Twitter Thread by Claire Ryan



Claire Ryan
@aetherlev

Right, I did some reading and here's what likely happened with Parler. Lots of crossed wires here.

First up: someone noticed that Parler uses sequential integers in the API endpoint to get content.

An API endpoint is just a URL with a value added onto the end that tells the system what you want to get back.

Using sequential integers means that a hacker can set up an automated script to start at 1 and count up, trying API calls over and over again, to get back content from Parler.

Parler apparently had no restrictions on this API endpoint, which frankly blows my mind as a web dev.

If you had a working URL, it just spat out whatever it had whether you were logged in or not.

It seems that EVERYTHING that had been uploaded - video, photos, text posts - was accessible whether it had been deleted or restricted in the app itself. Even uploaded photos of licenses etc etc.

I cannot describe how amateur hour this is, if true.

Now as well as that - Parler got kicked off Twilio so now there was no verification of phone numbers on signup. They let it fail open - allow registrations without verification. Hackers used this to create umpteen accounts, for shits n giggles apparently.

I think they closed registrations after the damage had been done.

Okay so the admin accounts - they discovered an API endpoint that let them enumerate admin users.

This is also so unbelievably bad that it boggles the mind, from a web dev perspective

Like I don't even know why that exists. That is not something that should exist.

The admin accounts were not compromised, apparently, but holy fucking shit you DO NOT expose admin account data

EVER. That is asking to get hacked even more.

Anyway the TL;DR on this is that your password probably hasn't been compromised (I hope) but anything else uploaded to Parler might be out in the wild now even if you deleted it in the app.

Happy fucking Monday, let the train wreck of this week begin

Further update: some lively discussion of it going on here: https://t.co/swpV9JUJ5p