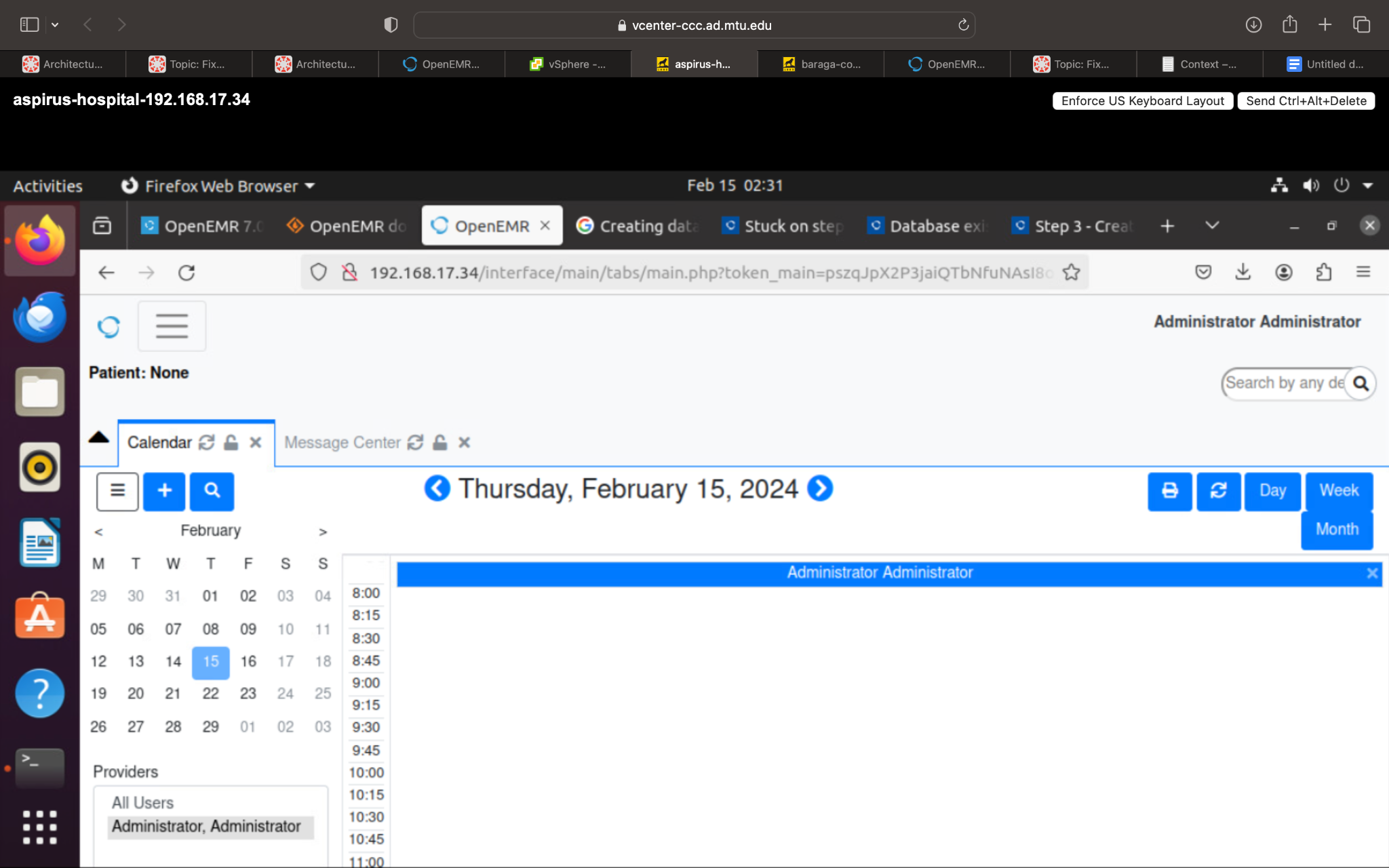
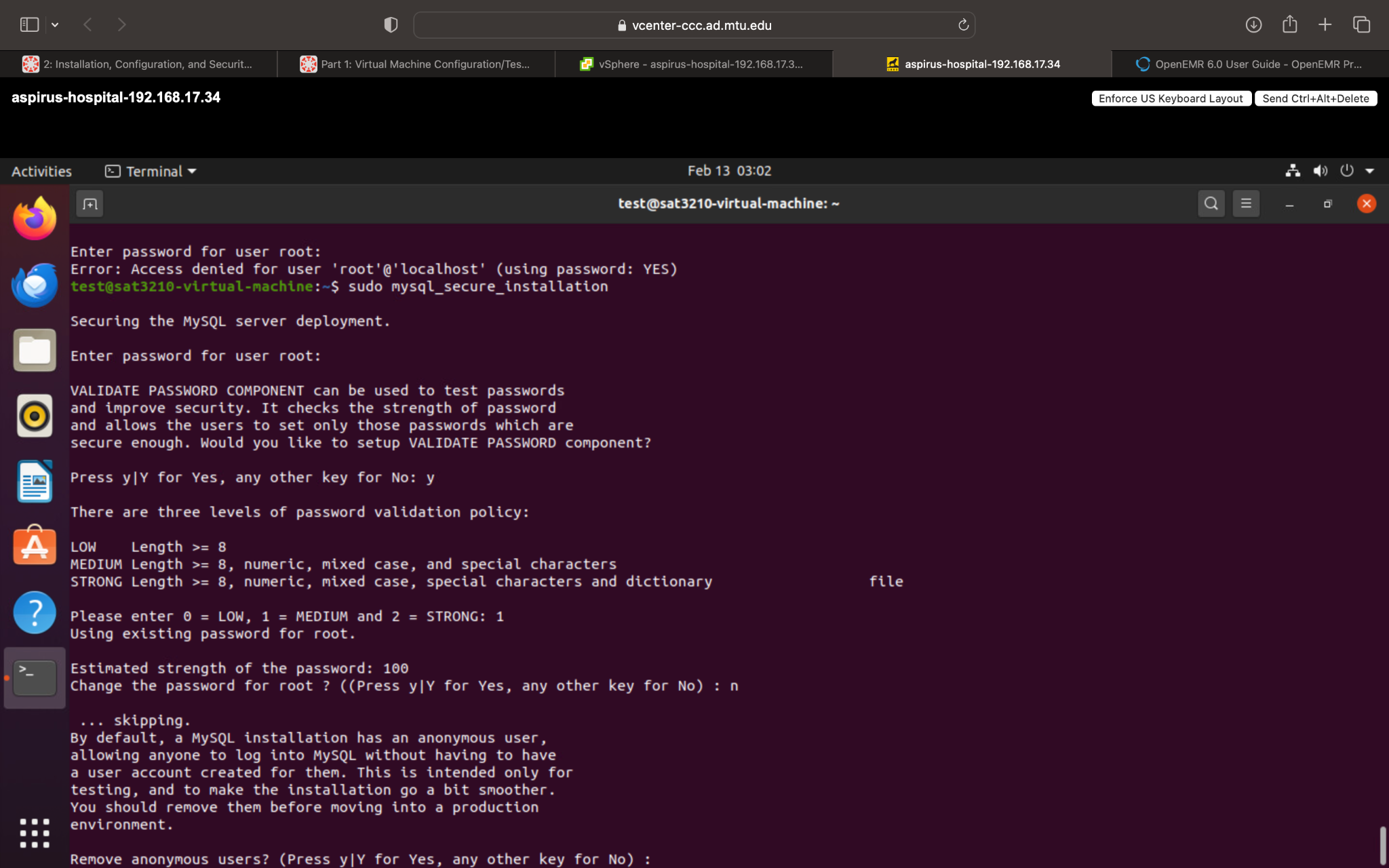
**A. Web page screenshot of the each hospital's successful installation of OpenEMR**

