Re: Security researchers organization

Source: http://www.derkeiler.com/Mailing−Lists/NT−Bugtraq/2003−11/0074.html

---

From: Drew Copley (*dcopley_at_EEYE.COM*)
Date: 11/24/03

```
Date:         Mon, 24 Nov 2003 12:50:44 −0800
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM
```

> −−−−−Original Message−−−−−
> From: Crispin Cowan [mailto:crispin@immunix.com]
> Sent: Wednesday, November 19, 2003 2:14 PM
> To: Thor Larholm
> Cc: Russ; Steven M. Christey; bugtraq@securityfocus.com;
> NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM; Sardonix Security Auditing
> Subject: Re: Security researchers organization
>
>
> Thor Larholm wrote:
>
> >>From: Russ [mailto:Russ.Cooper@rc.on.ca]
> >>(Was: Vulnerability Disclosure Formats (was "Re: Funny article"))
> >><snip http://tinyurl.com/ve83> Thor Larholm proposed the idea of a
> >>"Union" to me. While I don't like the concept of union's in
> this day
> >>and age, our field is one that could benefit from such an idea wrt
> >>discoverers. They are far too often bashed (and I have been
> guilty of
> >>this), and often not recognized for what they do.
> >>
> The Sardonix.org security auditing web site was designed to
> do something
> like this. It is not a "union", more like the Slashdot
> version of source
> code auditing. Sardonix provides:
>
*> * Auditing resources: pointers to how−to's, tools, etc.*
> http://sardonix.org/Auditing_Resources.html
*> * Indexed lists of audited packages*
> http://sardonix.org/Browse_Programs.html
*> * Web form for submitting an audit*
> http://sardonix.org/Submit_Audit.php which triggers a
> responsible
> disclosure process that follows the RFP
> <http://www.wiretrip.net/rfp/policy.html> disclosure protocol

*> * Mailing list for all the usual reasons*
> http://sardonix.org/Mailing_List.html
>
> The problem was that we threw a party and no one came:
> hundreds signed
> up for the mailing list, but a majority of submitted audits
> were pushed
> in by students of David Wagner @ Berkeley, who were told to submit
> audits as a class assignment.
>
> A subtle distinction may be the root cause here: Sardonix seeks to
> change the research model from "find a bug, win a prize!
> (fame & glory
> for half a day)" to "audit software, report what you find, and win a
> reputation for the long term." Having a pile of audited software is
*> *much* more useful to admins than an endless stream of*
> "gotcha again!"
> advisories. But from the lack of response from security
> investigators, I
> conjecture that "find a bug, win a prize!" is more fun to do, and so
> that's what investigators choose to do.
>
*> I would just *love* to be wrong here. If there is something I*
> can do to
> make Sardonix more attractive to investigators, without fundamentally
> changing its mission, sing out. I don't feel a need to change
> it over to
> "find a bug, win a prize" because Bugtraq, vuln−dev, etc. do
> a fine job
> of that: Sardonix is different to fill a perceived unmet
> need. But if it
> doesn't interest investigators, then it doesn't do anything
> at all. So
> how about it; what does it take to interest investigators?

Okay, I will bite. I have experience as QA Lead at an opensource company and have interests in seeing opensource code more secure.

Comments:

−> the existing audits are "okay", but they should never be considered exhaustive, as you know. If you really believe no one else has ever done auditing of Apache's code... Come on. And, did all of this code review prevent last year's Chunked Encoding bug? No. You only need one obscure security bug to make that "restful sleep" nightmarish.

−> The Bugtraq model works, but you want documented test cases, not just "bug reports". You want researchers to come together and work together. In the existing bugtraq model... It is more useful for researchers to keep their methods and test coverage hidden from other researchers then to reveal these things.

The primary question here for a researcher is "why". Where is the motivational model? Why should someone do this? You state above that the bugtraq model gives 'fifteen minutes of fame', whereas you would like to give a lasting reputation [paraphrasing].

But, really.

So, one, you must make a more clear mission statement and focus on building on that, in my opinion. You want a clearly spelled out "vision" for what kind of community you want here. And, two, you want to work with the motivational model of Bugtraq.

The last thing you want to do is to distance yourself from a model that works as well as the Full Disclosure model works.

Here is a type of motivational model that may work:

−> Organize code reviewers into teams
−> set teams to have "projects", such as to "review Apache"
  −> this provides a reason for individual team members to share their test methods and organize their attacks per lines of code
  −> consider a new way of sharing this information, such as across a p2p bulletin board type system, or a revamped bugzilla type system where team members can quickly point out potential problems in the code they are reviewing... It must be easy, otherwise they will be prone not to document, it must be clear −− so they immediately see the usefulness of this
−> You must have a rewards system in place. For instance, post "found bugs" to full disclosure, credit all of the team members, and be able to provide references to their combined team work which found this bug (or "these" bugs).
  −> This kind of rewarding system would provide a direct conduit to the Bugtraq system, but it would also provide the community invaluable insights into how bugs are actually found
  −> QA should always be judged on their results. Merely being able to test code and make the documentation look good means nothing if you can not find bugs.
  −> points should be given per team basis so that it can become "reputable" to belong to a certain team

That is just one potential "motivational model". There could be many such models. This is just a sample model. The major component in this model was first understanding your "vision" for this project.

The above model, a sample one, provides:

−> a reason for people to share their methods
−> a reason for people to share what code they have audited
−> a reason for people to separate code into line by line pieces, but also to work as teams in suspicious areas
−> a reason for people to actually find bugs, as opposed to just

claiming they tested an area of code
−> a reason for people to work hard at this −− all of their work will be
documented

In conclusion, you do need to revamp the idea, and now is a good time.
This is an excellent attitude to have. I applaud that you have this
idea. Very few people are able to start such programs and then actually
to admit "it is not working". Yet, this is required for any scientific
project.

>
> *Thanks,*
> *Crispin*
>
> −−
> *Crispin Cowan, Ph.D. http://immunix.com/~crispin/*
> *Chief Scientist, Immunix http://immunix.com*
> *http://www.immunix.com/shop/*
>
>
>

−−−−
NTBugtraq subscribers save $103.00 off the TICSA exam by using promo
code "NT1003" when registering to take the TICSA exam at www.2test.com.
Prove to your employer and peers that you have the knowledge and
abilities to be an active stakeholder in today's enterprise security.
Become TICSA certified www.trusecure.com/ticsa. Promotion expires
12/31/03 and cannot be used in combination with other offers.
−−−−