Executive Summary

The purpose of this assessment was to identify vulnerabilities that can lead the system to be exploited and to sever offensive purposes. The tests were carried out assuming the identitiy of an attacker or a malicious user but no harm was made to the functionality or working of the application/network.

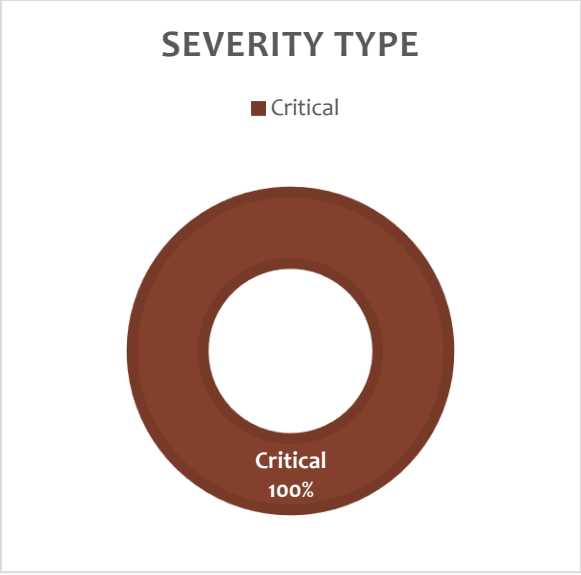
1.1 Scope of Testing

Security assesment includes testing for security loopholes in the scope defined below.

Machine: SAT_CTF

1.2 Graphical Summary

The below graphical representations from the assesment results will provide you an overall summary of the severity, respective CVSS Score.



1.3 List of The Vulnerabilities

#	Vulnerability	Severity	CVSS Score
1	CWE-1392: Default Tomcat Credentials	Critical	10.0
2	CWE-256: Plaintext MySQL Credentials	Critical	9.6
3	CWE-256: Plaintext User Credentials	Critical	9.6

1.4 Details of Discovered Vulnerabilities

Vulnerability#1

(Critical)

Definition: It is common practice for products to be designed to use default keys, passwords, or other mechanisms for authentication. The rationale is to simplify the manufacturing process or the system administrator's task of installation and deployment into an enterprise. However, if admins do not change the defaults, it is easier for attackers to bypass authentication quickly across multiple organizations.

Details: The website has credentials that come by default. Therefore, it can easily allow unauthorized access through a process called brute-force.

Vulnerability#2

(Critical)

Definition: Password management issues occur when a password is stored in plaintext in an application's properties, configuration file, or memory. Storing a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource. In some contexts, even storage of a plaintext password in memory is considered a security risk if the password is not cleared immediately after it is used.

Details: The "tomcat" user on the server placed his credentials in the ".bashrc" file in his directory to use them as environmental variables and easily access the MySQL server. This way, the ".bashrc" file automatically defines these certifications every time the user logs in. However, this means the person who hijacks the "tomcat" user can also read these credentials.

Vulnerability#3

(Critical)

