NIST Cybersecurity Framework (CSF) consists of standards, guidelines, and best practices to manage cybersecurity-related risk. It has five functional areas: identify, protect, detect, respond, and recover which are basically the lifecycle of cybersecurity. Each of these functional areas has categories and each category has sub-categories. By scoring each of these sub-categories, we can get overall scores and summaries about the level of security of the company or the application. Each one of the functional areas is described below regarding the application that we’re auditing.

* **Identify:** this section is specific for asset management, business environment, risk and supply chain management. Sub-categories of this section cannot be scored in our case of testing as we are performing source code auditing. But, we can estimate that based on some characteristics of the code.
* **Protect: this section address Information Protection Processes and Procedures as well as Identity Management, Authentication and Access Control. Also, it covers Awareness, Training, and Maintenance. By auditing the code, we can notice that the developer uses HTTPS and POST instead of GET which means that he is trained and aware of securing the application and not using HTTP for example.**
* **Detect: this section covers Anomalies and Events, Security Continuous Monitoring, and Detection Processes**
* **Recover: this section addresses recovery plans and communications which are not something that can be scored based on the source code.**
* **Respond: this section is about Response Planning and mitigation.**