VULNERABILITY REPORT

Software and Database Vulnerabilities

Prepared by:

Dinesh Servamsetty

Master's in Computer Security

Vulnerabilities Summary

SECURITY AUDIT CONTEXT:

AUDIT DATE	11/03/2019	11:15:00 AM
REPORT DATE	11/03/2019	20:30:00 PM
AUDIT DURATION	09:30:00	
TOOLS	WIRESHARK	

VULNERABILITY SUMMARY:

S.No	Method	Vulnerability	Impact
1	Secret present in the executable file	Yes	**Critical**
2	Password shown when typing	Yes	**Critical**
3	Network communication not encrypted	Yes	**Critical**
4	Admin options accessible from limited user	Yes	**Critical**
5	Weak passwords accepted	Yes	**Critical**
6	Secrets present in configuration file (config.ini)	Yes	**Critical**
7	Passwords stored in plaintext within database	Yes	**Critical**

RECOMMENDATIONS:

The following recommendations are based only on the results of the vulnerability scans.

1. Don’t store the passwords in executable files.
2. Make sure passwords are encrypted when typing.
3. Network communication should be encrypted.
4. Make sure administrative options are accessible to only authorised persons like network or system admins and block the access to unauthorised persons.
5. Don’t allow the users to set week passwords. Password length should be minimum 8 characters including special characters.
6. Don’t store the secrets in configuration files.
7. Encrypt the passwords stored in database.

INDEX

VULNERABILITIES

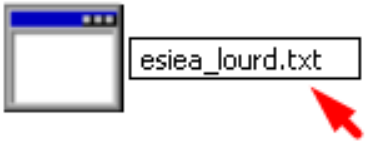
1. Secret present in the executable file

Description: Password is stored in executable file. It is possible to change .exe to .txt format. When the format has changed to .txt and search for password, master password is clearly visible as **superstar** which is used to login.

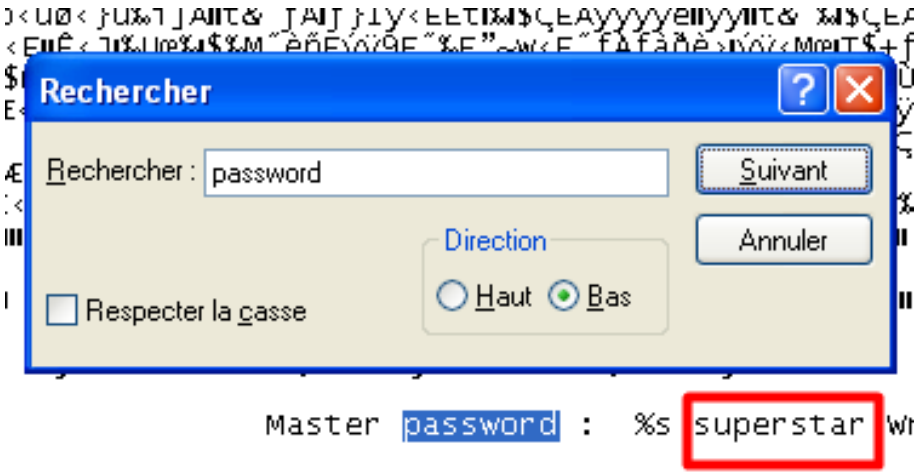
Exploitation:

Step:1 Find the **esiea_lourd.exe** file.

Step:2 Change the .exe file format to .txt as shown in below picture and save the format.



Step:3 Open .txt file and search (CNTRL+F) for password as show in below picture. It will display the master password as **superstar**



Recommendation:

- This issue occurs because password is stored in .exe file which is able to change in to .txt format easily.
- It is recommended not to store the passwords in executable file.
- Change the password storage format to **tier-3**, i.e. passwords should be encrypted and stored in database, not in application.
- Don't allow the .exe file to change into .txt file in which attackers can find confidential information.

