Django Security

- Cross Site Scripting (XSS) Protection
- Cross Site Request Forgery (CSRF) Protection
- SQL Injection Protection
- ClickJacking Protection
- SSL/HTTPS
- Host header validation
- Referrer Policy
- Session security
- User-Uploaded Content

Django Security

- Make sure that your Python code is outside of the Web server's root. This will ensure that your Python code is not accidentally served as plain text (or accidentally executed).
- Take care with any user uploaded files.
- 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.
- Keep your SECRET_KEY a secret.
- It is a good idea to limit the accessibility of your caching system and database using a firewall.