ASSET	THREATS	VULNERABILITIES
Database *Our MongoDB database holds both user/account information, along with posts of all types. This is essentially all the data that we process. It is critical that this data is not lost.*	- Data loss - Hackers trying to gain access to our data in order to steal or monitor it.	- MongoDB is known to be prune to data loss if a crash occurs.
Codebase *The source code behind our system.*	- Someone could potentially scan our code for vulnerabilities, and exploit them. - If we by mistake has left traces of passwords or account information in the code, it will be very easy to access our data.	- Our codebase is publicly available at Github at the time. This makes it easier to exploit vulnerabilities.
Servers *We've got two servers - one hosting the front-end, and one hosting the back-end. One is hosted at Hetzner, the other one at DigitalOcean.*	- We depend on these servers, and therefore the server hosts in order for our systems to function correctly. If one of the server hosts experiences a system breakdown, so will we. - Hackers trying to gain access to our server in order to control our services.	- We are not always correctly provided with alerts when a breakdown happens. This could lose us precious system up-time. - Open ports on our servers. Ports are a vulnerability, and open ports can be compromised. - Server “lock-out” potential. If our public keys are deleted from the server, we are potentially incapable of accessing the server again.
CI-tools *Jenkins and Travis CI are our continuous integration helper-tools. They provide build testing and release management for our system.*	- If someone accesses our Jenkins and/or Travis build portal, they potentially have access to inject dangerous pre- or post build commands that can be executed on the server side.	- We are bound to use the ‘sudo’ command every once in a while, in our pre-builds. This could potentially be exploited.