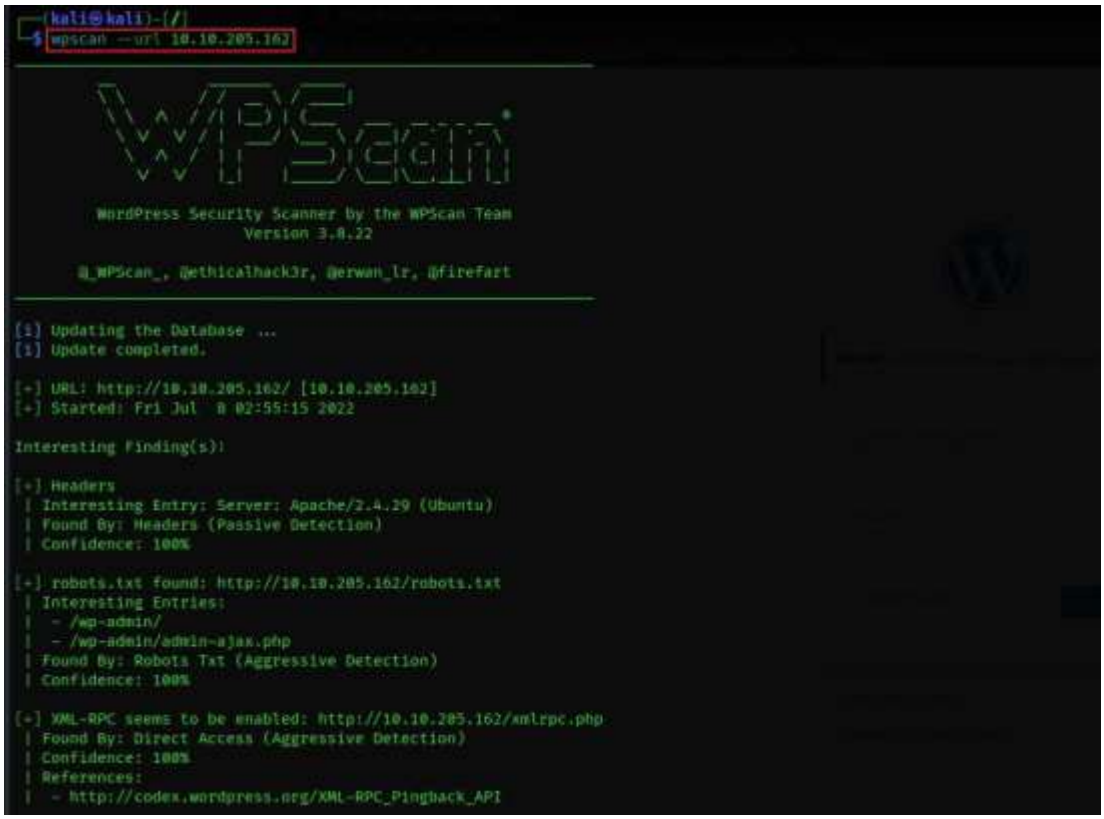
Wpscan

Wpscan is a WordPress security scanner used to test WordPress installations and WordPress-powered websites. This is a command line tool used in Kali Linux. This tool can be used to find any vulnerable plugins, themes, or backups running on the site. It is usually used by individual WordPress site owners to test their own websites for vulnerabilities and also by large organizations to maintain a secure website. This tool can also be used to enumerate users and perform brute-force attacks on known WordPress users.

WPScan is a popular tool for scanning WordPress installations for security vulnerabilities. It is designed to identify vulnerabilities in WordPress core files, plugins, and themes. WPScan is commonly used by security professionals and enthusiasts to assess the security posture of WordPress sites.

Examples: -

1. To have a basic wpscan use --url command along with the target IP.



2. Now to find out the users in target website use -e u flag.

3. To perform brute force attack over a user we will use -U and -P flag along with the wordlist. As shown below.