

Re: Who should security issues be reported to?

Source: <http://coding.derkeiler.com/Archive/Python/comp.lang.python/2005-01/4794.html>

From: Duncan Booth (duncan.booth_at_invalid.invalid)

Date: 01/28/05

Date: 28 Jan 2005 12:50:10 GMT

Paul Rubin wrote:

> *Duncan Booth <duncan.booth@invalid.invalid> writes:*
>> *In other words, I'm intrigued how you managed to come up with*
>> *something you consider to be a security issue with Python since*
>> *Python offers no security. Perhaps, without revealing the actual*
>> *issue in question, you could give an example of some other situation*
>> *which, if it came up in Python you would consider to be a security*
>> *issue?*
>
> *Until fairly recently, the pickle module was insufficiently documented*
> *as being unsafe to use with hostile data, so people used it that way.*
> *As a result, the Cookie module's default settings allowed remote*
> *attackers to take over Python web apps. See SF bug 467384.*

SF doesn't seem to know about any such bug any more.

Google finds me

<http://mail.python.org/pipermail/python-bugs-list/2001-October/007669.html>

which appears to be SF bug 467384, but it says nothing about security or the Cookie module, just that you wanted better documentation.

I think its a bit borderline whether this really was a security bug in Python rather than just a problem with the way some people used Python. It was a standard library which if used in the wrong way opens a security hole on your machine, but there are plenty of ways to open security holes. The response seems to have been to document that there is a security concern here, but it is still just as possible to use python to expose your machine to attack as it was before.

But thanks anyway, it does give me the sort of example I was asking for.