Submit a Zero Star "Customer Feedback"

The "Customer Feedback" form seems to require a star rating. Find a way to submit the form with zero stars.

Ideas

Observe the app's normal behavior first. How does this function work? Once you know that, think about how you might try to make it work differently...

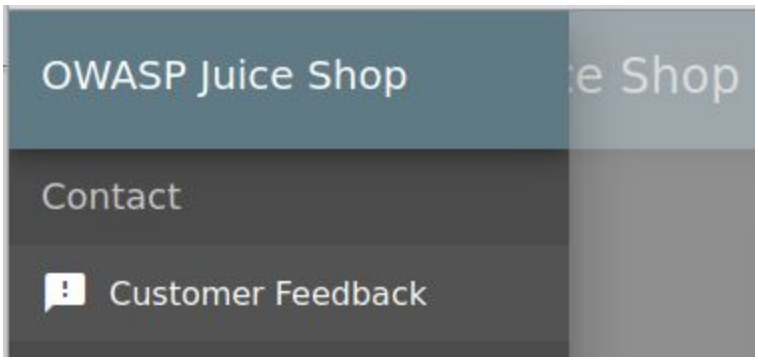
Alternatives

This walk-thru shows two methods of solving this challenge. The first uses Burp Suite in what feels to the instructor like the more "obvious" way of solving it. The second uses Developer Tools to show an alternative. When you know more than one way to achieve a goal, you are a more flexible and effective tester.

Walk-Thru: Burp Suite Method

Make sure you have Firefox set to use your Burp Suite as a proxy, and that the Proxy > Intercept pane says "Intercept is off"
Step by step with screenshots

1. Click on the "hamburger" menu at the top left and choose "Customer Feedback"



Customer Feedback in Top-Left Navigation Menu

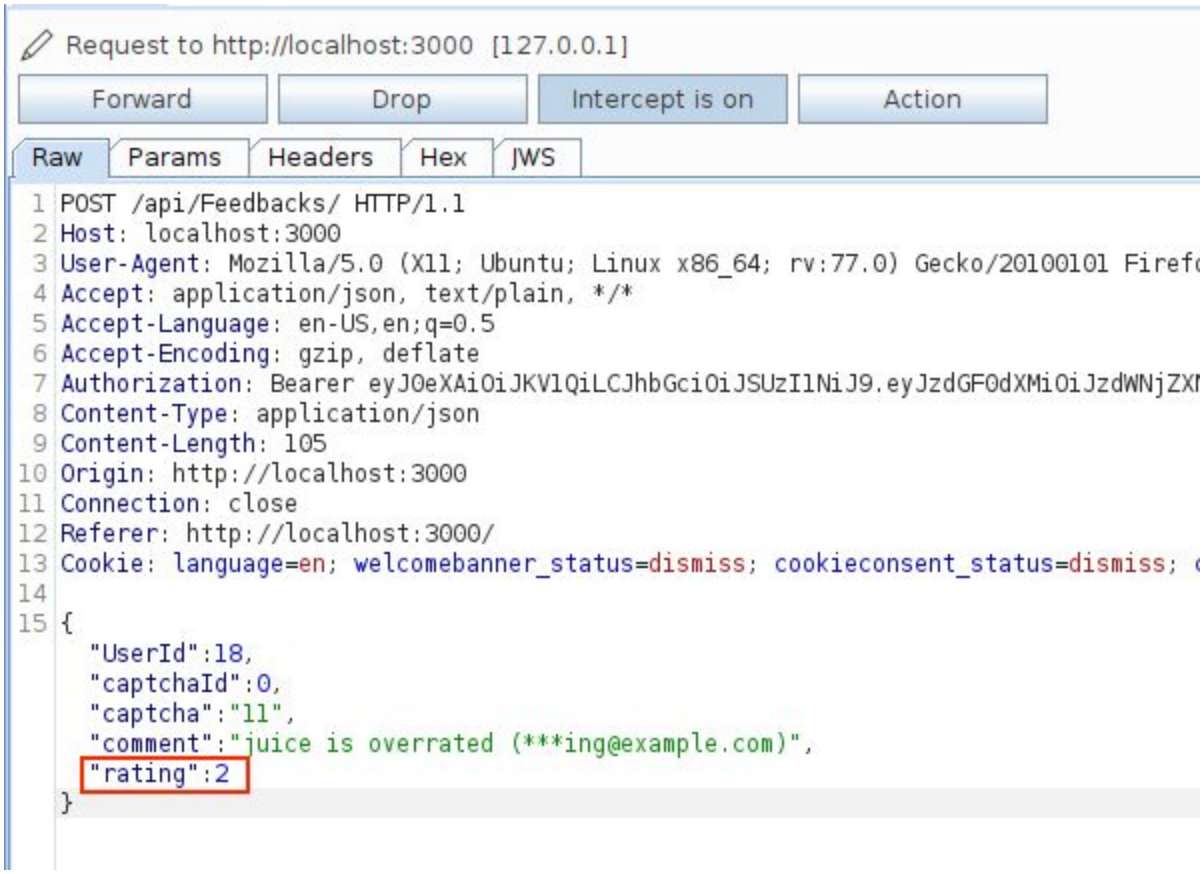
2. Type in any "Comment" and solve the CAPTCHA but DON'T CLICK ANY RATING YET: once you've clicked any rating, you cannot put it back to zero.

