Mini Project

Aim: Enumerate the Vulnerable Plugins and user on a local WordPress website using wpscan.

To Find:

1. Total number of plugins by default.
2. Default username retrieved by wpscan.
3. WordPress Version.
4. Vulnerable Plugins
5. Vulnerable users

SUBJECT WEBSITE: https://alert.com.pk

Observation:

1. There was a total of 12 plugins in the website namely,

wp-user-avatar, wordpress-seo, onesignal-free-web-push-notifications, post-hit-counter, Metronet-profile-picture, menu-icons, google-site-kit, gtranslate, enable-jQuery-migrate-helper, daily-prayer-time-for-mosques, and add-to-any.

1. There are 40 number of users, namely

Ibraheemawan, Akhtar, ikramuddin, ummerubaha, hashernaseer, zabihullahshah, rabiasultan, zaidnaveed, syedsaqibshah, shujaatqureshi, shoaibbhatti, shahzadmalik, ariframzan, abdulaleem, usmanayub, usmanwaheed, izzatullah, azmatkhan, allamazahidurrashdi, alihilal, inayatshamsi, farhankhan, faizullah, muhammadizaz, muhammadsaadsaadi, yousufhaider, muslimansari, musharrafhazarwi, jahanyaqoob, rasibkhan, azmat, Abdullah, sohail, wajihanaz, wahaj, shakirahmed, kamransarwar, webdesklhr and yamnasami.

1. There were no vulnerable plugins found but WordPress theme used: newspeak-child

with Directory listing enabled.

1. Users named shoaibbhatti, rasibkhan, Azmat, Abdullah and sohail have author access and are easily hacked using brute force.
2. WordPress version 5.9.2 identified, latest .