

INCIDENT REPORT: MP-15429- Admin Log In

Date:11-30-2022

Executive summary:

Using my OWASP Juice Shop application, log into the admin's account without using a password from the login page.

Results

Application details:

- Application URL: <https://mtpate-juice-shop.herokuapp.com/#/>

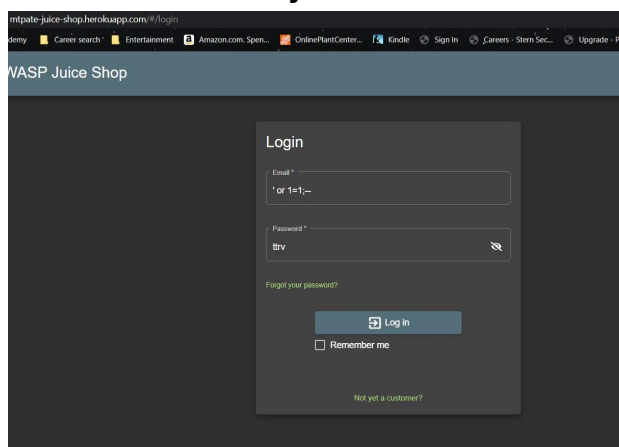
Attack Narrative:

First I checked to see if the login page was vulnerable to SQL injections by typing a single quote in the username and I knew it was vulnerable because it returned "[object Object]" instead of the standard "Invalid email or password". Next I entered ' or 1=1;-- in the username field and an arbitrary password (1=1 creates a true statement and -- ' is used to comment out the rest), at that point I was logged in as the admin. I also looked over the application and found the admin email address in the review of the Apple Juice.

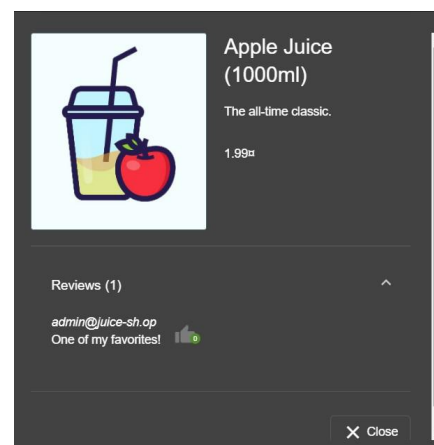
Conclusion:

mtpate-juice-shop application is vulnerable to SQL injections as well as having sensitive information in plain sight.

SQL injection



Admin email address



OWASP Juice Shop


Account

Your Basket

EN

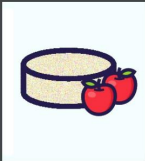
You successfully solved a challenge: Login Bender (Log in with Bender's user account.)

All Products




Apple Juice
(1000ml)
1.99€

Add to Basket



Apple Pomace
0.89€

Add to Basket



Banana Juice
(1000ml)
1.99€

Add to Basket