Notice that the "Submit" button is disabled until you click a star rating.

3. Once you've filled in a comment, solved the CAPTCHA, and selected a star rating, go to Burp Suite's Proxy tab and make sure the third button from the left says, "Intercept is on".

4. Return to the browser and submit the request, then come back to Burp Suite. Notice the request is sitting there for you to view (and edit!)

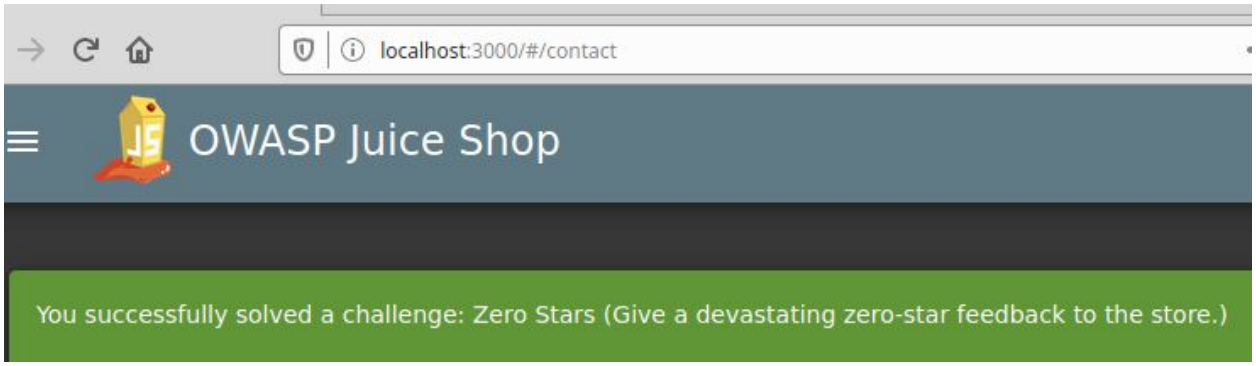
5. Notice the "rating" is submitted as an integer equal to the number of stars you clicked. Change it to zero and then click "Intercept is on" to release the request and stop intercepting.



Legitimate Request, Before Editing

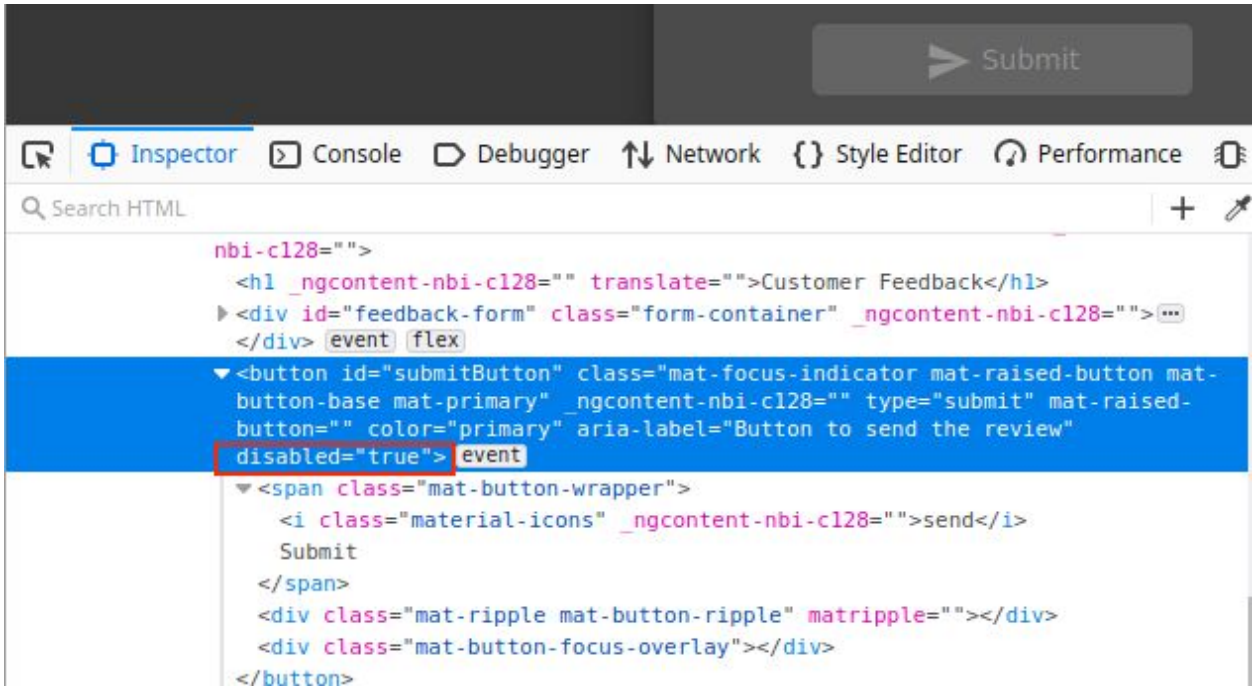
Change the "rating" to a zero (0) and release the request by clicking "Intercept is on" to ... disable the intercepting (confusing button? You'll get used to it)

