Uncovering Vulnerabilities in Terms & Conditions

In today’s digital landscape, users often agree to terms and conditions without realizing the hidden risks they might face. Many companies embed vulnerabilities within these agreements, which can threaten user privacy, security, and control over personal data. Your challenge is to develop an AI-powered solution that can analyze terms and conditions documents, detect hidden vulnerabilities, and explain their potential impact on users. We will use the latest Retrieval Augmented Generation (RAG) method to solve this.

By solving this challenge, you will help users understand the risks in their agreements and empower them to make more informed decisions.

Your Tasks:

1. Analyze Documents: Develop a tool that can process and extract relevant information from terms and conditions documents in PDF or text format.

2. Detect Vulnerabilities: Identify and flag critical issues within the terms and conditions that may pose risks to users.

3. Explain the Impact: Provide an analysis of whether each vulnerability could create problems for users and explain how it could affect them.

Validation Criteria:

1. Vulnerability Detection: Your solution must successfully extract and identify vulnerabilities from the terms and conditions.

2. Accuracy: Provide an accurate analysis of each detected vulnerability, assessing the potential impact or risk posed to users.

3. User-Friendly Output: Present your findings in a format that non-expert users can easily understand, making it accessible and actionable.

Next Step: 20 Questions

Start Building the RAG Solution

Check the RAG Document for Basic Pipeline

Check the Technical Document for basic Requirements

From the below mentioned vulnerability categories, we will select key areas and design 20 targeted questions. These questions will aim to test the participants’ understanding of each vulnerability, how to detect it in terms and conditions, and how it may impact users.

Vulnerabilities to Address:

1. Data Collection & Sharing

• Excessive Data Collection: Companies collect more personal data than is necessary for the service, risking user privacy.

• Data Sharing with Third Parties: User data is shared with external entities without transparent consent, raising privacy concerns.

2. Data Security & Protection

• Insufficient Data Protection: Weak data security measures leave user information vulnerable to breaches and cyberattacks.

• Lack of Transparency in Tracking: Companies do not fully disclose the scope of user tracking or how user data is utilized.

• No Opt-Out for Tracking or Data Use: Users are not given the option to decline tracking or the use of their data, even for non-essential services.

3. User Rights & Control

• Restrictions on Data Access: Users have limited access to their personal data and cannot fully control what they can view or manage.

• Limitations on User Control: Companies restrict users' ability to control their accounts, data, or service settings.

• Complex Opt-Out Procedures: Opting out of services or data collection is difficult due to convoluted processes, reducing user control.

• Cancellation or Account Deactivation: Companies make it difficult to cancel or deactivate accounts, leading to continued charges or data retention.

4. Legal & Financial Risks

• Unilateral Changes to Terms: Companies can change the terms of service without notifying users, putting them at a disadvantage.

• Binding Arbitration: Users must resolve disputes via arbitration rather than in court, limiting their legal options.

• Limited Liability for Company: Companies limit their legal and financial responsibility, even in cases of negligence or service failure.

• User Assumes Excessive Risk: Users are forced to accept all risks related to the service, shifting the burden away from the company.

5. Invasive Practices

• Invasive Tracking: Companies track user activity extensively, both on and off their platforms, often without clear disclosure.

• Claim on User-Generated Content: Companies claim ownership or broad rights over user-generated content, limiting user control.

• Reliance on Third-Party Services: Users must rely on third-party services that have their own terms and vulnerabilities, often beyond the company's control.

6. Ambiguity & Hidden Costs

• Ambiguity in Key Provisions: Terms and conditions are written in vague language, making it hard for users to understand their rights and obligations.

• Hidden Fees or Charges: Users are subject to additional costs that are not clearly disclosed in the terms and conditions, leading to unexpected financial burdens.

• Indefinite or Long-Term Contracts: Users are locked into long-term contracts with limited options for early termination, reducing flexibility.

Why This Matters:

The vulnerabilities hidden in terms and conditions can affect users in significant ways, from privacy breaches to financial losses, and even unknowingly restricting their rights. By detecting these issues, your solution will help users understand what they agree to and make more informed decisions about the services they use.

By participating in this hackathon, you will be working on a real-world challenge that can empower users to protect themselves online and hold companies accountable for their practices.