SOFTWARE AND DATABASE SECURITY
- PROF. ADEL KHALDI

Dated-23/03/2019

By,

Bharani Moorthy – M.E (Systems, Networks and Security)

Dinsan Loord -(M.Sc. Software Engineering)

Summary

a) Security Audit Context

Security Audit is for finding the weaknesses in the application:

The security audit is the assessment of the applications/Db functionality to finding the risks, vulnerabilities/loopholes in it. The security audit is paramount even before introducing and after the release of new applications/software products. Continues assessment of the software/app. and fixing the loopholes is super important to avoid getting hooked up from the fast-growing new cyber-attacks (zero-day attacks)

E.g.: www.yourmail.com/email.php?id=**01234** Checking that the Changing ID of the URL can we able to login another users' space

b) General ideas about vulnerabilities:

The weakness in the application is called as Vulnerabilities. This vulnerability leads the undesirable outcomes as cyber-attacks like user credential thefts, insecure software configurations, sniffing the data's, unauthorized access and compromise of accounts.

c) General ideas about recommendations:

Recommendation is the mitigation steps to fixing the weaknesses. By Understanding the functionality properly and fixing the patches /adopting the best security practices appropriately can fortified us from the cyber-attacks.

-Bharani Moorthy

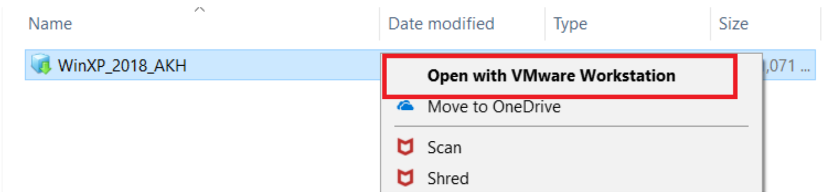
INDEX

ENVIRONMENTAL SETUP

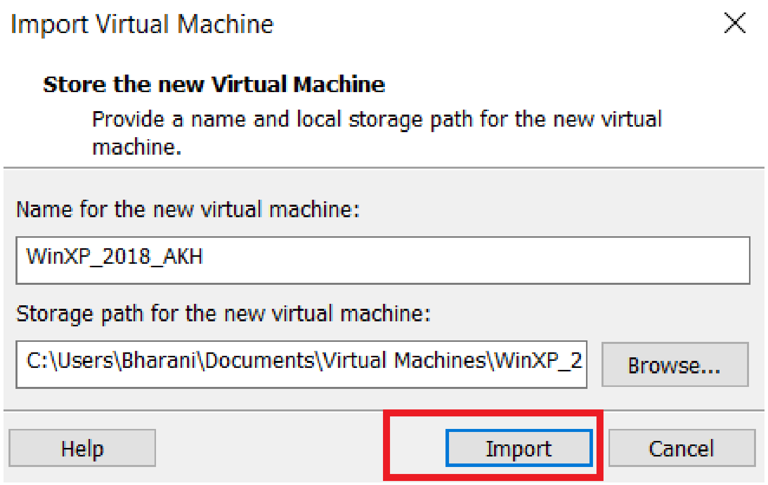
- Preparing the 2 VM's in VMware (client and server side)

Server side:

1. Created the server-side machine, right click the downloaded **WinXP.ova file** and selected Open with VMware Workstation.



2. It prompted to **import** virtual machine and click import to prepare the Windows XP Server machine.


Import Virtual Machine

Store the new Virtual Machine

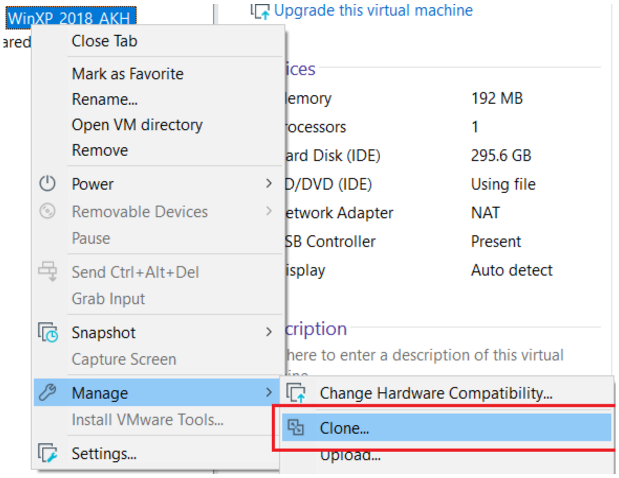
Provide a name and local storage path for the new virtual machine.

