

# **SOFTWARE AND DATABASE SECURITY**

## **SECURITY AUDIT REPORT**



**PROFESSOR:**  
**KHALDI ADEL**

**SUBMITTED BY,**  
**SOUMYA GUDURU**  
**SAHANA DEVARAJE GOWDA**

## SUMMARY

**(Below work is done by Sahana)**

### SECURITY AUDIT CONTEXT

This report documents the findings of the application esiea\_lourd. The Application testing was carried out from Date 11/03/2019 to Date 23/03/2019. A Series of tests were conducted against to the application using manual testing techniques and using Wireshark Tool to identify the exploitable security vulnerabilities.

### GENERAL IDEAS ABOUT VULNERABILITIES

No	Vulnerabilities	Impact	Description
1.	Secret present in the executable file.	Critical	Risk that puts the system/data in immediate danger.
2.	Password shown when typing.	High	A vulnerability wherein an attacker might have the ability to retrieve the password and get the access the application.
3.	Network communication not encrypted.	Critical	A vulnerability wherein an attacker might have the ability to get into the network and access the data and exploit application.
4.	Admin options accessible from limited user.	High	Indicates the more security matter that should be remedied appropriately within a system.
5.	Weak passwords accepted.	High	Security risk that does not pose immediate or short-term danger that should be taken care.
6.	Secrets present in configuration file (config.ini).	Critical	Risk that puts the system/data in immediate danger.
7.	Passwords stored in plaintext within database.	Critical	The flaw in the application which leads retrieve the database information.



---

## GENERAL IDEAS ABOUT RECOMMENDATIONS

**(Below work is done by Soumya)**

- 1) Architecture of the application should change from Two-Tier to Three Tier, so that the data won't be stored on the client tier.
- 2) Data transmitted through the network should always be encrypted.
- 3) Database should be encrypted in order to avoid the threat of data leakage in case any unauthorized person manages to enter the database.
- 4) User should be forced to create a strong password which is a combination of special characters and numerals.
- 5) No user should be provided direct access to the database.
- 6) Salt should be used along with the hashed passwords to avoid any brute force attack.



# INDEX

SL NO.	CONTENTS	PAGE NO.
1.	<i>ENVIRONMENT SET UP</i>	1
		1
	<i>1.1- Installing window xp on virtual machine</i>	1
	<i>1.2- Installing Truecrypt on Windows XP VM</i>	1
	<i>1.3- Setting up esiea_lourd application</i>	1
	<i>1.4- Installing Easyphp 12.1</i>	1
	<i>1.5- Cloning the windows XP VM</i>	1
2.	<i>NETWORK CONFIGURATION</i>	2
		2
	<i>2.1- Setting Windows XP Server Machine</i>	2
	<i>2.2- Setting Windows XP Client Machine</i>	2
	<i>2.3- Filesharing between host and VM</i>	2
3.	<i>VULNERABILITIES</i>	3-9
		3-4
	<i>3.1- Secret present in the executable file</i>	5-6
	<i>3.2- Password shown when typing</i>	7-8
	<i>3.3- Network communication not encrypted</i>	9-10
	<i>3.4- Admin options accessible from limited user</i>	11
	<i>3.5- Weak passwords accepted</i>	12-14
	<i>3.6- Secrets present in configuration file (config.ini)</i>	15-16
	<i>3.7- Passwords stored in plaintext within database</i>	



## ENVIRONMENT SET UP (Below Work is done by Soumya)

### INSTALLING WINDOW XP ON YOUR VIRTUAL MACHINE (CLIENT)

1. Download -> [http://www.adeleda.com/WinXP\\_2018\\_AKH.ova](http://www.adeleda.com/WinXP_2018_AKH.ova).
2. Open virtual machine -> Add the windows XP ISO file.
3. Right click on windows Xp VM ->Settings ->Network Adapter ->Select host only ->ok.
4. Right click on windows Xp VM ->Settings ->USB Controller ->Disable all the USB's ->ok.
5. Power the WINDOWS XP Virtual Machine.

### INSTALLING TrueCrypt on your WINDOWS XP VM

1. Click on Poste de travail -> Open C drive -> My tools.
2. Run helloworld.exe -> Check "I accept the licence Terms" and click NEXT ->Install.

### SETTING UP esiea\_lourd Application

1. Click on Poste de travail -> Open C drive -> My tools.
2. Now Run the Challenge\_0.tc file.
3. You will be prompted by a POP UP the select the driver Letter (example "Q").
4. Click on Mount and Enter the Password "3c7bc8f42a71dd221854ce8afa538d01 "and click ok.  
This will create a Q drive on your Computer.
5. Open the Q drive and open the folder "Challenges".
6. Select esiea\_lourd.rar and move it to the desktop.
7. Right Click on esiea\_lourd.rar and click Extract here=> you will get a esiea\_lourd folder on Desktop.

### SETTING UP EasyPHP 12.1:

1. Open Q drive.
2. Open challenges folder.
3. Navigate to EasyPHP 12.1 rar file.
4. Right click on it and click extract here from the panel.
5. Click on yes to All.

### CLONING the WINDOWS XP VM (SERVER)

1. Right Click on WinXP\_2018\_AKH -> Manage -> Clone ->Next-> Select "Clone the current state of the virtual Machine" -> Next -> Create a linked clone -> Name your Virtual Machine ->Finish.



## NETWORK CONFIGURATION

- # Original WindowsXP is your Client Machine.
- # CLONED WindowsXP is your SERVER Machine.

## SETTING WINDOWS XP SERVER MACHINE

### ➤ Module 1:

1. Navigate to poste de travail.
2. Open C drive.
3. Open Program Files folder.
4. Open EasyPHP 12.1 folder and Run EasyPHP-12.1.exe file.

### ➤ Module 2:

1. Click on demarrer(Start) ->Click to “Executer” ->Type “cmd” in the text box and click ok.
2. A terminal opens.
3. Type ipconfig and press Enter.
4. Note down the IP address (example: 192.168.80.128).

## SETTING WINDOWS XP CLIENTMACHINE

### ➤ Module 1:

1. Open the esiea\_lourd folder on the desktop.
2. Navigate to the application folder.
3. Open the cofig.ini file.
4. change the dbhost= IP address of the SERVER MACHINE (example: 192168.80.128).
5. save and close the document.

### ➤ Module 2:

1. Now run the esiea\_lourd .exe file from the application folder.
2. A terminal will be opened.
3. Enter the Master password = superstar.
4. USERNAME =agent.
5. PASSWORD =agent.

## FILESHARING BETWEEN HOST AND VM

1. Navigate to CLIENT WinXp.
2. Right click on WinXP\_2018\_AKH and Click Settings.
3. Navigate to Options and click on Shared Folders.
4. In the right-side panel select “Always enabled”.
5. Click on ADD & browser the path of the folder you want to Access in the Virtual Machine.
6. Navigate to demarrer(Start) and click on “Executer”.
7. Type [\\vmware-host\Shared Folders\](#) in the text box to access the shared folder.



