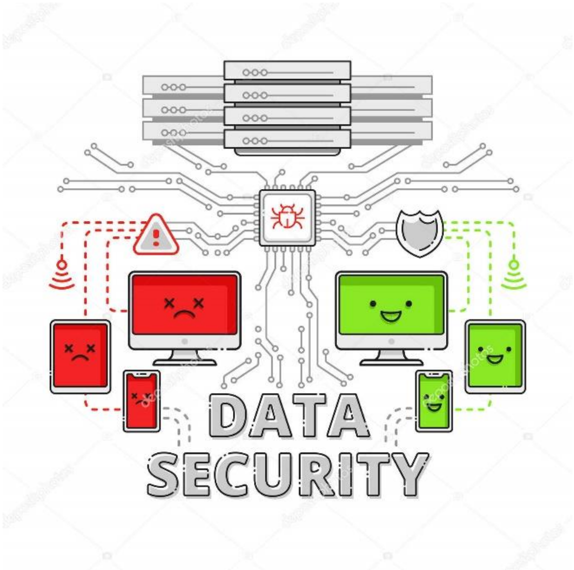
EPITA

ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

SOFTWARE AND DATABASE SECURITY

SECURITY AUDIT REPORT



-Indhu **ARIVALAGAN**

-Yogitha Sathyasai **PANTHAM**

SUMMARY

Introduction:

This Report shows security audit and vulnerabilities associated with esiea_lourd application and potential risks when they are exploited, as well as recommendations for avoiding such vulnerabilities.

Vulnerabilities:

1) Secret information stored in plain text.
    a) Config.ini
    b) Application executable file
2) Insecure storage of password in database.
3) Weak passwords are accepted.
4) Passwords shown while typing.
5) Bad profile segregation.
6) Arbitrary system command injection.
7) Network traffic is not encrypted.
8) SQL Injection.

Recommendations:

- Don't store your passwords in executable files.
- Use of hash functions and salted passwords which are used to safeguard passwords in storage.
- Use of Encryption algorithm to encrypt login credentials, stored in configuration file.
- Making the default configuration as hide password while entering the application's password.
- Admin can add to this segregation by using the password.
- Do not allow an attacker to insert special characters into the command.
- Using Hash functions to change a text password into a more complex set of characters using more complex operations.
- Alternatively wherever possible, use prepared statements, parameterized queries or stored procedures.

INDEX

ENVIRONMENTAL SETUP

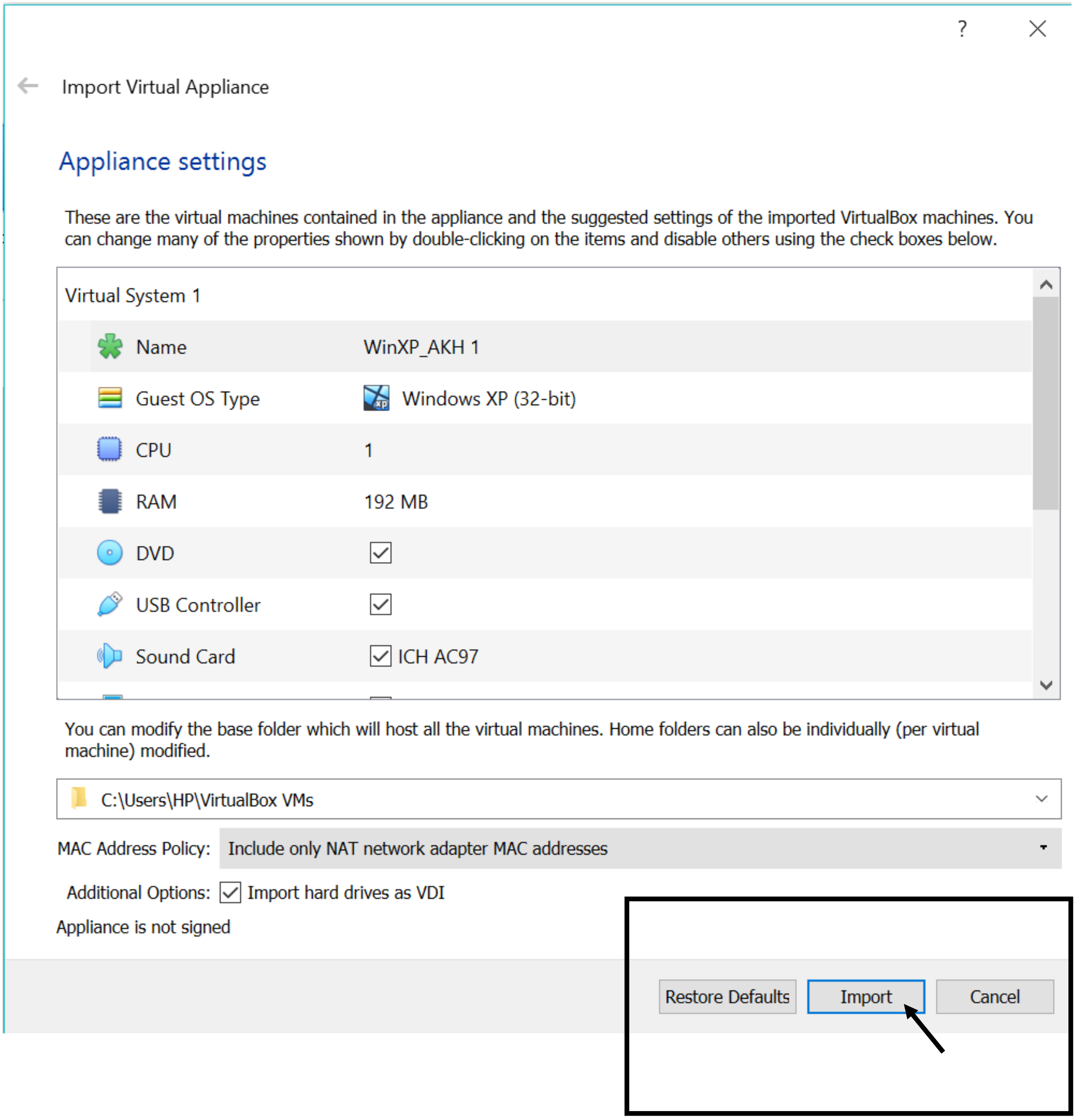
VM's (server and client):

Server:

Step 1: Open .ova file for windows XP, downloaded from the following link.

http://www.adeleda.com/WinXP_2018_AKH.ova

Step 2: After opening the .ova file by double-clicking it, it pops up with the appliance configuration window with the virtual box, where we click on the import option at the bottom of the screen.



Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1

Name	WinXP_AKH 1
Guest OS Type	Windows XP (32-bit)
CPU	1
RAM	192 MB
DVD	☑
USB Controller	☑
Sound Card	☑ ICH AC97

You can modify the base folder which will host all the virtual machines. Home folders can also be individually (per virtual machine) modified.

