Submit a Forged Review

The products can have reviews. The username of the user who submitted the review is displayed alongside their review. How does the application associate a review with the user who submitted it?

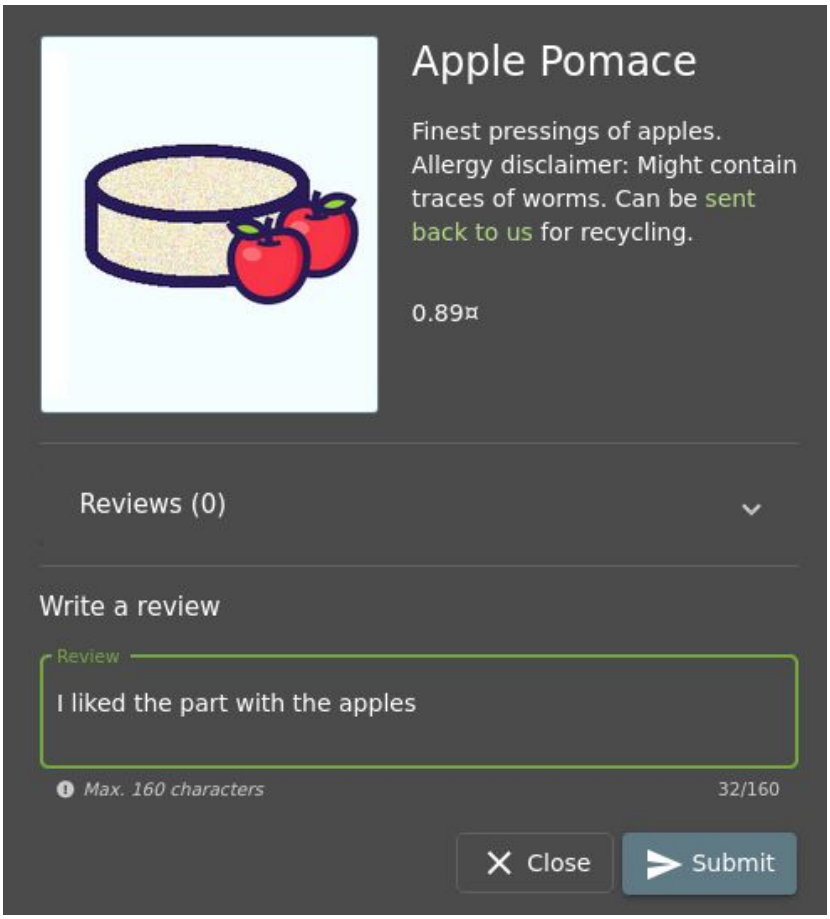
Ideas

Any time user identifiers are part of a request for a logged-in user, you should suspect that the server may be using that user-controllable input to make decisions (instead of relying on information stored in the session state on the server).

Walk-Thru

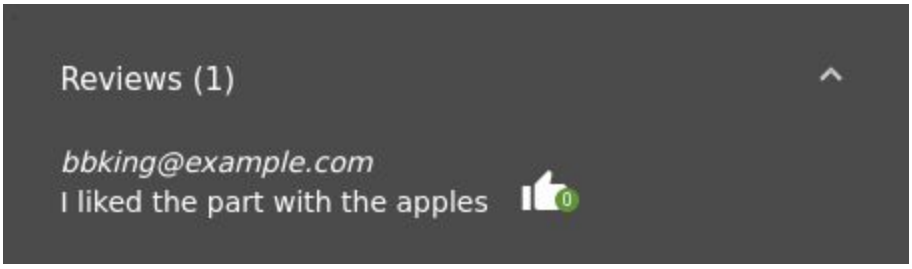
Make sure you have Firefox set to use your Burp Suite as a proxy, and that the Proxy > Intercept pane says "Intercept is off"

