Subject: Web/TServ [BUG][FIXED]
Posted by hojtsy on Sun, 02 Apr 2006 10:29:41 GMT

View Forum Message <> Reply to Message

This code in Web/TServ seems to be a failed attempt at being very tricky.
```
if(*_command == '\"') {
 while(*++_command && *_command != '\"' || *++_command == '\"')
  exec.Cat(*_command);
}
```
This could crash on a certain kind of unexpected input. If the string starts with a quote, but does not contain the closing pair, the memory after the \0 is read and compared to the quote char. This could be segfault in itself, but if it accidentally equals quote, the memory is read further. I suppose that the other side of the app does not send such invalid string, but it would still be more elegant to not crash on any kind of input.