Name for the new virtual machine: WinXP_2018_AKH

Storage path for the new virtual machine: C:\Users\Bharani\Documents\Virtual Machines\WinXP_2

Client side:

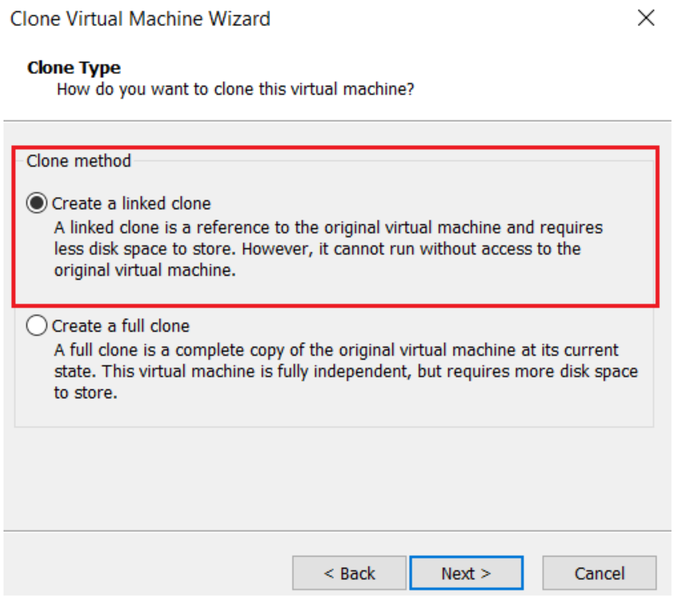
1. Created the Client-side machine, right click the server machine VM list and select Manage >**Clone** option to create the Client machine.



lemory	192 MB
ocessors	1
ard Disk (IDE)	295.6 GB
D/DVD (IDE)	Using file
etwork Adapter	NAT
SB Controller	Present
isplay	Auto detect

here to enter a description of this virtual

2. Selected the **Linked clone** to prepare the client machine


Clone Virtual Machine Wizard

Clone Type
How do you want to clone this virtual machine?

