

Stealth Exploitation: WordPress Configuration and SQL Database

Monitoring Overview & User Access

- SQL Database Alert
- Monitor server traffic for unauthorized attempts to access SQL Database
- Triggers when external/unauthorized IP connections are made to the SQL Database or any related files.
- Least privilege should be used in this case to restrict user access to the configuration file.

Mitigating Detection

- Employ IP address spoofing
- Brute-force SQL Database with Password cracking tool, Connect to the same network