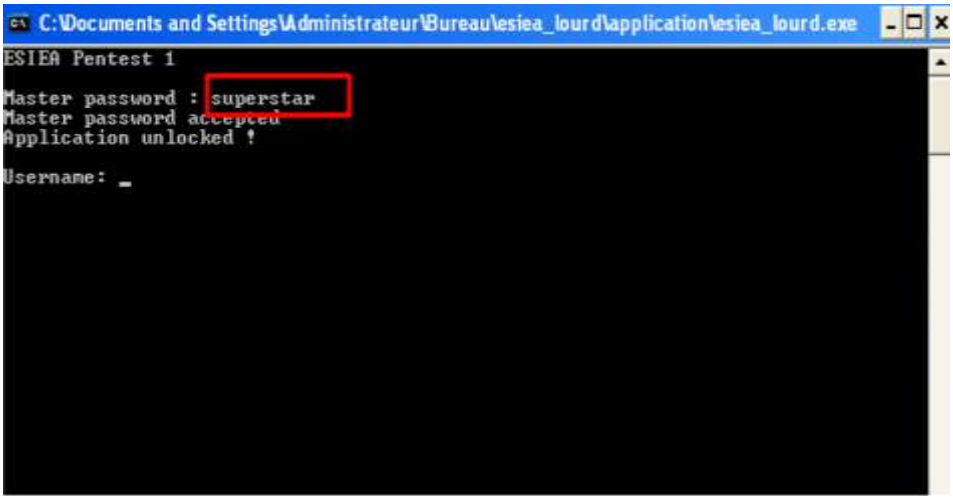
2. Password shown when typing

Description: When the password is entered in the admin interface, it is not encrypted and clearly visible. If the attacker has access to the user's system, they can watch the user's credentials, which leads to further attacks. Cryptographic algorithms for password protection are not used.

Exploitation:

Step 1: Open esiea_lourd.exe file

Step 2: Enter master password- superstar and here the password is not encrypted, it is visible.



Step 3: After entering master password, it will ask you for username and password of database, when you enter credentials, they are not encrypted.

Recommendation:

- The default configuration of displaying the credentials when typed can be configured to hide the passwords.
- Application developer must configure the code in such a way that password is not visible when entered.
- . Cryptographic algorithms for password protection should be used.

