Benjamin Heald Personal Security Blog

WHOAMI and Current Resume

Teradici and CVE-2020-10965: An issue of routing.

After nearly five years of working with Application Security I was finally able to discover a security bug that warranted a CVE. This vulnerability was in a software package owned by a major vendor, Teradici, which provides management software for several different kinds of remote workstation setups. The impact of this bug is critical, with almost no attacker interaction needed. Once reported to Mitre, this vulnerability was issued CVE-2020-10965. Within this blog post, I'll be giving an overview of the discovery process.

Continue Reading

The problem with Parse: A low-code server that endangers over 63,000,000 users.

The Parse Platform is a popular web server similar to Firebase that allows mobile application developers to spin up a fully fledged backend with API support within a very short amount of time and with very little programming experience. In just a few days of scanning the most popular Google Play applications, I was able to discover several vulnerable Parse instances that potentially endanger the data of a collective 63,000,000 users. In this blog post I will give an overview of the many security issues inherent in the Parse platform, as well as give recommendations to both developers and the maintainers of the Parse Platform for how to improve their security posture.

Continue Reading

Parse @ H@ctivityCon!

This blog post contains the slide deck and recording of the presentation I gave at Hackerone's HacktivityCon.

Continue Reading

Gather: A tool to screenshot domains

As more and more companies create bug bounty programs with open-ended scopes, hackers sometimes need to examine large amounts of domain names. Currently most people use tools such as Aquatone which provide a extremely nice looking report at extremely fast speeds.<

In this blog post, I introduce Gather, a domain screenshotting tool that allows a user to perform analysis on very large lsits of domain names, with a very low false negative rate.

Continue Reading

Elevate: A new tool for vertical domain discovery

As more and more companies create Bug Bounty programs with open-ended scopes, vertical domain discovery has become essential to bug bounty hunters. Vertical domain discovery describes an attempt to find all domain names owned by a given company. These other domain names can be used to host internal services, microsites, or services outside the company's main domain name. Since they exist outside the central domain, these webistes are often markedly less secure, making them easy targets for penetration testers.

Elevate is tool that I have created in order to automate the arduous process of collecting domain names owned by a given company. This tool utilizes API's from various sources in order to compile large domain lists. Users are able to search for domains by organization name, root domain name, or email address.

Continue Reading

How to examine iOS network traffic over an iOS cable.

In this blog post, I'll be showing you how to route your iOS device network traffic through Burp Suite proxy listener over your iOS cable, without the need of a local network proxy.

In a normal case, a penetration tester that wants to view the network traffic of a given iOS application would need to connect their phone to their Burp proxy listener that is exposed to the entire local network. Since the listener is exposed to the local network, this creates operational security issues if on a public network, and functional issues if on a network that disallows local servers. This second type of problem is extremely common on university networks, as it was in my case when I first developed this method.

Continue Reading

Netflix ID Dataset

A few years ago I wanted to make an application that gave the user the power to generate a random episode of any given US Netflix show. The main technical issue with this project was that Netflix does not have a public API and so matching each show or movie with the corresponding ID number found for in every episode or movie link was seemingly impossible. I however was able to find an API endpoint that allowed me to brute-force these ID #'s by simply sending thousands of requests. I have compiled this data into individual files.

Continue Reading