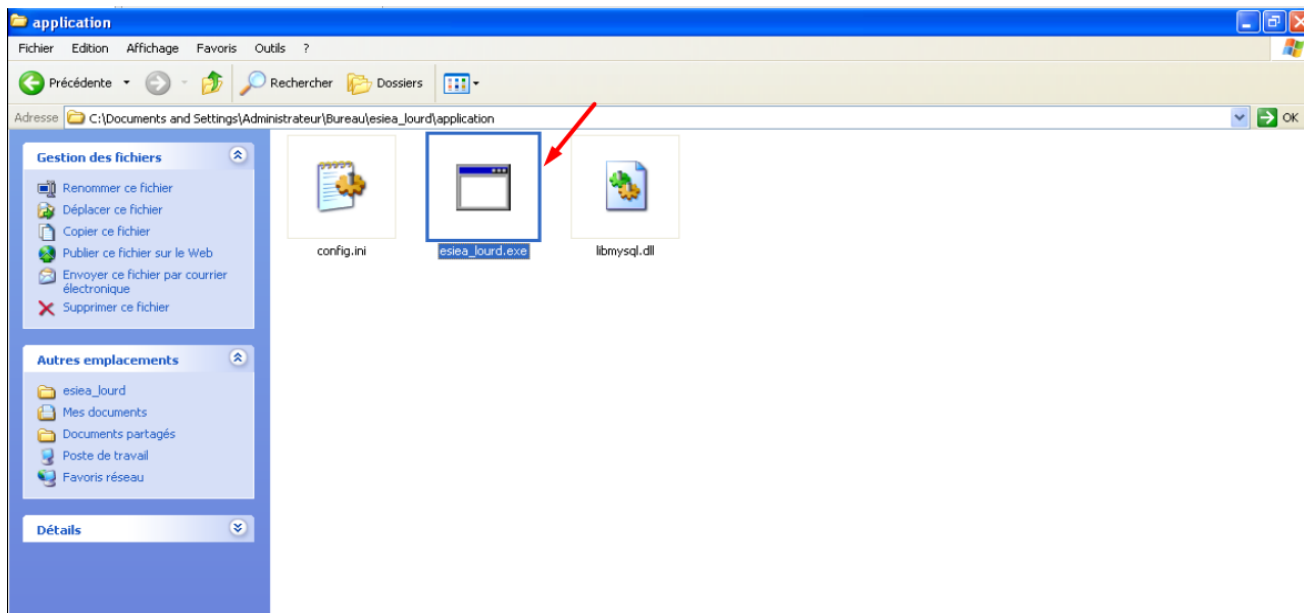
## VULNERABILITIES

### VULNERABILITIES 1- SECRET PRESENT IN THE EXECUTABLE FILE.

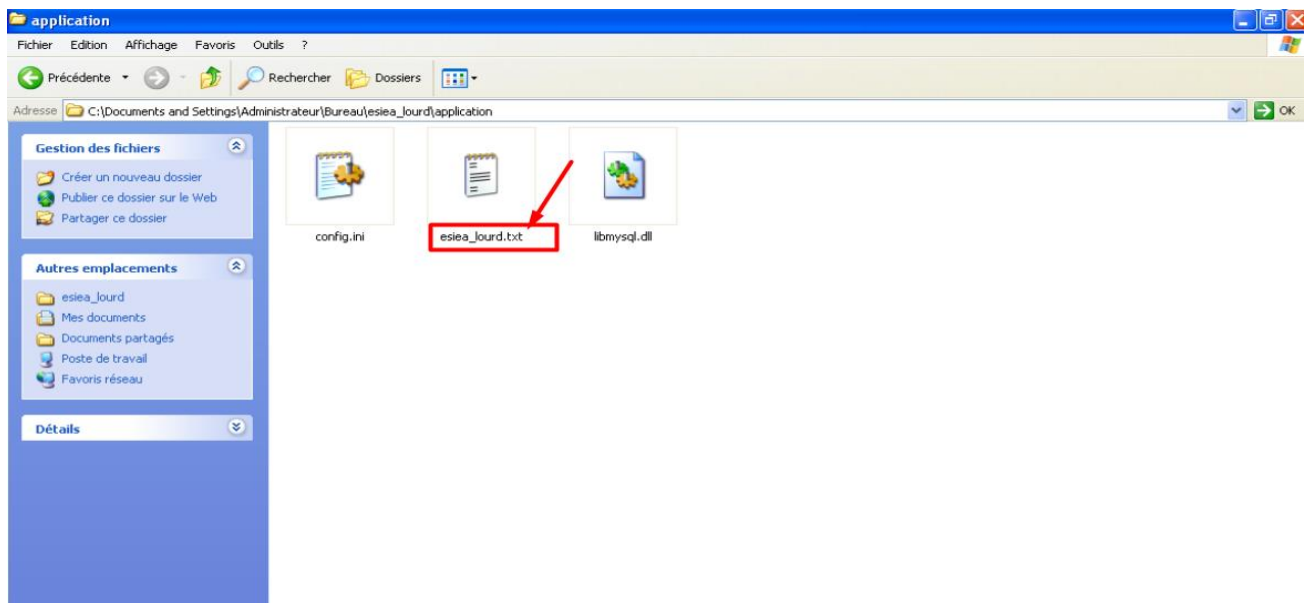
**DESCRIPTION:** Password being stored in the Application itself i.e. in the .exe file of the application.

**EXPLOITATION:**

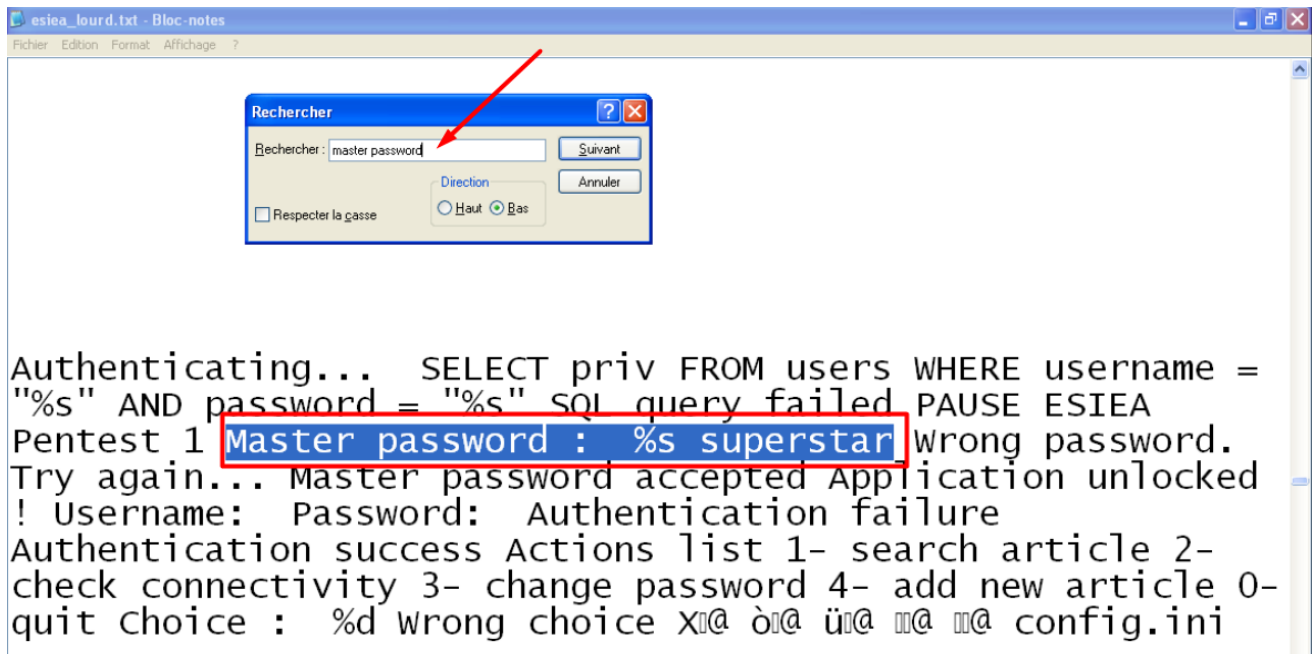
**Step 1:** Open the application folder from easie\_loder folder on the desktop