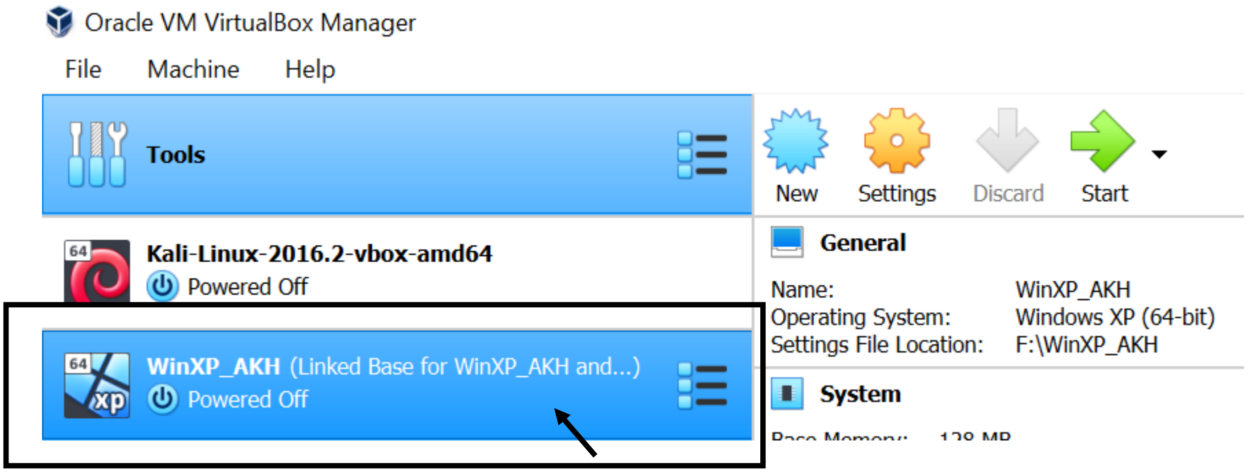
C:\Users\HP\VirtualBox VMs

MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: ☑ Import hard drives as VDI

Appliance is not signed

Step 3: After successfully importing Windows XP into the virtual box, as shown below, we can use windows XP in the virtual box home window.


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Settings
Discard
Start
Kali-Linux-2016.2-vbox-amd64
Powered Off
WinXP_AKH (Linked Base for WinXP_AKH and...)
Powered Off
General
System

Name: WinXP_AKH
Operating System: Windows XP (64-bit)
Settings File Location: F:\WinXP_AKH

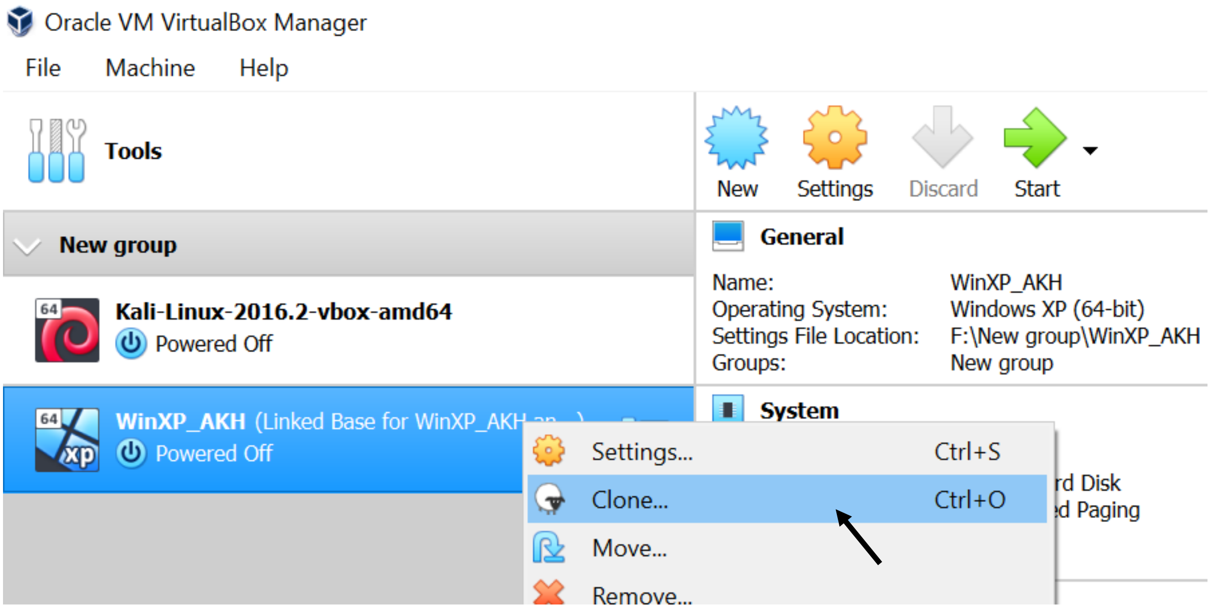
Step 4: Now we need to change the default settings as below,

- Disable the USB controller by unchecking the check box for the activated USB controller.
- Disable the configuration settings for network as well.

Client:

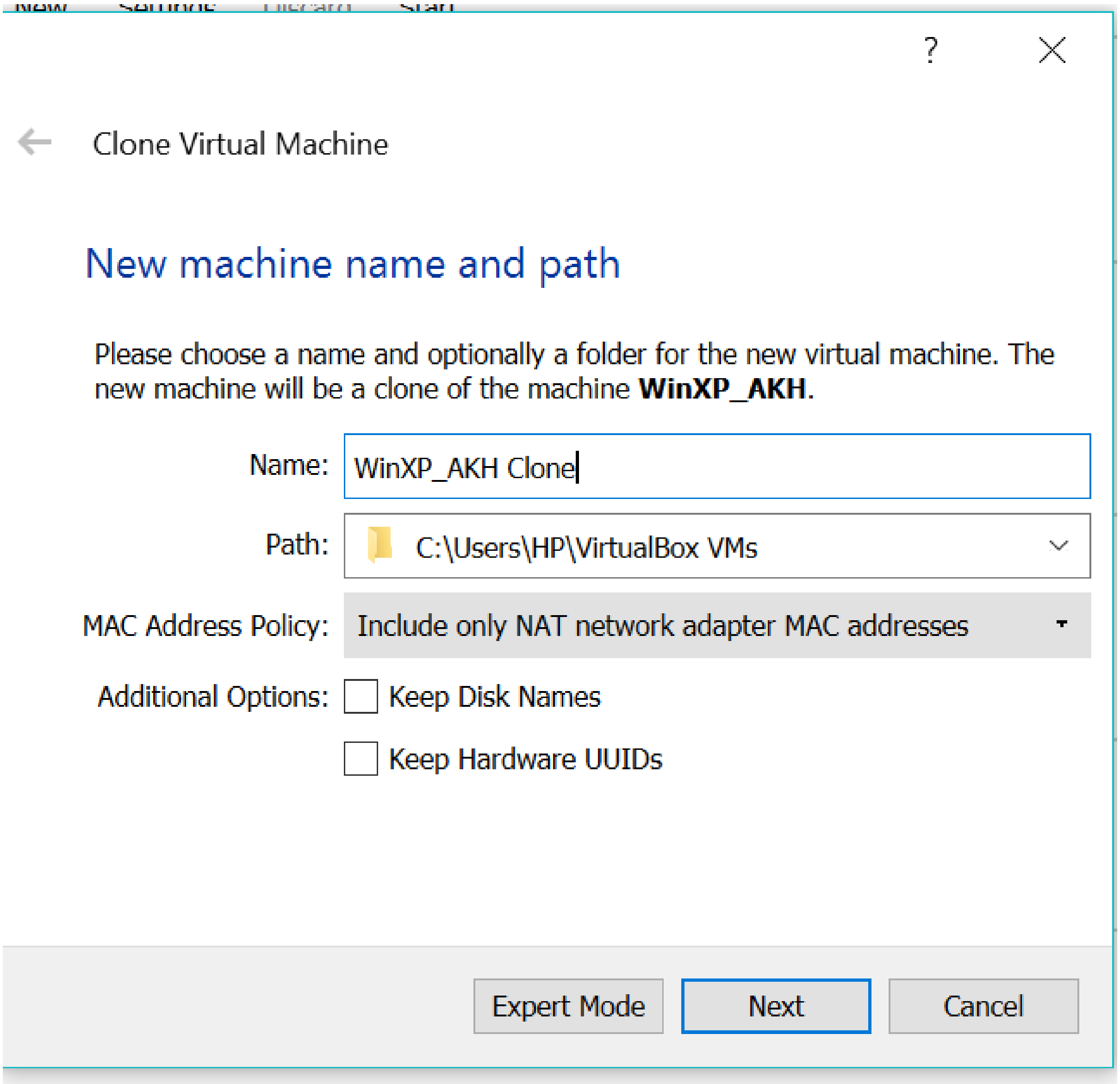
We can make the client machine by cloning the server machine as follows,

Step 1: For a virtual machine client, have to right-click the server machine and select the clone option as shown below.



