**Cowsay as a Service**

Bài này thật sự rất thú vị.

Khi bạn gửi yêu cầu đến url sau:

https://caas.mars.picoctf.net/cowsay/{message}

thì con bò sẽ nói tin nhắn của bạn.



Mình thật sự không hiểu lỗ hổng là gì cho đến khi đọc file index.js

const express = require('express');

const app = express();

const { exec } = require('child\_process');

app.use(express.static('public'));

app.get('/cowsay/:message', (req, res) => {

exec(`/usr/games/cowsay ${req.params.message}`, {timeout: 5000}, (error, stdout) => {

if (error) return res.status(500).end();

res.type('txt').send(stdout).end();

});

});

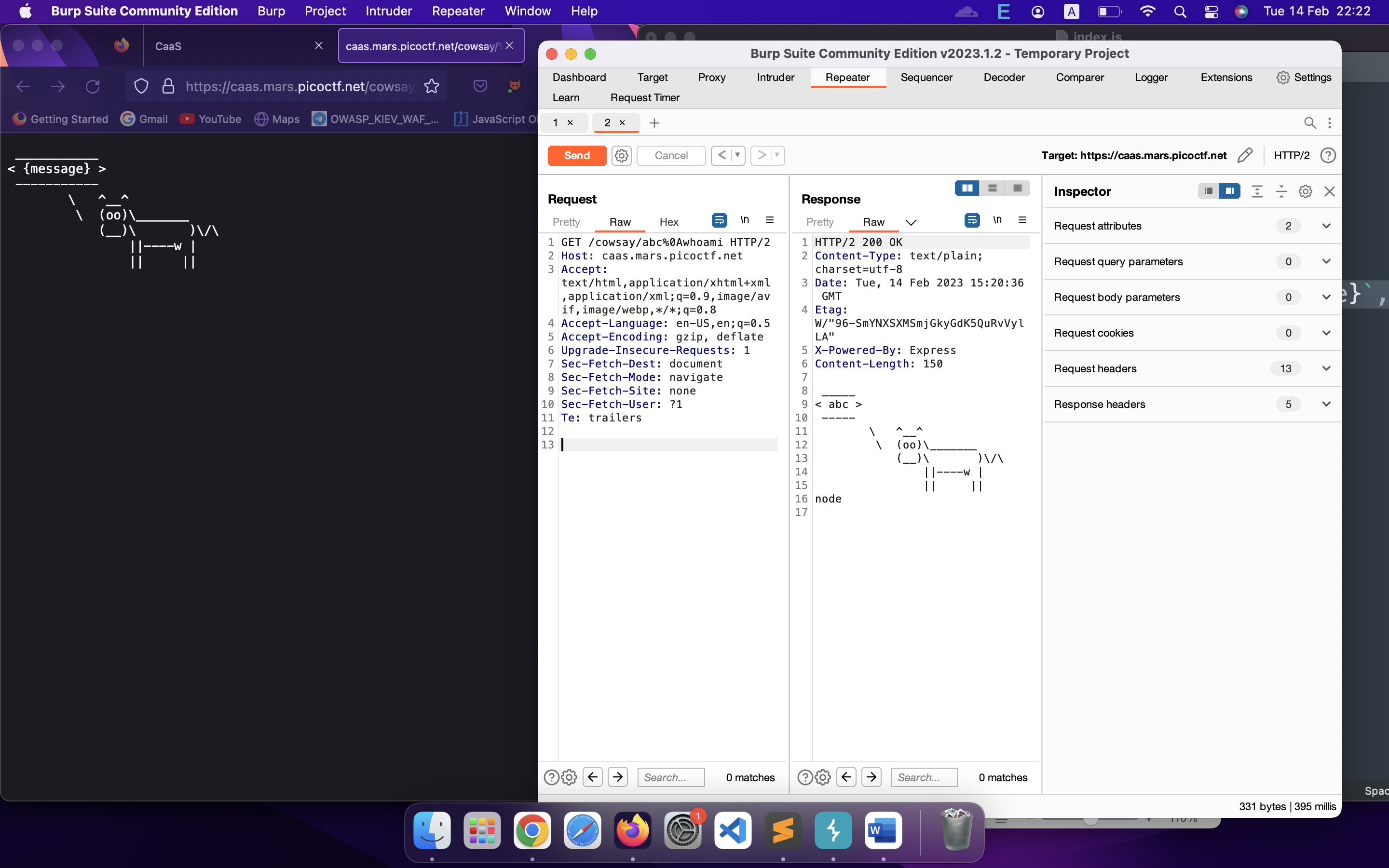
app.listen(3000, () => {

console.log('listening');