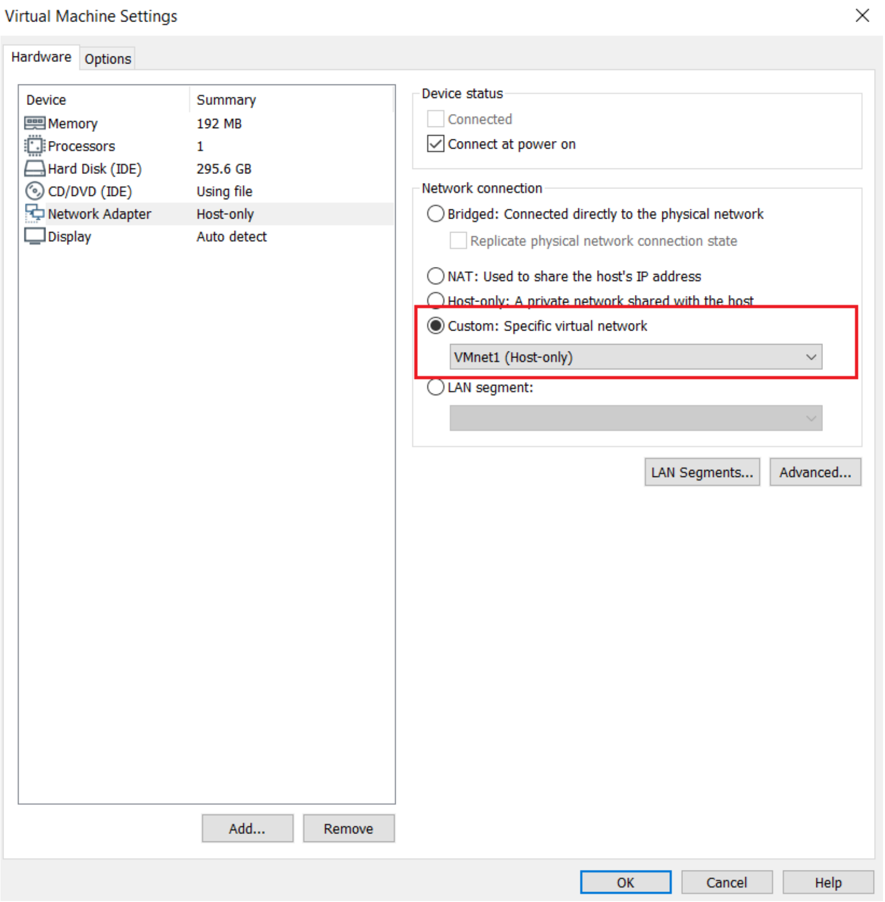
Clone method

● Create a linked clone
A linked clone is a reference to the original virtual machine and requires less disk space to store. However, it cannot run without access to the original virtual machine.

○ Create a full clone
A full clone is a complete copy of the original virtual machine at its current state. This virtual machine is fully independent, but requires more disk space to store.

- **Network configuration**

Made the Change in both the server and the client VM network settings by selecting custom option >VMnet1(**Host-only**)



Device	Summary
Memory	192 MB
Processors	1
Hard Disk (IDE)	295.6 GB
CD/DVD (IDE)	Using file
Network Adapter	Host-only
Display	Auto detect

Device status

☐ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

☐ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

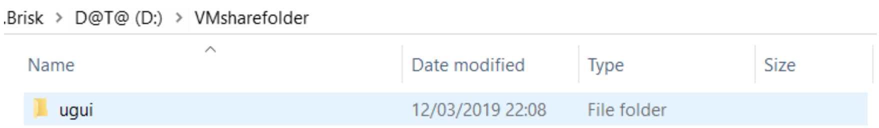
● Custom: Specific virtual network

VMnet1 (Host-only)

○ LAN segment:

- **Filesharing between host and VM**

1. Installed Vmware tools and Created the share folder(D:\VMsharefolder\ugui) in my host machine for the sharing the content from Host to VM.



.Brisk > D@T@ (D:) > VMsharefolder

Name	Date modified	Type	Size
ugui	12/03/2019 22:08	File folder	

2. Selected the virtual machine settings of both the client and the server and enable the shared folder as always, then add the host path as (D:\VMsharefolder\ugui)

VULNERABILITIES

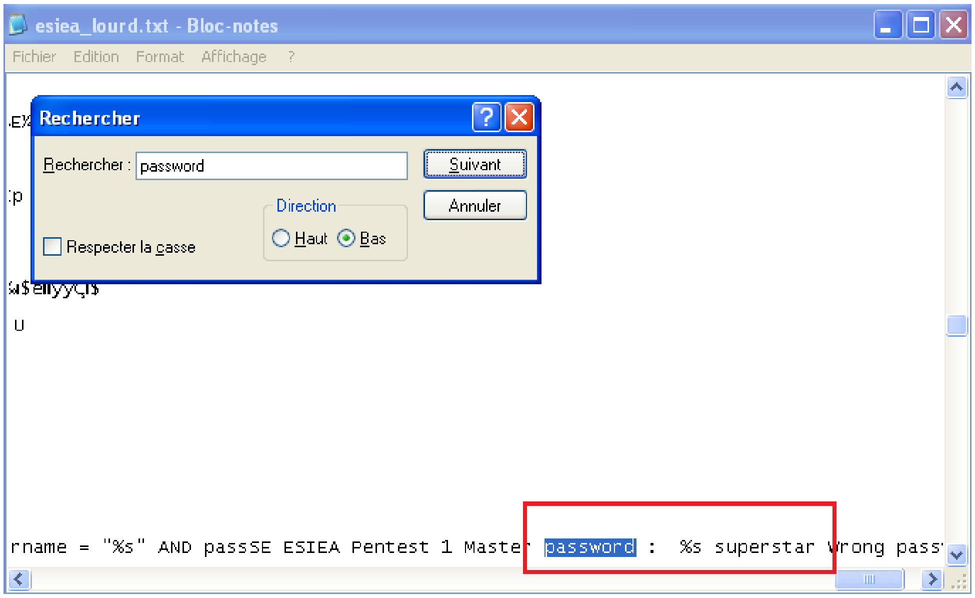
1- Secret present in the executable file

Description:

The .exe file of the software itself contains the password information in a readable form. This provides a backdoor to the attacker to trace the user credentials, once the attacker finds the credentials, he can able to access the Db directly and able to make change /access the sensitive data, because of the two-tier architecture.