**Step 2:** Rename the easiea\_lourd.exe file to easiea\_lourd.txt



**Step 3:** Open the txt file and press Ctrl+F. Search for the word master password



## RECOMMENDATIONS: (Below work is done by Sahana)

- Password should not be stored on the application itself i.e on the client tier.
- Architecture should change from Two-Tier to Three Tier and store the password on the server.
- Instead of a straight string value, we can store the text in some other binary form.
- Create a Hash of the password that you want to compare against, and store in the database
- Add a 'salt value', to the hashed password and store it in the exe file for comparison.
- The use of cryptography to hide the plain text/ data by modifying into a cipher text/data such that no third party can read it easily.
- The use of steganography, with the computer-based steganography we can hide the Passwords, text files almost any type of data inside images audio files and video files etc.
- To make use of the NTFS's Alternate Data Streams to our sensitive data. The Alternate data streams allows us to hide stream in a file. The stream is not visible or shown accessing the main file. To hide the password, add those as a simple text and hide them as a stream in some file name.





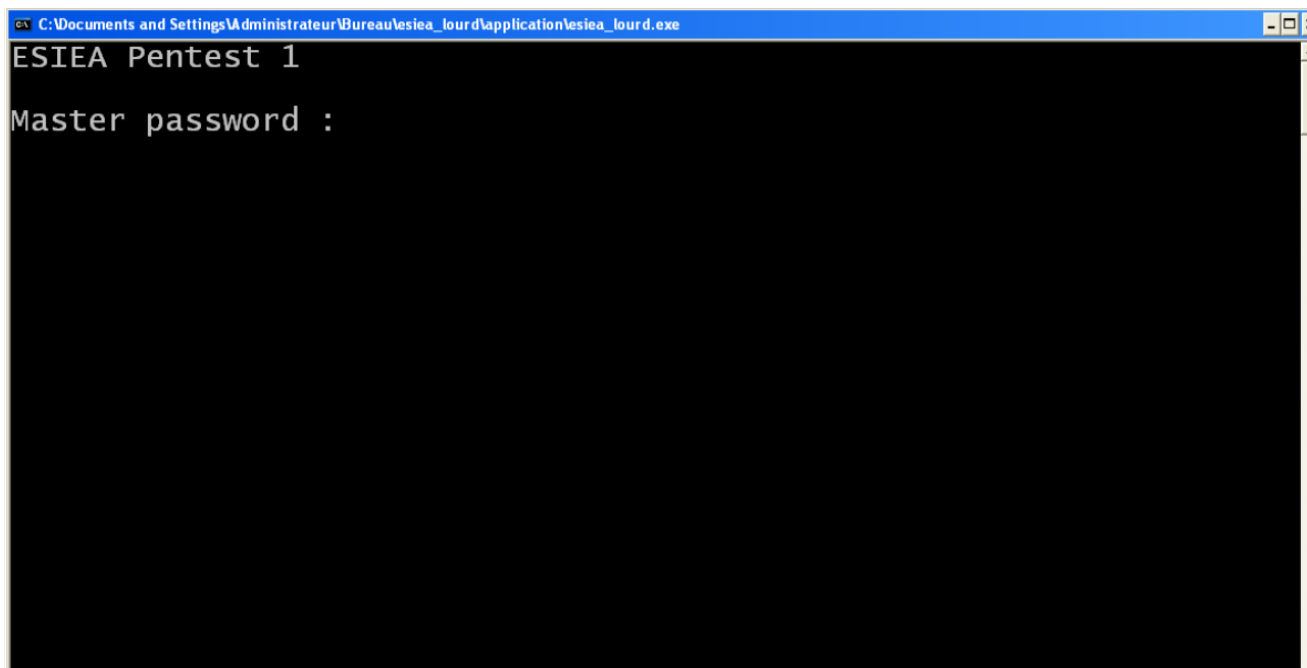
## VULNERABILITIES 2 - PASSWORD SHOWN WHEN TYPING

**(Below Work is done by Soumya)**

**DESCRIPTION:** Password being displayed on the screen while you are entering the password to log in. Any person passing by can see the typed Password while you are just logging into the application and memorize it.

### EXPLOITATION:

**Step 1:** Click on the easiea\_lourd.exe file from the application folder. A terminal will be opened and will ask for the “Master password”.



```
C:\Documents and Settings\Administrateur\Bureau\esiea_lourd\application\esiea_lourd.exe
ESIEA Pentest 1
Master password :
```



**Step 2:** Enter the master password “superstar”



```
Sélectionner C:\Documents and Settings\Administrateur\Bureau\esia_lourd\application\esia_lourd.exe
ESIEA Pentest 1
Master password : superstar
```

You can observe that the password “superstar” is visible on screen.

### RECOMMENDATIONS:

- The primary protection provided by password masking against shoulder surfing is to use Key Strokes which can be used for all the passwords.
- Password can be invisible on the screen while entering it.



### VULNERABILITY 3: NETWORK COMMUNICATION NOT ENCRYPTED

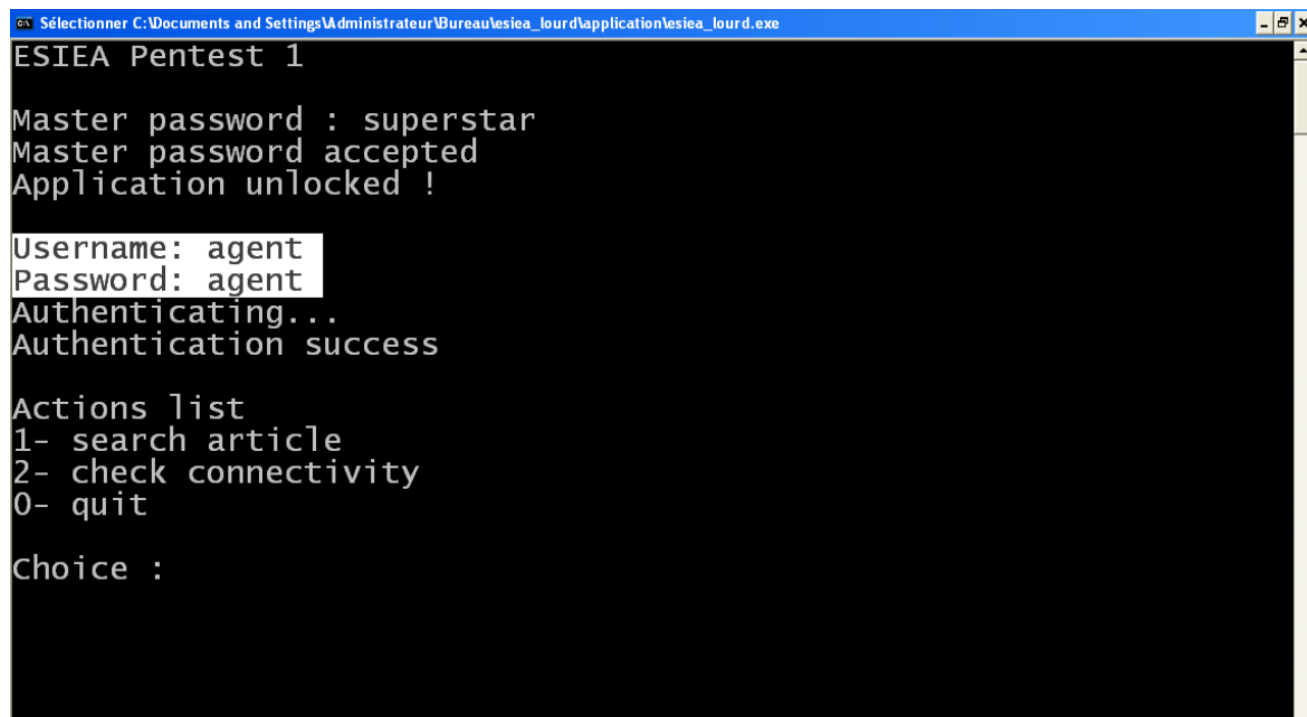
**DESCRIPTION:** Username and Password are stored on the server. Network traffic can be seen by anyone using a simple software like Wireshark. Password passing through the network can be sniffed by any person over the internet.

