WPScan Enumeration

Dashboard

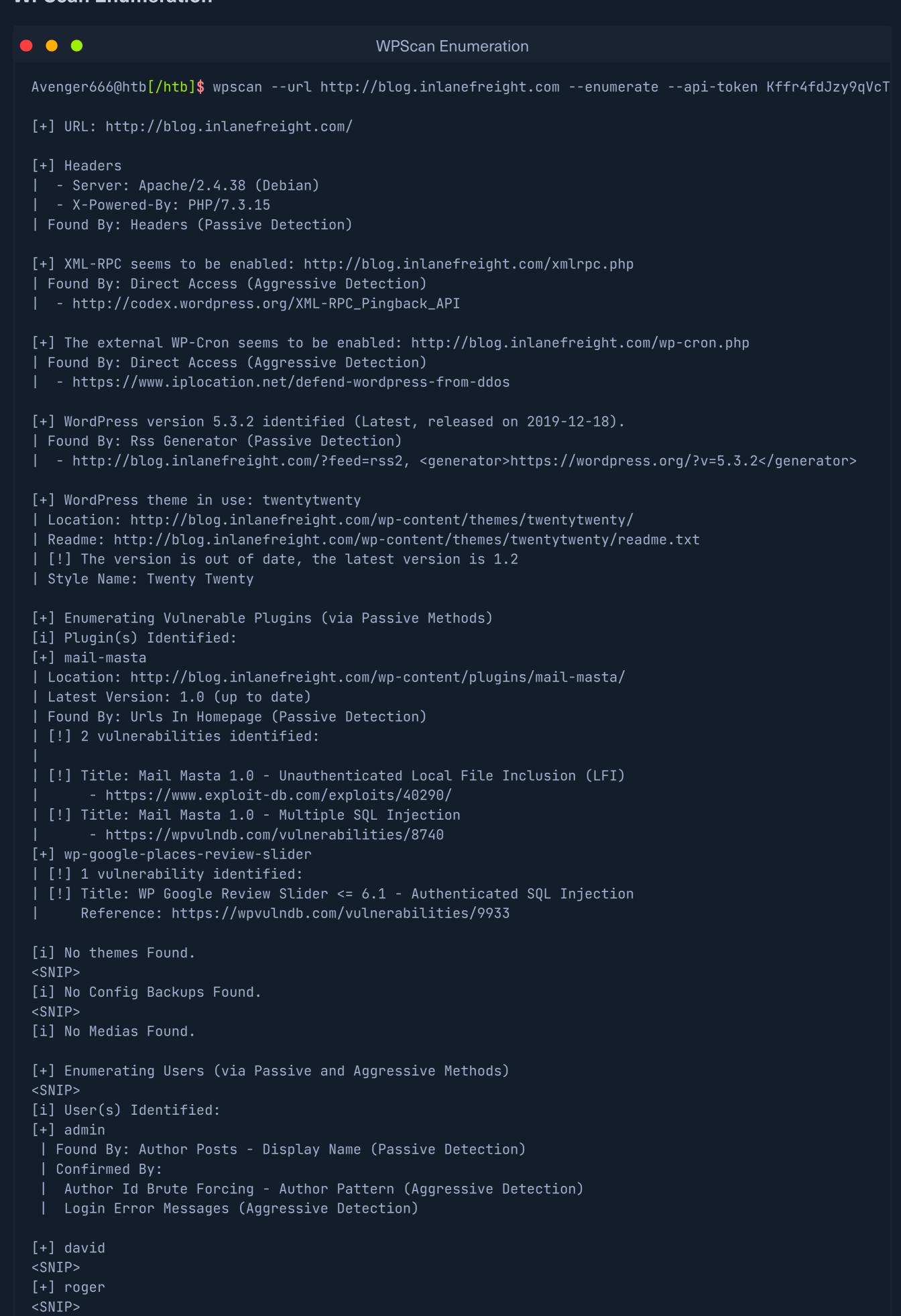
| ■ Modyles

Enumerating a Website with WPScan

The --enumerate flag is used to enumerate various components of the WordPress application such as plugins, themes, and users. By default, WPScan enumerates vulnerable plugins, themes, users, media, and backups. However, specific arguments can be supplied to restrict enumeration to specific components. For example, all plugins can be enumerated using the arguments --enumerate ap. Let's run a normal enumeration scan against a WordPress website.