Name: WinXP_AKH
Operating System: Windows XP (64-bit)
Settings File Location: F:\New group\WinXP_AKH
Groups: New group

Step 2: After selecting the clone option "new name and path" window, where we have to name the client machine and the path where we have selected the server machine and click next.



Clone Virtual Machine

New machine name and path

Please choose a name and optionally a folder for the new virtual machine. The new machine will be a clone of the machine **WinXP_AKH**.

Name: WinXP_AKH Clone

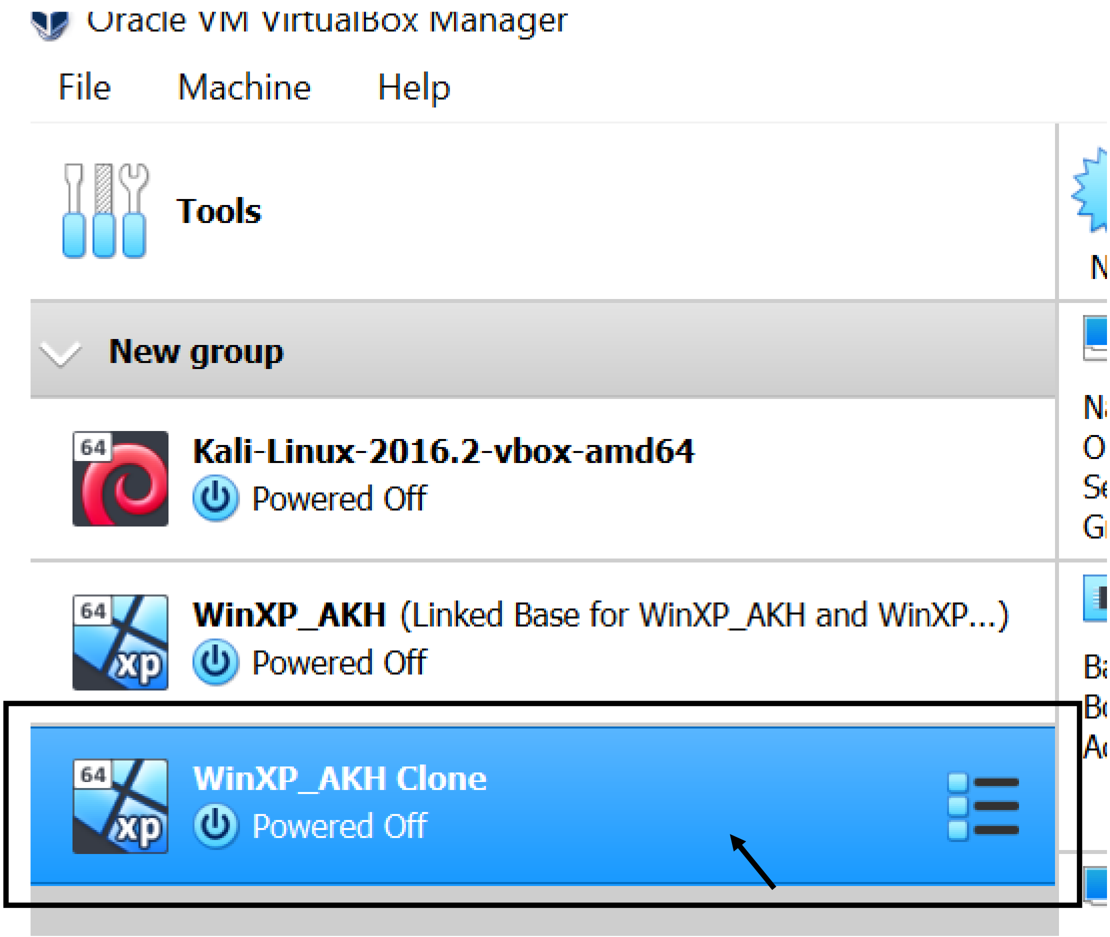
Path: C:\Users\HP\VirtualBox VMs

MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: □ Keep Disk Names

□ Keep Hardware UUIDs

Step 3: After successful cloning, the client machine appears in the virtual box next to the server machine as shown below.


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New group
Kali-Linux-2016.2-vbox-amd64
Powered Off
WinXP_AKH (Linked Base for WinXP_AKH and WinXP...)
Powered Off
WinXP_AKH Clone
Powered Off

Step 4: Now we have to change the default setting for the client machine just like we did for the server machine.

VULNERABILITIES

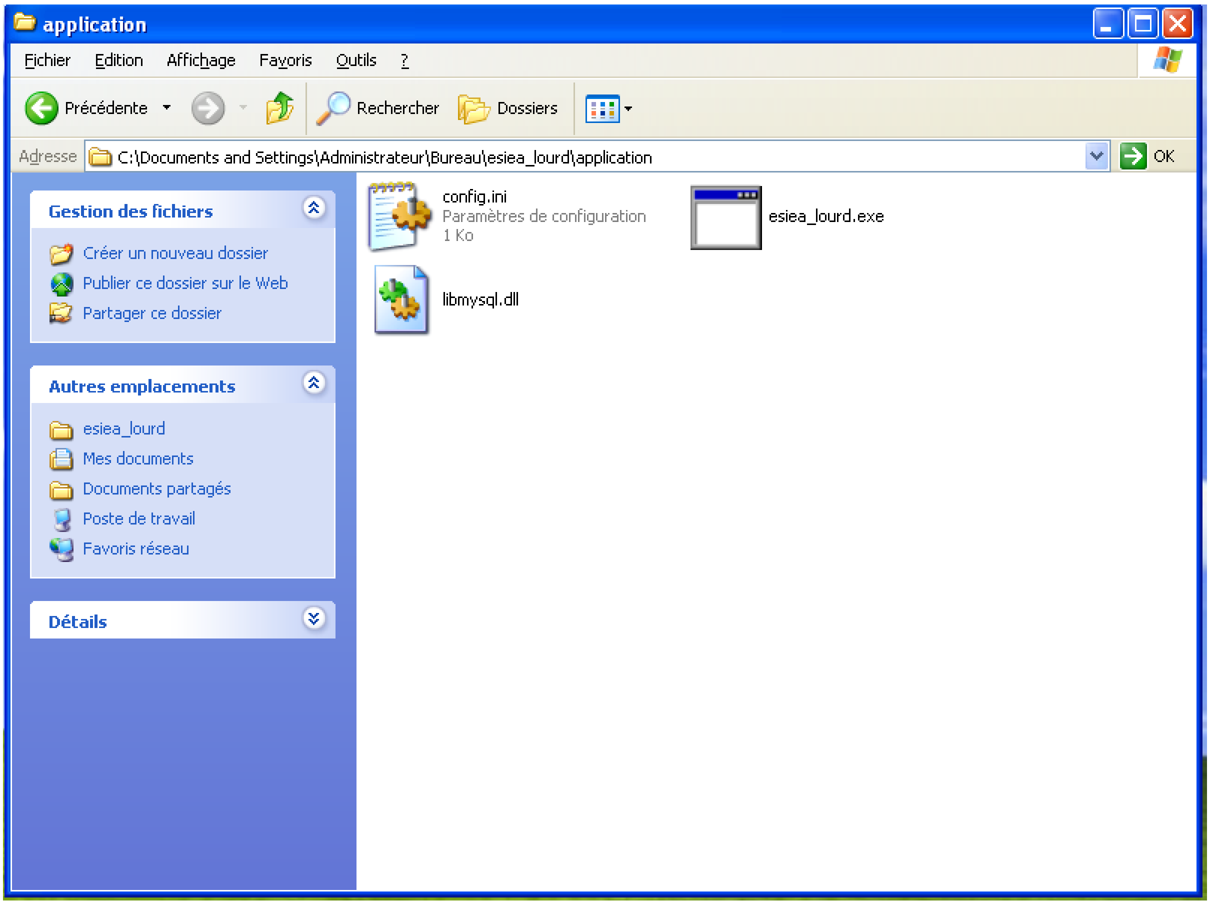
Vulnerability 1: “Secret information stored in plain text”

Description:

We are currently working on the esiea_lourd.exe file and we can verify that the password is directly available to the public, and we can use some resources like HxD and the standard notepad to get the username and password information.