Exploitation :

The copy of **esie_lourd.exe** file can be renamed as **esie_lourd.txt**, and it was opened in notepad. Once opened, CTRL +F to find the word ”Password”, click the next sequentially until to find the master password-**superstar.**



Rechercher : password

☐ Respecter la casse

Direction: ○ Haut ● Bas

```
.EX
:p
%$ellyyÇI$
 U
rname = "%s" AND passSE ESIEA Pentest 1 Master password :  %s superstar Wrong pass
```

Recommendation :

Encrypt the execution file folder by using software like TrueCrypt and Migrating from the 2 tier architecture to the 3 tier architecture is the best solution to enhance security by facilitate the middle layer [webserver authentication and citrix workspace]-even it is more difficult for the attacker to bypass the two layers of authentication to access the target Database.

More details:

- https://www.cgisecurity.com/database/oracle/pdf/threetier.pdf
- https://www.javaworld.com/article/2076964/scale-an-application-from-2-to-3-tiers-with-jDbc.html
- https://www.researchgate.net/figure/3-tier-architecture_fig1_277187696-

- Bharani Moorthy

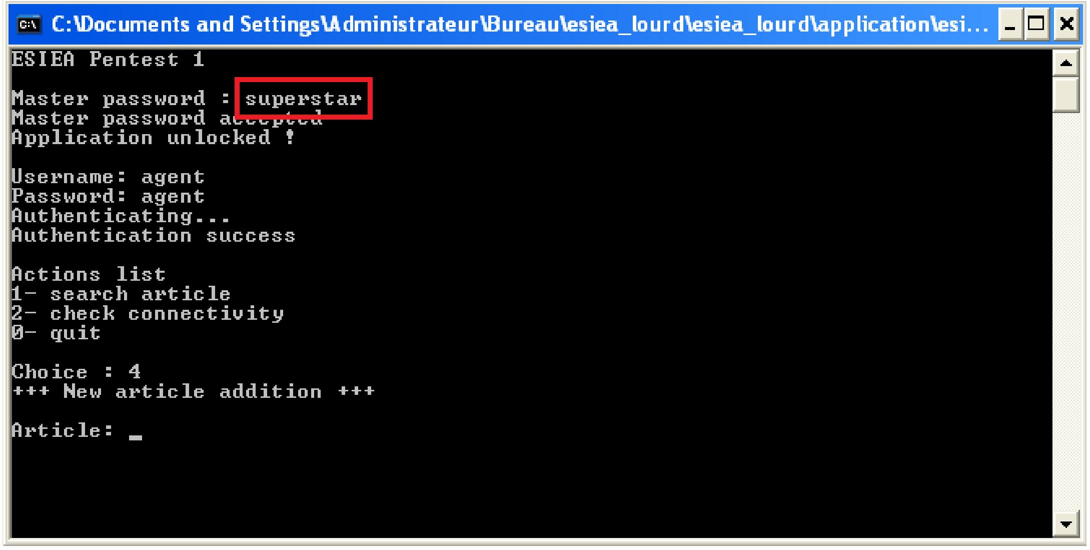
2- Password shown when typing:

Description:

While typing the master password, the text is visible to the user. Anybody behind the user can see the user password (“shoulder surfing”). It is a severe security loophole.

Exploitation:

While typing the master password as “superstar” in the console, the test is fully visible like the username, it is not masked.



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

```
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: _
```

Recommendation:

User must enable the password mask option in the MySQL operating system should be hide the complete password string while typing like the *** / Glitching curser. User can also make use of the password vault software like CyberArk to provide extra security according to the Privileged access.

