11 Tithe us your Alms of 0day!

Howdy, neighbor!

A man came to me, and he said, “Forgive me, Preacher, for I have sinned. I play piano in a brothel.”

I laughed, “That ain’t no sin, neighbor. Folks need their music. Go now in peace.”

But the man was worried, he said, “No, Preacher, I’ve really sinned. I need your forgiveness.”

So I laughed again, “Go now, you are forgiven! Stop wasting my time.”

“But Preacher, I teach children to use PHP!”

“Why would you lie to me about your profession like that?”

“Oh, you try confessing an occupation like that!”

“T’ain glad I don’t have to,” I said while finishing my drink, “cause until today I didn’t believe there was any fate I feared more than hell.”

Do this: write an email telling our editors how to reproduce ONE clever, technical trick from your research. If you are uncertain of your English, we’ll happily translate from French, Russian, Southern Appalachian, and German. If you don’t speak those languages, we’ll draft a translator from those poor sods who owe us favors.

Like an email, keep it short. Like an email, you should assume that we already know more than a bit about hacking, and that we’ll be insulted or—WORSE!—that we’ll be bored if you include a long tutorial where a quick reminder would do.

Just use 7-bit ASCII if your language doesn’t require funny letters, as whenever we receive something typeset in OpenOffice, we briefly mistake it for a ransom note. Don’t try to make it thorough or broad. Don’t use bullet-points, as this isn’t a damned PowerPoint deck. Keep your code samples short and sweet; we can leave the long-form code as an attachment. Do not send us \( \LaTeX \); it’s our job to do the typesetting!

Do pick one quick, clever trick and explain it in a few pages. Teach me how to write a memory-corruption exploit—not just shellcode!—that triggers the same bug without profiling on MIPS, PowerPC, x86, and AMD64. Show me how to write a 64-bit DOS extender, or how to extract firmware from locked regions on an MSP432’s funky flash protection.

Don’t tell me that it’s possible; rather, teach me how to do it myself with the absolute minimum of formality and bullshit.

Like an email, we expect informal (or faux-biblical) language and hand-sketched diagrams. Write it in a single sitting, and leave any editing for your poor preacherman to do over a bottle of fine scotch. Send this to pastor@phrack.org and hope that the neighborly Phrack folks praise be to them!—aren’t man-in-the-middling our submission process.

Yours in PoC and Pwnage,
Pastor Manul Laphroaig, D.D.