

SQL Injection

One exploit we found was SQL Injection. In the password box, the program will compare the input to check if it is correct, allowing the user to log in. To do this, we entered an already existing email into the email box. And for the password, we entered: anything' or 'x'='x

This allowed us to log in and successfully exploit cookie injection.