**Lab 5: Escape a container**

Mou Zhang

**User privileges in Docker containers**

<https://medium.com/jobteaser-dev-team/docker-user-best-practices-a8d2ca5205f4>

1. The first step is to set a secret, which is the target of our hacking. We set it as with root privilege so that only root user can view it. You may use the following command.

电脑萤幕的截图

描述已自动生成图形用户界面, 文本

描述已自动生成

As is shown in the picture, we (mou) have not access the information in the secret.txt.

1. Build a Dockerfile used for a python project and build an image. (This is only and example, which is not important. You can use other dockerfile)

电脑萤幕的截图

描述已自动生成

1. You can build an image for it

图形用户界面, 文本

描述已自动生成

1. Then you mount the while root file system of the host machine to the container and run it

图形用户界面, 文本

描述已自动生成文本

描述已自动生成

As you can see, after running this command, we get the root access to the system.

1. Once in the container, you will have the ability to access the root-owned files. So we can get the message from secret that only root can view. This is very simple. You only need to access the host directory and find the lab5 directory.

图形用户界面, 文本

描述已自动生成

1. For further steps, you can also add yourself to sudoers.d, so that you can run sudo without password. This is to gain the power of sudo account.

图形用户界面, 文本

描述已自动生成

1. Analysis:

By default, docker containers run as root. This provides us a chance to escape the container and get the root privilege and get control of the environment. If you mount the whole root system into the docker, then you can use the root privilege to access the whole root system.