More details:

- https://www.linuxtechi.com/10-passwd-command-examples-in-linux/
- https://forum.uipath.com/t/how-to-hide-password-completely/67167/4
- https://www.cyberark.com/resource/cyberark-core-privileged-account-security-solution/

-Bharani Moorthy

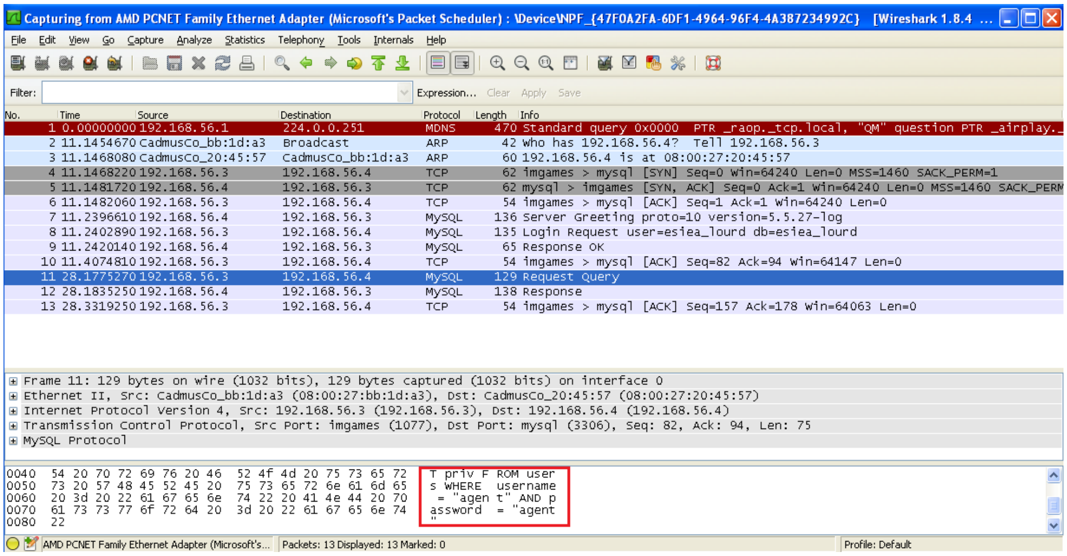
3- Network communication not encrypted

Description:

The network communication between the server and the client has not been encrypted, it allows the attackers can eavesdropping the information [Man in the Middle attack]. It is more vulnerable that anyone in outside can trap the communication

Exploitation :

In client server, while login the MySQL console, simultaneously we have started the packet capture software to sniffing the network traffic, by analysing one of the SQL login payload, the user name "**agent**" and password as "**agent**" was found as plain text without being encrypted.


Capturing from AMD PCNET Family Ethernet Adapter (Microsoft's Packet Scheduler) : \Device\NPF_{47F0A2FA-6DF1-4964-96F4-4A387234992C}   [Wireshark 1.8.4 ...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time        Source              Destination        Protocol Length Info
   1 0.00000000 192.168.56.1        224.0.0.251        MDNS      470 Standard query 0x0000  PTR _raop._tcp.local, "QM" question PTR _airplay._
   2 11.1454670 CadmusCo_bb:1d:a3   Broadcast          ARP        42 Who has 192.168.56.4?  Tell 192.168.56.3
   3 11.1468080 CadmusCo_20:45:57   CadmusCo_bb:1d:a3  ARP        60 192.168.56.4 is at 08:00:27:20:45:57
   4 11.1468220 192.168.56.3        192.168.56.4       TCP        62 imgames > mysql [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
   5 11.1481720 192.168.56.4        192.168.56.3       TCP        62 mysql > imgames [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM
   6 11.1482060 192.168.56.3        192.168.56.4       TCP        54 imgames > mysql [ACK] Seq=1 Ack=1 Win=64240 Len=0
   7 11.2396610 192.168.56.4        192.168.56.3       MySQL     136 Server Greeting proto=10 version=5.5.27-log
   8 11.2402890 192.168.56.3        192.168.56.4       MySQL     135 Login Request user=esiea_lourd db=esiea_lourd
   9 11.2420140 192.168.56.4        192.168.56.3       MySQL      65 Response OK
  10 11.4074810 192.168.56.3        192.168.56.4       TCP        54 imgames > mysql [ACK] Seq=82 Ack=94 Win=64147 Len=0
  11 28.1775270 192.168.56.3        192.168.56.4       MySQL     129 Request Query
  12 28.1835250 192.168.56.4        192.168.56.3       MySQL     138 Response
  13 28.3319250 192.168.56.3        192.168.56.4       TCP        54 imgames > mysql [ACK] Seq=157 Ack=178 Win=64063 Len=0
```