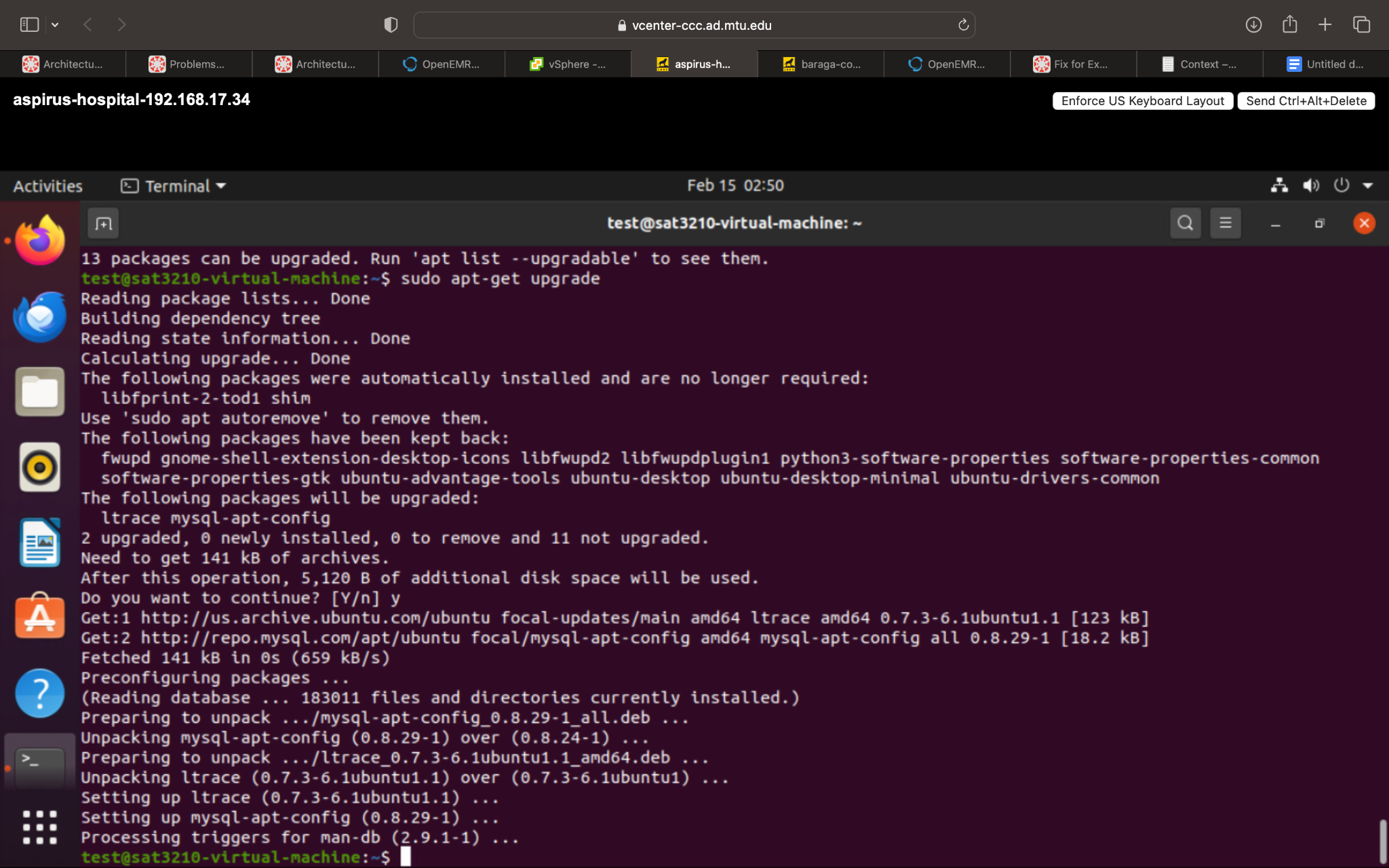
1. Aspirus Hospital



