found to check what used to be there. Maybe some of the old files (think .js files!) are still there? **/index**. From here you can then start scraping common endpoints & your recon data increases massively.

ParamScanner – A custom tool to scrape each endpoint discovered and search for input names, ids and javascript parameters. The script will look for <input> and scrape the name & ID and then try it as a parameter. As well as this it will also search for var {name} = “” and try determine parameters referenced in javascript. An old version of this tool can be found here https://github.com/zseano/InputScanner. Similar suchs include LinkFinder by @GerbenJavado which is used to scrape URLs from javascript files here: https://github.com/GerbenJavado/LinkFinder and @CiaranmaK has a tool named **parameth** used for brute forcing parameters. https://github.com/maK-/parameth

AnyChanges – This tool takes a list of URLS and regularly checks for any changes on the page. It looks for new links (via <a href>) and references to new javascript files as I like to hunt for new features that may not be publicly released yet. A lot of researchers have created similar tools but I am not sure of any public tool which does continuous checking at the time of writing this.

Can you spot the trend in my tools? I'm trying to find new content, parameters and functionality to poke at. Websites change everyday (especially larger companies) and you want to make sure you're the first to know about new changes, as well as taking a peek into the websites history (via waybackmachine) to check for any old files/directories. Even though a website may appear to be heavily tested, you can never know for sure if an old file from 7 years ago is still on there server without checking. This has led me to so many great bugs such as a full account takeover

from just visiting an endpoint supplied with a users ID!