Solving this SQL injection was quite simple as there was only one point where a query is executed. Looking at the run\_query\_injection(...) method, all of the injected SQL examples are in the form “or FOO=FOO;”, which made matching it incredibly easy. Using a regular expression tester online, I formed the expression “.\*or (.\*)=\1.\*” which was able to match all four of the injection statements with the ability to match even more. It took me a few tries to form the right expression as C++ does not support partial regex searching–only full–meaning the “.\*” tokens are necessary at both ends of the statement. My regular expression not only matches at the end of queries, but in the middle too, as a method of future-proofing.