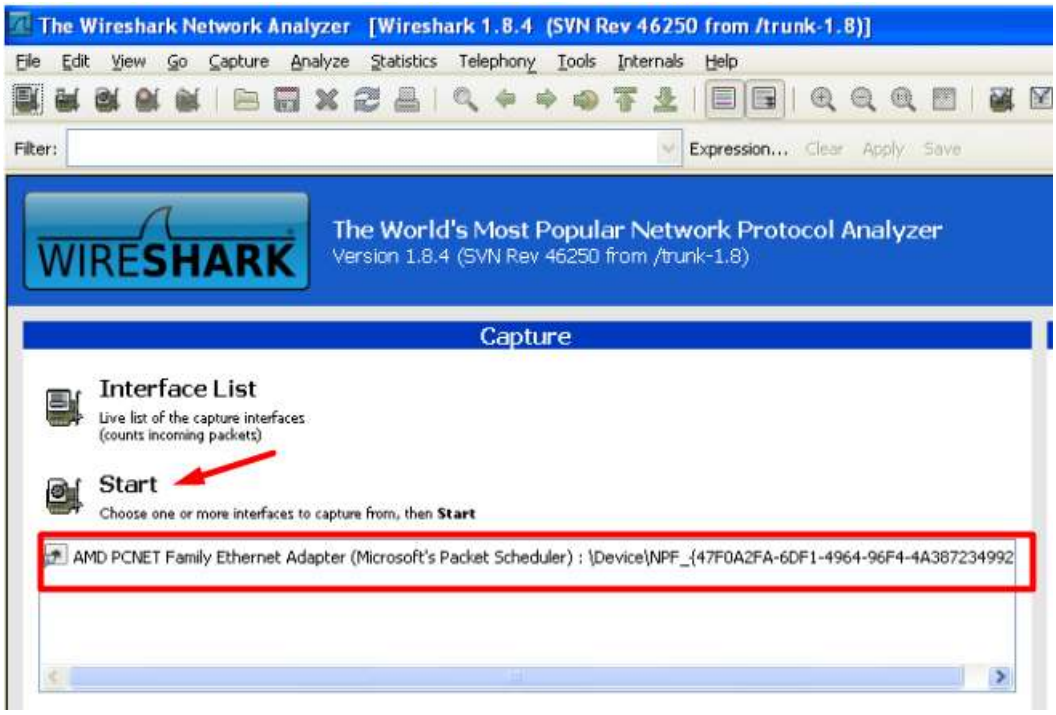
3. Network communication not encrypted

Description: Network communication is not encrypted and it is possible to sniff the credentials using Wireshark tool. If the communication is not encrypted, hackers can sniff the credentials by Man-in-the-Middle attack. Hacker can gain further information like source and destination Ip address, mac address, port no's, and protocols.

An attacker views a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users. The network can be flooded and the connection between two computers can be disrupted.

Exploitation:

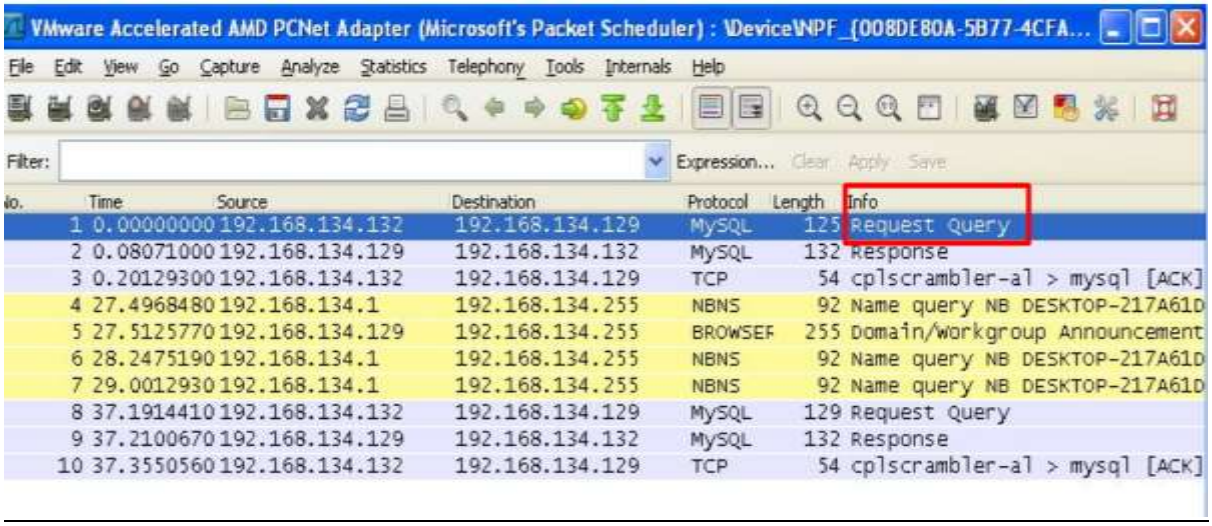
Step 1: Open Wireshark and select the network interface and click on start as shown in below picture.



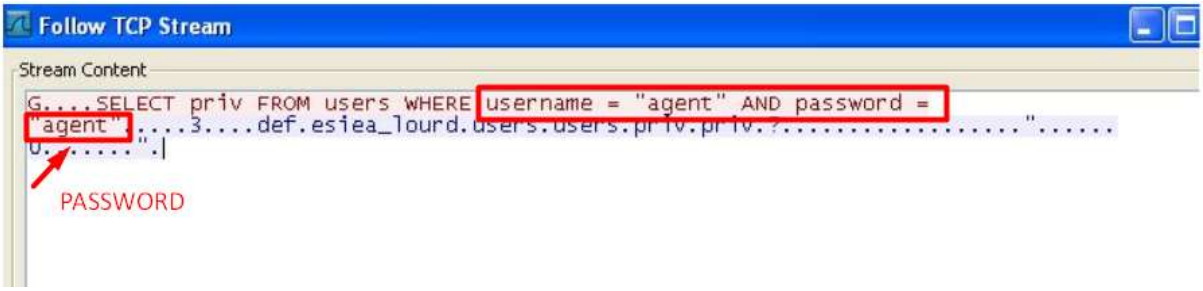
Step 2: Open executable file and enter username: agent and password: agent

Step 3: Now switch to Wireshark, you see the Wireshark capturing login packets "**Request Query**".

