

Re: Pentester convicted..

## Re: Pentester convicted..

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-05/msg00131.html>

---

- *From:* Stuart Thomas <[stuartpaulthomas@xxxxxxxxx](mailto:stuartpaulthomas@xxxxxxxxx)>
  - *Date:* Thu, 11 May 2006 18:26:10 +0100
- 

There are some interesting debates developing here! :-)

I would argue the main point in this case is – unauthorised access –

No matter how much good will is arguably present (think about the Daniel Cuthbert <[http://www.theregister.co.uk/2005/10/06/tsunami\\_hacker\\_convicted/](http://www.theregister.co.uk/2005/10/06/tsunami_hacker_convicted/)> case in terms of the same defense) you have gained unauthorised access. As ethical IT security experts, with all our knowledge, skill and esoteric talent, we do not have a right to gain unauthorised access. I hate to agree with Craig Wright (as I believe his comments on this list to be too acidic and un-supportive to the novice – although his frustration is completely understandable) however computer misuse legislation across the world carries a golden thread, you must have permission to access a computer system.

It is frustrating to observe the naivety and yet arguably the good will of these individuals who are sentenced to a jail terms (each case on it's own merits/demerits of course). I think generally the professional community is evolving through professionals bodies, and doing a good job. However I believe it is important to maintain the distinction between the professionals who follow a code of ethics and maintain good morals and practices, with those that are not and do not.

As ever the balance between liberty, freedom of speech, and suppression by the state/corporate entities is ever present as we walk through life.

Interesting times.

Stu

Ian Scott wrote:

So, one night, I'm taking a stroll along main street in my town. I stop for a rest, and happen to lean up against the front door of a store.

I notice the door gives a little bit – and out of curiosity and concern, push a little harder.

The door opens.

I immediately stop what I am doing, and notify the owners and the authorities that the premises are insecure.

Re: Pentester convicted..

Re: Pentester convicted..

By the absolute legal definition, I have indeed "broke and entered" the premises.

Where the hell is motive in all of this? I think that unless there was motive to do some harm, this conviction is utterly ridiculous.

That's my quickie opinion on the matter.

Best,

Ian Scott

On May 10, 2006 10:20 am, William Hancock wrote:

Hey there pen-testers, take this with a grain of salt, it just got me excited. I am really interested in everyones opinion on the matter or corporate responsibility and ownership.

<RANT>

In an article posted to slashdot today (<http://it.slashdot.org/article.pl?sid=06/05/10/112259&from=rss>) a man has been convicted of hacking when he casually and helpfully reported a security vulnerability to the owners of a web site, in this case The University of Southern California. It reads like it was some sort of simple SQL injection and upon gleaning the information he reported it.

What are we to do as a community I ask? We should we, the good guys, who are paid for our knowledge and ability to exploit mistakes, oversights, and weaknesses then professionally report them to aid in the securing of information capital (or anyone who reports the flaw for that matter) worry about prosecution. It lends itself to a forcing the technical community to sit on their laurels and wait for the people who don't report issues to exploit them. Further it sounds very clear that had he not notified them, they would have never known.

A security pro notices a flaw, checks to make sure he is not on crack by 'flipping a bit', deems the threat viable and is likely to be exploited, notifies the owners, then get arrested and charged with unauthorized access. We, as a or even The security community, should push corporations, governments, and organized body's to take responsibility and ownership of their problems. If they publish a site that is flawed or exposing information then they are authorizing the retrieval of that information. I'm not advocating that they laws should allow any jerk to try and brute his or her way in to a public or private web site, but come on.

If someone leaves their wallet in the park with no guard or protection, I pick it up and bring it back to the owner, the owner didn't want me to have it but I brought it back to him. Why in the hell should I have to go to jail for returning it to him, why should I/we be punished for doing the right thing?

Re: Pentester convicted..

I acknowledge this to be a rant but there must but some way to insist that when people make something available to the public that it is their responsibility to safeguard it and appreciate not persecute someone who let's them know (for free I might add) that a weakness exists. This is simple scapegoating, the University did something not advisable as a good practice and instead of owning up to it they villafied a professional pen–tester for offering valid advice.

</RANT>

Thanks,  
Bill

---

---- This List Sponsored by: Cenzic

Concerned about Web Application Security?  
Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: [http://www.cenzic.com/news\\_events/wpappsec.php](http://www.cenzic.com/news_events/wpappsec.php)  
And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxxxx for details.

---

This List Sponsored by: Cenzic

Concerned about Web Application Security? Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: [http://www.cenzic.com/news\\_events/wpappsec.php](http://www.cenzic.com/news_events/wpappsec.php) And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxxxx for details.

Re: Pentester convicted..