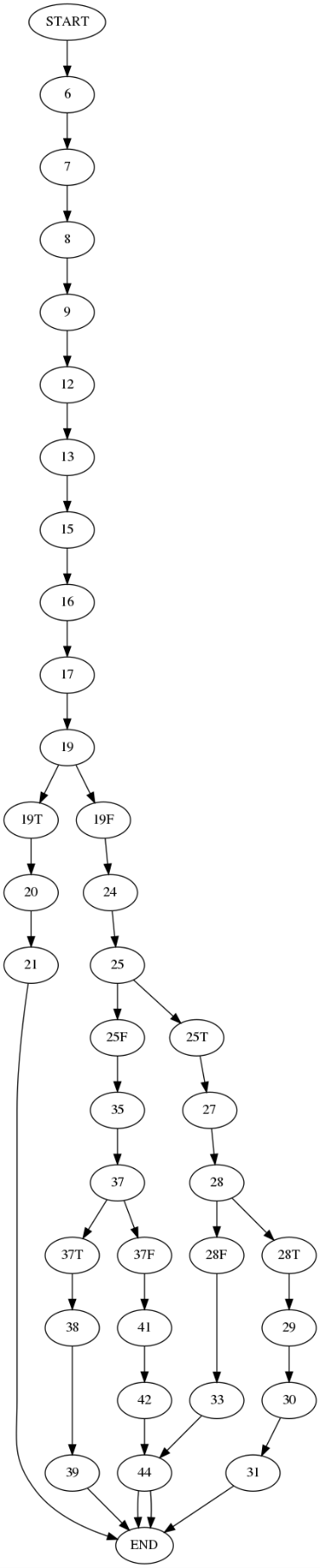
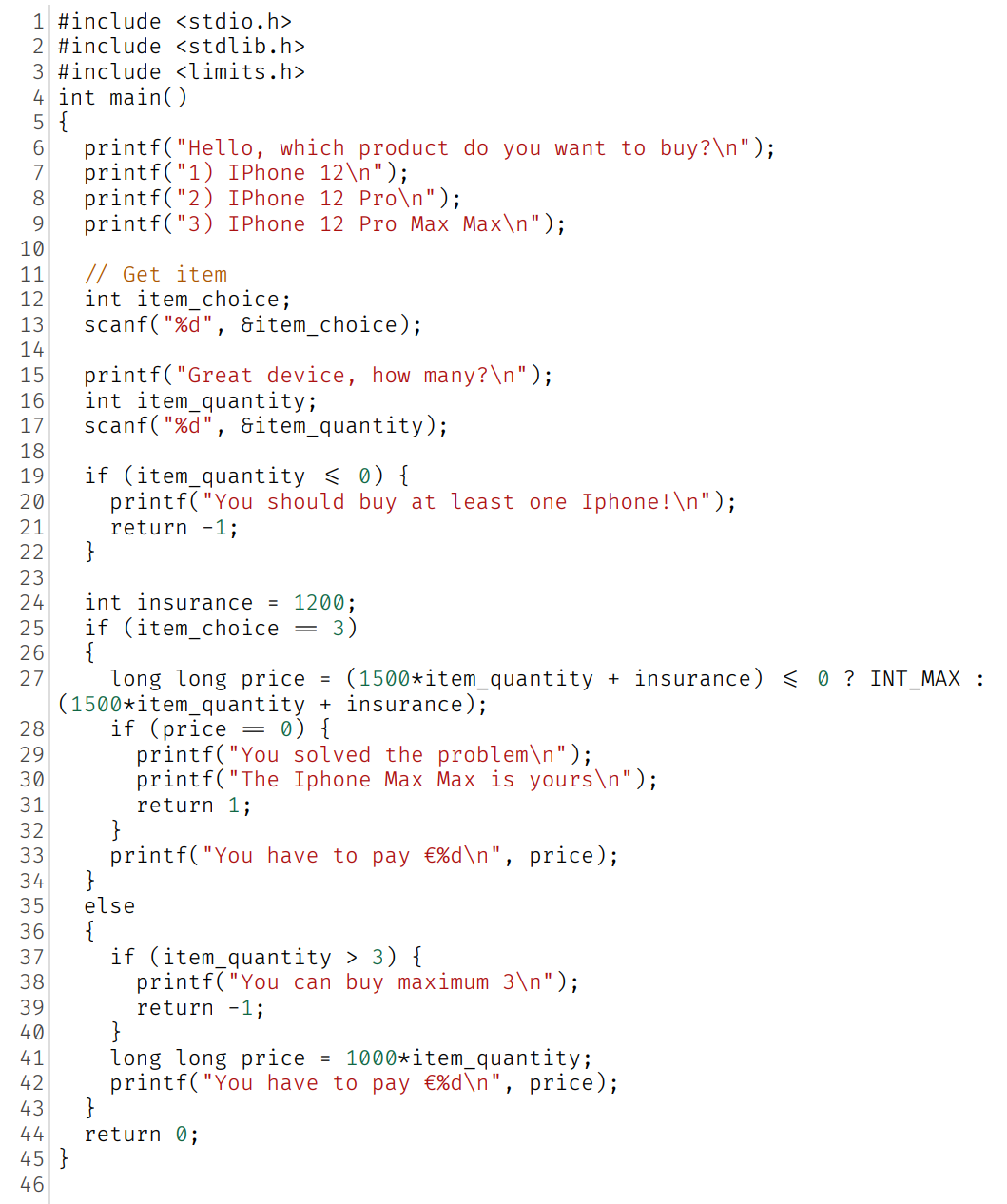
Assignment 4 221214 Matteo Franzil