Right click on request query packet and select **Follow tcp stream** option.



Step 4: In the below picture, username and passwords are captured.



Recommendations:

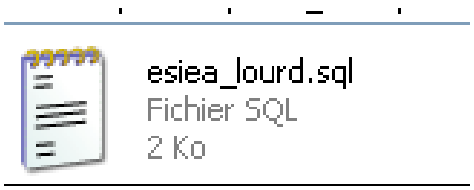
- The application should have strong encryption mechanism.
- Passwords should not be sent in plain text.

4. Admin options accessible from limited users.

Description: Confidential files of database are accessible to unauthorized persons. Access to admin with full permissions will be possible to **read, update and delete** arbitrary data from database.

Exploitation:

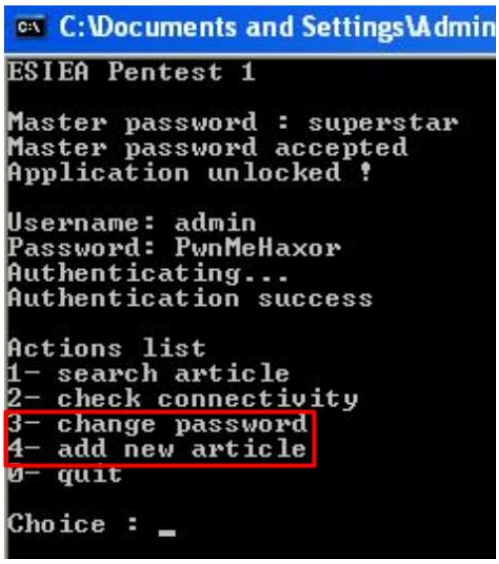
Step 1: Open esiea_lourd.sql file in database folder.



Step 2: In this file, admin username and passwords are stored in clear text.

```
TABLE IF NOT EXISTS `articles` (                `id` int(11) NOT NULL AUTO_INCREMENT,
 (`id`, `username`, `password`, `age`, `priv`) VALUES        (1, 'admin', 'PwnMeHaxor', 30, 0),
```

Step 3: Now open esiea_lourd.exe and enter the **master password** and **admin** username and password. Now you found, options 3 & 4 in **Actions list** where you can able to modify **change password & add new article.**



Recommendations:

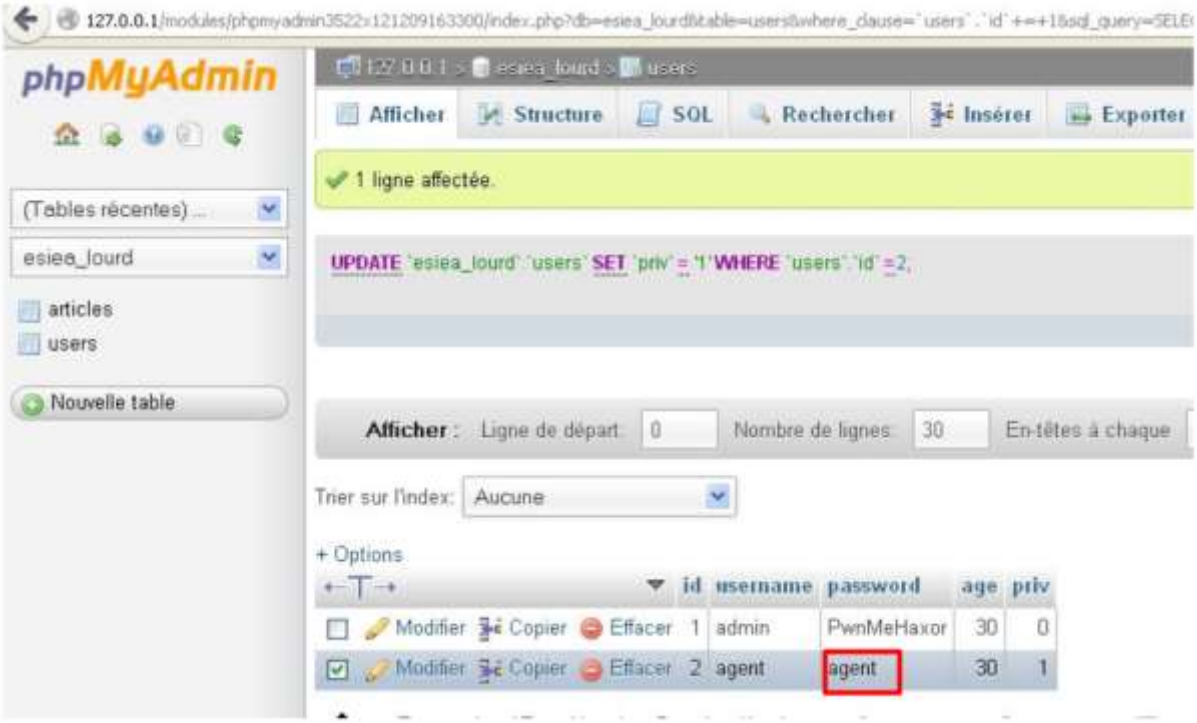
- Don’t allow the admin access to normal users
- Don’t store the admin credentials in clear text.
- Restricts the database files from unauthorized users.

