Joseph Grzywinski

CS-405

12/15/2024

Project 2 Transcript

Video: https://youtu.be/j4GZQMtnVfU

Slide 1

Hello everyone, today I am going to discuss the Green Pace security policy I have developed and go over what we mean to accomplish with this policy and why we are implementing it.

Slide 2

The security policy we are implementing here at Green Pace is meant to give a solid foundation for developers and architects of our applications for security and compliancy. The policy will go in depth into different standards that must be followed, that way every person is on the same page no matter what part of our infrastructure you work on. This will coincide with our defense in depth policy to make sure we have multiple levels of security in the case that a level is compromised.

Slide 3

This security matrix summarizes the main vulnerabilities we may encounter during development and how we will classify them. Vulnerabilities can be classified as low, medium, or high risk and some may be more likely to be compromised than others within our systems. This is how we refer to all of our vulnerabilities.

Slide 4

Listed here are the 10 standard security principles that we as a company will be following. Any coding standards that we look to focus on here at Green Pace will fall under one of these standards as it’s meant to be a baseline standard of how we should be handling security during planning and development.

Slide 5

While listing the ten security principles that are going to be the focus here at Green Pace, we have also chosen ten coding standards that we would like to focus on. The coding standards are mostly best practices that coincide with the ten coding standards that are set in the company but are common security risks we need to work on.

Slide 6

Encryption within an application can be used in flight, at rest, or in use. Encryption at rest is used to always encrypt data even when not in use. Encryption in flight policy is meant to secure data as it is being transferred through a network either between applications or between the application and the user. In use is meant to ensure that data is encrypted while it is being used. For our company’s application we want to ensure that any of the entrepreneurs are accessing their data for either information or changing data within their profile or dataset have a secure connection to protect their information.

Slide 7

The triple A framework is meant to ensure the authorized users have access to our systems while locking anyone else out. The first A, authentication, is meant to check a user to make sure that they are authorized to access the information being requested. The second A, Authorization, determines the permissions that are given to a type of user. The final a, accounting, will monitor user activity to see if any suspicious activity is taking place while their account is being accessed. These three working together gives us near full coverage over anybody accessing our systems and lets us catch anyone who does not belong.

Slide 8

As shown in this slide unit testing will be an integral part of our development and should be a standard set by each developer as well as QA member. This slide shows an example of unit tests done for our systems. The first example is a check to make sure we can increase the collections size. The second test is testing to make sure we can add an entry out of the bounds of the collection. The final test is making sure we can decrease the size of the collection successfully. These types of unit tests will be used on every application.

Slide 9

Automation summary

Most of the automation tools discussed in this document will be used within the Pre-production phase of the applications lifecycle. Tools such as sonar scans or Cppcheck will be implemented before the builds are sent to QA teams for testing. Developers should be running checks like this to speed up the development as it would take much more time to send to QA for them to run tests like this and send them back to the developer with a vulnerability list. Instead, a developer should have access to the list before submitting for testing so they can deal with issues on site and in real time.

Slide 10

The primary focus of security within our devsecops pipeline is to make sure security is implemented within every layer of our application. This starts with the pre planning of each app and involves both developers and architects discussing not only how our apps should function but also how we can protect each section to make sure there are no data leaks or cracks within security coverage.

Slide 11

While our major focus is going to be security with our new applications, we need to ensure that this does not slow production down in the long run. This includes the development of new apps as well as maintaining applications in the future. Too much security within our infrastructure can cause major problems that will cost time and money to fix.

Slide 12

This is not really a gap within the security policy but more of a note worth mentioning, but this policy only works if everyone within the company is following the standards set within the policy. Anything that is developed that is not in line with what has been set within the document can take much linger to figure out as the policy is supposed to be standard among developers and architects to make it easier to identify vulnerabilities as they come up.

Slide 13

In the future we should see more standards that should be adopted for security on our databases for updates and creation. These databases are the main target for most attackers and most of the policies set within this document are for coding standards. Securing the database directly and having backups should be just as important if all else were to fail within these coding standards.

Slide 14

**References:** Sei cert C++ coding standard. SEI CERT C++ Coding Standard - SEI CERT C++ Coding Standard - Confluence. (n.d.). https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88046682