```
⊞ Frame 11: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits) on interface 0
⊞ Ethernet II, Src: CadmusCo_bb:1d:a3 (08:00:27:bb:1d:a3), Dst: CadmusCo_20:45:57 (08:00:27:20:45:57)
⊞ Internet Protocol Version 4, Src: 192.168.56.3 (192.168.56.3), Dst: 192.168.56.4 (192.168.56.4)
⊞ Transmission Control Protocol, Src Port: imgames (1077), Dst Port: mysql (3306), Seq: 82, Ack: 94, Len: 75
⊞ MySQL Protocol
```

```
0040  54 20 70 72 69 76 20 46  52 4f 4d 20 75 73 65 72   T priv F ROM user
0050  73 20 57 48 45 52 45 20  75 73 65 72 6e 61 6d 65   s WHERE  username
0060  20 3d 20 22 61 67 65 6e  74 22 20 41 4e 44 20 70    = "agen t" AND p
0070  61 73 73 77 6f 72 64 20  3d 20 22 61 67 65 6e 74   assword  = "agent
0080  22                                                 "
```

```
AMD PCNET Family Ethernet Adapter (Microsoft's...   Packets: 13 Displayed: 13 Marked: 0   Profile: Default
```

Recommendation:

The entire connection between the SQL server and client should be encrypted by using Always Encrypted (Database Engine) and the ODBC Driver for SQL Server to fix this vulnerability and using the salt+hash cryptography algorithm.

More details:

- https://docs.microsoft.com/en-us/sql/connect/oDbc/using-always-encrypted-with-the-oDbc-driver?view=sql-server-2017
- https://blogs.sentryone.com/johnmartin/security-nuggets-encrypting-connections/

-Dinsan Loord

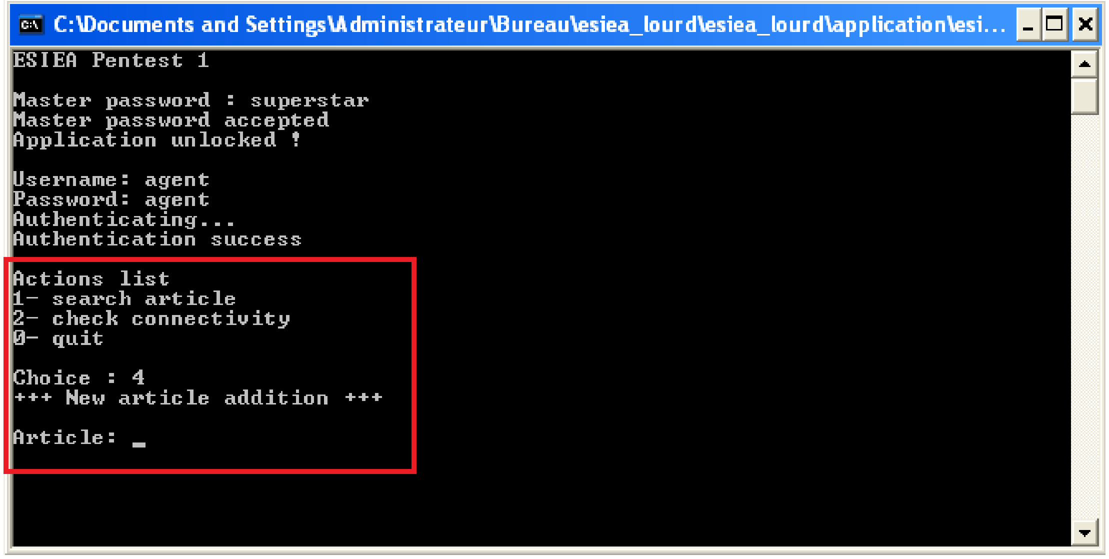
4- Admin options accessible from Limited user

Description:

There are no privileged restrictions has been enabled in the MySQL server users. The limited user can also make the changes as the administrator users do. It leads to severe drawbacks like password changes in the server.

Exploitation:

In client system, we logged in as the “agent”- limited privilege, and we selected the action list as password changing/article addingooopolkloki:oo, it has the access to change the password of the admin



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

