**Danger log**

1. The SECRET\_KEY and ALLOWED\_HOST in settings.py which is upload should be kept secretly and safely.

2. The “<style class={{ var }}>…</style>” we is not protect and to HTML, using Django templates which can “escape specific characters” is very dangerous.

3. “Django does not throttle requests to authenticate users. To protect against brute-force attacks against the authentication system, you may consider deploying a Django plugin or Web server module to throttle these requests.”

4. In our views.py, the authentication for different roles are not set, which means the all the users can view the event.

5. HTTP is not safe as HTTPS

6. The password reset and sign up for email are not verified.

7. The web application has a security problem is the cross-site request forgery. If a user visits our website, and the cookies are created. At the same time, the user accesses a danger website B. This website will ask visit our website, which leads to a leakage of user information.

8. Except for the home page, some other URLs can be access without signing up or signing in.

9. The email may be used many times when users sign up. When we send emails to the guest, the database may send wrong event to someone else.

10. We have insecure direct object references of some values or name, but we do not validate that whether the user has the authority or not.