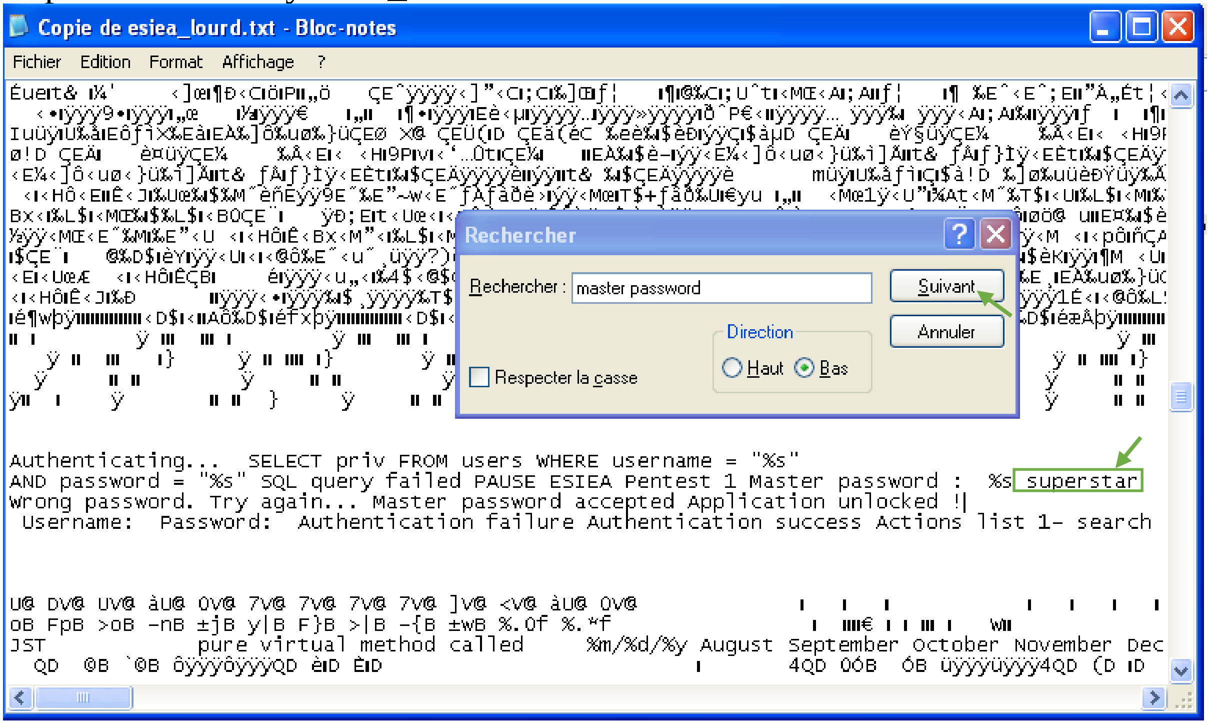
Exploitation:

The most important and most sensitive data is leaked from the application to the user.



Adresse C:\Documents and Settings\Administrateur\Bureau\esiea_lourd\application

Import the directory esiea_lourd.exe to HxD


Copie de esiea_lourd.txt - Bloc-notes
Fichier Edition Format Affichage ?
Rechercher
Suivant
Annuler
Direction

Rechercher : master password

□ Respecter la casse

○ Haut ● Bas

```
Authenticating...  SELECT priv FROM users WHERE username = "%s"
AND password = "%s" SQL query failed PAUSE ESIEA Pentest 1 Master password :  %s superstar
Wrong password. Try again... Master password accepted Application unlocked !
 Username:  Password:  Authentication failure Authentication success Actions list 1- search

JST              pure virtual method called      %m/%d/%y August September October November Dec
```

- First of all, you need to extract the esiea_lourd.rar file , we will get the config and the application files.
- Import the esiea_loaurd.exe file to HxD application, use CTRL+F to find the text-string and type the password and enter it. You can see the password for this application. That is superstar.
- Another method to check the plain text using notepad, as I explained in previous page, is to open the esiea_lourd.exe file.
- Use CTRL+F to search for a file and type password, displays Master Password: superstar.

Recommendation:

1) I would say that encryption of passwords is much easier for this vulnerability.
2) If the user uses this tool to find the encrypted password, it is very difficult to decrypt without knowing the key.

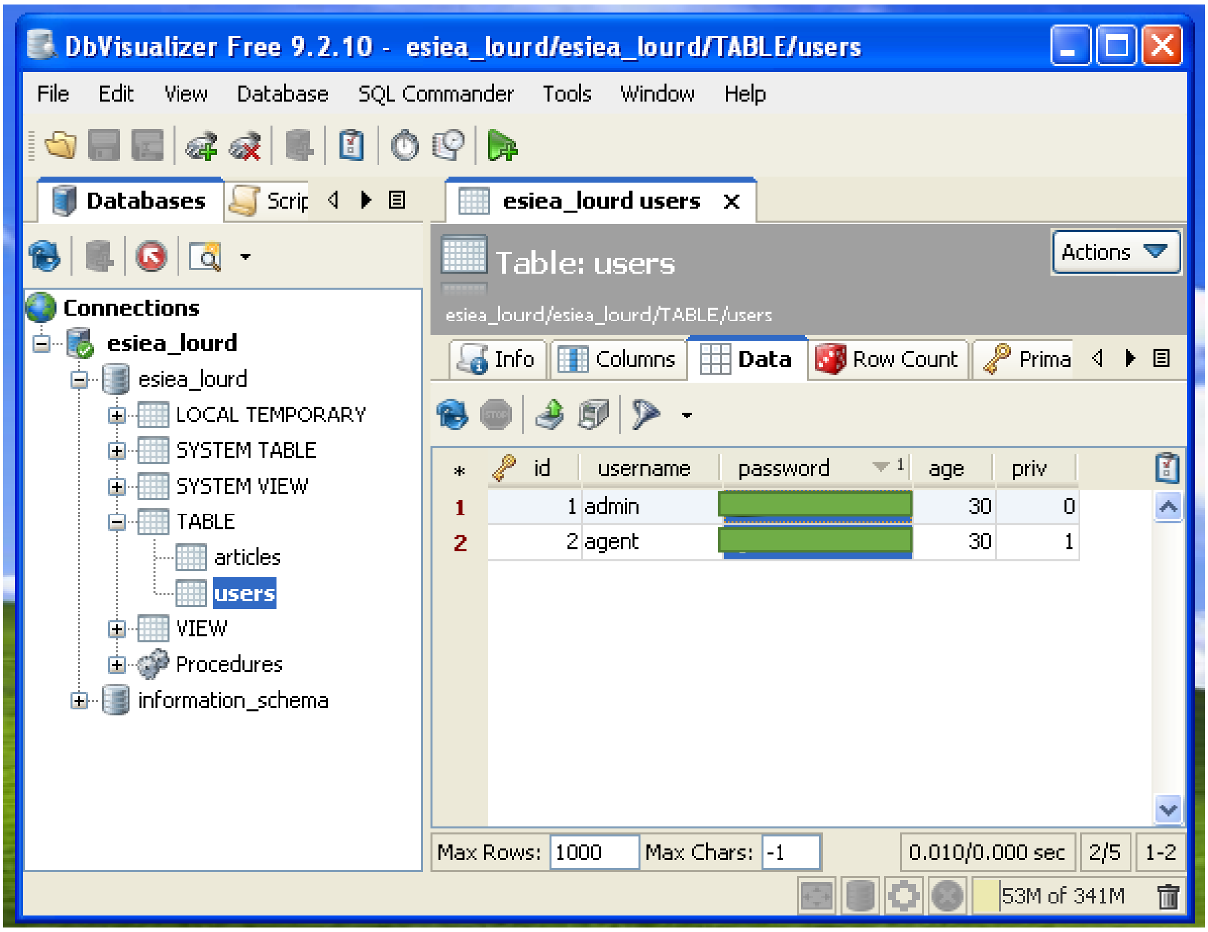
Vulnerability 2: “Insecure storage of password in database”

