Security Research and Computer Crime - Where do we Draw the Line?

By *srlinuxx*
Created *12/05/2006 - 12:43am*
Submitted by srlinuxx on Friday 12th of May 2006 12:43:08 AM Filed under Legal [1]

This is interesting - the case of Eric McCarty, a security researcher and sysadmin charged by Federal prosecutors last month with "knowingly having transmitted a code or command to intentionally cause damage" to the University of Southern California's applicant website (I noticed the FBI press release uses the word "sequel" instead of SQL. I hope that wording didn't come from the complaint itself...).

Apparently, McCarty exploited a SQL injection flaw to access student data (which included social security numbers and dates of birth) in the database backing USC's website. He then notified SecurityFocus via email, who notified USC of the vulnerability. USC shut their site down for two weeks while it was being fixed (my guess is the "damage" comes from the fact that USC had to take their applicant website offline, since McCarty didn't do anything malicious with the information). Here is the text of the statute he is alleged to have violated (see section (5)(A)( ).

The case, and others like it, show the ethical conflict involved in some computer crime prosecutions.

Full Story [2].

Legal

Links:
[1] http://www.tuxmachines.org/taxonomy/term/106
[2] http://geekpit.blogspot.com/2006/05/security-research-and-computer-crime.html