51D8E8BBBBF2F9EA5ABF111ADA444F0
[*]  The following users have GRANT Privilege:
[*]   User: root Host: localhost
[*]   User: root Host: %
[*]  The following users have CREATE USER Privilege:
[*]   User: root Host: localhost
[*]   User: root Host: %
[*]  The following users have RELOAD Privilege:
[*]   User: root Host: localhost
[*]   User: root Host: %
[*]  The following users have SHUTDOWN Privilege:
[*]   User: root Host: localhost
[*]   User: root Host: %
[*]  The following users have SUPER Privilege:
[*]   User: root Host: localhost
[*]   User: root Host: %
[*]  The following users have FILE Privilege:
[*]   User: root Host: localhost
[*]   User: root Host: %
[*]  The following users have POCESS Privilege:
[*]   User: root Host: localhost
[*]   User: root Host: %
[*]  The following accounts have privileges to the mysql databse:
[*]   User: root Host: localhost
[*]   User: root Host: %
[*]  The following accounts are not restricted by source:
[*]   User: root Host: %
[*] Auxiliary module execution completed
msf auxiliary(mysql_enum) > mysql_sql a11y.text mysql_sql The mysql_sql module performs SQL
queries on a remote server when provided with a valid set of credentials. msf > use
auxiliary/admin/mysql/mysql_sql
msf auxiliary(mysql_sql) > show options


Module options (auxiliary/admin/mysql/mysql_sql):
   Name      Current Setting   Required  Description
   ----      ---------------   --------  -----------
   PASSWORD                    no        The password for the specified username
   RHOST                       yes       The target address
   RPORT     3306              yes       The target port
   SQL       select version()  yes       The SQL to execute.
   USERNAME                    no        The username to authenticate as
```

To configure the module, we provided the PASSWORD, RHOST, and USERNAME settings and we will leave the default query to pull the server version.

```
msf auxiliary(mysql_sql) > set PASSWORD s3cr3t
PASSWORD => s3cr3t
msf auxiliary(mysql_sql) > set RHOST 192.168.1.201
RHOST => 192.168.1.201
msf auxiliary(mysql_sql) > set USERNAME root
USERNAME => root
msf auxiliary(mysql_sql) > run

[*] Sending statement: 'select version()'...
[*]  | 5.1.41 |
[*] Auxiliary module execution completed
msf auxiliary(mysql_sql) >
```

Next Admin MSSQL Auxiliary Modules Prev Admin HTTP Auxiliary Modules