|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| If the risk is realized | What steps will performed lowering risk | Probability that the risk will occur | The severity of the impact on the project | Risks |
| Find the offending users and remove all their entries from the database. | A captcha on the registration page and an additional captcha that will appear on the entry submission form after a user have submitted several entries in an improbable timeframe. | The probability for this risk to occur is a function of the exposure the service gets. | Spam bots that submit garbage values to the database (Google's Datastore) and corrupt the authenticity of the data (Global statistics won't be as accurate). | Spam Bots |
| Once a DoS attack has been identified, the CDN will be turned on to help mitigate the attack. | Using CDN services such as Cloudflare to help mitigate the attacks. | As mentioned above, the probability is a function of the exposure and success level of the service. | Overload the website with requests that cause the website to work slowly or not at all. | Denial of Service |
| Reset the user's password, send it to his mail, and block attacker. | After 2 failed login attempts a captcha will be added to the login page. | Depends on the will of the person to get the information. | Hack a Budgeteer account by brute forcing the password and tamper with the data. | Brute Force Attacks |
|  |  |  |  |  |