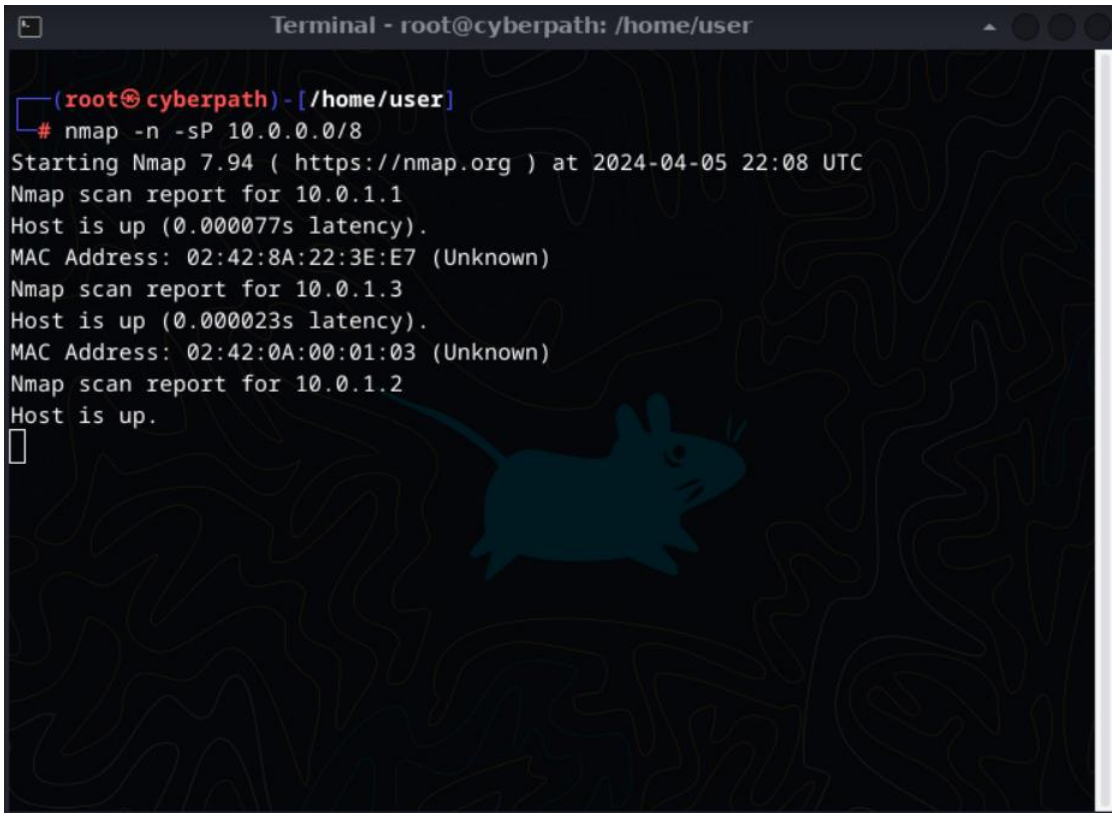
Definition: Password management issues occur when a password is stored in plaintext in an application's properties, configuration file, or memory. Storing a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource. In some contexts, even storage of a plaintext password in memory is considered a security risk if the password is not cleared immediately after it is used.

Details: After the MySQL credentials were obtained, access was gained to the MySQL server located on the eth1 interface of the network. Databases were scanned and username and password were obtained in plaintext in one of them. This may enable attackers to increase their privileges by using these credentials in compromised systems.