**Taint analysis exercises**

Initial premise: both exercises have been analyzed with state numbers corresponding with their line numbers. Additionally, both have been fixed in-line without changing the line number, so CFGs for both do not differ between tainted and fixed versions. CFGs were made using DOT and exported in PNG. Finally, the all curly brackets have been left out of the tables for reading clarity (due to a large amount of clutter).

**Exercise 1**

The CFG for the integer overflow can be found on the left. The two tables, the first for the initial iteration comprising kill, get, out and in = {}, and the second comprising the second iteration (no more are needed), can be found in the following pages.



A little note has to be made regarding the taint analysis itself for the vulnerable code. The if on line 37, checking whether the item\_quantity variable in that case is greater than 3, automatically sanitizes it. This is because of the previous “if” on line 19. Therefore, the item\_quantity variable in this case falls in the range [1, 2]. This, however, does not hold for the item\_choice == 3 case.

In order to address this issue, the code was fixed and specifically in line 27. The code written above features two methods of fixing the issue, which are not reliant on each other and can be used separately.

The first way is adding an if check, implemented with a C ternary in order to check whether the price did overflow or reach 0. Doing this sets the price to the INT\_MAX variable.

The second way, which is more elegant and should be preferred, is setting the type of the price variable to long long. This mathematically assures that it will never overflow: since item\_quantity may reach 216 -1 as its max value, multiplying it by 1500 (210) makes it impossible to even reach 264-1. This implementation, however, is not platform-independent as the C type system does not enforce upper bounds for types – this means that both int and long long could theoretically be of length 128 bits. In order to be fully protected, the \_\_builtin\_mul\_overflow function should be used.

