

Friday, May 16. 2008

Paypal XSS, ethics and the law

Today a man by the name of Harry Sintonen announced that the paypal payment processing site was exploitable by an XSS attack. In the back of my mind I was thinking how fitting his last name was "Sin"tonen. Apparently he demonstrated this to a journalist and during the "online interview" executed an XSS attack that exploited the vulnerability on the paypal website and used an alert pop-up to show the issue. The article is [here](#)

Now, I understand that its important that these types of companies (such as paypal) need to be looking for this type of bug and I'm certain that Paypal has an army of security personnel that are slated to ensure this sort of thing does not happen. What I'd like to take issue with is the fact that the public has no business executing attacks against websites on the internet and the fact that they are doing so is not only unethical but criminal. Its great that people know how to execute attacks, XSS and SQL injections are not that tough, especially given that paros proxy, web scarab and tamperdata for firefox etc allow you to easily push these to websites using your desktop. But just cause you CAN do something doesn't mean that you should and I feel publicizing this sort of this is just downright irresponsible and if its not illegal in finland, it darned well should be!

Posted by Lawrence Pingree in Security at 15:05

Unauthorised access to a computer system is illegal in many jurisdictions. Demonstrating that it is possible to make a particular dialog box pop up in your own browser, on your own PC, is not unauthorised access to a computer system, in Finland or anywhere else.

This researcher injected javascript into the Paypal page displayed by his own browser. He has not "hacked into Paypal", or stolen anyone's Paypal details. He merely demonstrated that a phishing attack is possible - we have no reason to believe he actually directed it at anyone else.

So it's not illegal, and if Paypal doesn't object to the method of disclosure, which as far as I'm aware hasn't happened, I don't think it's unethical either. Even if Paypal were to object to the public disclosure it might not be unethical, depending whether they had already been informed, if so how long ago, etc.

"I'm certain that Paypal has an army of security personnel that are slated to ensure this sort of thing does not happen."

Sure. And that army needs help from outsiders, since in point of fact they did not ensure this sort of thing does not happen.

Independent researchers, the ones who report their results rather than selling them to credit card fraudsters, make sites more secure, not less. Prosecuting them as if they were criminal hackers would be counter-productive, even if they had broken the law (which I don't believe happened here).

Analogies are cheap online, so feel free to ignore this bit, but it's like losing your wallet and then prosecuting the guy for theft who picks it up and hands it in to the cops. After all, he walked off with your wallet, right? If that's not illegal in Finland, it should be!

"XSS and SQL injections are not that tough"

If that's true, then "bad guys" can easily perform attacks if they want to. Since they presumably want to, they presumably are. So I don't see any harm in a "good guy" demonstrating that it is possible.

Or rather, there isn't any **security** harm. Obviously there is some **PR** damage to Paypal and perhaps also Verisign's EV SSL system.

But surely you wouldn't advocate that they protect themselves from that PR damage using spurious arguments about security risks?

Comment (1)

Anonymous on May 16 2008, 16:56

Please, rename your blog to "Ostrich security by Lawrence A Pingree".

Comment (1)

Anonymous on May 16 2008, 16:56

"He embarrassed me! SEIZE HIM!"

Comment (1)

Anonymous on May 16 2008, 17:24

Excellent feedback Steve. I guess I stand corrected, I'm happy to see some of you have opinions about this topic. I'd bet you might feel differently about public disclosure if your bank account were emptied and all because of a disclosure about PayPal, but I digress and appreciate your opinion.

I do still believe that probing systems and injecting unintended traffic into a website should be illegal, I am certain that he didn't just start by "knowing" the parameter to tamper right off the bat, I bet more than likely he probed many times to find the hole and many jurisdictions would prosecute for such activities under unauthorized use clauses.

Comments (5)

Anonymous on May 16 2008, 18:38

Attacking websites and looking for security holes is technically illegal in Finland, but the law says there needs to be a malicious intent or an intent to use any found security holes.

So, the law doesn't really apply here, although you never know what the courts might decide if things get there. Afterall, one poor kid accidentally portscanned a bank's address range when he was looking for proxy servers. The courts judged that since a proxy server in a bank network could've enabled him to get into bank's internal network, and he certainly was looking for proxies to use them, it meant he had intended to break into the bank's internal network. Ouch! To add insult to injury, he also had to pay the bank for the costs involved in improving the security after the "incident".

I personally believe looking for security holes in third party services should be allowed, especially since they're so common and often easy to find. As a user, I want the services I use to be secure, because I trust them with my personal information. In case of paypal and online banks, I also trust them with my money. Why should I blindly trust these sites?

Or let's ask it like this: if you knew an SQL injection hole could be found in 5 minutes in a service you use, would you still use it? Would you buy from an online store with such a hole, if you knew your credit card data could be stolen by an attacker at any time?

Knowing that good people are checking sites for security holes makes me feel more secure about using those sites.

PS. sorry for the messy and unorganized reply.

Comment (1)

Anonymous on May 17 2008, 04:02

Thanks for the comment, as far as third party checking I'm fine with that as long as it is under the guise of helping the service. Paypal and others have a fiduciary responsibility to repair or fix any security related issues already for PCI and GLBA. What I take issue with is the public disclosure which places all paypal users at risk. I'd be happy if the gentleman worked with Paypal to fix the issues privately, but in fact when you do an interview on TV, Print or online its just to gain notoriety and fame, a precept that bothers me and I do think is unethical as it directly places others at risk and only for the persons ego glory. In the "good old days" security testing was performed by administrators against other administrator's systems and there was a code of ethics to let the administrator (then called a sysop) know that the hole existed so they could address it. Whats lacking today is that honor code, now its all about getting glory off being in the media outlets which I feel is somewhat sad.


Comments (5)

Anonymous on May 17 2008, 10:11

I'm working to rename it soon. Excellent suggestion!

Comments (5)

Anonymous on May 17 2008, 10:14

I thought this was fitting 

<http://youtube.com/watch?v=7SmeNAZYi5A&feature=related>

Comments (5)

Anonymous on May 17 2008, 10:51

I apologize if I Embarrassed you, hopefully we can make amends.

Comments (5)

Anonymous on May 17 2008, 10:54