1. Log in as your user, choose a product and submit a review.



Submit Any Review

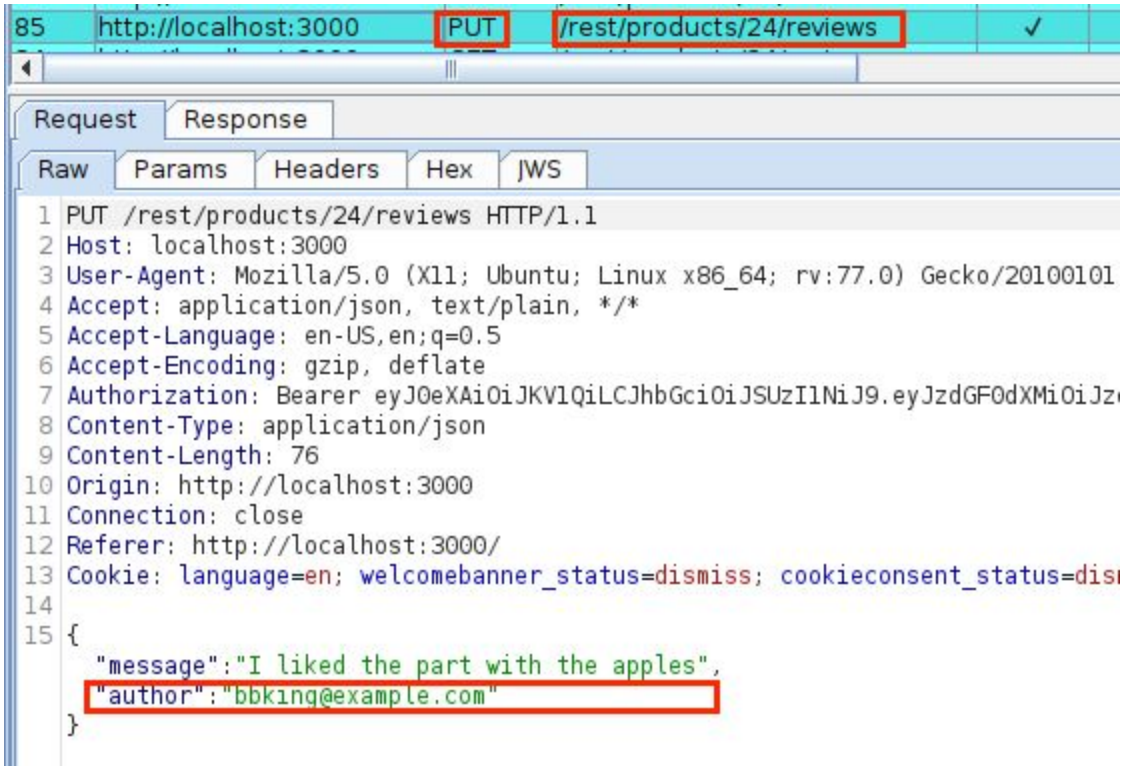
2. Look at the reviews for the product you chose and notice that yours is there now.



Your Helpful Review

3. Look in Burp's Proxy History (Proxy Tab > HTTP history tab) for the PUT request sent to `/rest/products/24/reviews` (Mine was for product number 24, yours may have a different product number.)

4. Click on that item and look at the body of the request. Notice that there's an "author" parameter and its value is your user's email address.



Author Email is Part of Request: SUSPICIOUS!

5. Send this request to Burp Repeater (select it and tap Ctrl-R). In Repeater, send it again to make sure it still works. This will add your review again, but it tells you that your base request works, and duplicate reviews are fine here.

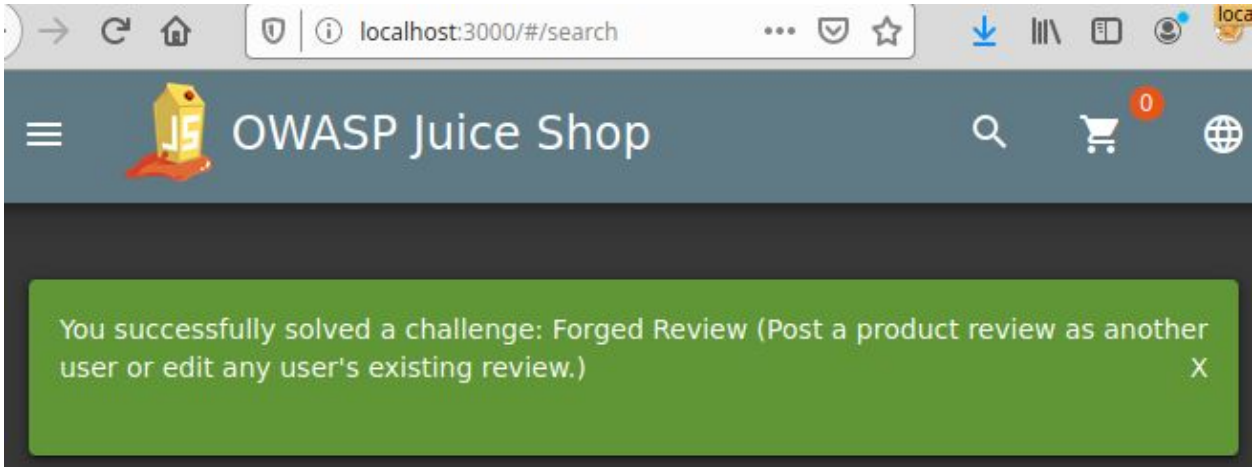
6. In the "Request" pane, edit the "author" to be someone else, and change the "message" to something incriminating like the one below.
You might think it will require the email address of a user that exists on the system - and it might - but if it doesn't, the attack is easier and potentially more damaging so why not try that first?

```
{
  "message":"I once put an emtpy milk carton back in the fridge.",
  "author":"My_Brother@example.com"
}
```

Edit the "message" and the "author"

7. Click "send" in Repeater

8. Go back to your browser and see your achievement.



9. Now check the reviews. My Brother is IN TROUBLE NOW!!!