# A Fly in the Ointment

Frankly, I picked up the idea of this technique after reviewing source code validating some input. I remember, programmers even called it "cheating". But since then, I successfully tried it on different applications without having an access to the source code - so, obviously, there are some patterns.

## The idea

User data traverse through a few validation layers. What is valid at one layer, might be invalid for another. Data also get transformed and fed into other modules which may or may not have comprehensive validation of internal input.

## The idiom

"A fly in the ointment" means a small defect that spoils something valuable or is a source of annoyance while being even in a tiny proportion.

## The heuristic

Creating combinations of valid and invalid data sometimes allows passing through, or triggers program to transform data into something causing problems internally.

A few examples in today's tip.

## Some "restricted" characters

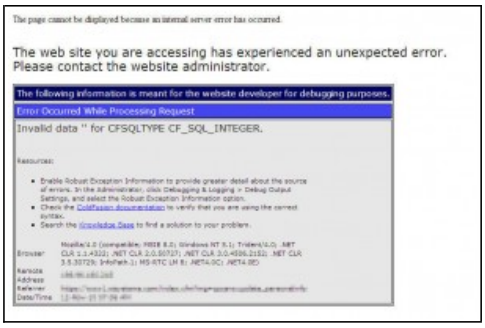
- Backslash (\). This character is used to "escape" other system characters, and to create system commands as well.
- Less than (<), Greater than (>), Ampersand (&). These characters have a primary meaning as tags in mark-up languages.
- Space character.
- Asterisk (*) is used as a wildcard in queries and regular expressions.

## Some combinations to try

- Valid inputs wrapped up by tag characters. Examples: "<123>", "</123>"
- Restricted characters "escaped" with a backslash. Examples: "\&", "\\"
- System commands created with a backslash. Examples: "\d", "\t"
- Asterisk alone or in combination with a valid input. Examples: "*", "Toronto*"
- Space characters before, after, or around delimiters. Examples: " 123", "1. 23"

Armed with the examples provided above I went on the hunt and picked a couple of publicly open web-sites belonging to large organizations...

You can see results below.




Filed under: Heuristics, Testing Techniques

Leave a comment

Comments (0) Trackbacks (0) ( subscribe to comments on this post )

No comments yet.

## Leave a comment

Name (required)

Mail (will not be published) (required)

Website

Submit

« Keyboard shortcuts

Data generation on-the-fly »


Albert Gareev's website

Anne-Marie Charrett's blog

Jonathan Kohl's blog

Julian Harty's website

Karen Johnson's blog

Mike Kelly's blog

**Pages**

About