Attack Narrative

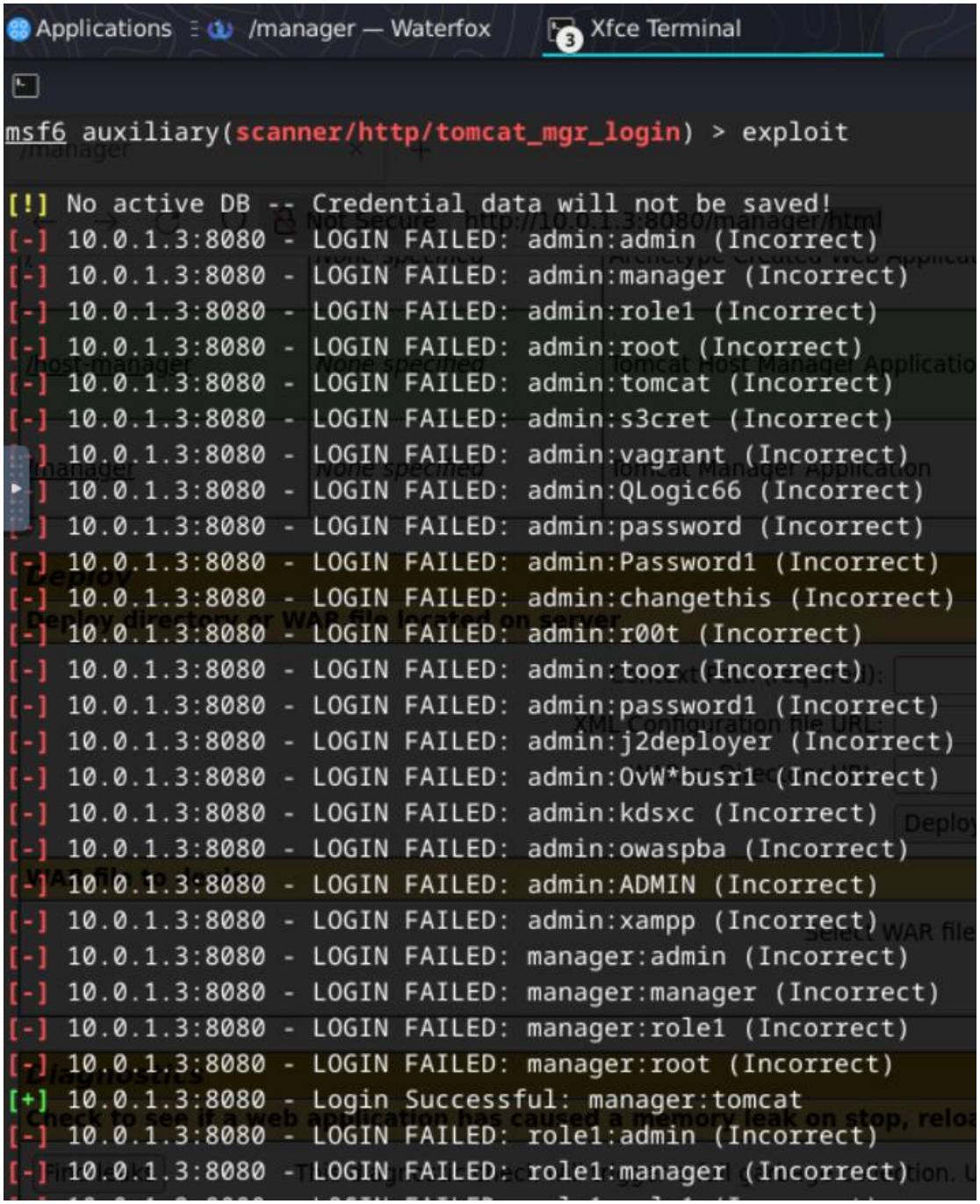
Reconnaissance

Using Nmap, the entire subnet in the system was scanned and the target IP address was found. Using various techniques, the target IP was determined to be 10.0.1.3



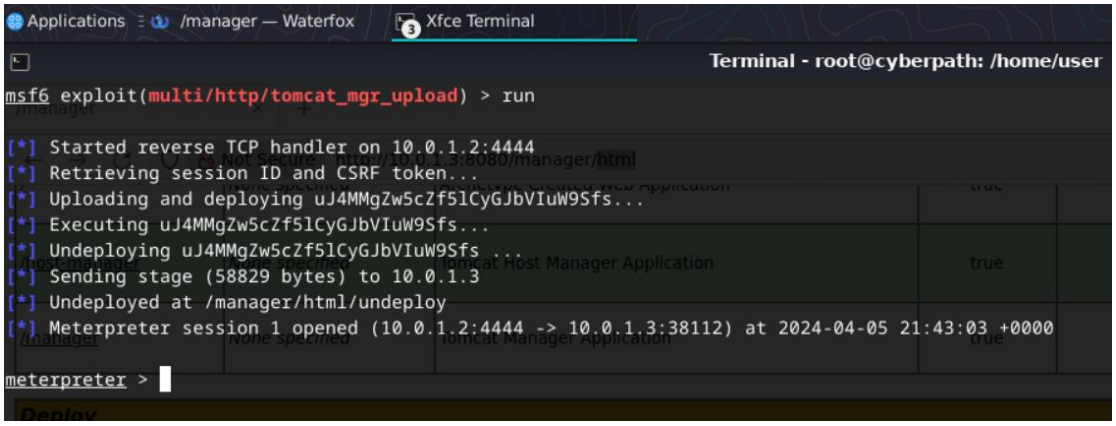
Weaponization

It was seen that the 8080 port (http) of the target IP was open and a brute-force attack was launched. One credential pair was obtained.