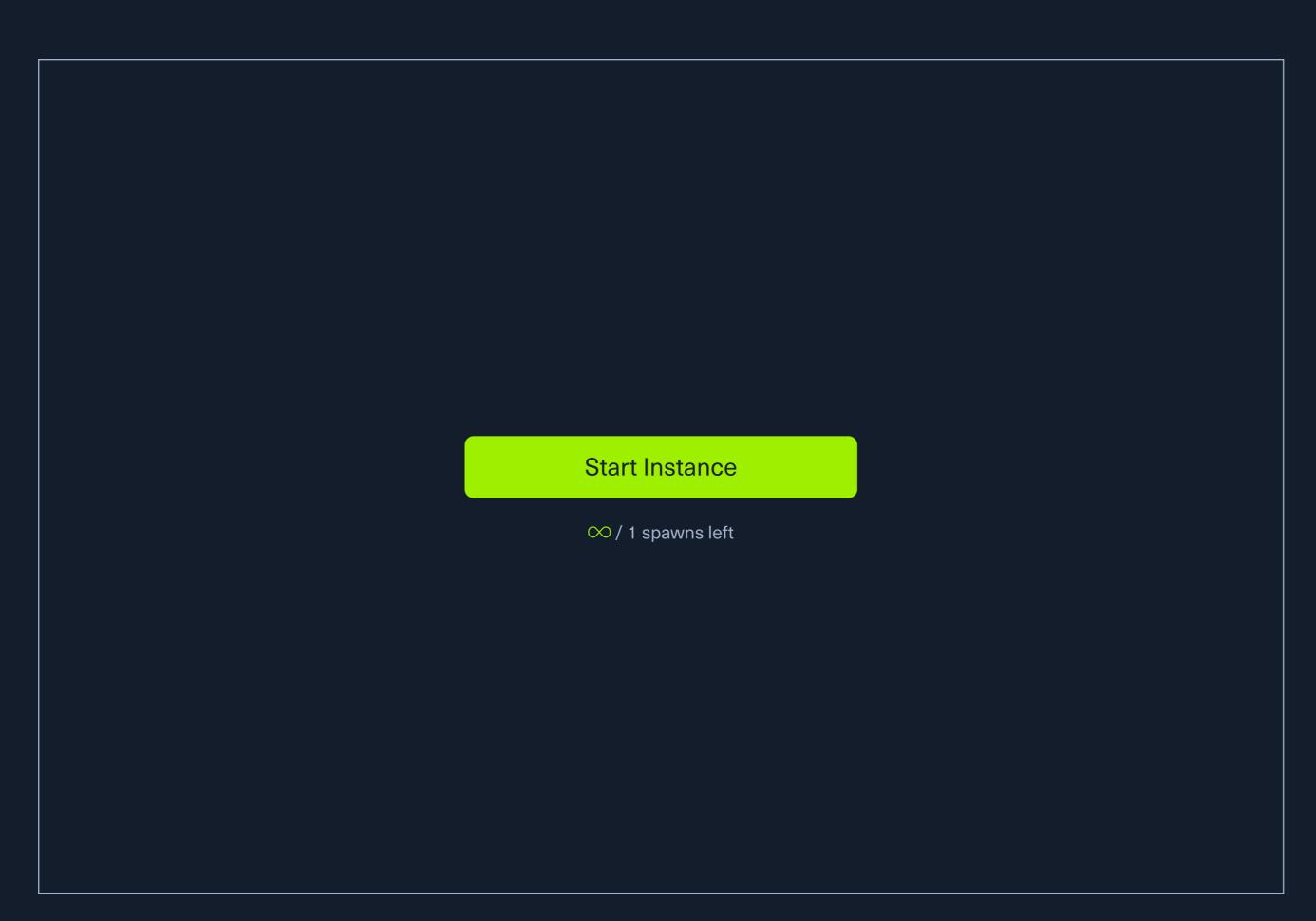
Note: The default number of threads used is 5, however, this value can be changed using the "-t" flag.