```
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: _
```

Recommendation:

Restricting the limited users by providing the privileged access to the respective user access control could be solution for this vulnerability

More details:

- https://stackoverflow.com/questions/36159318/allow-mysql-user-with-limited-database-access-to-create-more-users-with-similar
- https://dev.mysql.com/doc/refman/5.5/en/privilege-system.html
- https://docs.plesk.com/en-US/12.5/reseller-guide/website-management/website-databases/managing-database-user-accounts.69539/

-Dinsan Loord

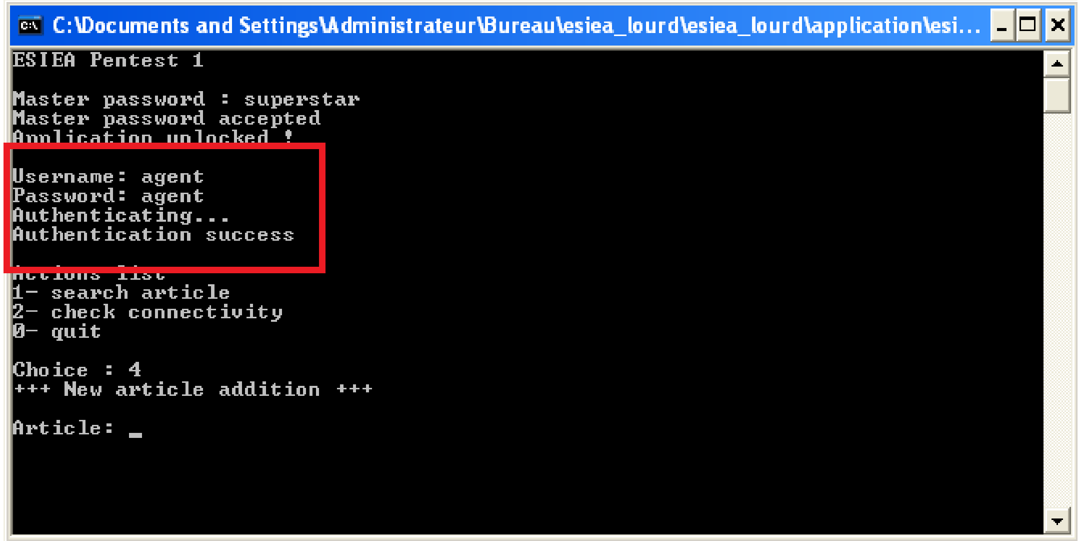
5- Weak Password Accepted:

Description:

The password of the “agent” is used as the “agent” and it is easy to predict and can login into the DB by anybody. Moreover, the master password also used as the weak- simple phrase.

Exploitation:

After login into the DB by using the master password, we just random-try as admin- admin, agent-agent into the system, we can able to login into the DB and can-do necessary changes.


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

```
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: _
```

Recommendation:

Enable the MySQL Password validation plugin. And the user should follow the password policy best practices like avoid using weak password and dictionary strings, phrase without special character and user can also use the Password generator software to generate strong passwords.

More details:

- https://dev.mysql.com/doc/refman/5.6/en/validate-password.html
- https://www.dummies.com/programming/networking/be-aware-of-password-vulnerabilities-to-avoid-getting-hacked/

-Bharani Moorthy

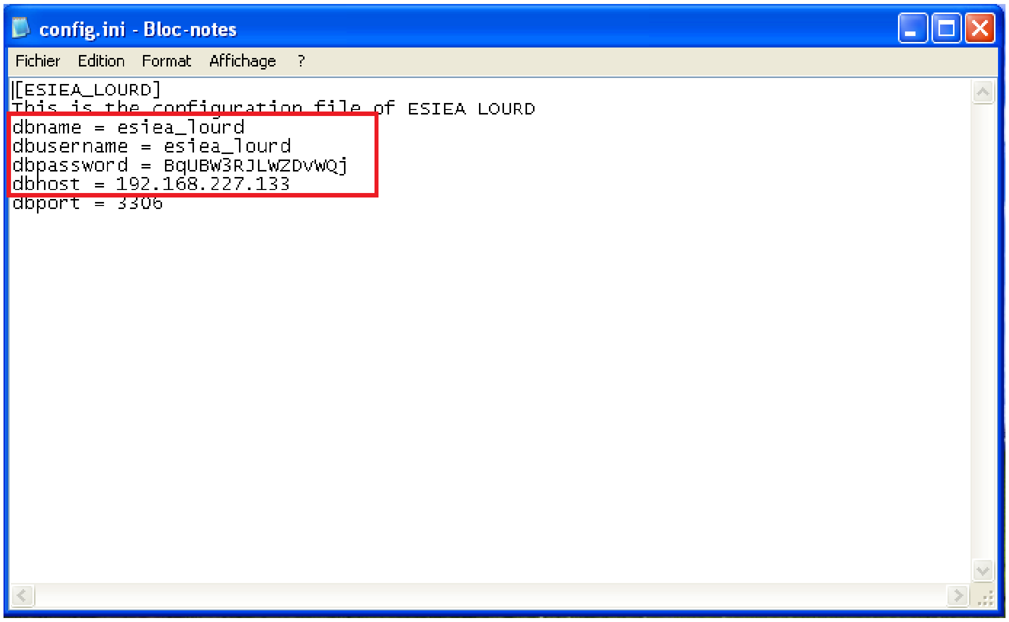
6- Secrets present in configuration file (config.ini)

Description:

The config.ini of the MySQL itself contains the DB credentials and it is easy to read by the attacker/user in the client side and can able to login MySQL server.

Exploitation:

While opening the configuration file of the MySQL, we found the DB credentials to connection with Esiea lourd DB.