Description:

Passwords stored in plain text within database enables attackers to access and change the information in the database.

Exploitation:

For the esiea_lourd application database, we can see password as an agent for the user agent in the image below.



*	id	username	password	age	priv
1	1	admin	[redacted]	30	0
2	2	agent	[redacted]	30	1

Max Rows: 1000 Max Chars: -1

Recommendation:

Usage of hash functions and salted passwords used in storage to secure passwords.

For more details:

https://www.techopedia.com/7/29786/security/how-can-passwords-be-stored-securely-in-a-database

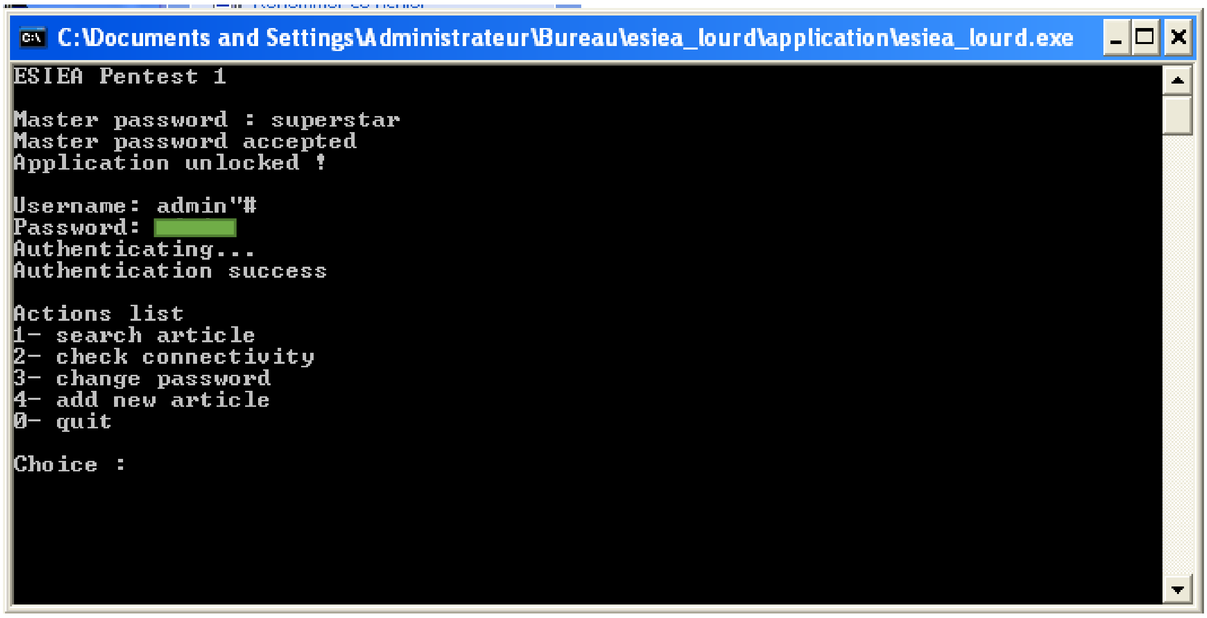
Vulnerability 3: “Weak passwords are accepted”

Description:

Accepting weak password set for authentication when accessing application or database leads to high security threat as attacker can easily guess weak passwords and thus attacker can gain full access to application database and files that can be modified by the attacker.

Exploitation:

Useful information can be leaked without the password being entered.


C:\Documents and Settings\Administrateur\Bureau\esiea_lourd\application\esiea_lourd.exe

```
ESIEA Pentest 1

Master password : superstar
Master password accepted
Application unlocked !

Username: admin"#
Password: [redacted]
Authenticating...
Authentication success

Actions list
1- search article
2- check connectivity
3- change password
4- add new article
0- quit

Choice :
```

Recommendations:

1) Use relatively strong passwords that are not easy to guess by the Attackers.

2) Password should not refer to the personals details of the user, such as their surnames , birth info, mobile numbers, etc.

For more information:

https://www.oracle.com/technetwork/database/security/secure-passwords-082531.html

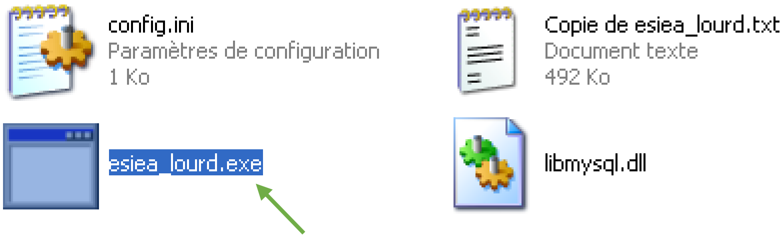
Vulnerability 4: “Passwords shown while typing”

Description:

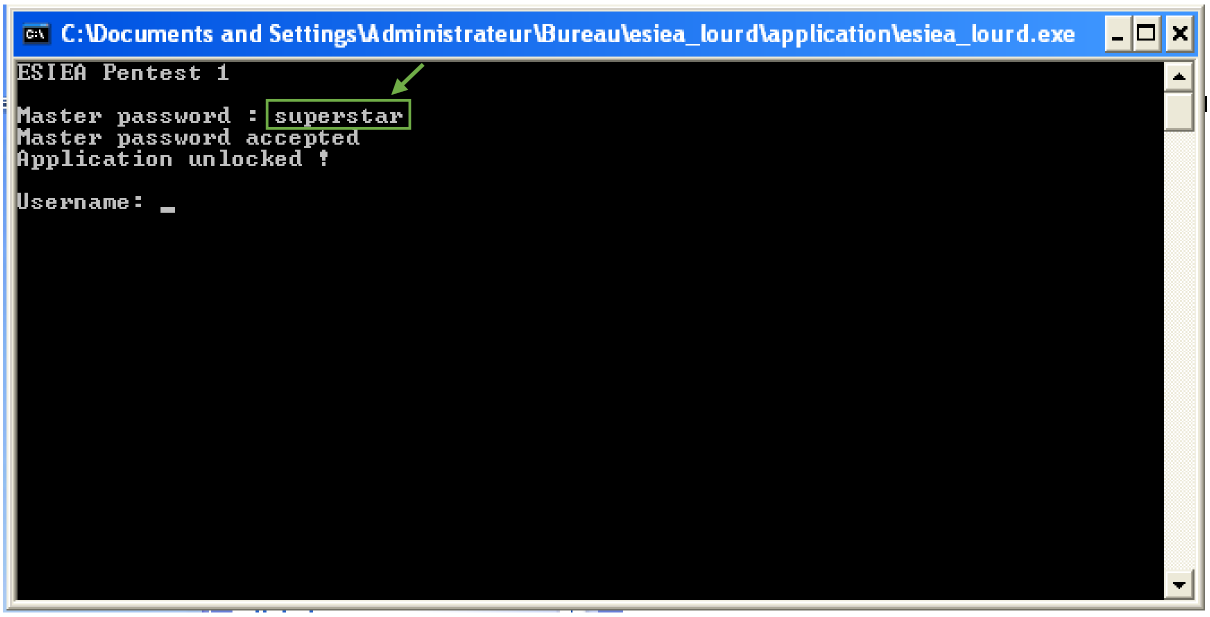
When the password is entered on the admin interface, it is not encrypted and clearly visible. If the attacker has access to the user’s system, the user’s credentials can be monitored, which leads to further attacks. Cryptographic password protection algorithms are not used.

