Removing Defaults and Hardening

Introduction

You may wish to change the defaults for several sensitive items before deploying Open-AudIT. These are detailed below.

MySQL credentials

Open-AudIT User

Open-AudIT (as per any normal web application) uses a configured set of credentials to access the MySQL database.

These can be found in :

Windows: c:\xampp\open-audit\code_igniter\application\config\database.php

Linux: /usr/local/open-audit/code_igniter/application/config/database.php

To create a fresh new database user, run the below (if using Windows, first do **cd c:\xampp\mysql**.

If you have installed Open-AudIT on a newly installed database, in the installer you may have elected to set the root user password. By default this password is **openauditrootuserpassword**.

On some Linux distributions, if you **sudo su** to the root user, no password is required, hence remove the **-p** options from the commands below.

Substitude your username and password for YOUR_USER and YOUR_PASSWORD in the commands below.

```
mysql -u root -p -e "CREATE USER YOUR_USER@localhost IDENTIFIED BY 'YOUR_PASSWORD';"

mysql -u root -p -e "GRANT ALL PRIVILEGES ON openaudit.* TO YOUR_USER@localhost IDENTIFIED BY 'YOUR_PASSWORD';
FLUSH PRIVILEGES;"
```

Now test running a query by the command below.

NOTE - There is no space between the **-p** and **YOUR_PASSWORD**.

```
mysql -u YOUR_USER -pYOUR_PASSWORD openaudit -e "SELECT * FROM configuration WHERE name = 'internal_version';"
```

You should see a result as below.

```
+-----+------------------+----------+--------+----------+-----------+---------------------
+-------------------------------------+
| id  | name             | value    | type   | editable | edited_by | edited_date         |
description                          |
+-----+------------------+----------+--------+----------+-----------+---------------------
+-------------------------------------+
| 115 | internal_version | 20220126 | number | n        | system    | 2000-01-01 00:00:00 | The internal
numerical version.     |
+-----+------------------+----------+--------+----------+-----------+---------------------
+-------------------------------------+
```

Once you have confirmed the user can access the openaudit database, we need to change the credentials file.

Edit the file as above, replacing the username and password fields.

```
$db['default']['username'] = "YOUR_USER";
$db['default']['password'] = "YOUR_PASSWORD";
```

Root User

Changing the password of the MySQL root user can also be completed as above. I would recommend the below though, for safety.

You will need two shells on the Open-AudIT server open.

Log on as the MySQL root user in session #1.

```
mysql -u root -p
```

In the second shell (after successfully logging in above) run the below command, substituting YOUR_NEW_ROOT_PASSWORD.

```
mysql -u root -p -e "USE mysql; SET PASSWORD FOR 'root'@'localhost' = password('YOUR_NEW_ROOT_PASSWORD'); FLUSH
PRIVILEGES;
```

Now try to log in using that same (second) shell.

```
mysql -u root -pYOUR_NEW_ROOT_PASSWORD
```

If you can log in, you're all done!

If you cannot log in, something has gone wrong - and that is why we have the second session open and already logged in.

Your root user may have different items set, such as it's **Host** attribute. You should use the already logged in user to check, as below.

```
SELECT User, Host, Password FROM mysql.user;
```

And change the **SET PASSWORD** command above to reflect the Host value in the second session.

Restricting MySQL to localhost

On our shipped version for Windows, we already restrict to localhost.

On some Linux distributions, you *might* find MySQL listening on **all** IP addresses. Unless you have a specific reason for this, it is very much recommended to restrict this to localhost.

You can check the listening address by running the below command.

For Debian and Ubuntu

```
sudo grep -R bind /etc/mysql/
```

For Redhat and Centos

```
sudo grep -R bind /etc/my.cnf.d/
```

If you don't get a result, try runnig the below netstat command.

```
sudo netstat -lntup | grep mysqld
```

If you see an IP address of 0.0.0.0 with a port of (usually) 3306 (as below), this means MySQL is listening on all available IPs.

```
root@dev:/etc/mysql# sudo netstat -lntup | grep mysqld
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      8491/mysqld
```

You should configure the **bind-address** to be 127.0.0.1 in:

Debian / Ubuntu: /etc/mysql/mariadb.conf.d/50-server.cnf

Redhat / Centos: /etc/my.cnf.d/server.cnf

```
bind-address                = 127.0.0.1
```

Credentials Encryption Key

Open-AudIT encrypts credentials when it stores them in the database, but we must be able to decrypt them in order to use them when querying devices. Because this is reversible encryption, we need a shared secret (or key). This is kept in the file:

Windows: c:\xampp\open-audit\code_igniter\application\config\config.php

Linux: /usr/local/open-audit/code_igniter/application/config/config.php

Look for the variable as below.

```
$config['encryption_key'] = "openaudit";
```

Warning - If you are using the Collectors feature of Open-AudIT Enterprise, this key must be changed on ALL instances - both Server and Collector(s).

Warning #2 - If you already have credentials stored in the database, changing this key will render them unable to be decrypted. I'd suggest exporting the credentials, deleting them all, changing the key, then importing them.

Exporting, deleting and Importing can be done using the GUI.

Admin User and Licensing

You are free to change the password for the Admin user, but the user name itself should be left as is. If changed the license entry will be broken.

This is because at the moment we restrict access to the license functionality based on username, with no GUI options to change it.

If you **must** change the username, set your license before doing so.

This will be addressed in a future version, however Opmantek can be contacted to walk you through editing files and inserting a license if **absolutely** required. This is non-trivial.