

Ifexer

Incognicat

Danang

R.A.

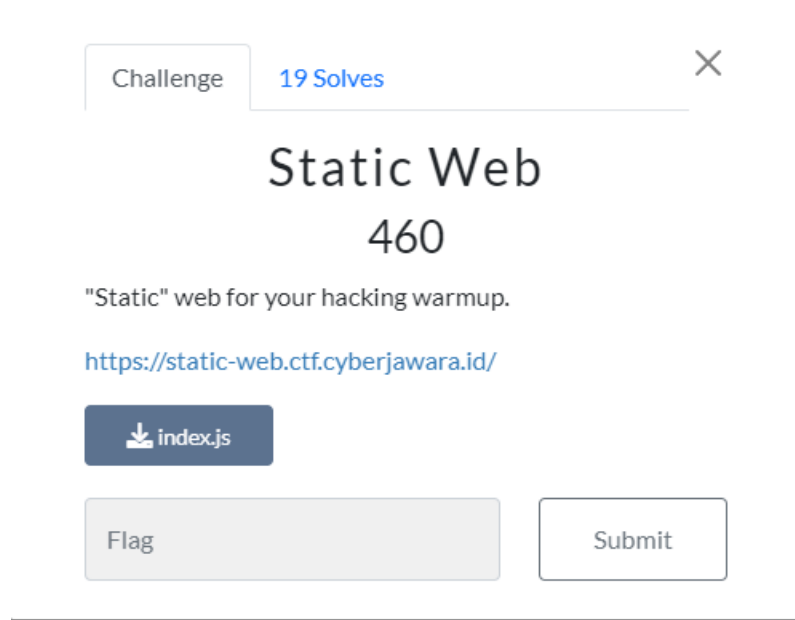
Daftar Isi

WEB

Static Web (460pts)

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.

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Comparer

Logger

Organizer

Extensions

Learn

Settings

Site map

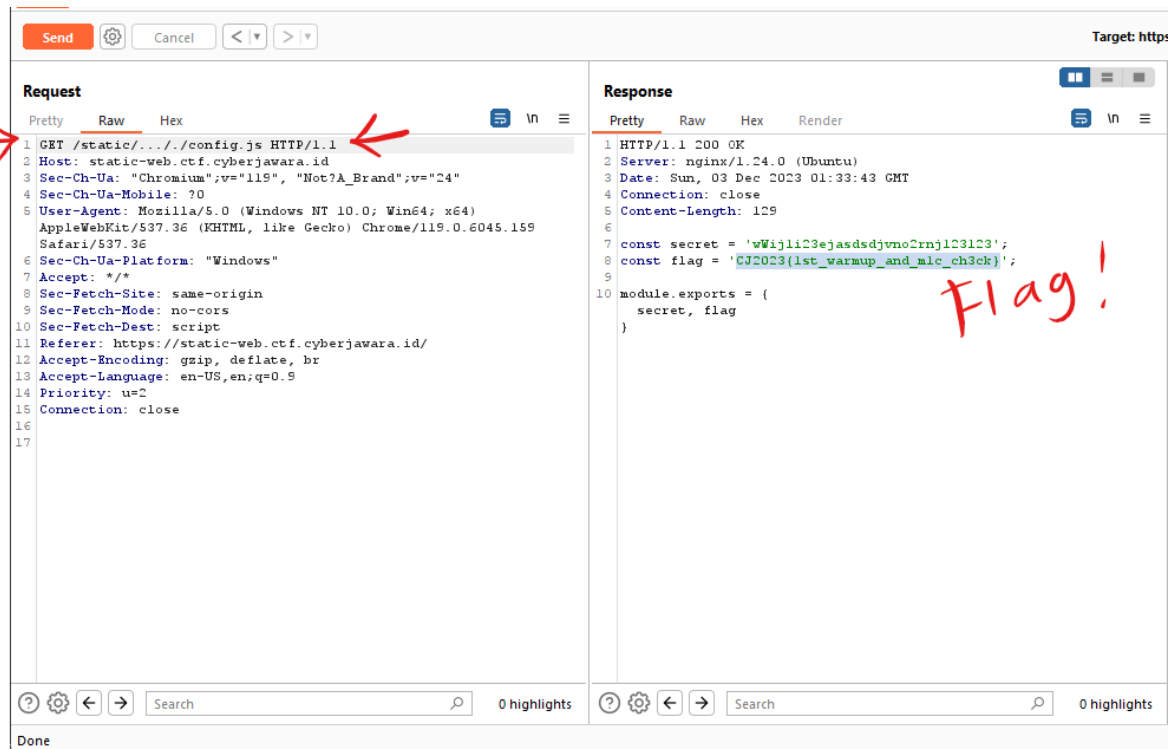
Issue definitions

Scope settings

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

	Host	Method	URL	Params	Status co...	Length	MIME type	Title	Notes	Time requ...
>	https://magic-1.ctf.cyberjawa.id									
>	https://static-web.ctf.cyberjawa.id	GET	/		200	9111	HTML	CYBER JAWARA 2023...		08:31:30 3 ...
>	https://static-web.ctf...	GET	/static/all.min.js		200	1195091	script			08:31:35 3 ...
>	https://www.google.com	GET	/static/bootstrap.bundle.min.js		200	80550	script			08:31:31 3 ...
>	https://www.gstatic.com	GET	/static/bootstrap.min.css		200	233044	script			08:31:31 3 ...
		GET	/static/jquery.min.js		200	86838	script			08:31:31 3 ...
		GET	/static/partides.js		200	43208	script			08:31:31 3 ...
	https://static-web.ctf...	GET	/static/cb-logo.png							

Website disadap dengan Burpsuite kemudian dilakukan 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}`