MULHERN-PRESENATION-8.2

"SECURITY CONTROLS IN SHARED CODE REPOSITORIES"

- WHEN USING CODE REPOSITORIES IT IS OFTEN COMMON PRACTICE TO USE AN ENVIRONMENT VARIABLES FILE.
- IN NODE.JS AN ENVIRONMENT VARIABLES MODULE IS REFERRED TO AS DOTENV
- IT IS NAMED THIS WAY BECAUSE IN ORDER TO USE IT ONE MUST CREATE A .ENV FILE
- ALL THE ENVIRONMENT VARIABLES ARE STORED IN THE .ENV FILE AND IT IS INCLUDED IN THE .GITIGNORE FILE AND IS NOT UPLOADED TO GITHUB
- THEREFORE PEOPLE DON'T MESS WITH YOUR DATABASE OR OTHER ENVIRONMENT VARIABLES (NPMJS, 2020).

- STORING ENVIRONMENT VARIABLES ON THE BACKEND IS GOOD AND ALL BUT THIS BRINGS THE QUESTION OF "HOW ARE ENVIRONMENT VARIABLES STORED ON THE FRONTEND"?
- FIRST ONE INSTALLS DOTENV INTO THE ANGULAR PROJECT
- NEXT ONE TO DECLARE THEIR ENVIRONMENT VARIABLES IN THE .ENV FILE
- LASTLY DOTENV IS CONFIGURED IN THE ENVIRONMENT.TS FILE
- DOTENV MAY ALSO BE CONFIGURED IN ANOTHER FILE (NINNAD SUBBA, 2020).

- THIS PROCESS FOR ANGULAR ALLOWS FOR THE STORING OF ENVIRONMENT VARIABLES IN A .ENV FILE
- THE DOTENV FILE IS THEN NOT UPLOADED TO GITHUB OR OTHER CODE REPOSITORY SITES
- ALSO THE USE OF .GITIGNORE FILES CAN BE USEFUL
- THIS ALLOWS FOR CERTAIN FILE S TO NOT BE UPLOADED TO GITHUB
- SUCH AS THE NODE_MODULES FOLDER OR .ENV FILE.

- THERE ARE ALSO SOME OTHER PRACTICES THAT ALLOW FOR SECURITY TO BE TAKEN INTO CONSIDERATION IN TERMS OF STORING CODE ON GITHUB.
- ONE TIP IS TO NEVER STORE PASSWORDS ON GITHUB (SIMON MAPLE, 2018).
- ANOTHER IS TO BE CAREFUL OF WHAT DATA YOU POST TO GITHUB (SIMON MAPLE, 2018).
- YOU CAN ALSO MAKE YOUR CODE REPOSITORIES PRIVATE TO THE PUBLIC.
- THIS DISALLOWS PEOPLE FROM SEEING YOUR CODE.

- ANOTHER WAY TO PRACTICE GOOD GITHUB SECURITY PROCEDURE IS TO ADD A SECURITY.MD FILE (SIMON MAPLE, 2018).
- ONE CAN ALSO USE SECURITY PRACTICES BY SECURITY TESTING ONES APPLICATION (SIMON MAPLE, 2018).
- THIS CAN BE DONE USING A VARIETY OF TOOLS
- YOU CAN ALSO USE HELMENT.JS WHICH DISALLOWS CROSS SITE SCRIPTING
- ONE CAN ALSO PRACTICE GOOD GITHUB PRACTICES BY RENEWING KEYS (SIMON MAPLE, 2018).

- ANOTHER POPULAR CODE REPOSITORY FOR JAVASCRIPT DEVELOPERS IN NPM.
- NPM CAN BE USED TO CREATE PACKAGES THAT CAN BE USED IN JAVASCRIPT CODE.
- ONE CAN AVOID MALICIOUS HACKERS HURTING YOUR STUFF BY AVOIDING PUBLISHING ENVIROMENT VARIABLES TO NPM (LIRAN TAL, 2019).
- THIS CAN BE DONE BY USING A .ENV AND .GITIGNORE FILE WITH GITHUB
- ONE CAN ALSO TEST NPM MODULES USING A TOOL CALLED SNYK (LIRAN TAL, 2019).

- ANOTHER WAY TO SECURE YOUR CODE ON NPM IS TO ENABLE 2FA (LIRAN TAL, 2019).
- THIS ALLOWS FOR THERE TO BE A CODE SENT TO YOUR CELLULAR DEVICE
- NPM THEN CONFIRMS IF THE CODE IS CORRECT
- THIS IS A WAY TO SECURE YOUR NPM
- 2FA CAN ALSO BE DONE WITH GOOGLE AUTHENTICATOR

- ALL IN ALL IN THIS PRESENTATION WE LEARNED ABOUT HOW ONE CAN SECURE THEIR CODE REPOSITORIES
- THESE REPOSITORIES WERE FOCUSED AROUND THE JAVASCRIPT DEVELOPER
- THESE INCLUDE GITHUB AND NPM
- COMMON SECURITY PRACTICES INLCUDE USING A .ENV FILE
- AS WELL AS USING A .GITIGNORE FILE

REFERENCE

- Npmjs. (2020). Dotenv. Retrieved from https://www.npmjs.com/package/dotenv.
- Ninad Subba. (2020). Setup dotenv to Access Environment Variables in Angular 9. Retrieved from https://medium.com/javascript-in-plain-english/setup-dotenv-to-access-environment-variables-in-angular-9-f06c6ffb86c0.
- Simon Maple. (2018). 10 GitHub Security Best Practices Retrieved from https://snyk.io/blog/ten-git-hub-security-best-practices/
- Liran Tal. (2019). 10 npm Security Best Practices. Retrieved from https://snyk.io/blog/ten-npm-security-best-practices/?utm_campaign=td-flow.