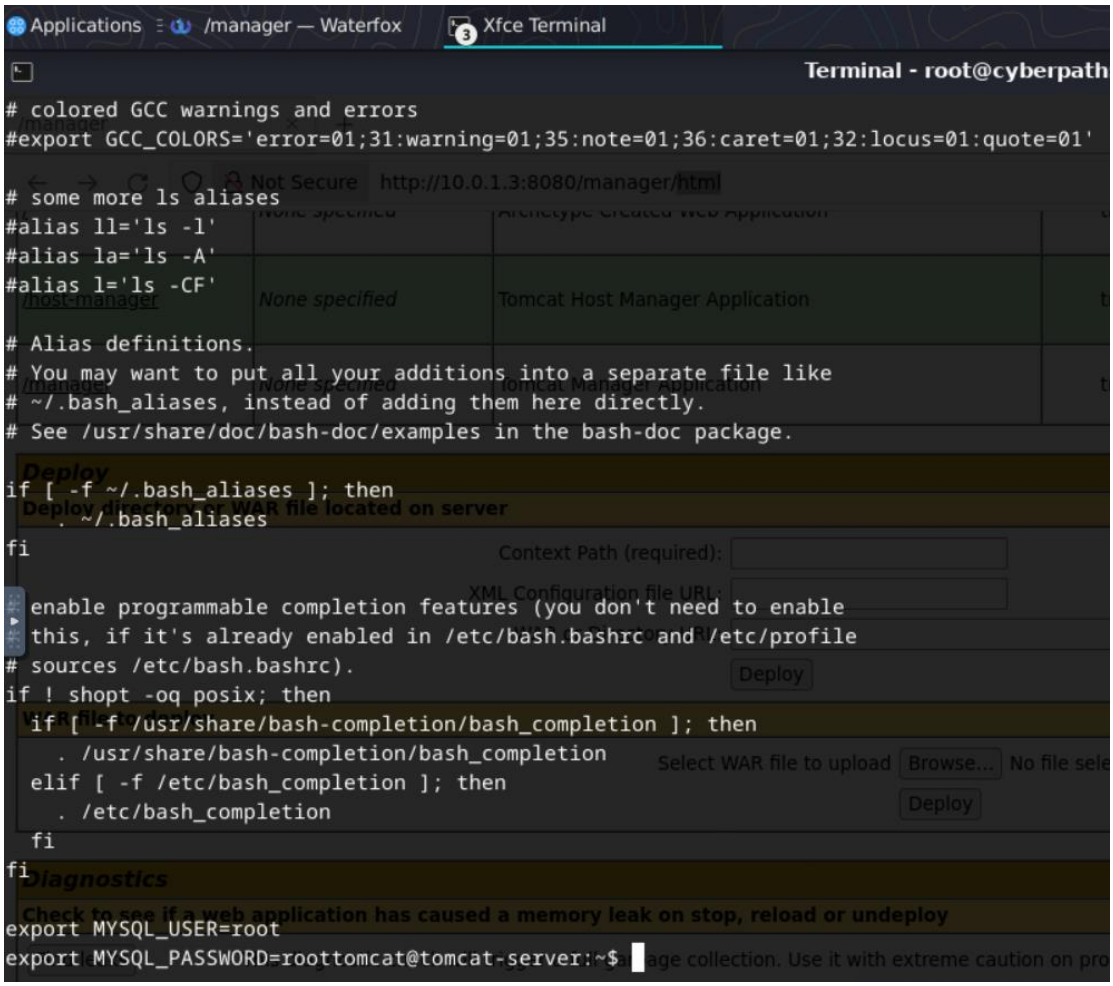
Delivery/Exploitation

Reverse shell was obtained using credentials.

