# 1200 - A New Era of SSRF - Exploiting URL Parser in Trending Programming Languages!

Friday at 12:00 in Track 3
45 minutes | Demo, Tool, Exploit
Orange Tsai*Security Consultant from DEVCORE*

We propose a new exploit technique that brings a whole-new attack surface to bypass SSRF (Server Side Request Forgery) protections. This is a very general attack approach, in which we used in combination with our own fuzzing tool to discover many 0days in built-in libraries of very widely-used programming languages, including Python, PHP, Perl, Ruby, Java, JavaScript, Wget and cURL. The root cause of the problem lies in the inconsistency of URL parsers and URL requesters.

Being a very fundamental problem that exists in built-in libraries, sophisticated web applications such as WordPress (27% of the Web), vBulletin, MyBB and GitHub can also suffer, and 0days have been discovered in them via this technique. This general technique can also adapt to various code contexts and lead to protocol smuggling and SSRF bypassing. Several scenarios will be demonstrated to illustrate how URL parsers can be exploited to bypass SSRF protection and achieve RCE (Remote Code Execution), which is the case in our GitHub Enterprise demo.

Understanding the basics of this technique, the audience won't be surprised to know that more than 20 vulnerabilities have been found in famous programming languages and web applications aforementioned via this technique.
Orange Tsai
Cheng-Da Tsai, also as known as Orange Tsai, is member of DEVCORE and CHROOT from Taiwan. Speaker of conference such as HITCON, WooYun and AVTokyo. He participates numerous Capture-the-Flags (CTF), and won 2nd place in DEF CON 22 as team member of HITCON.

Currently focusing on vulnerability research & web application security. Orange enjoys to find vulnerabilities and participates Bug Bounty Program. He is enthusiasm for Remote Code Execution (RCE), also uncovered RCE in several vendors, such as Facebook, Uber, Apple, GitHub, Yahoo and Imgur.

#defcon25/by_track/track3/friday #defcon25/By_Day/_Friday