5. See your acknowledgement in the browser.



Walk-Thru; Developer Tools Method

On the "Customer Feedback" form, enter a comment and solve the CAPTCHA, then right click on the "Submit" button and choose "Inspect Element"

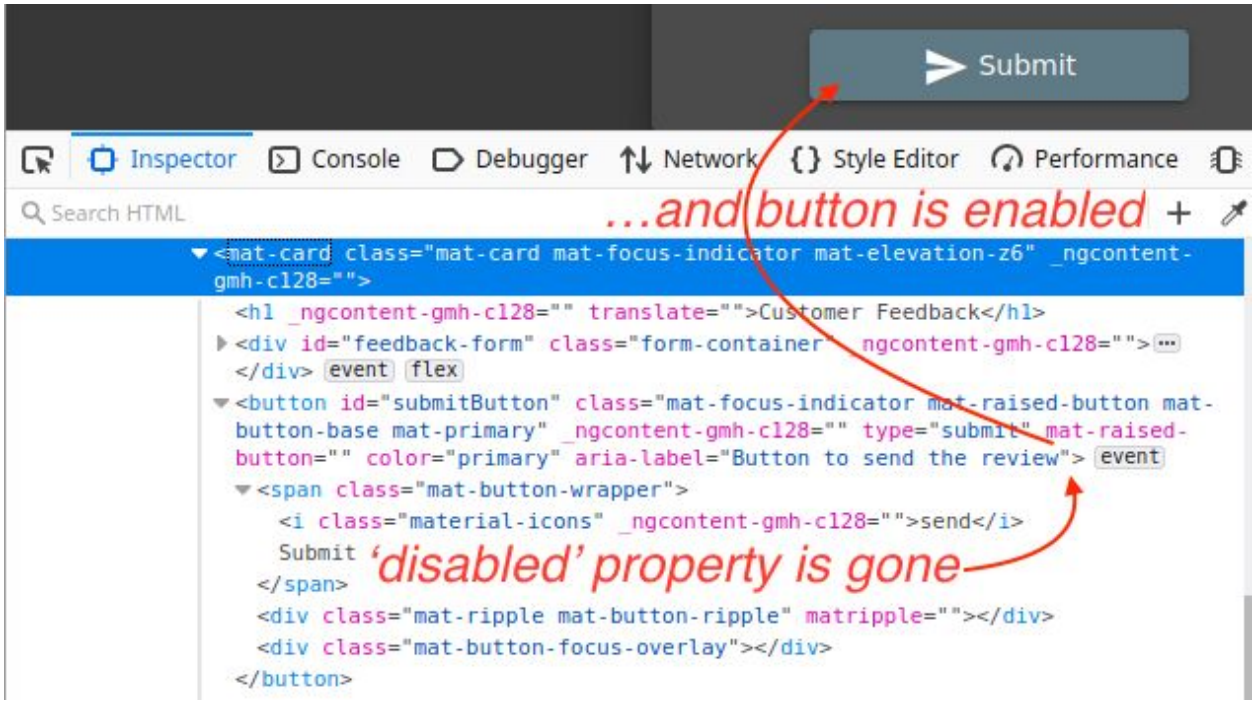


Inspect Element Reveals "disabled" Attribute

2. Notice the button element has an attribute called "disabled"
You may think that because it is set to "true" you could re-enable it by setting it to "false" but that's not how this attribute is defined in the HTML spec.
When the "disabled" attribute is present (with any value) the item is disabled. When the "disabled" property is not present, the item is enabled. You have to remove the attribute entirely to reverse its effects.

https://html.spec.whatwg.org/multipage/form-control-infrastructure.html#enabling-and-disabling-form-controls:-the-disabled-attribute

3. Double-click on the word "true" then delete the entire string, starting with the word "disabled" and continuing through the quote after the word "true," then hit enter or click outside the Inspector.



Once the "disabled" attribute is gone, submit the form.

4. Now that the "Submit" button is enabled, click it without clicking on the stars first.

For Further Practice: Digi.Ninja labs

- Client-Side Authentication: https://authlab.digi.ninja/ClientSide
- Permissions based on user-agent: https://authlab.digi.ninja/UserAgent
- IP Address based authentication: https://authlab.digi.ninja/Bypass