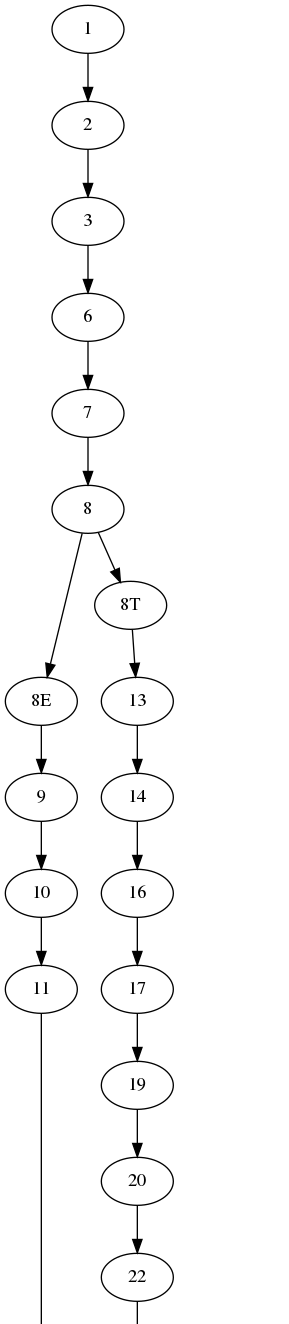
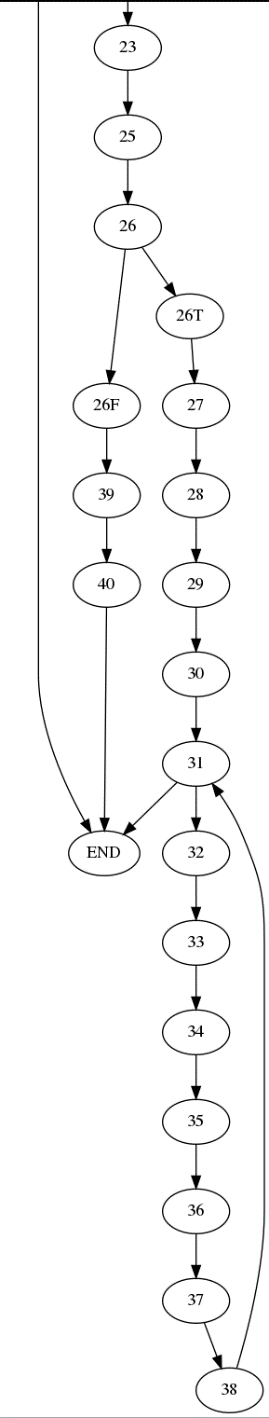
The following table features the aforementioned iterations for the tainted version of the code.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | gen | kill | in | out |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 12 |  |  |  |  |
| 13 | item\_choice |  |  | item\_choice |
| 15 |  |  |  |  |
| 16 |  |  |  |  |
| 17 | item\_quantity |  |  | item\_quantity |
| 19 |  |  |  |  |
| 19T |  |  |  |  |
| 20 |  |  |  |  |
| 21 |  |  |  |  |
| 19F |  |  |  |  |
| 24 |  |  |  |  |
| 25 |  |  |  |  |
| 25T |  |  |  |  |
| 27 | [item\_quantity->T | insurance -> T]price | [item\_quantity->F & insurance -> F]price |  | price |
| 28 |  |  |  |  |
| 28T |  |  |  |  |
| 29 |  |  |  |  |
| 30 |  |  |  |  |
| 31 |  |  |  |  |
| 28F |  |  |  |  |
| 33 |  |  |  |  |
| 25F |  |  |  |  |
| 35 |  |  |  |  |
| 37 |  |  |  |  |
| 37T |  |  |  |  |
| 38 |  |  |  |  |
| 39 |  |  |  |  |
| 37F |  | item\_quantity |  |  |
| 41 |  |  |  |  |
| 42 |  |  |  |  |
| 44 |  |  |  |  |
|  |  |  |  |  |
| It. 2 |  |  |  |  |
|  | gen | kill | in | out |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 12 |  |  |  |  |
| 13 | item\_choice |  |  | item\_choice |
| 15 |  |  | item\_choice | item\_choice |
| 16 |  |  | item\_choice | item\_choice |
| 17 | item\_quantity |  | item\_choice | item\_choice, item\_quantity |
| 19 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 19T |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 20 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 21 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 19F |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 24 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 25 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 25T |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 27 | [item\_quantity->T | insurance -> T]price | [item\_quantity->F & insurance -> F]price | item\_choice, item\_quantity | item\_choice, item\_quantity, price |
| 28 |  |  | item\_choice, item\_quantity, price | item\_choice, item\_quantity, price |
| 28T |  |  | item\_choice, item\_quantity, price | item\_choice, item\_quantity, price |
| 29 |  |  | item\_choice, item\_quantity, price | item\_choice, item\_quantity, price |
| 30 |  |  | item\_choice, item\_quantity, price | item\_choice, item\_quantity, price |
| 31 |  |  | item\_choice, item\_quantity, price | item\_choice, item\_quantity, price |
| 28F |  |  | item\_choice, item\_quantity, price | item\_choice, item\_quantity, price |
| 33 |  |  | item\_choice, item\_quantity, price | item\_choice, item\_quantity, price |
| 25F |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 35 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 37 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 37T |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 38 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 39 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 37F |  | item\_quantity | item\_choice, item\_quantity | item\_choice |
| 41 |  |  | item\_choice | item\_choice |
| 42 |  |  | item\_choice | item\_choice |
| 44 |  |  | item\_choice | item\_choice |