Exploitation:

1) Open esiea_lourd.exe file.

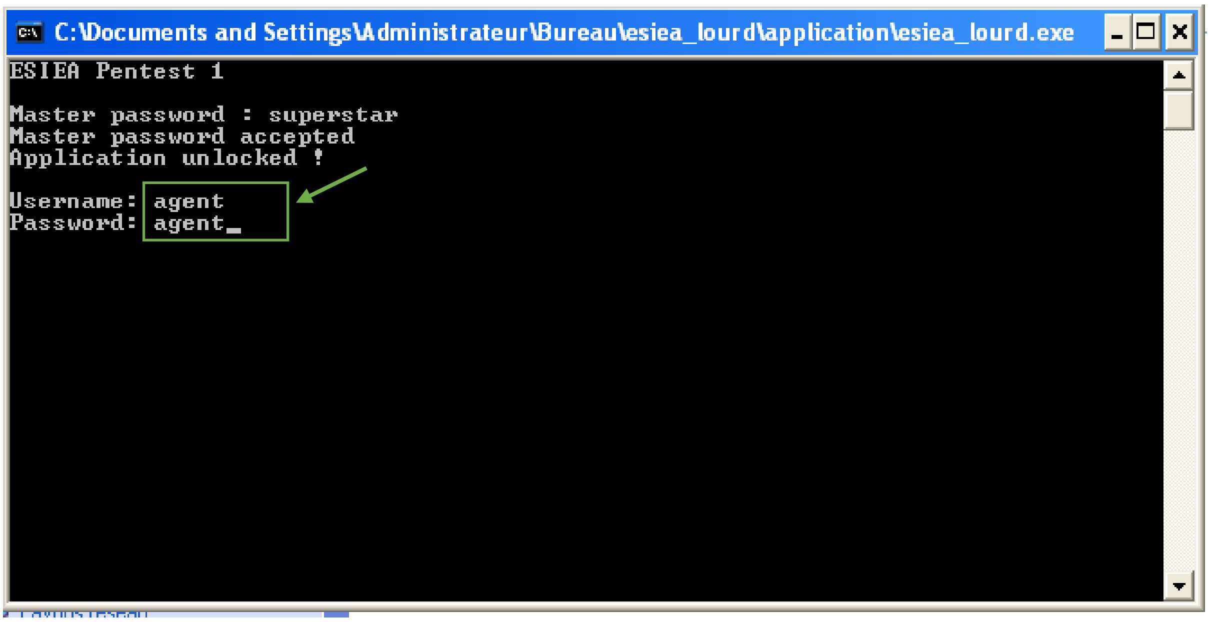


2) Enter master password – superstar, and here the password is not encrypted, it’s visible.


C:\Documents and Settings\Administrateur\Bureau\esiea_lourd\application\esiea_lourd.exe

```
ESIEA Pentest 1

Master password : superstar
Master password accepted
Application unlocked !

Username: _
```

3) It will ask you for username and server password after entering master password, once you enter passwords, they are not encrypted.


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_
```

Recommendations:

1) Making the default configuration as hide password while entering the application's password.
2) Use Hash functions, to change a text password to a more complex set of characters by using more complex operations.

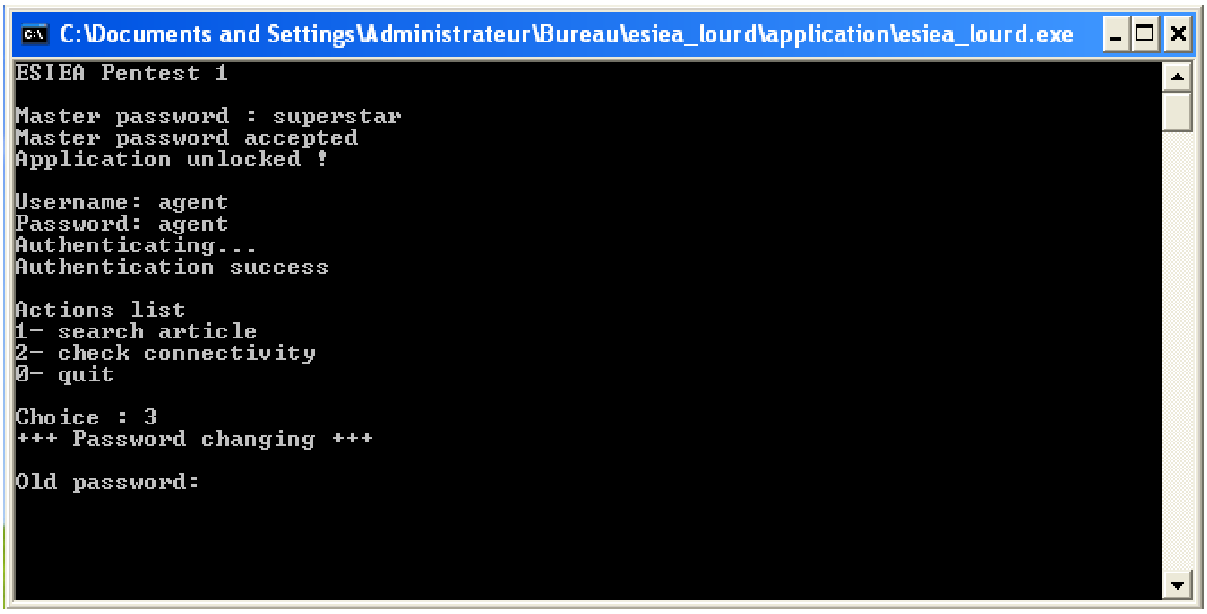
For more Information:

https://www.techopedia.com/7/29786/security/how-can-passwords-be-stored-securely-in-a-database

Vulnerability 5: “Bad profile segregation”

Description:

- You can see that authentication is successful after entering username and password and showing the action list to perform actions.
- In the actions list we can see three action choices but if you give additional choice 3 and press enter it will ask you to change your password.
- choice 4 also provides additional information.

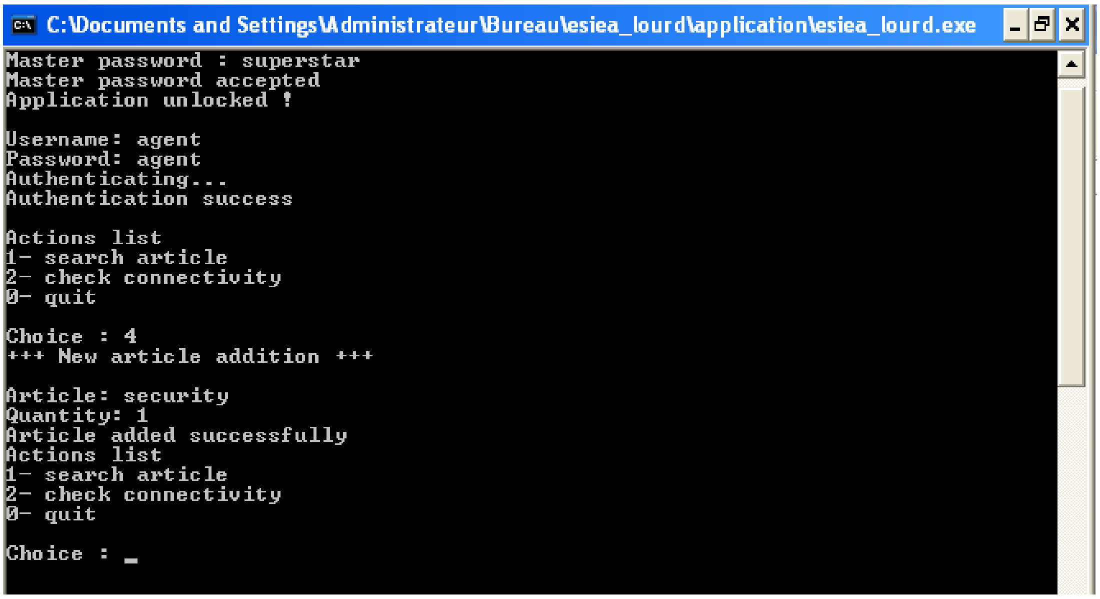


C:\Documents and Settings\Administrateur\Bureau\esiea_lourd\application\esiea_lourd.exe