#### EXPLOITATION:

**Step 1:** Enter the username & password on the terminal of easiea\_lourd and login to the application.

Username: agent

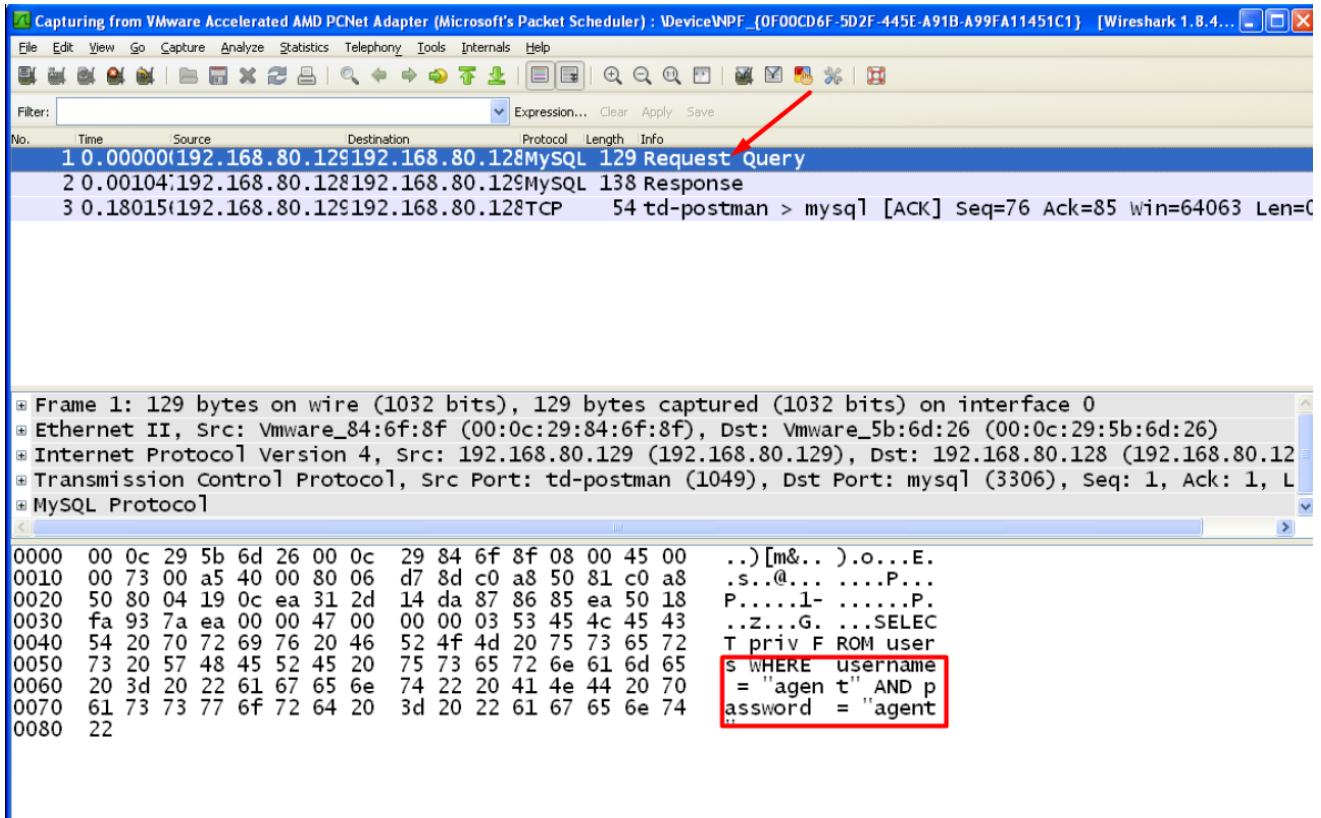
Password: agent



```
ESIEA Pentest 1
Master password : superstar
Master password accepted
Application unlocked !
Username: agent
Password: agent
Authenticating...
Authentication success
Actions list
1- search article
2- check connectivity
0- quit
Choice :
```



**Step 2:** Open the Wireshark application and click on the Request Query. Use can see the username and password in the bottom section of the Wireshark application.



## RECOMMENDATIONS:

- Data passing through the network should be Encrypted i.e we should use Encryption techniques.
- Use a VPN (Virtual Private Network) to protect the data from the people trying to sniff over the internet.
- Use an SSH (Secure Shell) Proxy: SSH tunnel will act as the middleman between computer and the dubiously secure servers on the internet so that everything sent between computer and SSH will be encrypted.