WPScan Enumeration

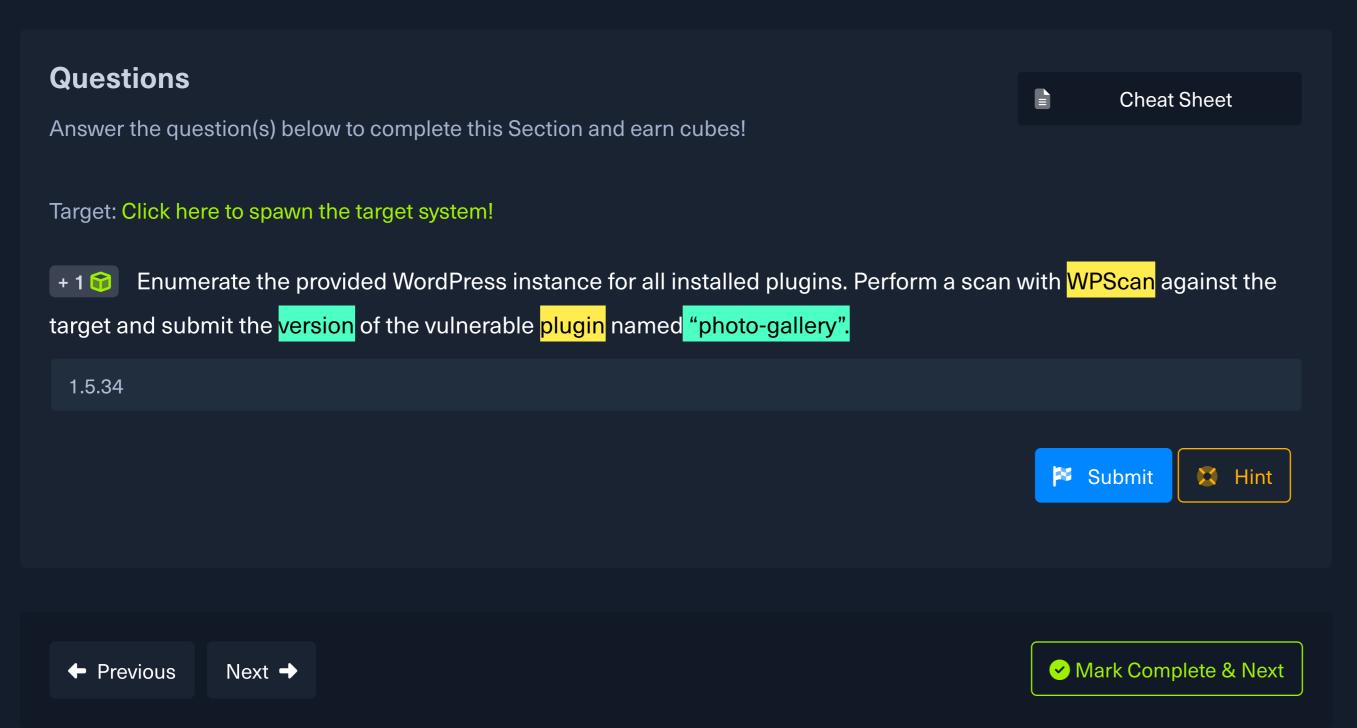


WPScan uses various passive and active methods to determine versions and vulnerabilities, as shown in the scan output above.





Waiting to start...



Cheat Sheet ? Go to Questions **Table of Contents** Introduction Intro WordPress Structure WordPress User Roles Enumeration WordPress Core Version Enumeration Plugins and Themes Enumeration Directory Indexing **User Enumeration 1** Login WPScan Overview **WPScan Enumeration** Exploitation **6** Exploiting a Vulnerable Plugin Attacking WordPress Users RCE via the Theme Editor Attacking WordPress with Metasploit **Security Measures** WordPress Hardening **Skills Assessment** Skills Assessment - WordPress My Workstation OFFLINE Start Instance

∞ / 1 spawns left