Ifexer

Incognicat

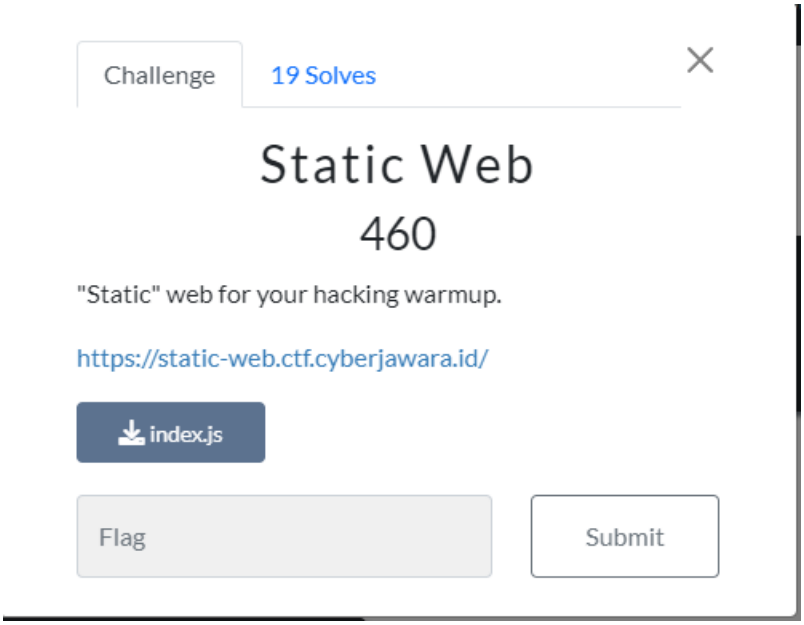
Danang

R.A.

Daftar Isi

WEB

Static Web (460pts)



Diberikan soal dengan source code.

Index,js

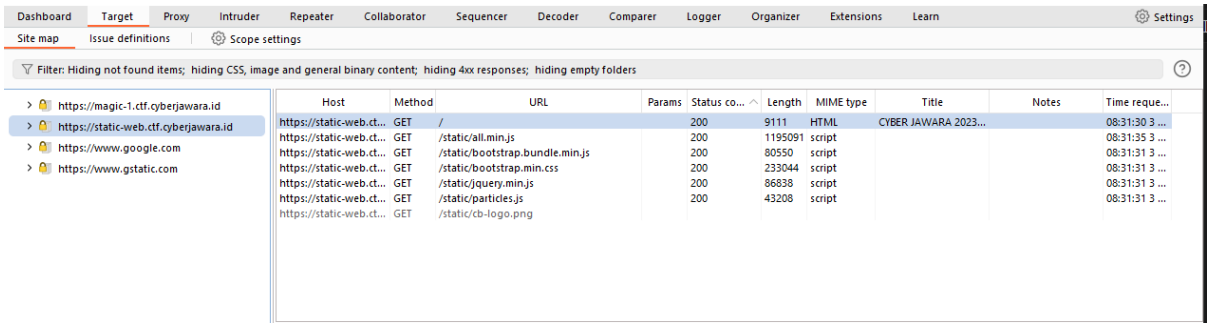
```
const server = http.createServer((req, res) => {
    if (req.url.startsWith('/static/')) {
        const urlPath = req.url.replace(/\.\.\//g, '')
        const filePath = path.join(__dirname, urlPath);
        fs.readFile(filePath, (err, data) => {
            if (err) {
                res.writeHead(404);
                res.end("Error: File not found");
            } else {
                res.writeHead(200);
                res.end(data);
            }
        });
```

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

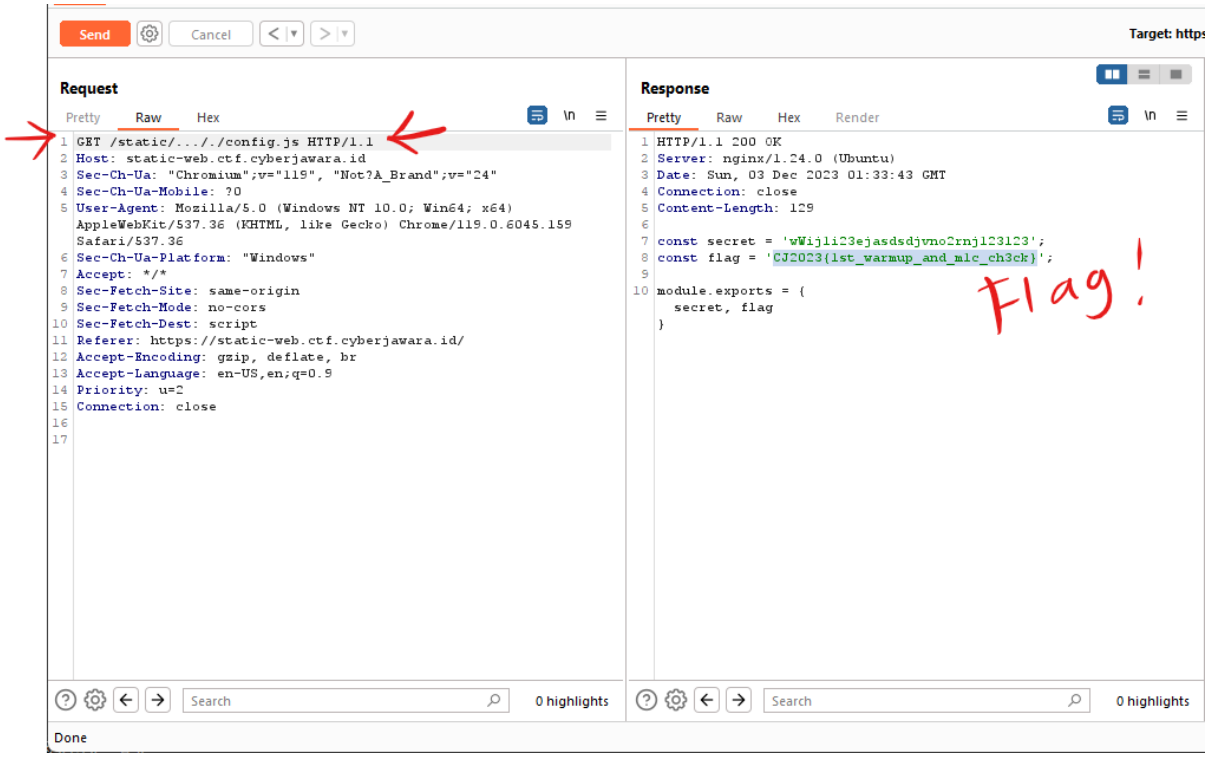
```
} else if (req.url === '/get-flag') {
    res.writeHead(200);
    res.end(config.flag);

} else if (req.url.startsWith('/admin/')) {
    const parsedUrl = url.parse(req.url, true);
    const queryObject = parsedUrl.query;
    if (queryObject.secret == config.secret) {
        res.writeHead(200);
        res.end(config.flag);
    } else {
        res.writeHead(403);
        res.end('Nope');
    }
```

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}