SHELLSHOCK Vulnerability

Bash before 4.3 — Apache CGI-BIN (61) — Openssh - sshd

Allows for remote code execution using shell callouts to bash. payload can be sent simply using curl in http headers (-H)

Exploitation : Curl - shocker.py - Metasploit

Mitigation : Update bash > 4.3 - Dislable shell callouts in /cgi-bin

HTB Shocker

- cgi-bin contains bash script user.sh
- Shellshock exploitation
- sudo -l to root