MST-SC

Overview

This repository focuses on common web application vulnerabilities, including parameter tampering, Cross-Site Scripting (XSS), and SQL Injection. Each section provides an overview of the respective vulnerability, examples of how it can be exploited, and guidance on how to prevent it.

Detailed Sections

- Parameter Tampering
- Cross-Site Scripting (XSS)
- SQL Injection (SQLi)

Contributing

We welcome contributions to this repository! If you would like to contribute, please follow these guidelines:

1. **Create a new branch**: Create a new branch for your changes to keep your work organized and separate from the main branch
2. **Clone the repository**: Use the following command to clone the repository to your local machine:

   ```
   git clone https://github.com/StepSisStuck/MST-SC.git
   ```

Or using GitHub Desktop

3. **Make your changes**: Implement your changes, whether adding a new feature, or improving documentation.
4. **Commit your changes**: Use the following commands to stage and commit your changes:

   ```
   git add .
   git commit -m "Description of your changes"
   ```

5. **Push your changes**: Push your changes to your branch:

   ```
   git push origin your-branch-name
   ```

6. **Create a pull request**: Go to the original repository on GitHub and click the "New pull request" button. Select your branch and provide a clear description of your changes. Submit the pull request for review.

We appreciate your contributions and will review your pull request as soon as possible. Thank you for helping us improve this!

Workflow to Convert Markdown Files to Text

This repository includes a workflow to convert markdown files to text files. The workflow is defined in `.github/workflows/ConvertMarkDowntoTXT.yml`. It runs on push to the main branch, IT WILL NOT WORK IF YOU TRIGGER IT MANUALLY. The converted text files are stored in the `txt` directory.