The following tables, on the other hand, show the taint analysis of the fixed code.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | gen | kill | in | out |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 12 |  |  |  |  |
| 13 | item\_choice |  |  | item\_choice |
| 15 |  |  |  |  |
| 16 |  |  |  |  |
| 17 | item\_quantity |  |  | item\_quantity |
| 19 |  |  |  |  |
| 19T |  |  |  |  |
| 20 |  |  |  |  |
| 21 |  |  |  |  |
| 19F |  |  |  |  |
| 24 |  |  |  |  |
| 25 |  |  |  |  |
| 25T |  |  |  |  |
| 27 | price | price |  |  |
| 28 |  |  |  |  |
| 28T |  |  |  |  |
| 29 |  |  |  |  |
| 30 |  |  |  |  |
| 31 |  |  |  |  |
| 28F |  |  |  |  |
| 33 |  |  |  |  |
| 25F |  |  |  |  |
| 35 |  |  |  |  |
| 37 |  |  |  |  |
| 37T |  |  |  |  |
| 38 |  |  |  |  |
| 39 |  |  |  |  |
| 37F |  | item\_quantity |  |  |
| 41 |  |  |  |  |
| 42 |  |  |  |  |
| 44 |  |  |  |  |
|  |  |  |  |  |
| It. 2 |  |  |  |  |
|  | gen | kill | in | out |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 12 |  |  |  |  |
| 13 | item\_choice |  |  | item\_choice |
| 15 |  |  | item\_choice | item\_choice |
| 16 |  |  | item\_choice | item\_choice |
| 17 | item\_quantity |  | item\_choice | item\_choice, item\_quantity |
| 19 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 19T |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 20 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 21 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 19F |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 24 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 25 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 25T |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 27 | price | price | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 28 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 28T |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 29 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 30 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 31 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 28F |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 33 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 25F |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 35 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 37 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 37T |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 38 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 39 |  |  | item\_choice, item\_quantity | item\_choice, item\_quantity |
| 37F |  | item\_quantity | item\_choice, item\_quantity | item\_choice |
| 41 |  |  | item\_choice | item\_choice |
| 42 |  |  | item\_choice | item\_choice |
| 44 |  |  | item\_choice | item\_choice |

