Login Bypass by SQL Injection

Again the title gives away more than you'd get in a real test, but ... not by a lot, actually. You should always test for this one.

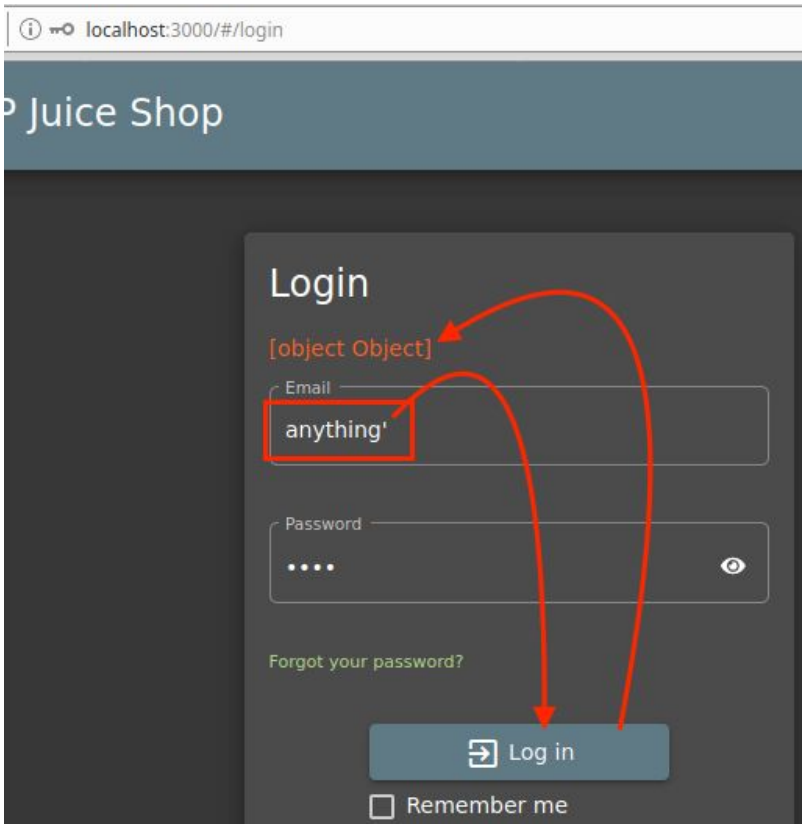
Ideas

How might you trigger an error at the SQL layer from the login form?
What might that error look like in the response?

