HTB Keeper

Enumeration

`sudo nmap -sC -sV -oA nmap/keeper 10.10.11.227`

Discovery

Subdomain

- `tickets.keeper.htb`

Endpoints

- `tickets.keeper.htb/rt`

Relevant CVEs

- `CVE-2023-32784`

Credentials

- default creds for `Request Tracker (RT) version 4.4.4+dfsg-2ubuntu1`
  - user: `root`
  - pass: `password`
- credential disclosure on `http://tickets.keeper.htb/rt/Admin/Users/Modify.html?id=27`
  - email: `lnorgaard@keeper.htb`
  - pass: `Welcome2023!`

Vulnerabilites

Exploitation

- Login page default credential
- ssh using user credential
- Exfil Keepass database
- Using known CVE to retrieve master key (?)

Appendix

User Flag: `9c0404cde714105f804724b7b156e5df`

Root Flag: `???`