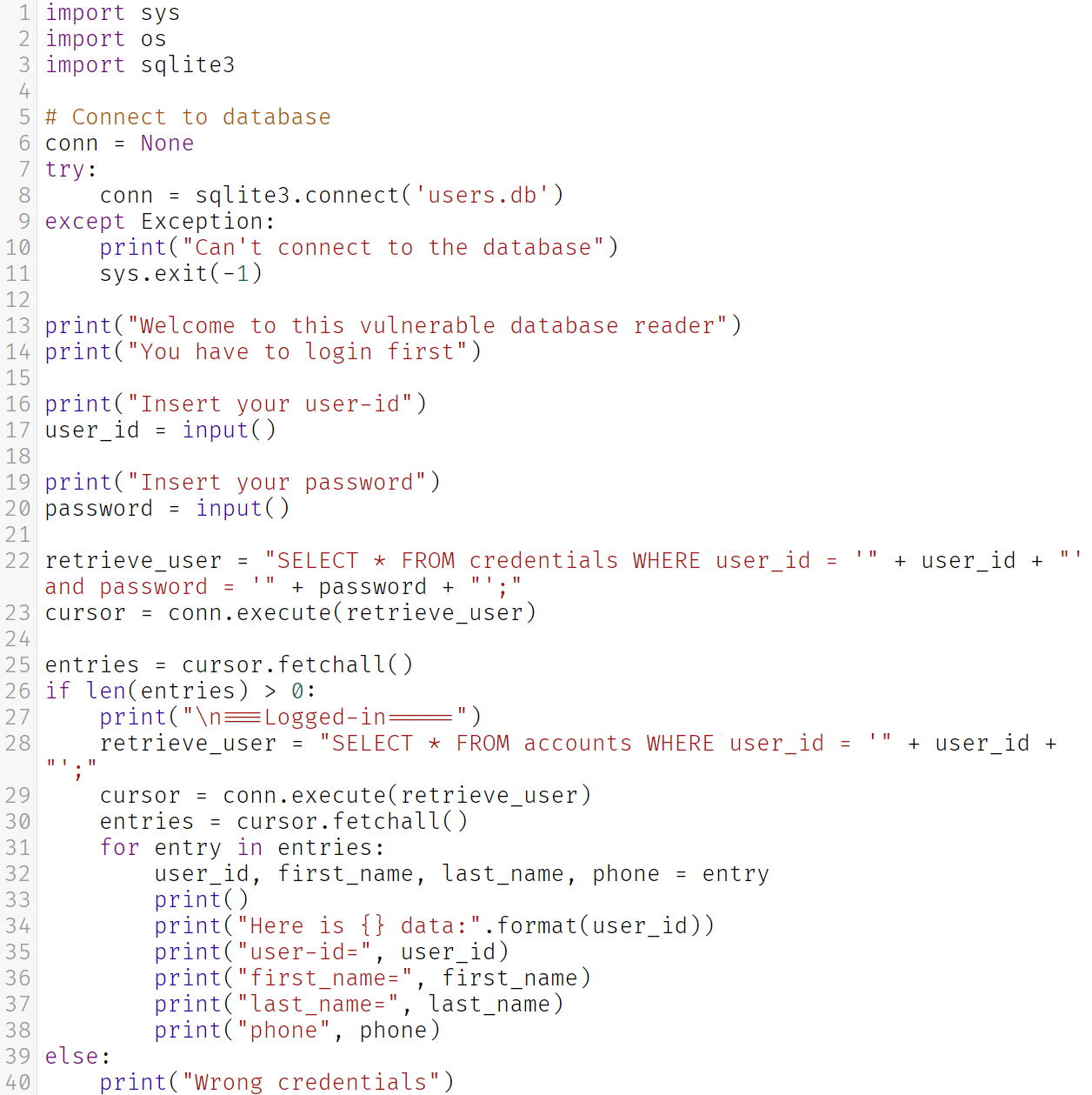
**Exercise 2**

The CFG for the SQL injection exercise can be found on the left, split in two parts for clarity. The code can be found in the following page.

