

Wikiprint Book

Title: Vulnerability Example

Subject: Java Path Finder - projects/jpf-mango/vulnerabilityExample

Version: 12

Date: 02/22/2013 02:39:57 AM

Table of Contents

Vulnerability Example	3
Training	3
Test	3
Mango Test Command	4

Vulnerability Example

Vulnerability testing is starting to work. Training occurred on the first method [shown below](#) for detection of the [disclosure of confidential info in thrown exception](#) vulnerability. The vulnerability was then [detected](#) via the [new Mango Test command](#). The crucial point being, the two methods are not all that similar, but the test performed nominally with no false positives. Also, although the second method is a giant case split with >thousands of ground cases, a significant proportion, probably around 1/5, of these cases are in fact vulnerability hits. So a random walk hits the vulnerability fairly quickly. In this case, after computing 50 steps through case-splits, there was a hit, with a traceback of 14 steps. Random walk took about a minute, but with optimization should get down to seconds.

The traceback allows for visually replaying the exact circumstances of the hit, but you have to start at the beginning of the trace-back and work through all 14 steps. This is useful for debugging Mango, but in general too cumbersome for user work flow. The immediate plan is to just select the source code lines associated with the traceback of a hit. This should in most cases give the user the information that is necessary to fix the problem.

Training



```
*/
final public class RawContact {

    // DEMO EXAMPLE
    public JSONObject EZtest() {
        JSONObject json = new JSONObject();

        try {
            if (mDeleted) {
                json.put("d", mDeleted);
            }
        } catch (final Exception ex) {
            Log.i(TAG, "Error converting RawContact to JSONObject" + ex.toString());
        }

        return json;
    }
    // END DEMO EXAMPLE
}
```

Test

