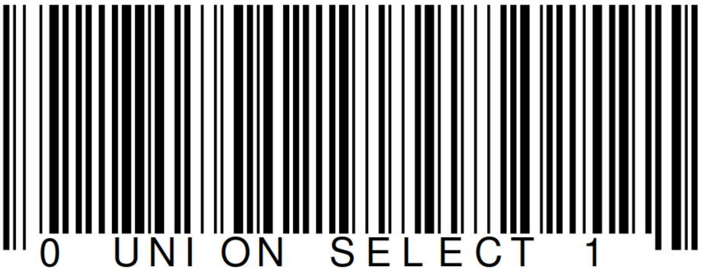
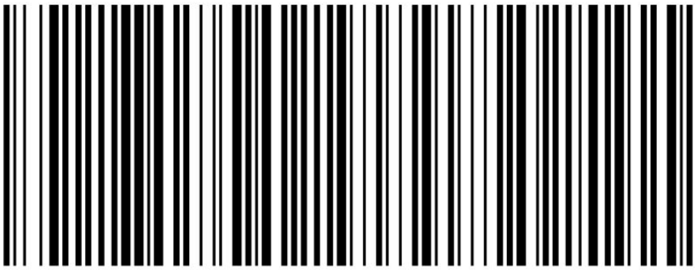
Assignment 12

Task 1

Barcodes





Vulnerability

Description

The vulnerable point is in the query execution at line 23:

```
cur.execute("SELECT price FROM products WHERE id = %s" % barcode)
```

To exploit this, one can pass in *“0 UNION SELECT 1”* as the id*.* The query then becomes:

```
SELECT price FROM products WHERE id = 0 UNION SELECT 1
```

The above query only works if there are no products in the database with ID = 0. Given this, the query will always return 1.

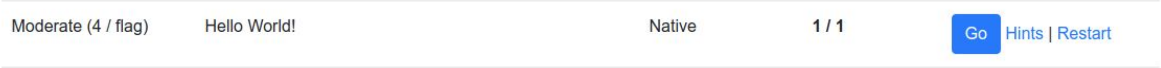
Fix

The problem lies in using string interpolation with *%,* since it won’t escape the input parameters correctly. To fix the vulnerability, replace line 23 with this:

```
cur.execute("SELECT price FROM products WHERE id = %s", barcode)
```

This will properly escape the input parameters, making SQL-injection impossible.

Task 2



Moderate (4 / flag) Hello World! Native 1 / 1

Fig 1. Hello World ctf completed