What should you secure for this project?

At the very minimum, you should:

- Configure and enable modsecurity
- Update php and reprogram php database calls to use mysqli library
- Configure pfSense and move CTF9 into the private subnet behind pfSense

To get more than the minimum passing grade, you can and should do a few more things. To give you all a place to start, I list some of them below. Some things will be easy, and other things will take more time. 1-2 harder items will bring you to an "A" grade, where it might take 3-4 easier items to get you to an "A" grade.

Partial List of items to do to secure vulnerable CTF 9:

- Install a light local firewall like shorewall [medium]
- Fix and prevent XSS and SQL injection attacks (look in /var/www/html for php files) [harder]
- Fix user and application permissions/settings [easier]
- Fix weak configurations/harden services [easier]
- Lessen information leaked through banners, errors [easier]
- Strengthen authentication and passwords (look up PAM) [medium]
- Other weaknesses?

Partial List of items for firewall:

- Install and configure Snort on PfSense along with rules that make sense for the firewall and server [harder]
- Enable a secure way to view logs reported from both this machine and CTF 9 (perhaps using Splunk or rsyslog) [harder]
- Other things?