The main reasoning points about the exercise are the following:

* Prepared statements fix lines 22/23 and 28/29. The user\_id and password variables do remain tainted, but are sanitized in the process of addition to the statement so that the cursor is not tainted at all
* The entries variable, at a first glance, may appear tainted if and only if the cursor was tainted by a malicious statement. However, we can never be sure of what we are retrieving from a DB (maybe some other malicious code was injected by a different program), so we consider it tainted no matter what. Therefore, we need to properly sanitize with a map the variables unpacked in the loop starting from line 31. This ensures that echoed variable are not tainted. Due to this, in the analysis the entries variables is shown as always tainted instead of adding a condition based on cursor ([cursor=T]entries for gen and [cursor=F]entries for kill).
* An additional point, not included in the main taint analysis (because it would have generated confusion), is that libraries may not be as safe as they appear to. For example, the sqlite3 library may contain a vulnerability in a certain version, and this may compromise any program written with it. Therefore, it may be considered as tainted. For the purposes of this exercise, it hasn’t been.

As before, the fixes have been inserted as one liners, therefore leaving the line numbering schema intact.



In the following pages we can find the tables for the taint analysis. There are six tables, which represent:

* Tainted code analysis – first step
* Tainted code analysis – second step (two cell differences due to a loop)
* Tainted code analysis – final table
* Untainted code analysis – first step
* Untainted code analysis – second step
* Untainted code analysis – final table (just a cell difference due to a loop)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | SQL injection first |  |  |  |
|  | gen | kill | in | out |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 8E |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 8T |  |  |  |  |
| 13 |  |  |  |  |
| 14 |  |  |  |  |
| 16 |  |  |  |  |
| 17 | user\_id |  |  | user\_id |
| 19 |  |  |  |  |
| 20 | password |  |  | password |
| 22 | [user\_id = T | password = T]retrieve\_user | [user\_id = F & password = F]retrieve\_user |  | retrieve\_user |
| 23 | [retrieve\_user = T]cursor | [retrieve\_user = F]cursor |  | cursor |
| 25 | entries |  |  | entries |
| 26 |  |  |  |  |
| 26F |  |  |  |  |
| 39 |  |  |  |  |
| 40 |  |  |  |  |
| 26T |  |  |  |  |
| 27 |  |  |  |  |
| 28 | [user\_id = T]retrieve\_user | [user\_id = F]retrieve\_user |  | retrieve\_user |
| 29 | [retrieve\_user = T]cursor | [retrieve\_user = F]cursor |  | cursor |
| 30 | entries |  |  | entries |
| 31 | entry |  |  | entry |
| 32 | [entry = T]user\_id, [entry = T]first\_name, [entry = T]last\_name, [entry = T]phone | [entry = F]user\_id, [entry = F]first\_name, [entry = F]last\_name, [entry = F]phone |  | user\_id, first\_name, last\_name, phone |
| 33 |  |  |  |  |
| 34 |  |  |  |  |
| 35 |  |  |  |  |
| 36 |  |  |  |  |
| 37 |  |  |  |  |
| 38 |  |  |  |  |
|  | SQL injection second |  |  |  |
|  | gen | kill | in | out |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 8E |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 8T |  |  |  |  |
| 13 |  |  |  |  |
| 14 |  |  |  |  |
| 16 |  |  |  |  |
| 17 | user\_id |  |  | user\_id |
| 19 |  |  | user\_id | user\_id |
| 20 | password |  | user\_id | user\_id, password |
| 22 | [user\_id = T | password = T]retrieve\_user | [user\_id = F & password = F]retrieve\_user | user\_id, password | user\_id, password, retrieve\_user |
| 23 | [retrieve\_user = T]cursor | [retrieve\_user = F]cursor | user\_id, password, retrieve\_user | user\_id, password, retrieve\_user, cursor |
| 25 | entries |  | user\_id, password, retrieve\_user, cursor | user\_id, password, retrieve\_user, cursor, entries |