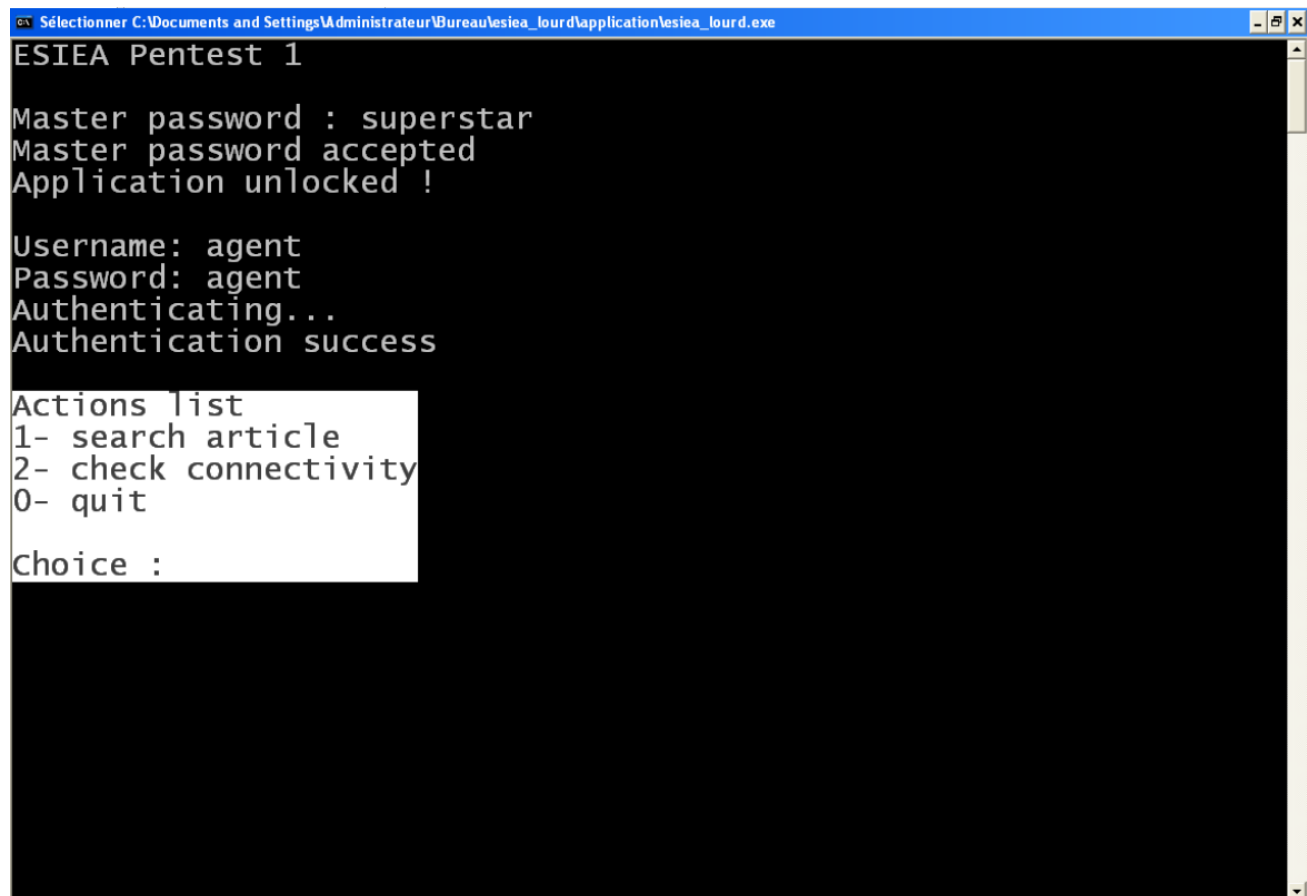


## VULNERABILITY 4: ADMIN OPTIONS ACCESSIBLE FROM LIMITED USER

**DESCRIPTION:** Some options are limited only to the Admin like “New article addition” in this Application. Accessing to other options to which user is not authorized is possible from the user interface in this application. In this Application admin options are just hidden from the user on the Front End rather than restricting the access to Users. If the user tries random options which are not displayed to them, user can get access to the Admin options and change the system settings and other stuff.

### EXPLOITATION:

**Step 1:** Login in to the easiea\_lourd application using the password “agent”. You can see the options “1, 2, 0” provided to the user.



```

Sélectionner C:\Documents and Settings\Administrateur\Bureau\esiea_lourd\application\esiea_lourd.exe
ESIEA Pentest 1

Master password : superstar
Master password accepted
Application unlocked !

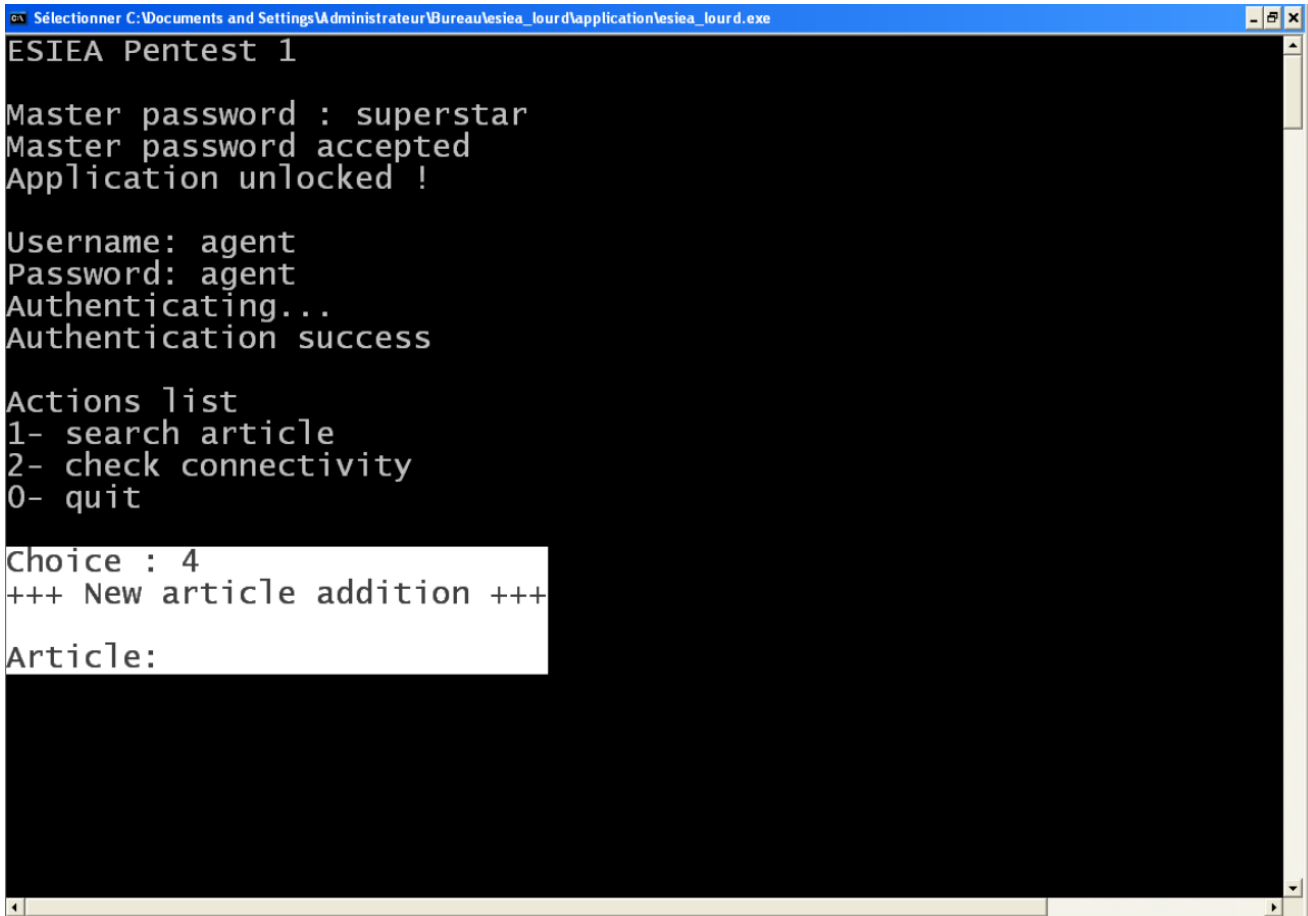
Username: agent
Password: agent
Authenticating...
Authentication success

Actions list
1- search article
2- check connectivity
0- quit

Choice :
  
```



**Step 2:** Enter any option other than 1 or 2 or 0 for example 4, which is an option not available to the user.



```
ESIEA Pentest 1
Master password : superstar
Master password accepted
Application unlocked !
Username: agent
Password: agent
Authenticating...
Authentication success
Actions list
1- search article
2- check connectivity
0- quit
Choice : 4
+++ New article addition +++
Article:
```