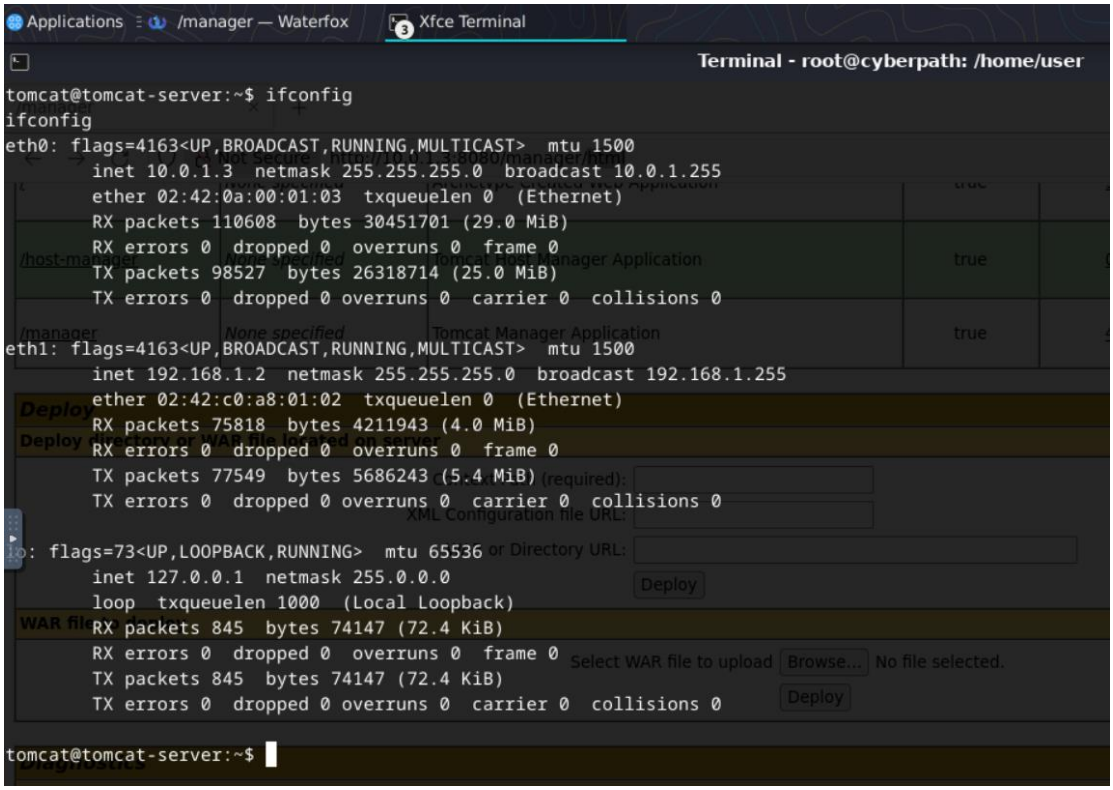


Post Exploitation

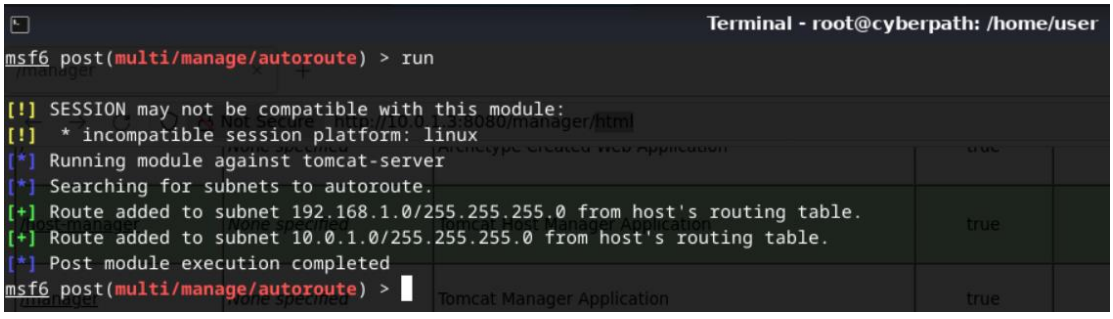
After accessing the system, directories allowed by the "tomcat" began to be scanned, and the credentials of a MySQL account were captured.



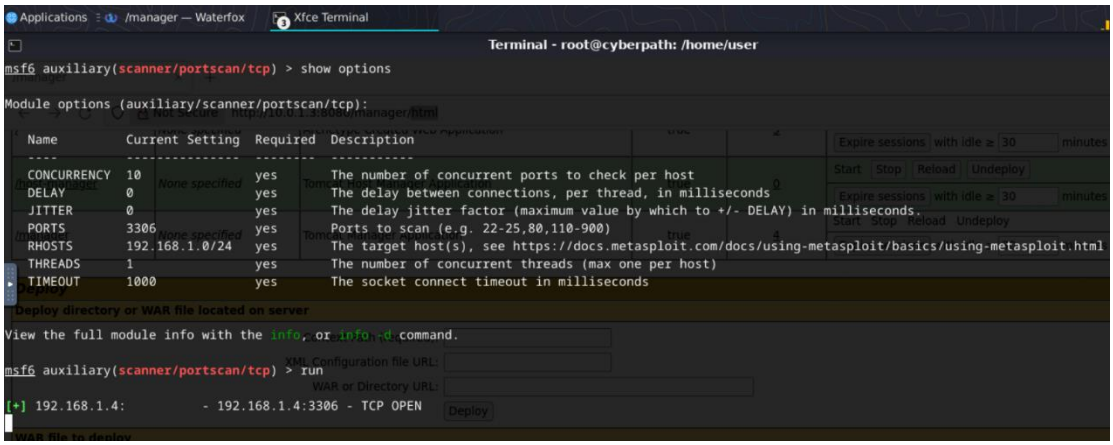
It was also seen that there were two network interfaces in the system. Since there was no place to use these credentials on the current interface, the other interface started to be scanned.



