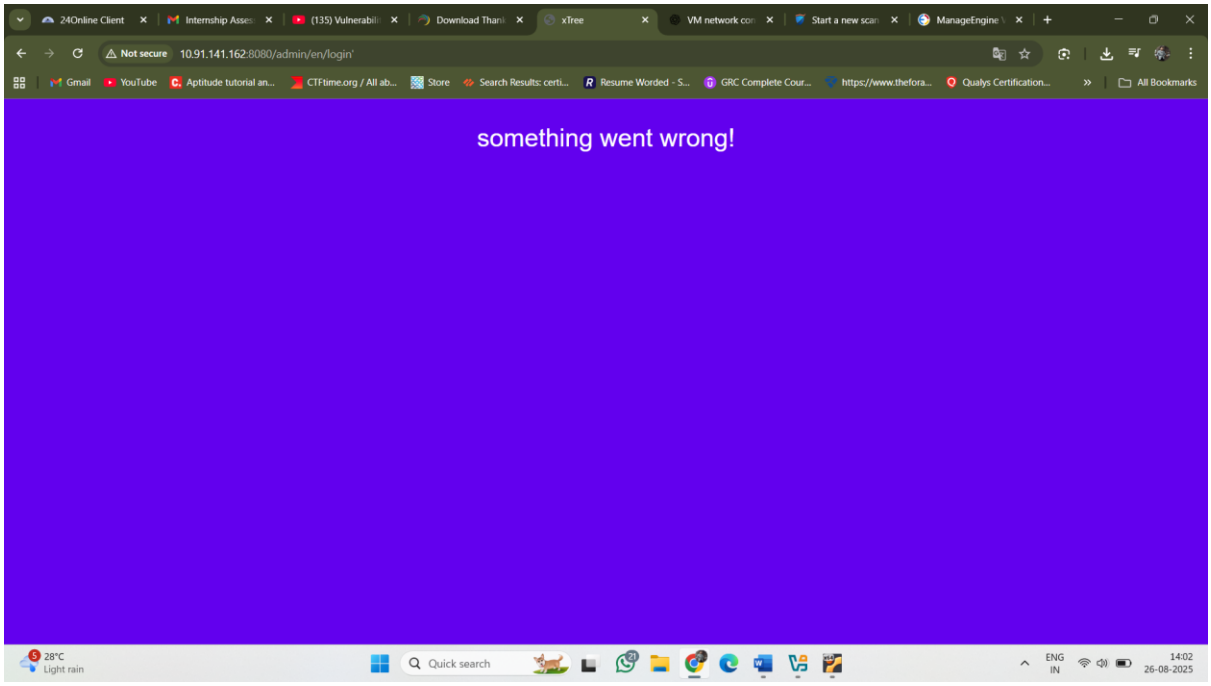


👍 —
From your link:

`http://localhost:8020/webclient#/uems/patch-mgmt/systems/scan-systems`

using **ManageEngine Endpoint Central (formerly Desktop Central)**, which has **patch & vulnerability management** built in.

🔗 Steps to Add Your VM for Vulnerability Scanning

☐Make Sure Your VM is Reachable

- First confirm your **VM (Ubuntu xbersec)** has an IP your host can reach:
- `ifconfig`

  Example: `192.168.190.5` (if Host-only) or `192.168.1.105` (if Bridged).

- From your host machine, try:
- `ping 192.168.190.5`

  If ping works, you're good.

2️⃣ Enable Required Services on VM

The VMS usually connects over:

- **SSH** (Linux) → port 22 must be open
- **WMI/SMB** (Windows) → ports 135, 445, etc.
  Since your VM is Ubuntu, make sure `openssh-server` is installed:

```
sudo apt update
sudo apt install openssh-server -y
sudo systemctl enable ssh
sudo systemctl start ssh
```