5. Weak passwords accepted

Description: The password is main key to the entire database system and all its files. If the weak passwords are accepted by database due to low security policies then attacker can easily guess the password. This vulnerability is high severity alert and is susceptible to dictionary or brute force attacks.

Exploitation:

Step 1: As user **agent** password is set to **agent** in unencrypted format as shown in below picture.



Step 2: When I change the password from **agent** to **123** as week password. It has successfully accepted.

Recommendations:

- Password length should be minimum 8 characters with uppercase and lowercase letters
- Password should contain special characters
- Password should not contain username
- Password should not be easily guessable like username, data of birth, company names, pet names.
- Change the password every 60-90 days.
- Password should not contain any words from dictionary like orange, computer, television etc.
- For more information visit https://cwe.mitre.org/data/definitions/521.html

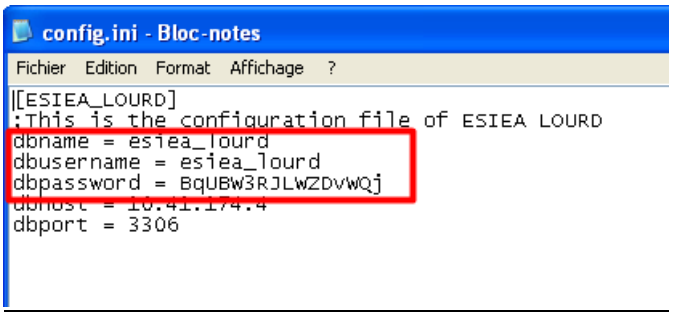
6. Secret present in configuration file (config.ini)

Description: The database username and password are stored in configuration file which is accessible to unauthorized person. If the hacker gained this config file, may result in database compromise.

Exploitation:

Step 1: Open config.ini file.

Step 2: dB name, dB username, dB password are present in config.ini file.



Recommendations:

