Lesson 4 of 4

Integrate security into the workstream to find/fix vulnerabilities

Commit the change…

git add .

git commit –m ‘<TAG>’

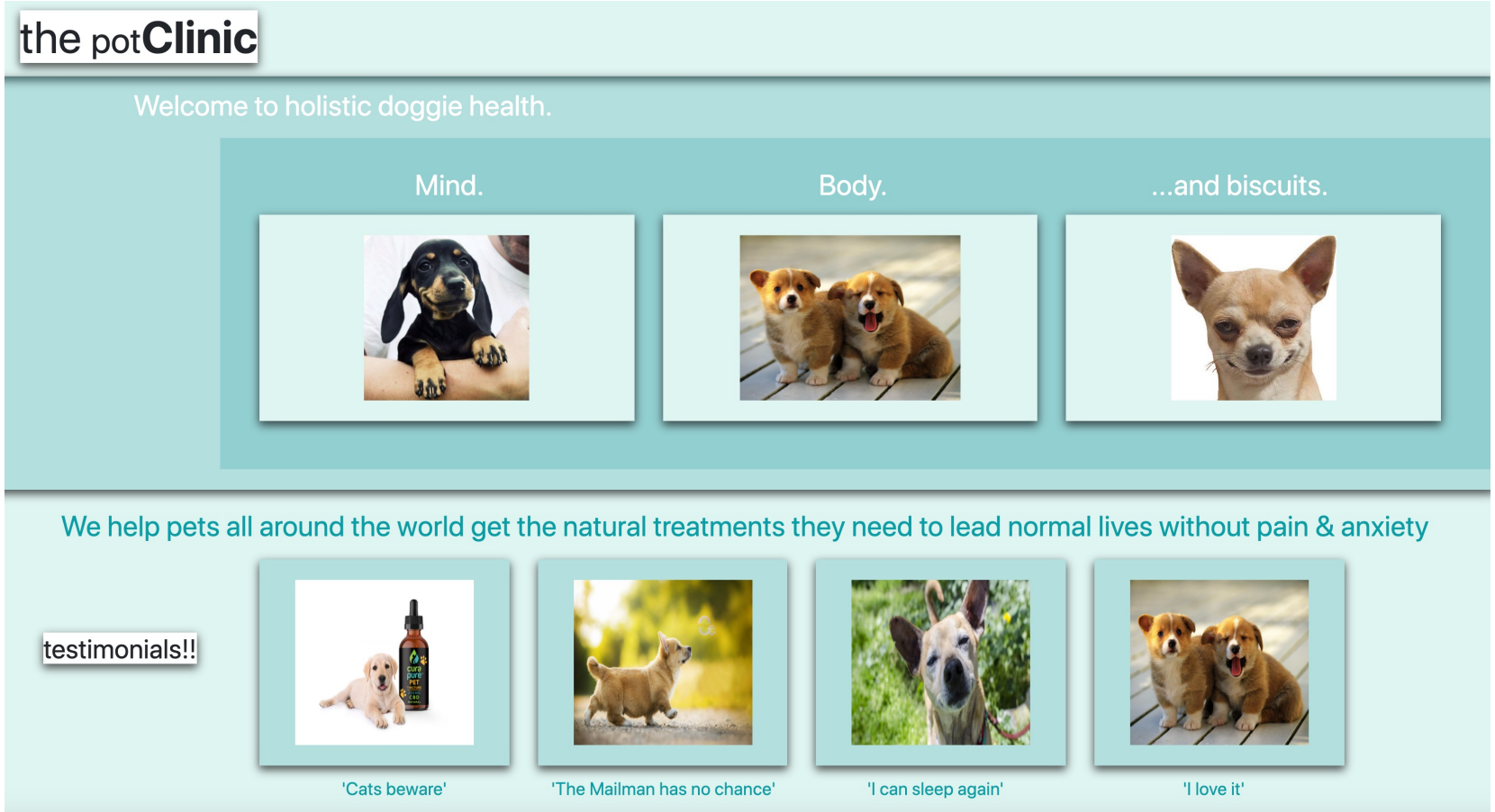
git push origin new-app

Watch the magic…

- Log into your github.com URL, find your repository, and navigate to `Actions`
- Click into `All workflows` and finally click into the executing workflow to see the output logs
- Once the automation completes, navigate towards the bottom of the workflow output and copy and paste the `url` of the deployed azure spring cloud application
- Paste the `url` value into your web browser to verify the deployment

The new App…

- Spring PotClinic (PetClinic 2.0)



Start testing

- Click through the UI and simulate testing
- Vulnerabilities are found by the embedded agent sensors and forwarded to the Contrast Security Team Server…

Open the Contrast Team Server UI

- Go to `https://ce.contrastsecurity.com` and login with the login details provided by your instructor
- Navigate to the `Applications` window to see your onboarded application
- Step through the onboarded application and Server

Contrast OSS

- Highlight which libraries are used by the application and how often down to the specific class, file, or module
- Prioritize remediation workflows based on which libraries are actually called at runtime
- Foster goodwill with developers by helping them focus on the most relevant third-party software risk

- ****Note - Current Bug – why the `Libraries` aren't showing up**

Contrast Assess

- Generates simple diagrams that illustrate the application’s major architectural components.
- Helps the developer quickly identify the meaning of a vulnerability that Contrast pinpoints and can form a starting point for threat modeling remediation.
- Enables developers to fix vulnerabilities easily without the need of security expertise.
- Provides developers a mapping of the URL and routes of their software that are executed during the testing phase of the SDLC.
- Helps security teams increase confidence in the coverage of the Assess solution as well as developers identify the effectiveness of their overall testing practice.

Contrast Protect

- Accurate, compliant, and dynamic runtime exploit prevention
- Application runtime instrumentation on the inside verifies exploitable attacks
- Dramatically reduces noise and accelerates security posture
- Rapid response to zero-day attacks with virtual patching

Ensure our IP is protected

- Go back into the new application and try to exploit the vulnerability after enabling Contrast Protect for a certain exploit

We’ve Foiled the Attempt!

- Now that we have our IP protected, let’s talk about how this translates into enhancing our security posture moving forward…

Future Looks Bright ☺

- We've successfully taken our implementation, enhanced it using a new look and foiled Garth's attempt at compromising our IP with a couple simple steps.
- Now we can move forward and start making some revenue on this new business venture, knowing our application is safe, secure, and ready for the masses!