I set up an outdated PHPMyAdmin panel in a remote directory on one of my sites. Anyone performing server recon and directory bruteforcing using Wfuzz (as described in Chapter 7) would have been able to find it.

My cover story was simple. Once I found the panel, I ran a wide search for any email/password combinations that could be discovered from my email addresses (this technique will be discussed in the next chapter).

I set the PHPMyAdmin login to an older username/password combo from a random data leak. Using the passwords “discovered” from various data leaks, I pretended to gain access by bruteforcing the PHPMyAdmin panel.

To prove I was there, I “hacked” my own WordPress site by directly modi- fying the WP database table, and replaced the front page with the image shown in Figure 17.8.

But why stop there? I assumed Cyper and his team would want to personally verify the access and login themselves, so prior to my victory announcement I took the liberty of setting up strict firewall rules on my server designed to completely block any connections from known TOR, VPN IP, proxy, or other known bad IPs. I then set up logging to monitor for any incoming connections.

When the trap was set, I made a celebratory post on the forum’s contest thread (Figure 17.9).

Not bad, right? How many people would expect someone to hack their own website?

NSA asked me a lot of questions about how I was able to do it, all of which was completely plausible; and it worked!

NSA and his team had their fun logging in and playing around my panel, and as my reward, I got to record all of their IP information. The PHPMyAdmin URL was so obscure (and so brand new) that any hits were obviously relevant—which included the fake web scraping bots that suddenly appeared.

The point of this story is that if you are going to SE a target, why hold back? Sometimes the most outrageous ideas are the best ones.