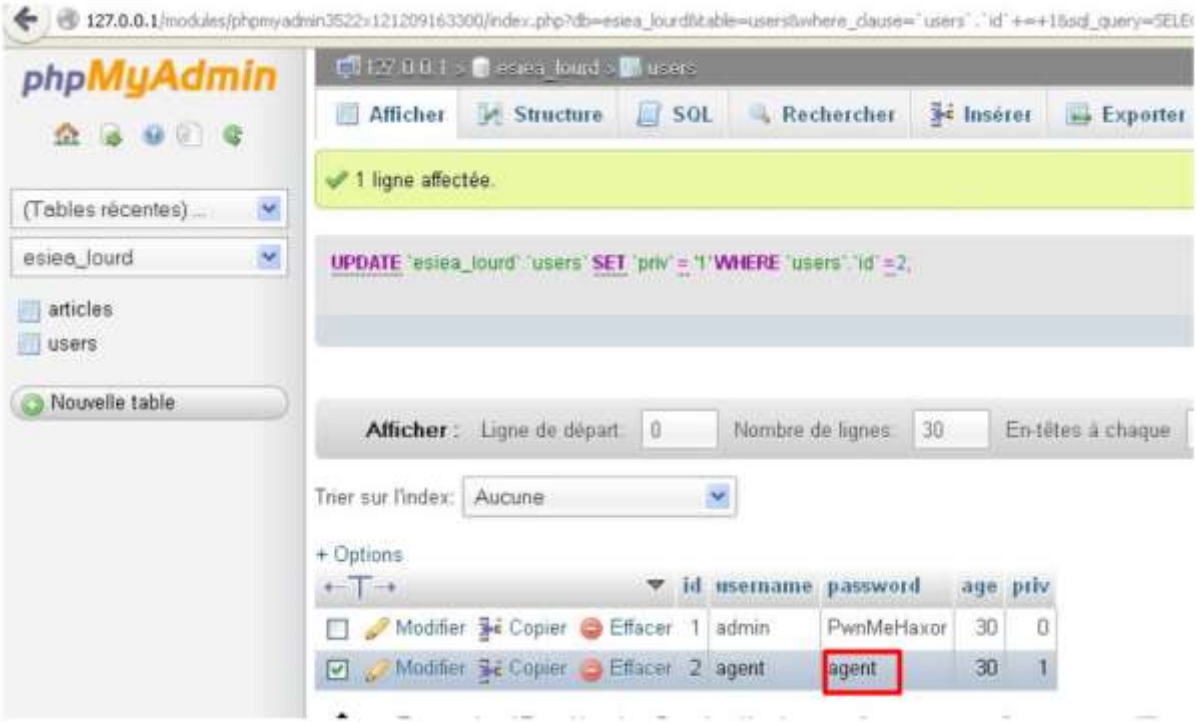
- Username and password should not be included in configuration file in plain text.
- Use standard algorithms and to encrypt the credentials stored in configuration files.
- Configuration files should be protected from accessing to unauthorized users.
- For more information visit
  https://cwe.mitre.org/data/definitions/13.html
  https://cwe.mitre.org/data/definitions/256.html
  https://cwe.mitre.org/data/definitions/260.html

7. Passwords stored in plaintext within database

Description: Storing passwords in plaintext is highly vulnerable and it allows attackers to access to the password-protected resource.

Exploitation:

Step 1: As shown in below picture, user **agent** password is not encrypted.



Recommendations:

- Use hashing algorithms, password salting or strong password library such as Bcrypt, Scrypt to encrypt the passwords in database.
- Ensure the database password hashes are stored and locked down as possible.
- For more information visit https://cwe.mitre.org/data/definitions/312.html

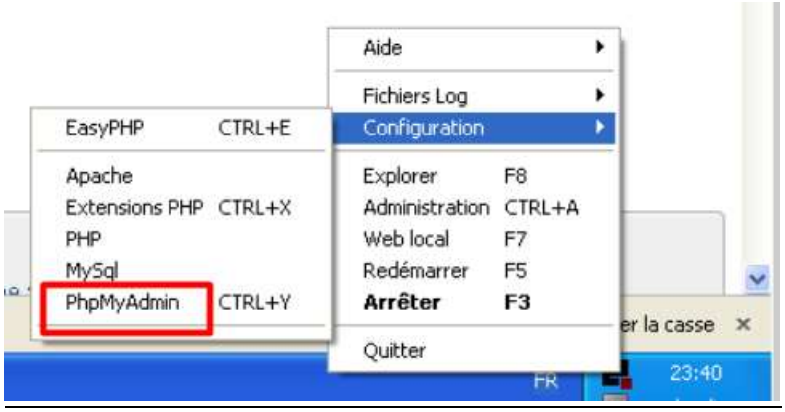
8. Database is accessible to unauthorized users.

Description: Database user has admin privileges in which user can gain full access to the database server. Access of database with full permissions will be possible to **read, update and delete** arbitrary data from database. Depending on the platform and the database system user, an attacker might carry out a privilege escalation attack to gain administrator access to the target system.