## RECOMMENDATIONS:

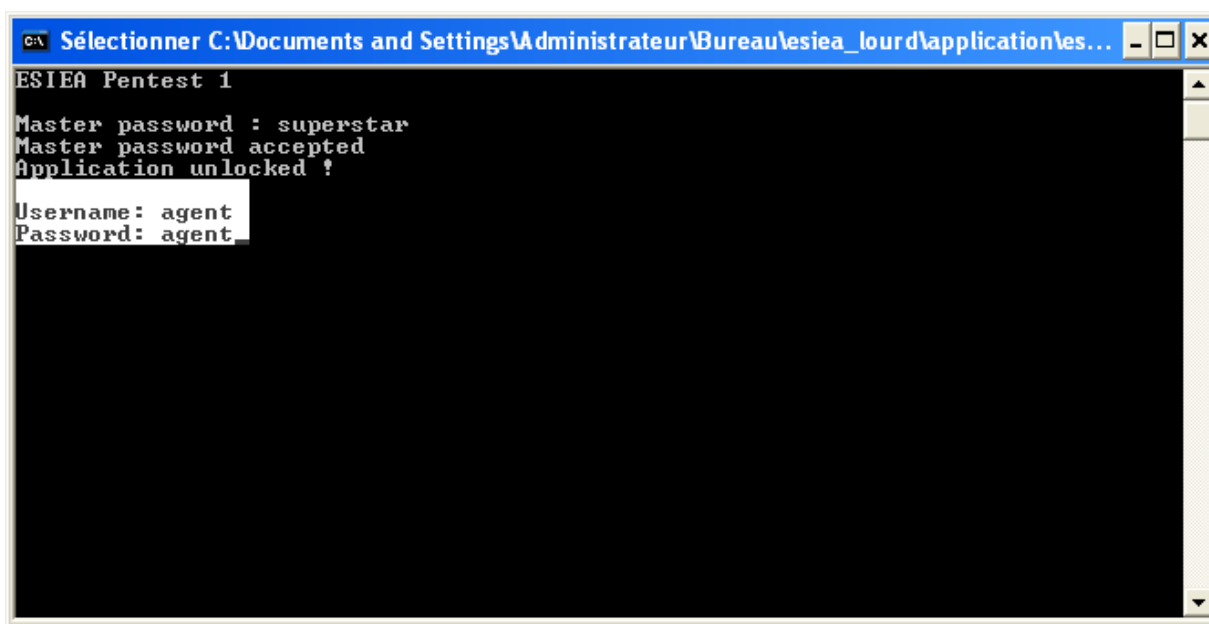
- Rather than hiding the admin options from the user on the Front End, user must be restricted from accessing admin options by providing password authentication to the restricted areas. During the development of the Application this issue should be taken care off.



## VULNERABILITY 5: WEAK PASSWORDS ACCEPTED (Below work is done by Sahana)

**DESCRIPTION:** Weak passwords are words which are easy to guess, or which are definite words that can be found easily by using every word from the dictionary. Passwords same as Usernames are the easiest to guess. Any password of small length or definite words like the names of our family members or DOB's can be easily guessed without much effort.

**EXPLOITATION:** Open the application and login with the password same as username



```

C:\> Sélectionner C:\Documents and Settings\Administrateur\Bureau\esia_lourd\application\esia...
ESIEA Pentest 1
Master password : superstar
Master password accepted
Application unlocked !
Username: agent
Password: agent
  
```

### RECOMMENDATIONS:

- Password same as Username should never be accepted. This issue should be taken care from the development phase.
- User should be obligated to set a difficult password which is a combination of certain length including letters, special characters and numericals
- You can use a password management tool, such as LastPass or KeePass, to generate a long, complex password for each site and remember those passwords for you. User can lock this file with a password leaving you with only one master password to recall.

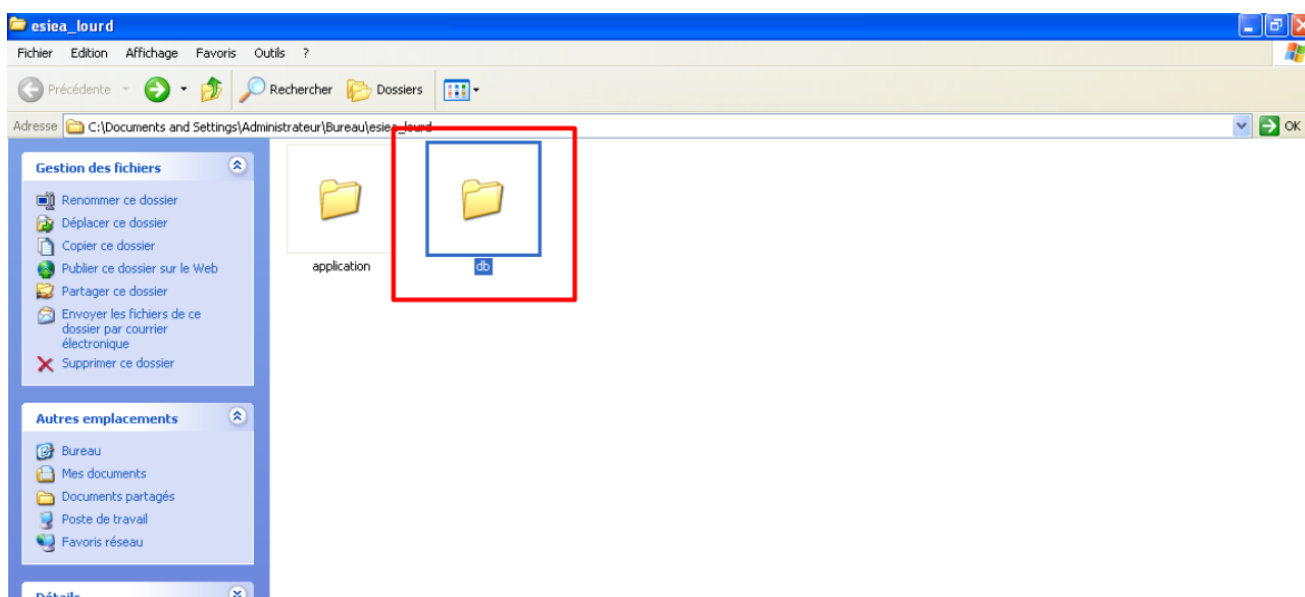


## VULNERABILITY 6: SECRETS PRESENT IN CONFIGURATION FILE (CONFIG.INI)

**DESCRIPTION:** All the details required to connect to the Database are stored in the config.ini file. Anybody can connect to the database using the details present in the Config.ini file. Once the person is connected to the Database, he can modify or steal all the data and spasswords from the database if they are stored directly without hashing.

