Audit conducted by: Marshall Whittaker

Audit: businesslistingsite.com

* + PHP 7.4.33, LiteSpeed httpd, OpenSSH 8.0, MariaDB 11.8.3, ProFTPd (guessing it runs Linux)
  + Backend database host db.capitalb.ca
  + SQLi confirmed in https://db.capitalb.ca/src/functions/getListings.php (POST req, search param)
  + 19 password hashes recovered
  + Database plugins in use: mysql\_native\_password, mysql\_old\_password, binlog, THREAD\_POOL\_WAITS, partition, cgroup
  + Large amount of database data exfiltrated (dbs - information\_schema, u346308959\_bd)
  + SSH server runnning on nonstandard port 65002 (accepts both pubkey and password auth)
  + MySQLd listening on public interface
  + The user julie@capitalb.ca from database references probably cooresponds to Julie Breton (name found from exif data of png logo image)
  + Lots of logins to the server from Montreal, Canada and Lago Vista, USA.
  + Server admin’s ASN info: AS577 (Bell Canada)
  + Admin runs Ubuntu on dev boxaccess the web.
  + Machine hostname: us-phx-web736.main-hosting.eu
  + /srv/mariadb1183 (exists)
  + SSL Keys location: /var/lib/mysql/ssl/hostinger.key and /var/lib/mysql/ssl/tls-ca-bundle.pem
  + Dir writable by mysqld: /var/lib/mysqltmp