HTB Codify

By: HyggeHalcyon
relevant scripts and files can be found at github

Foothold

Visiting the web, it's simple and small, nothing much. The web run javascript code in a sandboxed environment using `vm2`. Node modules that are allowed to use are being whitelisted as consequence we can't use `child_process`.

A bit of googling we found a public PoC of CVE-2023-37466 which gaves us RCE, this will be used to gain reverse shell.

Then we can go to `/var/www/contact` where we'll find a user credential of joshua in `tickets.db`. We can crack the password using john and rockyou.

Privesc

running `sudo -l` we can run `mysql-backup.sh` as sudo. Though it still ask you for the root password, the comparison being done here `[[ $DB_PASS == $USER_PASS ]];` is insecure since we can just put a `*` wildcard and it'll pass the check.

With this in mind we can then brute force each of the password character one bye one. I wrote a `privesc.py` script to leak the password.

We can then `su root` to switch to root and pwn the machine.

Appendix

user: `c01e108e689ffa2eaaa041d2dcfb3182`
root: `d52acc033d33d7f336208a239ef8bdb2`