Walk-Thru

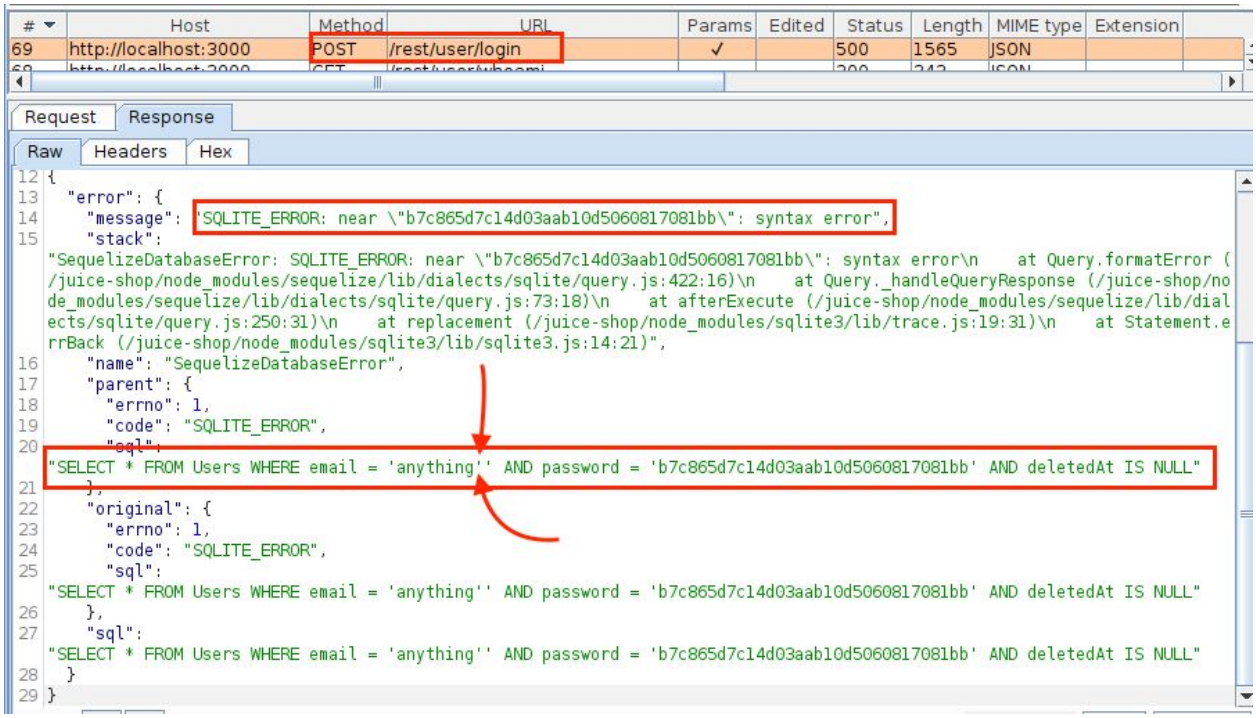
Make sure you have Firefox set to use your Burp Suite as a proxy, and that the Proxy > Intercept pane says "Intercept is off"

1. On the login page, type something in the "Email" field that has an apostrophe (also called a "single quote") in it. Type any password and click "Log in"
2. Notice the response includes [object Object] in red above the form. This is one way Javascript reports an unhandled error condition.



[object Object] is Javascript for, "wait, what did you mean now?"

3. Look at the HTTP request and response in Burp Suite's Proxy History. Notice a very detailed error message. This has gotten pretty rare in real applications, but it helps to show you clearly what's actually happening for this lab. For a harder challenge, ignore these details and only go with what you see in the browser.



Verbose Error Message Provides Useful Information

Here's that broken query as text and line breaks added for readability:

```
"SELECT *
FROM  Users
WHERE email = 'anything''
AND   password = 'b7c865d7c14d03aab10d5060817081bb'
AND   deletedAt IS NULL"
```

The error is because...
A. The query on the server uses single quotes to surround strings
B. Our input for the email address included a single quote
C. The server simply passed our string (including the quote) to the SQL interpreter.
...so...
D. The syntax of the query is broken, and it fails to execute, returning the "syntax error" you see in the response in Burp's Proxy History.