### EXPLOITATION:

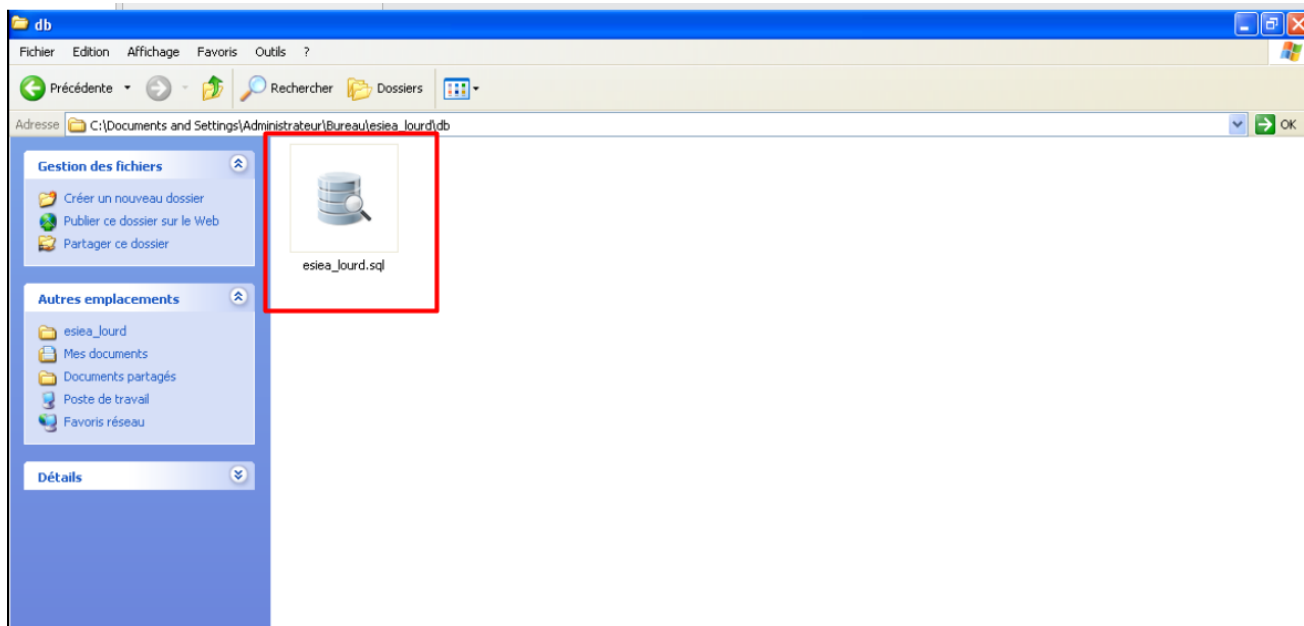
**Step 1:** Open the db folder from easiea\_lourd folder on the desktop



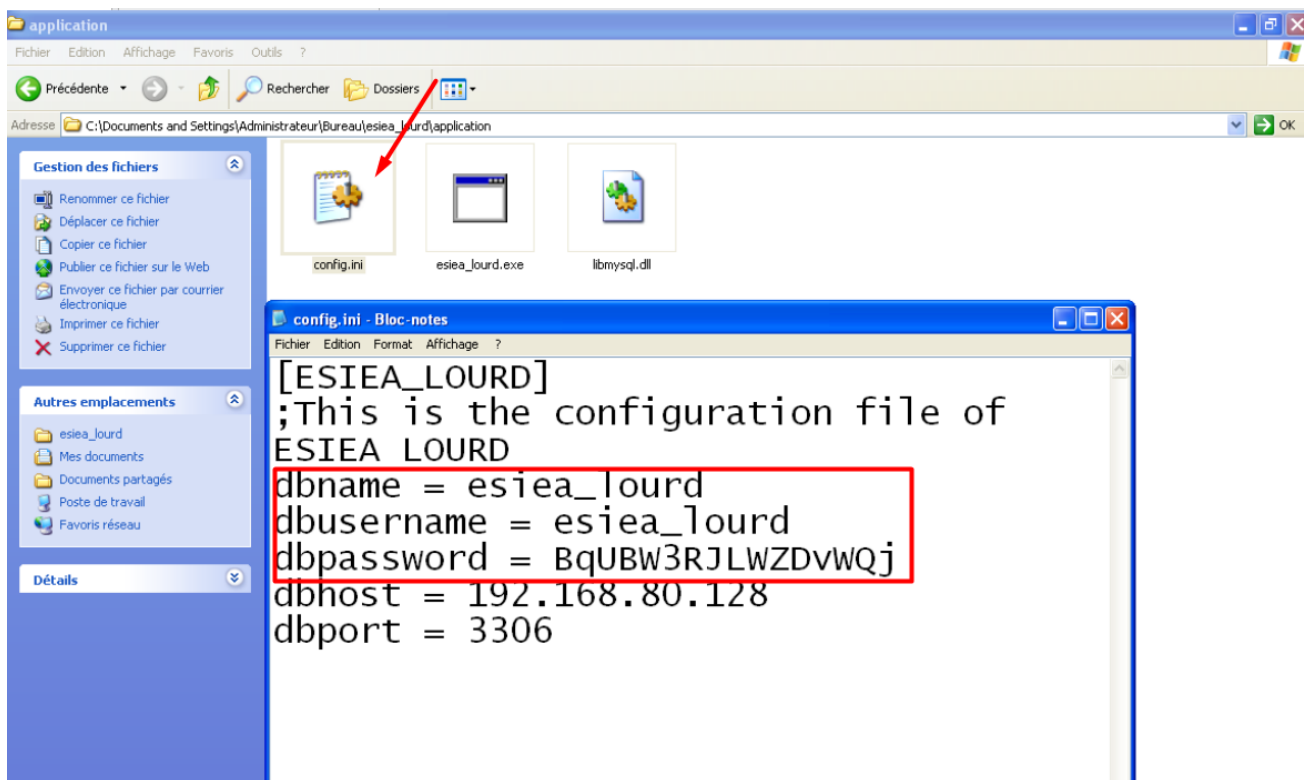
**Step 2:** Double click and open the application.

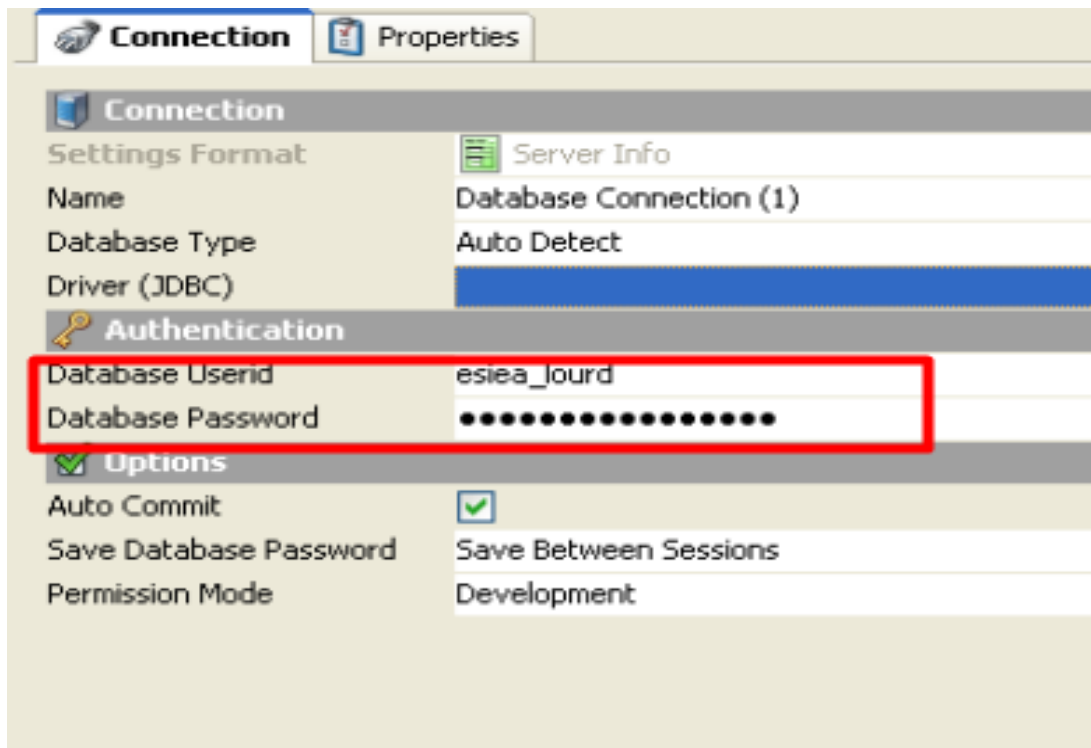






**Step 3:** Login To the database using the details present in the config file.





## RECOMMENDATIONS:

- Database details should not be stored on the client Tier. Rather than that, they should be stored on the server.
- Access to the database should be provided only from the server which can be achieved by shifting the architecture from Two-Tier to Three Tier.
- It is a good practice to provide the folder permissions for the user to read the files by using normal windows file permissions.
- The passwords in the config.ini file can be destroyed after the database connections are made.
- Making the file unreadable via the web using rules in .htaccess. htaccess files often used to specify the security restrictions for the particular directory.



