# User/Abuse Diagram

## "To do List" Webpage

### Usage

**Simple task management Calendar**. A user or admin can create a list of tasks in order to manage their schedule. One can choose to mark tasks complete or choose to delete them on their personal task management page.

**Project Task:** List number of tasks needed to finish assignment; you can sign complete once you finish each of them, and also return each time you. Need to review what has been done.

**Dynamic list:** working on teams, list can be use by multiple users; "to do list" events will be created and erase by teammates; each one will add what need to be done, and once job done, it can be erase or left complete for knowledge of others

### Risk

An attacker can obtain personal information about the user (by compromising their "to-do" list.

Attacker can compromise user schedule by entering false information on his "to do list".

An attacker can inject a malicious script that the user can accidentally run on their machine by an XSS attack, potentially leading to the compromise of one's machine or other private information.

An attacker can obtain personal information about the user (by compromising their "to-do" list.

### Potential Threats

**SQL:** compromise user privacy, as attacker is able to access its "to do list", learn about it, and change it as he desires.

**XSS:** although being able to insert html provide variety of useful advantage such as save image or highlight some "to do"; an attacker that access on different account has the power to insert malicious code that user will encounter next time it open his "to do list".

**CSFR:** this vulnerability is dangerous as it allows attacker to change the "to do list" of user making him lose focus of what he need to do.

**IDOR/Manipulation:** An attacker can directly access a user's "to-do" list by entering the right link. This attack not only bypasses the security provided by the login, but also compromises the users security.

### Security Policy Violation

User can't use "to do list" event supported with HTML; any intend of using HTML even if it is not a threat will me answer with the elimination of the account.

User is responsible for its account and its password; share password is not advise as it increase probabilityh of being stole and increase the risk of account being compromise.