SQL Attacks

We give an overall score from 0 to 1, where 1 is likely and 0 is not likely. We broke up each type of attack and created a sub-score for each type. Then we average all non-zero attack types, since they are not necessarily related to each other. Any attack type that has a score over .5 yields a message about what type of attack is likely. The attack types are:

- Invalid/illogical statement
- Tautology
- Union Queries
- Piggy-backed queries
- Inference
- Alternate encoding

Invalid/Illogical Statement

We test for common terms used for illegal queries like ‘convert’, ‘xtype’, ‘varchar’, and other sql-related terms that could potentially cause errors. Each term that is found in the query adds to the score.

Tautologies

We test for any pattern matching (a number) = (a number) or (a number) = convert(something), since those are likely ways to create tautologies and were not a part of the original query. Each match adds to the score.

Union Select

We test for the words “union select”. Since that is pretty much the deciding factor and union select isn’t a part of the original query, we return 1 if it’s there, 0 if it’s not.

Piggyback Queries

We look for any semicolons in the statement. If there is one, it’s probably just the end of our query, but any more means they are more than likely ending ours early to piggy back their own query, so we return a 1.

Inference

We look for any if statements, since there were none in our original queries. If we find one, it’s very likely that it’s a test to infer information and not the name of a product. Since it could be a product name though, we only return 0.9.

Alternate Encoding

We test for anything that has exec(char(0x(and some letters or numbers here) . We don’t have any exec or char function calls in our original query, so this is almost definitely an alternate encoding attack and we return 1.