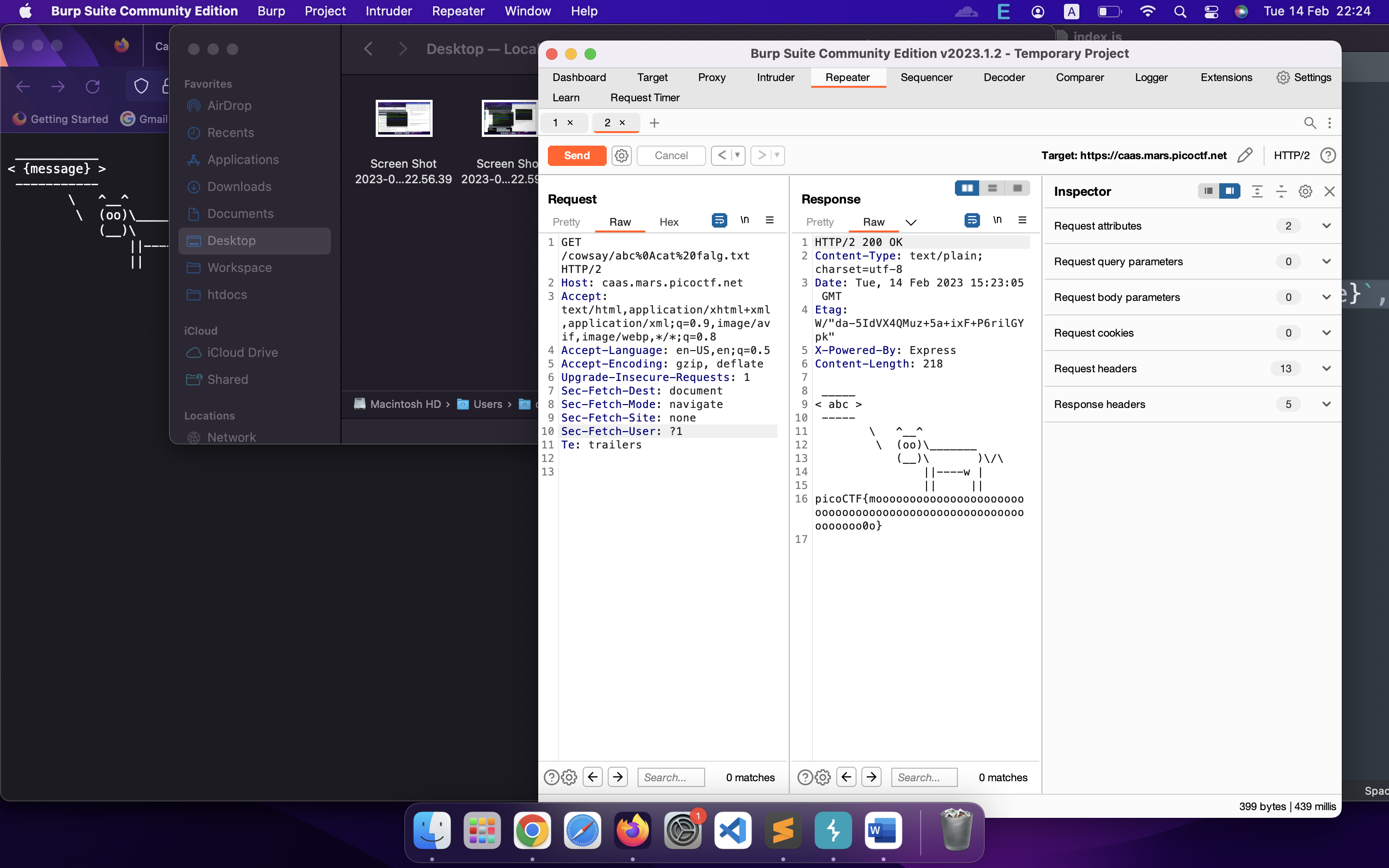
});

Bạn chỉ cần chú ý những điểm mình highlight thôi. Dữ liệu mình kiểm soát là tham số message. Ứng dụng thực thi lệnh qua tham số đó. (exec) 🡪 Lỗ hổng command injection.

Nó đã chặn &,&&,|,||. Mình phải dùng %0A mới được.



Đến đây thì dễ. Mình liệt kê những tập tin có trong thư mục và lấy flag.



**Flag:picoCTF{moooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo0o}**