```
[ESIEA_LOURD]
This is the configuration file of ESIEA LOURD
dbname = esiea_lourd
dbusername = esiea_lourd
dbpassword = BqUBW3RJLWZDvWQj
dbhost = 192.168.227.133
dbport = 3306
```

Recommendation:

Hiding the information by encrypting using WordPress config security and Making the config.ini must not opened by the users side the DB username and password

More details:

- https://blogtimenow.com/wordpress/wordpress-security-keys-salts-generator/
- https://stackoverflow.com/questions/15962527/how-to-hide-database-password-in-config-file

-Bharani Moorthy

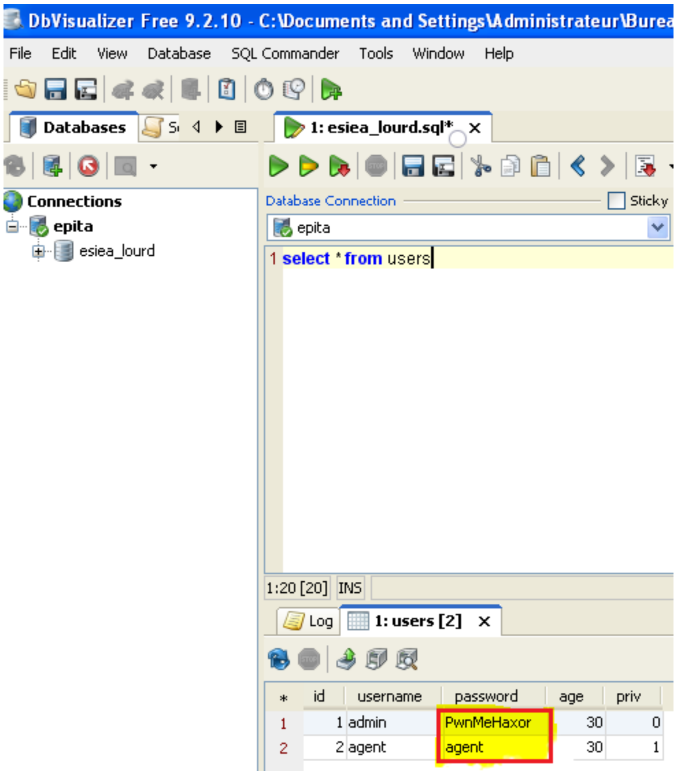
7- Passwords stored in plaintext within database

Description:

If attacker successfully login into the Db/employees in the company like latest news of facebook, anybody can able to see the user name and password. Because it is stored as the plaintext.

Exploitation:

After connection via Dbvisualiser, Select * from table ,on the first 2 column of the table we can find the user name and the password in readable form.



```
select * from users
```

	id	username	password	age	priv
1	1	admin	PwnMeHaxor	30	0
2	2	agent	agent	30	1

Recommendation:

Passwords should never be stored as plain text in any database. Hashing passwords using BCrypt is a safe solution that is easy to make use of by Blowfish and by using salt+ hash.

More details:

- https://nakedsecurity.sophos.com/2013/11/20/serious-security-how-to-store-your-users-passwords-safely/
- https://dev.mysql.com/doc/refman/5.6/en/password-hashing.html

-Bharani Moorthy