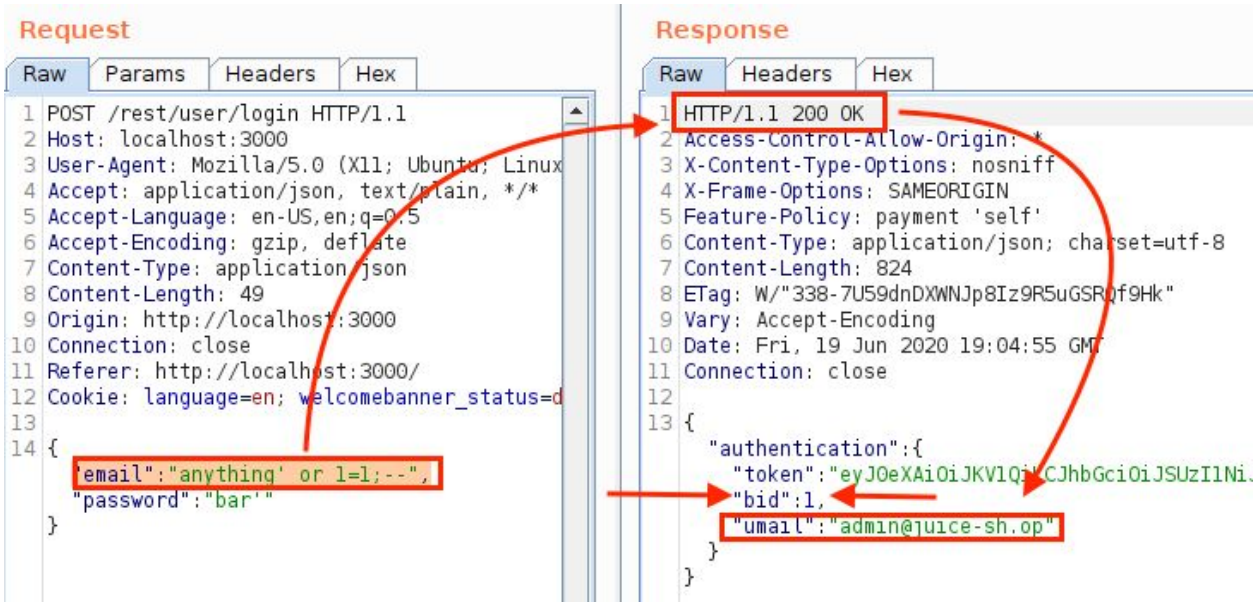
4. Your goal is to make the query run successfully and return at least one result. Because it's all on one line in the actual program (as the error message so kindly informs you) you can use the SQL comment characters to make the database ignore anything after your input.

5. Send the request from the proxy history to Burp Repeater (right-click on it and choose "Send to Repeater" from the menu, or just tap Ctrl-R).

6. Send the request again to make sure it still works. You should get the same error as before.

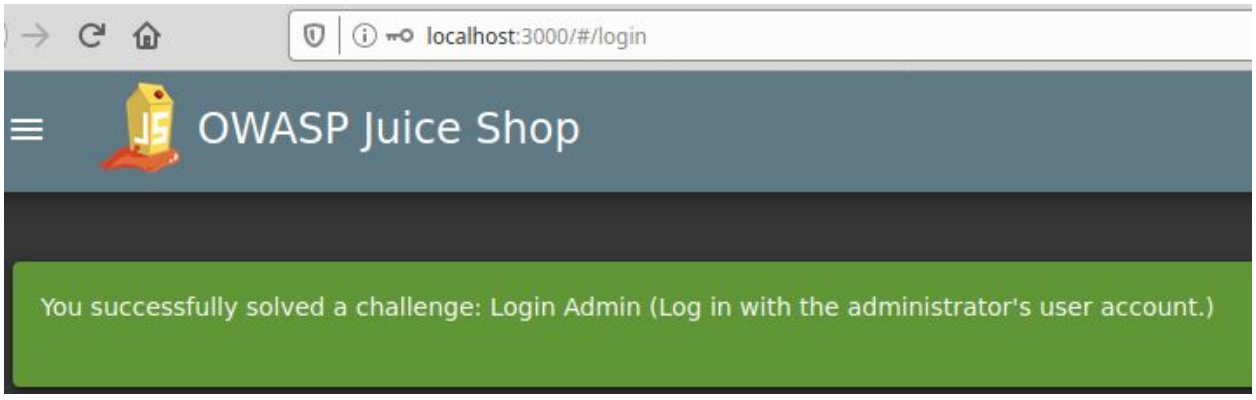
7. Change the value of the "email" parameter so that whole line looks something like this:
`"email":"anything' or 1=1;--",`
then click "Send" in Repeater

8. Notice the response shows you now logged in as the administrator user!



Successful Login as Admin via SQL Injection

9. Return to the browser page and get some recognition for your achievement.



For Further Practice

Check out the 'q' parameter in the Product Search request..
http://localhost:3000/#/search?q=