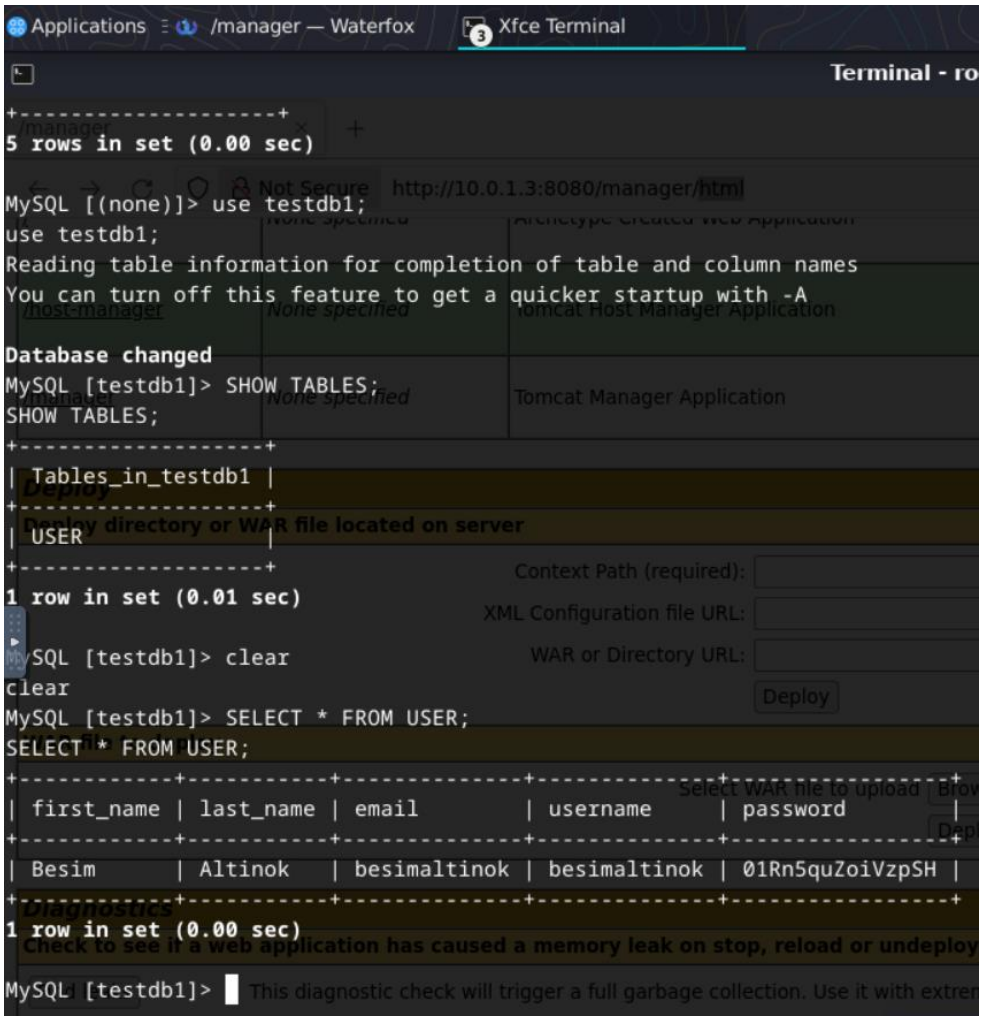
First, pivoting was done.



Then, the IP addresses on the other network were scanned and it was seen that the MySQL service was open on the IP address "192.168.1.4".



The MySQL service was accessed and important information was found.



Prepared By

METUCyber