| 26 |  |  | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 26F |  |  | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 39 |  |  | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 40 |  |  | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 26T |  |  | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 27 |  |  | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 28 | [user\_id = T]retrieve\_user | [user\_id = F]retrieve\_user | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 29 | [retrieve\_user = T]cursor | [retrieve\_user = F]cursor | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 30 | entries |  | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 31 | entry |  | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries, entry |
| 32 | [entry = T]user\_id, [entry = T]first\_name, [entry = T]last\_name, [entry = T]phone | [entry = F]user\_id, [entry = F]first\_name, [entry = F]last\_name, [entry = F]phone | user\_id, password, retrieve\_user, cursor, entries, entry | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone |
| 33 |  |  | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone |
| 34 |  |  | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone |
| 35 |  |  | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone |
| 36 |  |  | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone |
| 37 |  |  | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone |
| 38 |  |  | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone |
|  | SQL injection third |  |  |  |
|  | gen | kill | in | out |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 8E |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 8T |  |  |  |  |
| 13 |  |  |  |  |
| 14 |  |  |  |  |
| 16 |  |  |  |  |
| 17 | user\_id |  |  | user\_id |
| 19 |  |  | user\_id | user\_id |
| 20 | password |  | user\_id | user\_id, password |
| 22 | [user\_id = T | password = T]retrieve\_user | [user\_id = F & password = F]retrieve\_user | user\_id, password | user\_id, password, retrieve\_user |
| 23 | [retrieve\_user = T]cursor | [retrieve\_user = F]cursor | user\_id, password, retrieve\_user | user\_id, password, retrieve\_user, cursor |
| 25 | entries |  | user\_id, password, retrieve\_user, cursor | user\_id, password, retrieve\_user, cursor, entries |
| 26 |  |  | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 26F |  |  | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 39 |  |  | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 40 |  |  | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 26T |  |  | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 27 |  |  | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 28 | [user\_id = T]retrieve\_user | [user\_id = F]retrieve\_user | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 29 | [retrieve\_user = T]cursor | [retrieve\_user = F]cursor | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 30 | entries |  | user\_id, password, retrieve\_user, cursor, entries | user\_id, password, retrieve\_user, cursor, entries |
| 31 | entry |  | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone | user\_id, password, retrieve\_user, cursor, entries, entry |
| 32 | [entry = T]user\_id, [entry = T]first\_name, [entry = T]last\_name, [entry = T]phone | [entry = F]user\_id, [entry = F]first\_name, [entry = F]last\_name, [entry = F]phone | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone |
| 33 |  |  | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone |
| 34 |  |  | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone |
| 35 |  |  | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone |
| 36 |  |  | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone |
| 37 |  |  | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone |
| 38 |  |  | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone | user\_id, password, retrieve\_user, cursor, entries, entry, user\_id, first\_name, last\_name, phone |
|  | SQL injection fixed first |  |  |  |
|  | gen | kill | in | out |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 8E |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 8T |  |  |  |  |
| 13 |  |  |  |  |
| 14 |  |  |  |  |
| 16 |  |  |  |  |
| 17 | user\_id |  |  | user\_id |
| 19 |  |  |  |  |
| 20 | password |  |  | password |
| 22 |  |  |  |  |
| 23 |  |  |  |  |
| 25 | entries |  |  | entries |
| 26 |  |  |  |  |
| 26F |  |  |  |  |
| 39 |  |  |  |  |
| 40 |  |  |  |  |
| 26T |  |  |  |  |