```
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 : 3
+++ Password changing +++

Old password:
```

Exploitation:

Attacker can create a new password and it would be dangerous for the company.


C:\Documents and Settings\Administrateur\Bureau\esiea_lourd\application\esiea_lourd.exe

```
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: security
Quantity: 1
Article added successfully
Actions list
1- search article
2- check connectivity
0- quit

Choice : _
```

Recommendations:

1) I would claim that they should only be open to the administrator for this vulnerability.
2) If admin wants more choice, by using his password, admin can add it.

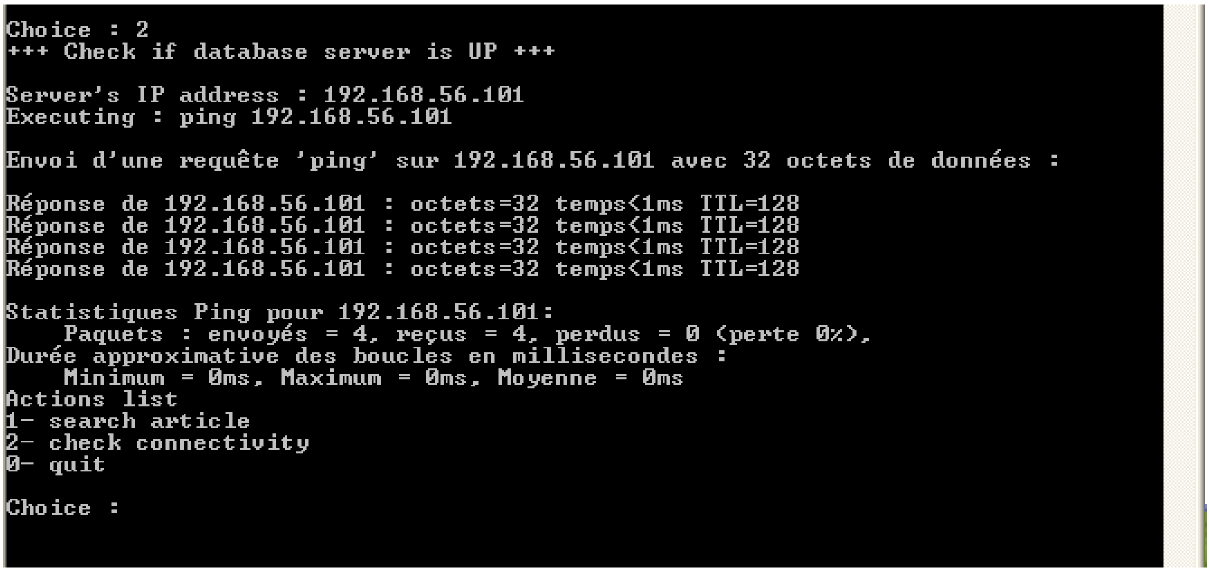
Vulnerability 6: “Arbitrary system command injection”

Description:

- Upon entering the password, 3 choices are shown, and when you pick 2nd choice, the IP address of the database server is requested.
- If you enter the address of the Internet Protocol with & / ; / , all directories within the application will be displayed.

Exploitation:

1) Attackers can use those special characters to inject system commands, by using this attack, the data can be accessed, modified and deleted by the attacker.
2) This means that attackers can quickly take full control of a web server, so developers should be very careful how to pass user input to one of those features.



```
Choice : 2
+++ Check if database server is UP +++

Server's IP address : 192.168.56.101
Executing : ping 192.168.56.101

Envoi d'une requête 'ping' sur 192.168.56.101 avec 32 octets de données :

Réponse de 192.168.56.101 : octets=32 temps<1ms TTL=128
Réponse de 192.168.56.101 : octets=32 temps<1ms TTL=128
Réponse de 192.168.56.101 : octets=32 temps<1ms TTL=128
Réponse de 192.168.56.101 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.56.101:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
Actions list
1- search article
2- check connectivity
0- quit

