Julian Welge
8/7/2021

Link: https://portswigger.net/daily-swig/black-hat-2021-warcannon-simplifies-web-wide-vulnerability-research

Summary:

According to this article, a tool unveiled at Black Hat USA called WARCannon can be used to "non-invasively test regex patterns across the entire internet for corresponding vulnerability indicators." Within a couple hours and for $100, one can utilize WARCannon to process multiple regular expression patterns across 400TB. Practice lead for cloud security architecture at Observian, Brad Woodward, was quoted in this article saying, "Consider a researcher who spends two days finding a vulnerability in one place … they can then plug their findings into WARCannon and turn one vulnerability into five, 500, or 50,000."

Why We Care:

If I'm understanding this correctly, this tool, while somewhat expensive, provides an insane amount of power for those looking for regex vulnerabilities across the web. While most of this article is written in the context of research and helping people, this tool also seems like an easy way for black hat hackers to be able to sniff out what systems across the web have the same regex vulnerabilities as one of the few they just came across. This then allows for exploiting those vulnerabilities at a large scale which can be dangerous to the entire interdependency of the internet. If a common practice throughout most up-to-date systems is found to be vulnerable, entire infrastructures could collapse if exploited.