What should you secure for this project?

At the very minimum, you should:

- Configure and enable modsecurity
- Update php to 8.3 and reprogram php database calls to use mysqli library
- Configure pfSense and move CTF9 into the private subnet behind pfSense. Port forward all ports that CTF9 accepts through the firewall to CTF9.

(Groups of 2 must do at least two of these things.)

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. They are rated with [easier], [medium], and [harder] tags below.

For a group of 3: 2 harder items will bring you to an "A" grade, where it might take 3-4 medium/easier items to get you to an "A" grade.

For a group of 2: 1 harder item will bring you to an "A" grade, where it might take 2-3 medium/easier items to get you to an "A" grade.

<u>Partial list of other things to do:</u>

- Install a light local firewall like shorewall or UFW. Configure it with reasonable rules. Document those rules. [medium]
- Configure Snort on pfSense, configure it with rules that make sense (e.g. if you aren't hosting a mailserver, don't have mailserver rules) [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]
- Aggregate logs from your CTF9 server and firewall using syslog-ng or another log aggregator [harder]
- Configure fail2ban [easier]
- Add XSS headers [easier]
- Encrypt passwords in mysql database, make sure users can still authenticate [harder]
- Other things?