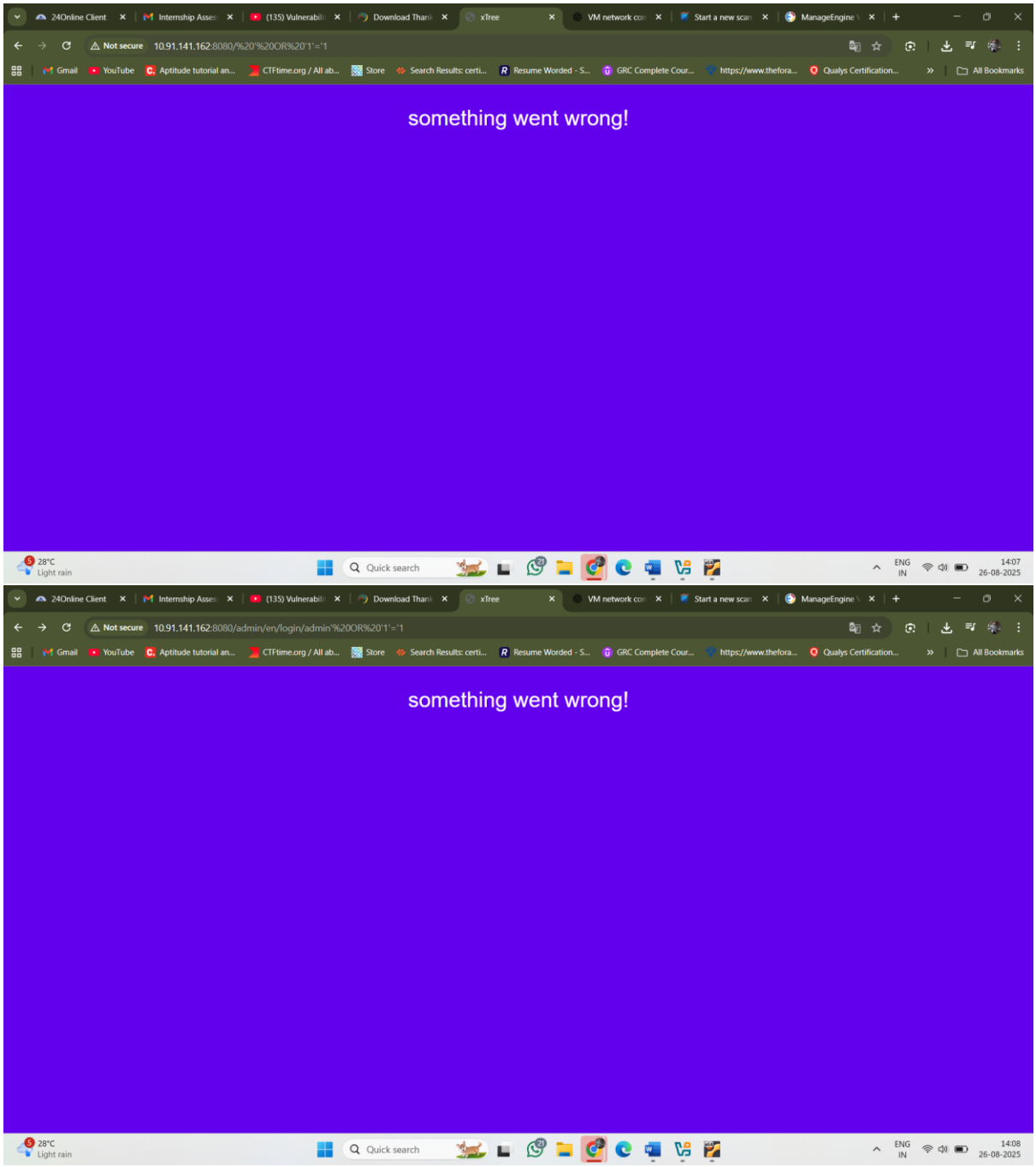
3️⃣ Add the VM in Endpoint Central (VMS)

1. Open your console:
2. `http://localhost:8020/webclient#/uems/patch-mgmt/systems/scan-systems`
3. Go to **Patch Management → Systems → Scan Systems**.
4. Click **Add Systems** (or Import).
5. Enter:
   - **IP Address / Range:** the VM IP (`192.168.190.5`)
   - **OS Type:** Linux
   - **Authentication:** provide the SSH login credentials (username = `xbersec`, password = `qwerty@123`).
6. Save & start a scan.
   - The VMS will connect over SSH and enumerate installed packages, configs, and vulnerabilities.

4️⃣ Verify the Webserver is Detected

Since your vulnerable app runs on **port 8080**, you might also want to:

- Check if the VMS scans **web applications** on open ports.
- If not, you may need to run a **separate web vulnerability scanner** (like OWASP ZAP, Nikto, or Burp Suite) against `http://192.168.190.5:8080`.



1) Sql injection when I give single quotation and 1=1 the web server communicate with me Instead of throw a error like 404 status error something