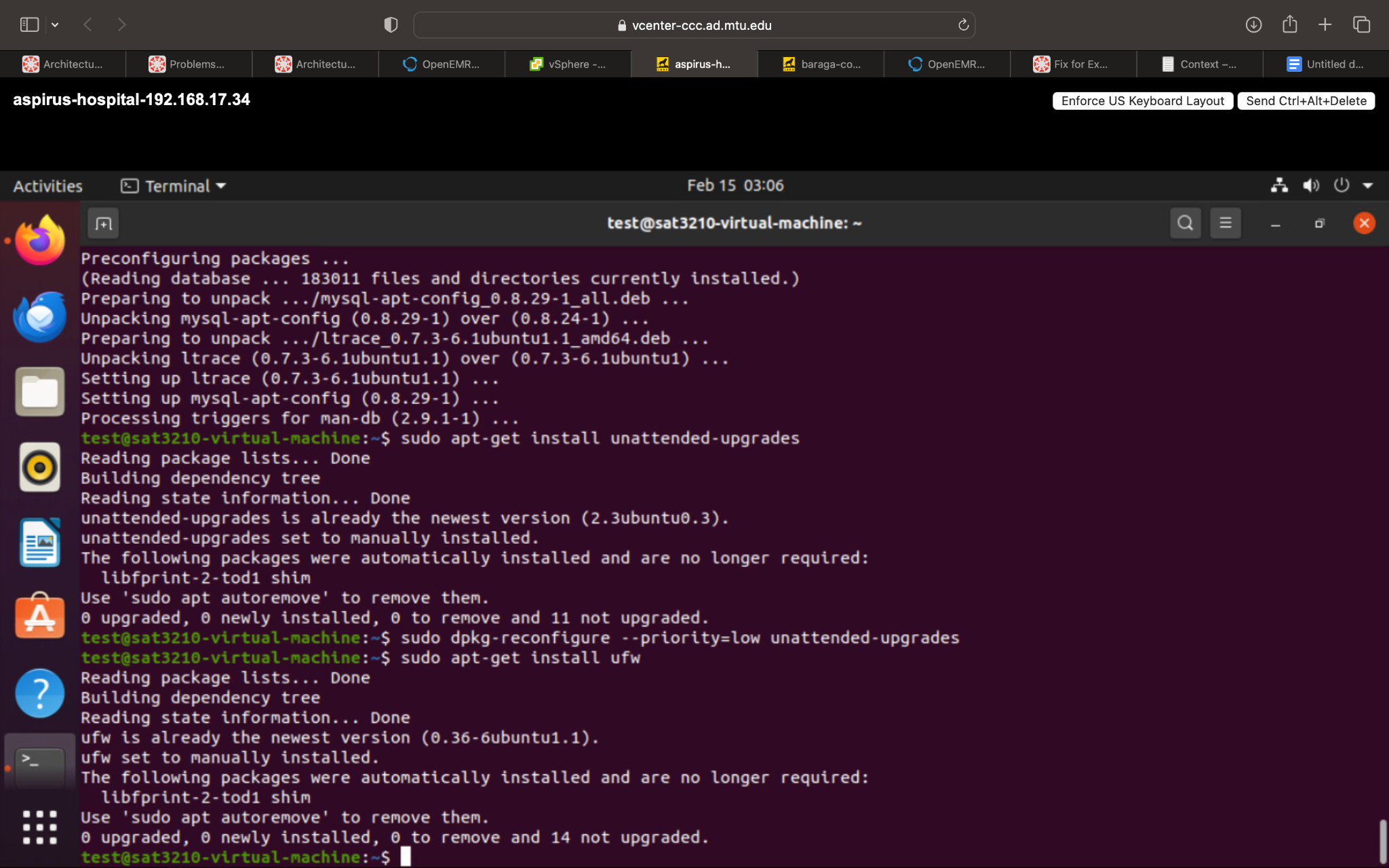
**B. Show the steps and commands you used to secure OpenEMR**