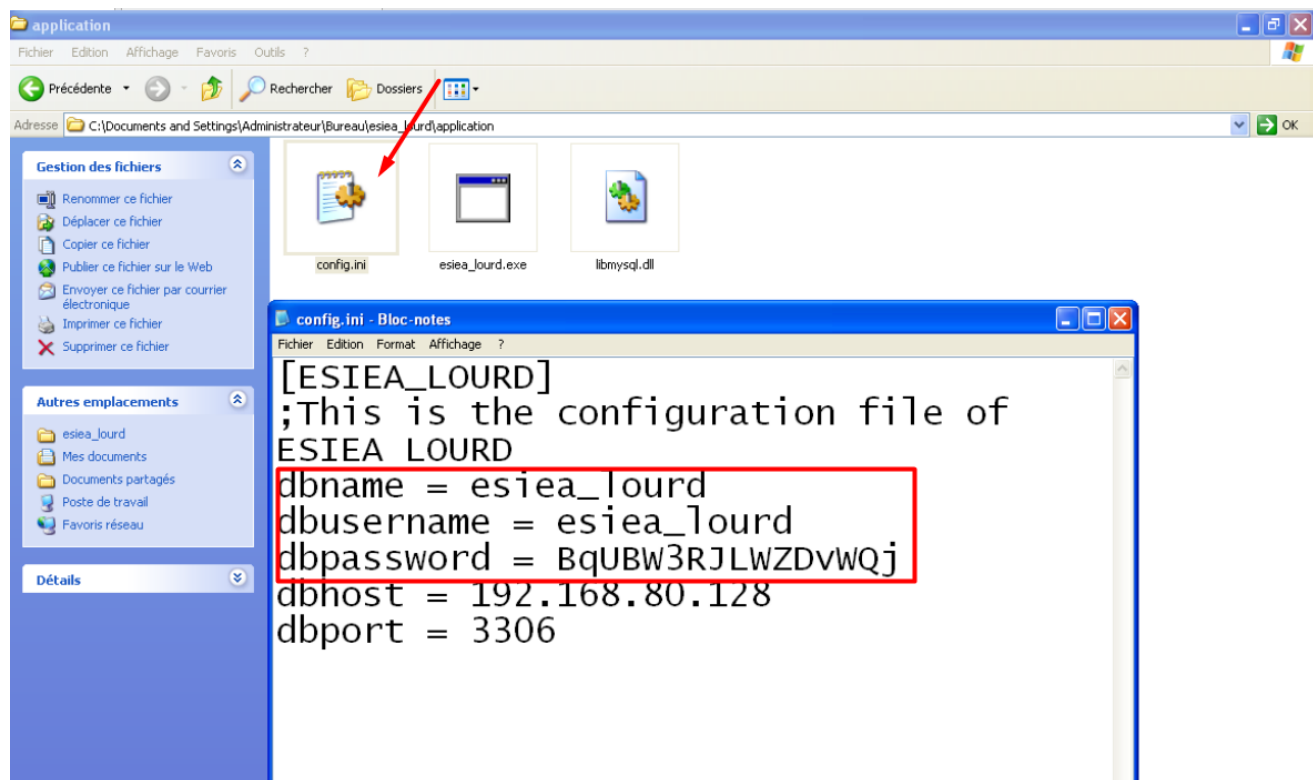
## VULNERABILITY 7- PASSWORDS STORED IN PLAINTEXT WITHIN DATABASE

**DESCRIPTION:** Passwords in the Database are stored without encryption. Any person who manages to access the database can gain access to the application.

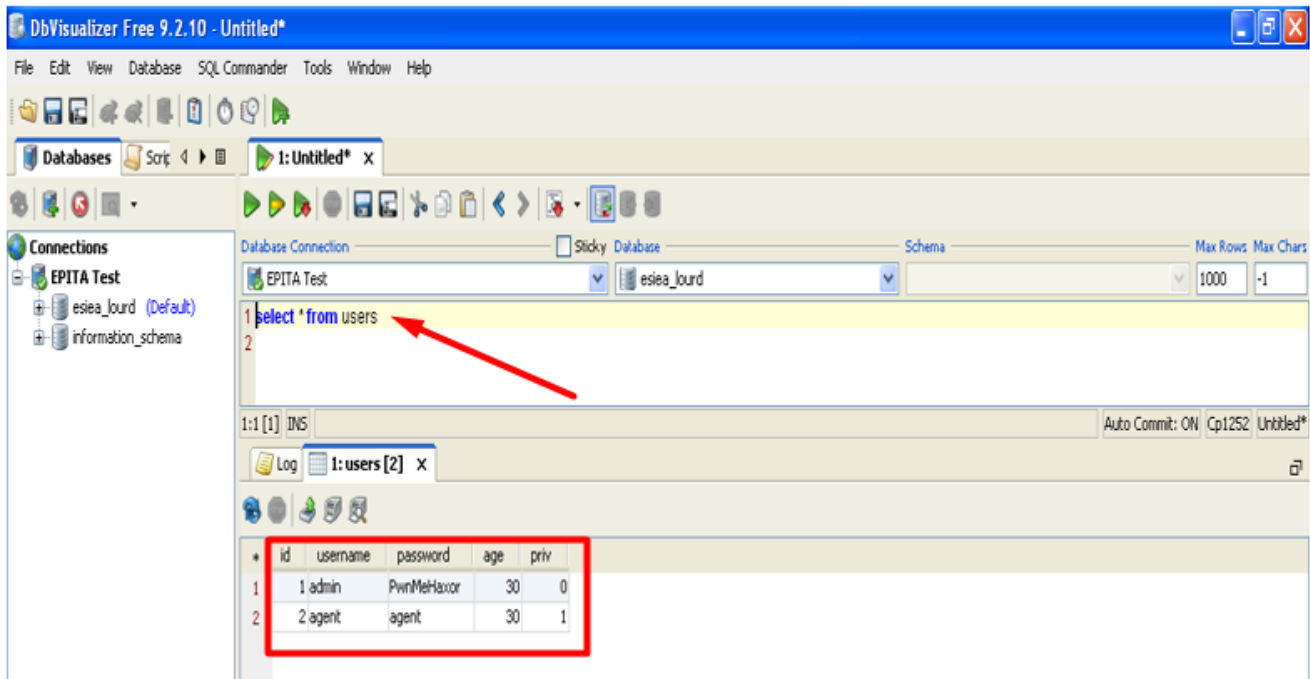
### EXPLOITATION:

**Step 1:** Login To the database using the details present in the config file.

Anybody who access the database can see all the user passwords along with their data



**Step 2:** Type the query “select \*from users” and run the query. You can see the table contents, which are the username and password details of user and admin.



## RECOMMENDATIONS:

- All the Data along with the passwords must be encrypted before being stored in the Database.
- Hashing Techniques can be applied for the password to store in the database.
- Salts can be applied to the passwords and then stored in the Database instead of storing it in the plain text.

