**Ifexer**

Incognicat

Danang

R.A.

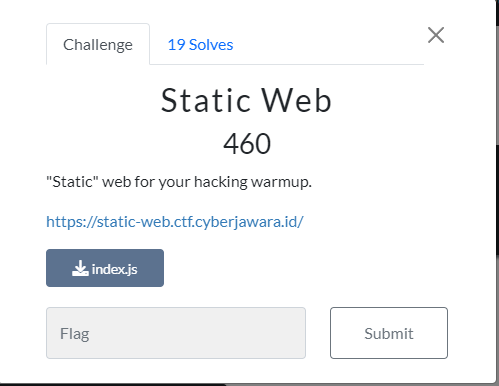
Daftar Isi

[WEB](#_Toc152513055)

[Static Web (460pts)](#_Toc152513056)

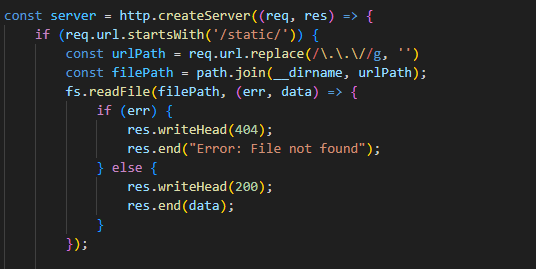
# WEB

## Static Web (460pts)

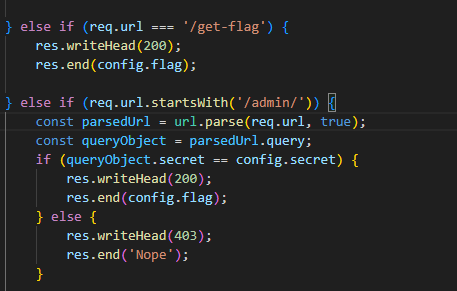


Diberikan soal dengan source code.

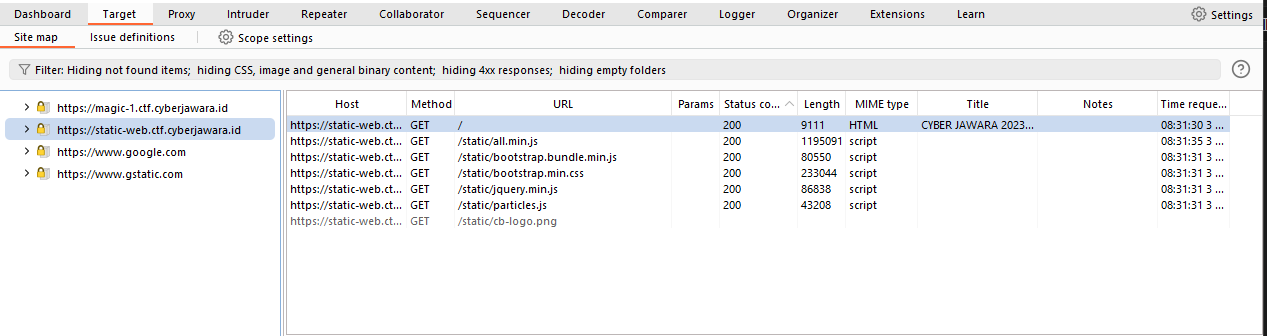
**Index.js**



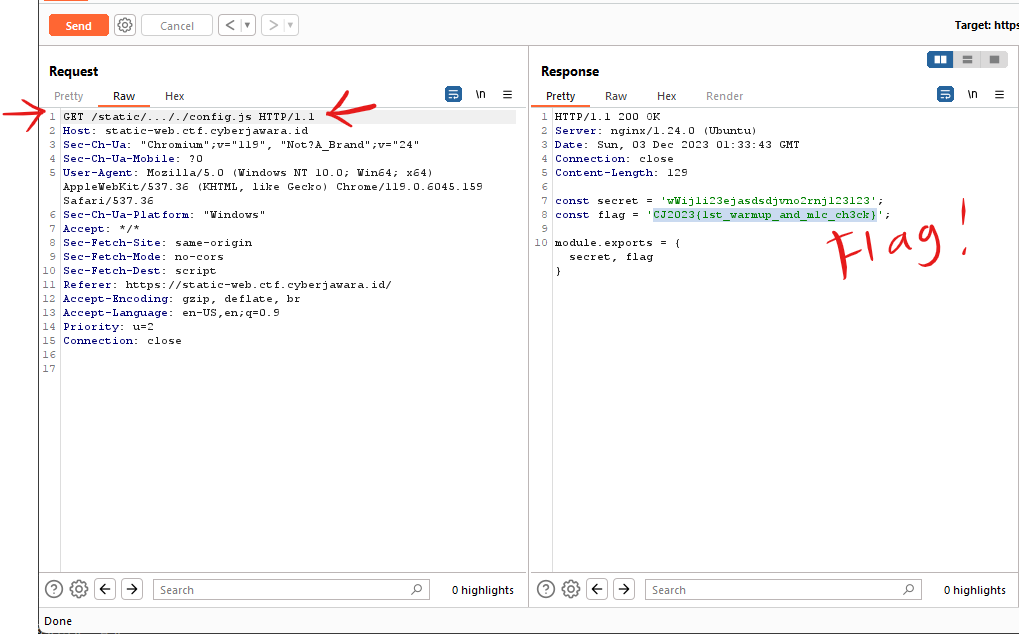
Pada bagian **req.url.replace(/\.\.\//g, ‘’)** terindikasi memiliki kerentanan directory traversal /path traversal.



Flag berada di directory admin dan akan terlihat jika string secret cocok dengan config.secret dan config.secret berada pada config.js yang ter-include. Karena tidak tahu secret maka dilakukan path traversal melalui direktori /static/ untuk mengambil flag yang berada dalam config.js.



Website disadap dengan Burpsuite kemudian dilakuan breakpoint repeater pada salah satu proses GET.



Lakukan path traversal /static/…/./config.js, kemudian send dan akan menampilkan response dengan menampilkan isi config.js.

Flag : CJ2023{1st\_warmup\_and\_mlc\_ch3ck}