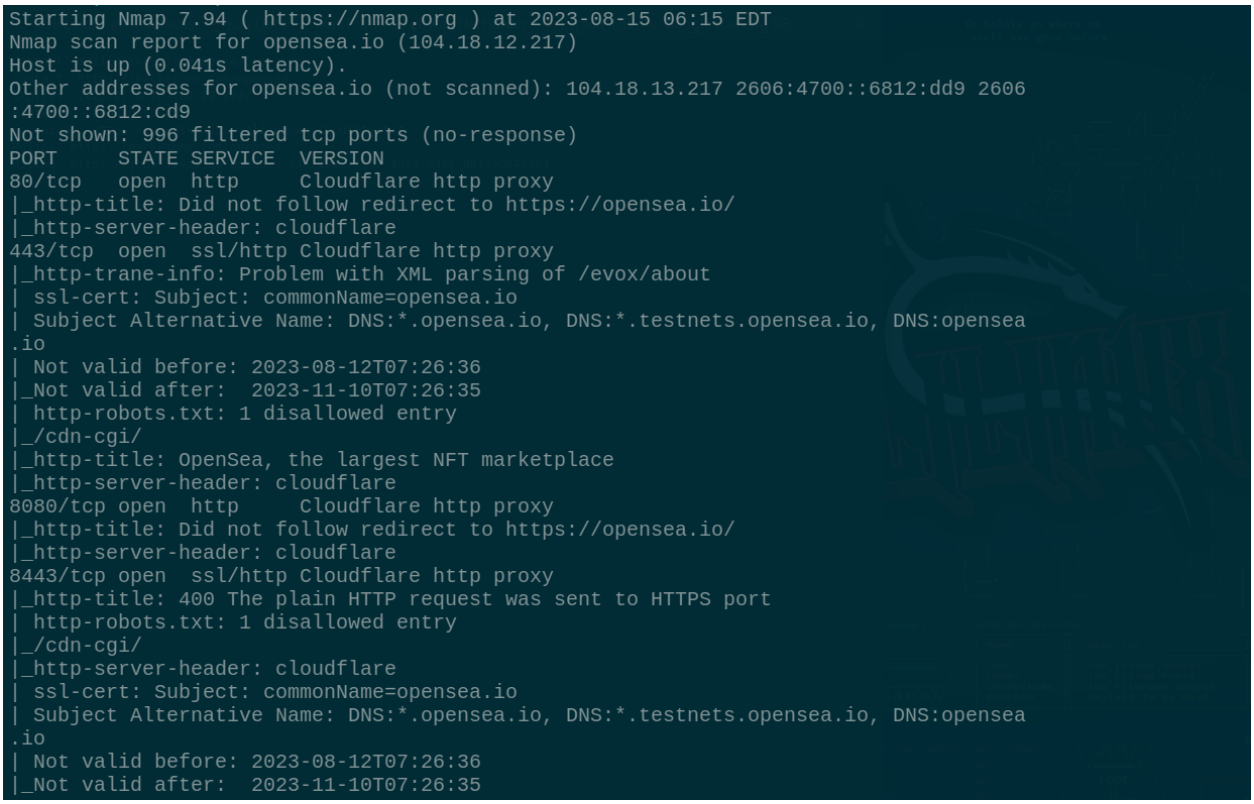
Opensea.io report findings.

Low risk Vulnerability: CWE-312, CWE-200

Open ports and Server software and technology found.



```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-15 06:15 EDT
Nmap scan report for opensea.io (104.18.12.217)
Host is up (0.041s latency).
Other addresses for opensea.io (not scanned): 104.18.13.217 2606:4700::6812:dd9 2606
:4700::6812:cd9
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Cloudflare http proxy
|_http-title: Did not follow redirect to https://opensea.io/
|_http-server-header: cloudflare
443/tcp  open  ssl/http Cloudflare http proxy
|_http-trane-info: Problem with XML parsing of /evox/about
| ssl-cert: Subject: commonName=opensea.io
| Subject Alternative Name: DNS:*.opensea.io, DNS:*.testnets.opensea.io, DNS:opensea
.io
| Not valid before: 2023-08-12T07:26:36
|_Not valid after:  2023-11-10T07:26:35
| http-robots.txt: 1 disallowed entry
|_/cdn-cgi/
|_http-title: OpenSea, the largest NFT marketplace
|_http-server-header: cloudflare
8080/tcp open  http     Cloudflare http proxy
|_http-title: Did not follow redirect to https://opensea.io/
|_http-server-header: cloudflare
8443/tcp open  ssl/http Cloudflare http proxy
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| http-robots.txt: 1 disallowed entry
|_/cdn-cgi/
|_http-server-header: cloudflare
| ssl-cert: Subject: commonName=opensea.io
| Subject Alternative Name: DNS:*.opensea.io, DNS:*.testnets.opensea.io, DNS:opensea
.io
| Not valid before: 2023-08-12T07:26:36
|_Not valid after:  2023-11-10T07:26:35
```

Open ports: 80 443 8080 8443

Risk described: An attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation: I recommend you eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

Information(no risk)

Security.txt file is missing.

```
Contact: mailto:security@opensea.io
Contact: https://hackerone.com/opensea
Expires: 2025-01-01T07:00:00.000Z
Preferred-Languages: en
Canonical: https://opensea.io/.well-known/security.txt
Policy: https://hackerone.com/opensea
Hiring: https://jobs.lever.co/OpenSea/04622947-f167-4d39-ad3c-d0a3ede4ffc4
```

URL: https://opensea.io/.well-known/security.txt

Risk Described: I have detected that the server is missing the security.txt file. There is no particular risk in not creating a valid Security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

Recommendation: I recommend you implement the security.txt file according to the standard, in order to allow researchers or users to report any security issues they find, improving the defensive mechanisms of your server.