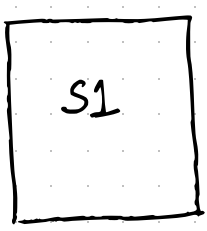
S1

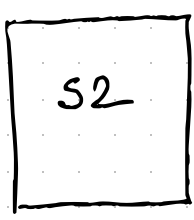
- Client/server
- This is where the web application runs

S2

- Private repository server
- Runs Verdaccio (this is where our package will be hosted.

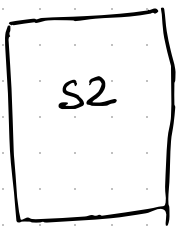
NORMAL SCENARIO

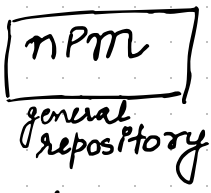




1) We unpack the application
2) $: npm install
3) private pulls the package from S2
4) Package is installed
5) $ npm start or PM2 to run the application
6) website runs normally.

ATTACK SCENARIO





1) We unpack the application
2) $ npm install
3) pulls our malicious package (which we uploaded once the package name was leaked)
4) package is installed also our code is executed
   - call backs to attacker server
   - DNS: 53
   - HTTPS: 443
5) $npm start → website fails build/run fails