**Problem**

The *secrethash*, which the application relies for multiple security measures, can be brute forced. The hash is quite small, with only 10 characters of only hexadecimal, making 16^10 possibilities ( 1.099.511.627.776 ). The SHA1 of the secret can be obtained via a captcha string and brute-forced offline with an GPU.

**lhc\_web\cli\lib\install.php**

$cfgSite->setSetting( 'site', 'secrethash', **substr(md5(time() . ":" . mt\_rand()),0,10)**);

**lhc\_web\modules\lhinstall\install.php**

$cfgSite->setSetting( 'site', 'secrethash', (!empty(getenv('LHC\_SECRET\_HASH')) ? getenv('LHC\_SECRET\_HASH') : **substr(md5(time() . ":" . mt\_rand()),0,10)**));

**Fix**

**lhc\_web\cli\lib\install.php**

$cfgSite->setSetting( 'site', 'secrethash', **erLhcoreClassChat::generateHash(80)**)

**lhc\_web\modules\lhinstall\install.php**

$cfgSite->setSetting( 'site', 'secrethash', (!empty(getenv('LHC\_SECRET\_HASH')) ? getenv('LHC\_SECRET\_HASH') : **erLhcoreClassChat::generateHash(80)**));

16^80 possibilities (much safer)