Choice :
```

Recommendation:

1) To prevent an attacker from injecting special characters into the command, seek to typically avoid possible system calls.

2) Under all conditions, avoid any kind of user input inside the file unless it is necessary and disable the feature in the configuration file of your language unless you need it.

Vulnerability 7: “Network traffic is not encrypted”

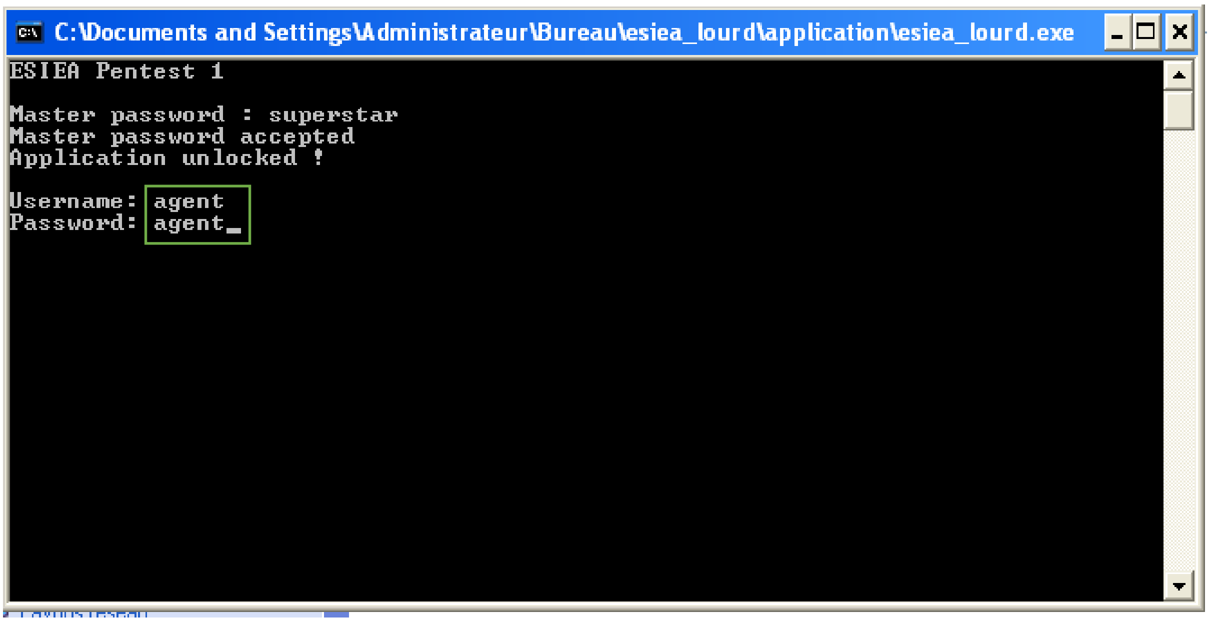
Description:

- There is no encryption for network communication and passwords can be sniffed using Wireshark software.
- If the communication is not encrypted, by man-in-the-middle attack, attackers will sniff the passwords.
- Attackers may gain additional information such as IP address, MAC address, port no’s and protocols for source and destination.
- An attacker views the network traffic of a legitimate user may record and track their application interactions and gain any information provided by the user.
- In addition, the application could be used by an attacker capable of modifying traffic as a platform for attacking its users.
- It can overload the network and interrupt the connection between two machines.

Exploitation:

Open Wireshark and select the network interface, and click start as shown in the image below.

Open the executable file and enter the username: agent
password: agent

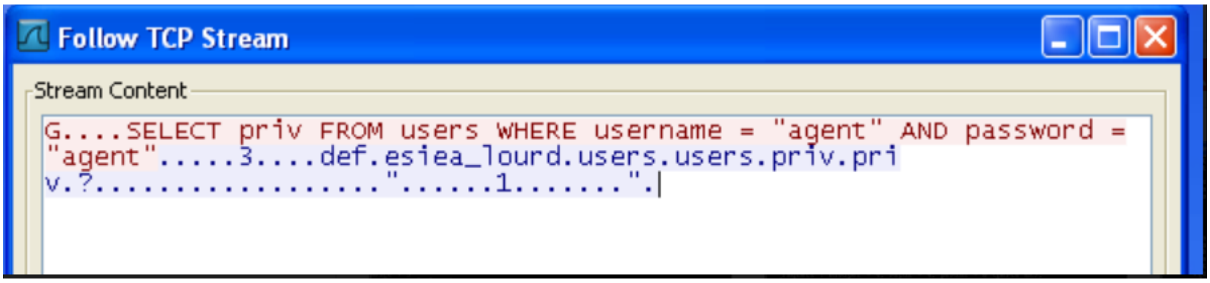

C:\Documents and Settings\Administrateur\Bureau\esiea_lourd\application\esiea_lourd.exe

```
ESIEA Pentest 1

Master password : superstar
Master password accepted
Application unlocked !

Username: agent
Password: agent_
```

- Now switch to Wireshark, you see “Request Query” capturing Wireshark login packets.

- Right click the request query packet and select the option to follow the TCP stream.

- Username and Passwords are shown in the image below.



```
G....SELECT priv FROM users WHERE username = "agent" AND password =
"agent".....3....def.esiea_lourd.users.users.priv.pri
v.?................."......1.......".
```

Recommendations:

1) Strong encryption mechanism should be available for the application.

2) Don’t send passwords in plain text.

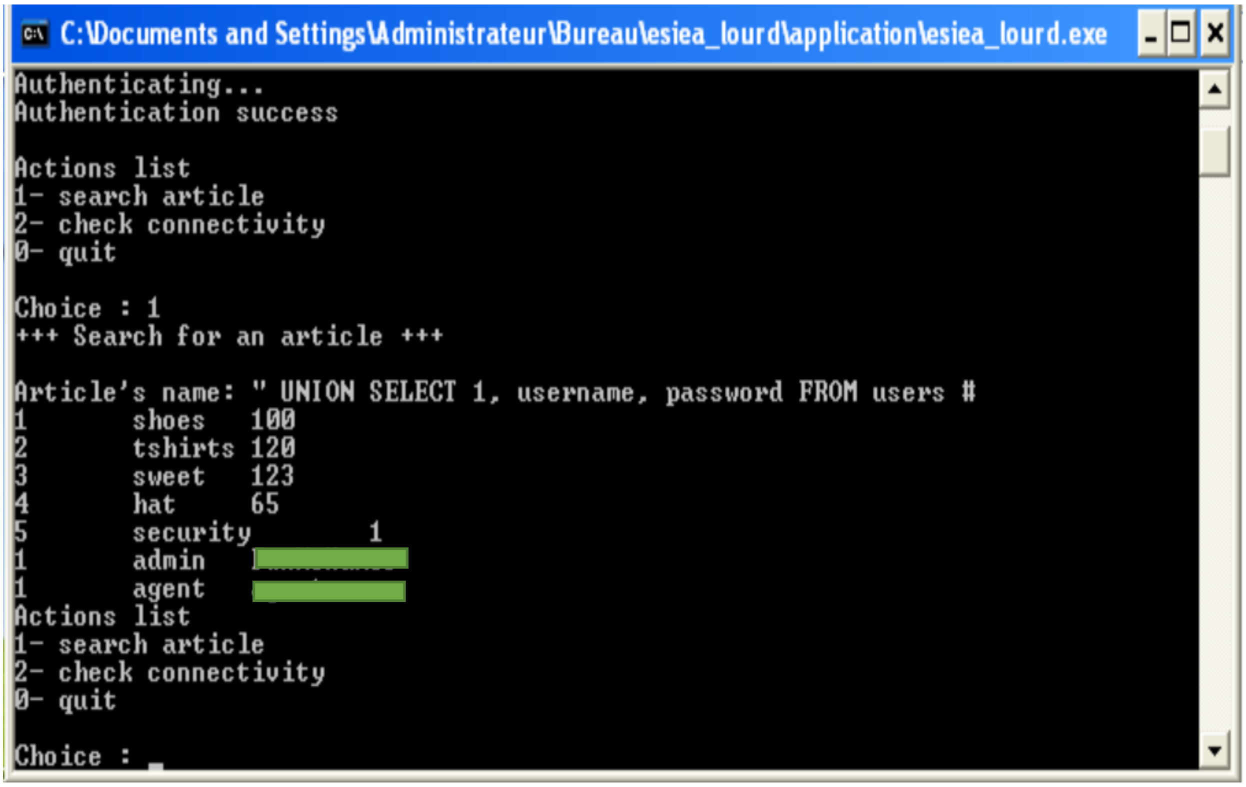
Vulnerability 8: “SQL Injection”

Description:

- Creating websites were easy in the early days of the internet: No JavaScript No CSS.
- But as the web became popular, more advanced technologies such as ASP, JSP, PHP were needed.
- The vulnerability of SQL injection is one of the most dangerous issues in web applications for data confidentiality and integrity.

Exploitation:

- This SQL injection effectively removes the validation of the username and in this case returns a dataset to an existing “user-admin”.
- The attacker can now log in with the account of an administrator without specifying a password.


C:\Documents and Settings\Administrateur\Bureau\esiea_lourd\application\esiea_lourd.exe

```
Authenticating...
Authentication success

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

Choice : 1
+++ Search for an article +++

Article's name: " UNION SELECT 1, username, password FROM users #
1       shoes   100
2       tshirts 120
3       sweet   123
4       hat     65
5       security        1
1       admin   [redacted]
1       agent   [redacted]
Actions list
1- search article
2- check connectivity
0- quit

Choice : _
```

Recommendation:

- Do not use dynamic SQL.
- Do not create user input queries.
- Also data sanitization protocols may be faulty, so wherever possible, use prepared statements, parameterized queries or stored procedures instead.
- Vulnerabilities are regularly discovered in applications and databases that attackers can exploit using SQL injection, so it is vital that patches and updates be applied as soon as possible. The investment might be worth a patch management solution.