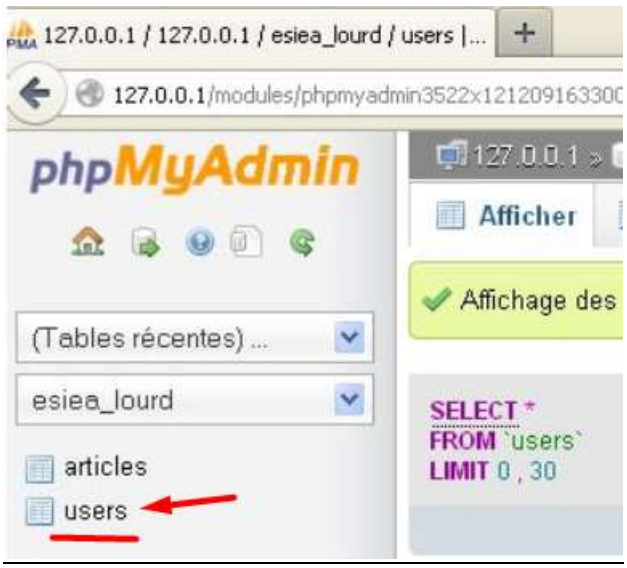
Privileges of agent in database is set to **1** and change the privilege to **0**. Now, open the application and login with **agent** credentials, then you can able to modify the **change password and add new article**. Admin options accessible should have rights to only admin and for other users also.

Exploitation:

Step 1: Right click on **easyPHP->configuration->PhpMyAdmin**



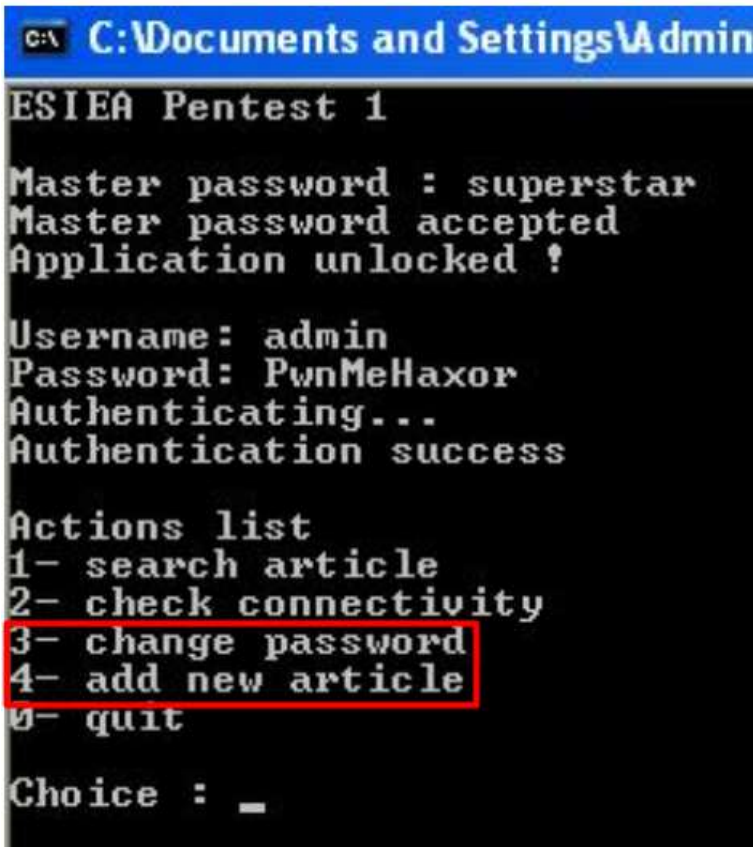
Step 2: Database will be opened and on left side select **users** as show in below picture.



Step 3: In options, as shown in below picture, you can see the **privileges** are set to 1 for username **admin.**

Step 4: Change the **privilege** to **0**

Step 5: Now open esiea_lourd.exe and enter the master password-**superstar, username and password** as **agent, agent**. Now you found, options 3 & 4 in **Actions list** where you can able to modify **change password & add new article.**



Recommendations:

- Create a database user with the least possible permissions for your application and connect to the database with that user. Always follow the principle of providing the least privileges for all users and application
- Privilege escalation can be defeated with query-level access control, it can restrict privileges to minimum required data and operations.
- Visit https://www.bcs.org/content/ConWebDoc/8852 to more information.