1. Secure password

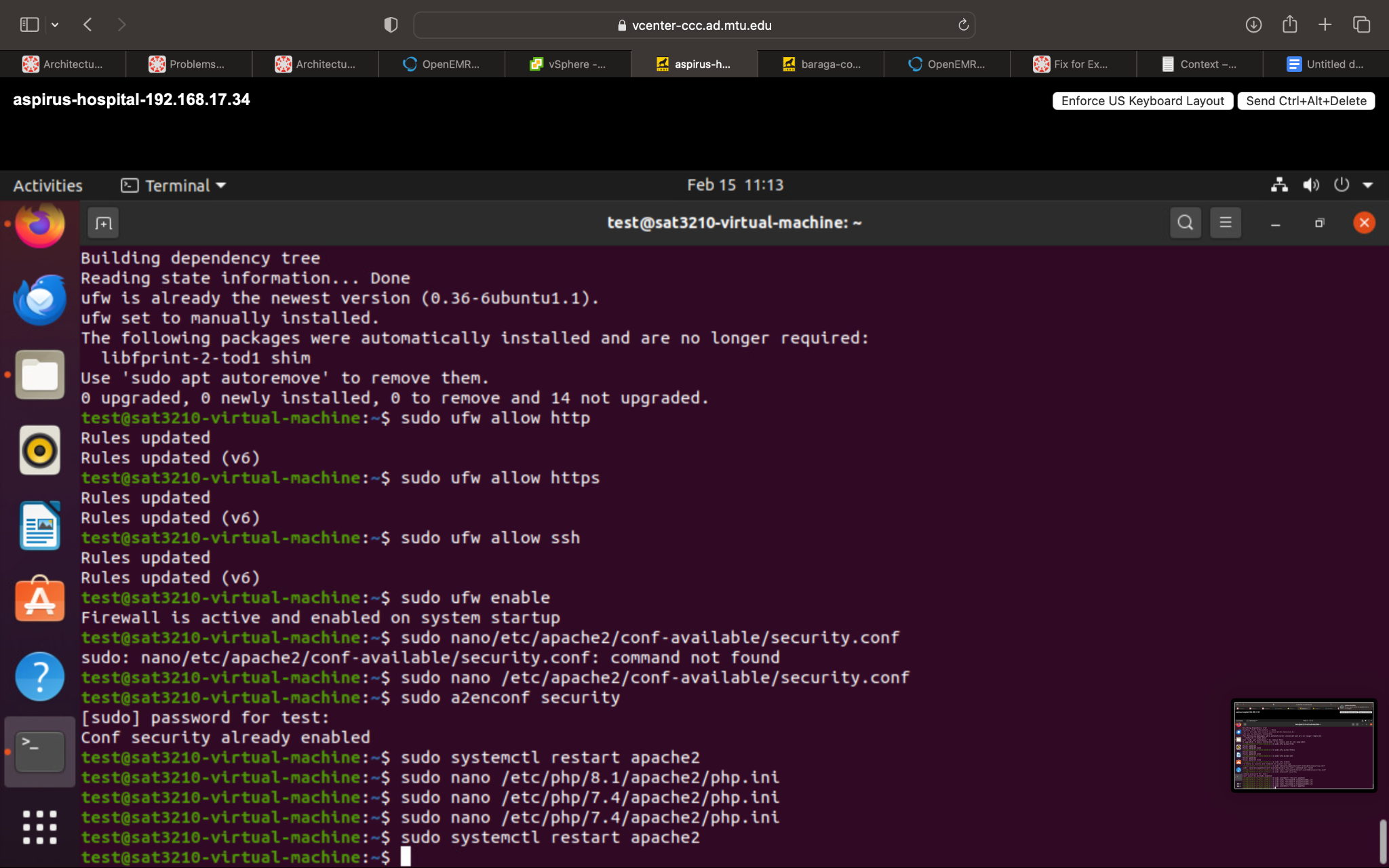


2. Update and upgraded OS

3. Enabled Automatic Security updates



4. Configured Firewall



5. Secured Apache (above)

6. Secured PHP(above)

**C. What other types of attacks would still be susceptible to the OpenEMR platform?**

Some of the major attacks that OpenEMR can still be vulnerable to are:

1. Denial of Service attacks: Attackers could overwhelm the system with traffic which could deny legitimate users access to the system.
2. File Injection Attacks: Malicious users could upload malicious files.
3. Remote Code Execution: Authenticated user could take advantage of improperly sanitized value on server and use it escalate privileges on server.
4. SQL injection (SQLi) vulnerabilities: OpenEMR has had several SQLi vulnerabilities as SQL codes could be injected via input fields
5. Authentication bypass: Attackers could gain access by navigating from login pages.
6. Cross-Site Request Forgery (CSRF): An attacker tricks a user into unknowingly submitting a request. This can result in unauthorized actions being performed on behalf of the user.