| 27 |  |  |  |  |
| 28 |  |  |  |  |
| 29 |  |  |  |  |
| 30 | entries |  |  | entries |
| 31 | [entries = T]entry | [entries = F]entry |  | entry |
| 32 |  |  |  |  |
| 33 |  |  |  |  |
| 34 |  |  |  |  |
| 35 |  |  |  |  |
| 36 |  |  |  |  |
| 37 |  |  |  |  |
| 38 |  |  |  |  |
|  | SQL Injection fixed second |  |  |  |
|  | gen | kill | in | out |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 8E |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 8T |  |  |  |  |
| 13 |  |  |  |  |
| 14 |  |  |  |  |
| 16 |  |  |  |  |
| 17 | user\_id |  |  | user\_id |
| 19 |  |  | user\_id | user\_id |
| 20 | password |  | user\_id | user\_id, password |
| 22 |  |  | user\_id, password | user\_id, password |
| 23 |  |  | user\_id, password | user\_id, password |
| 25 | entries |  | user\_id, password | user\_id, password, entries |
| 26 |  |  | user\_id, password, entries | user\_id, password, entries |
| 26F |  |  | user\_id, password, entries | user\_id, password, entries |
| 39 |  |  | user\_id, password, entries | user\_id, password, entries |
| 40 |  |  | user\_id, password, entries | user\_id, password, entries |
| 26T |  |  | user\_id, password, entries | user\_id, password, entries |
| 27 |  |  | user\_id, password, entries | user\_id, password, entries |
| 28 |  |  | user\_id, password, entries | user\_id, password, entries |
| 29 |  |  | user\_id, password, entries | user\_id, password, entries |
| 30 | entries |  | user\_id, password, entries | user\_id, password, entries |
| 31 | [entries = T]entry | [entries = F]entry | user\_id, password, entries | user\_id, password, entries, entry |
| 32 |  |  | user\_id, password, entries, entry | user\_id, password, entries, entry |
| 33 |  |  | user\_id, password, entries, entry | user\_id, password, entries, entry |
| 34 |  |  | user\_id, password, entries, entry | user\_id, password, entries, entry |
| 35 |  |  | user\_id, password, entries, entry | user\_id, password, entries, entry |
| 36 |  |  | user\_id, password, entries, entry | user\_id, password, entries, entry |
| 37 |  |  | user\_id, password, entries, entry | user\_id, password, entries, entry |
| 38 |  |  | user\_id, password, entries, entry | user\_id, password, entries, entry |
|  | SQL Injection fixed third |  |  |  |
|  | gen | kill | in | out |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 8E |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 8T |  |  |  |  |
| 13 |  |  |  |  |
| 14 |  |  |  |  |
| 16 |  |  |  |  |
| 17 | user\_id |  |  | user\_id |
| 19 |  |  | user\_id | user\_id |
| 20 | password |  | user\_id | user\_id, password |
| 22 |  |  | user\_id, password | user\_id, password |
| 23 |  |  | user\_id, password | user\_id, password |
| 25 | entries |  | user\_id, password | user\_id, password, entries |
| 26 |  |  | user\_id, password, entries | user\_id, password, entries |
| 26F |  |  | user\_id, password, entries | user\_id, password, entries |
| 39 |  |  | user\_id, password, entries | user\_id, password, entries |
| 40 |  |  | user\_id, password, entries | user\_id, password, entries |
| 26T |  |  | user\_id, password, entries | user\_id, password, entries |
| 27 |  |  | user\_id, password, entries | user\_id, password, entries |
| 28 |  |  | user\_id, password, entries | user\_id, password, entries |
| 29 |  |  | user\_id, password, entries | user\_id, password, entries |
| 30 | entries |  | user\_id, password, entries | user\_id, password, entries |
| 31 | [entries = T]entry | [entries = F]entry | user\_id, password, entries, entry | user\_id, password, entries, entry |
| 32 |  |  | user\_id, password, entries, entry | user\_id, password, entries, entry |
| 33 |  |  | user\_id, password, entries, entry | user\_id, password, entries, entry |
| 34 |  |  | user\_id, password, entries, entry | user\_id, password, entries, entry |
| 35 |  |  | user\_id, password, entries, entry | user\_id, password, entries, entry |
| 36 |  |  | user\_id, password, entries, entry | user\_id, password, entries, entry |
| 37 |  |  | user\_id, password, entries, entry | user\_id, password, entries, entry |
| 38 |  |  | user\_id, password, entries, entry | user\_id, password, entries, entry |