LimeSurvey Security Settings

Most GemsTracker installations use a LimeSurvey installation. LimeSurvey is a separate program and is fairly secure out of the box. As GemsTracker does not store user identifying information in LimeSurvey this is usually sufficient. However, some simple measures exist that make the installation more secure.

Global settings in LimeSurvey

These are LimeSurvey settings that you can set after logging in to the administration panel.

If your surveys do not use any JavaScript, set **Filter HTML for XSS** to **Yes**.

Always set **Force HTTPS** to **On**.

Settings in config.php

The file `application/config/config.php` is created during the LimeSurvey installation. The file returns an array with settings.

In addition to those settings you can add other features to extend protection in several key areas.

- Add a new top level entry for `request` settings.
  - Set `enableCsrfValidation` to `true` for extra Cross Site Request Forgery protection.
  - Set `hostInfo` to your domain name including `https:` and trailing slash for Cross Site Scripting protection.
  - Create `csrfCookie` as an array containing your domain name for the `domain` element.
- Add a new top level `session` setting.
  - Create a `cookieParams` array that sets `secure` and `httponly` to `true` and `domain` to you domain for cookie protection.

These settings are usually not documented on the LimeSurvey site, but LimeSurvey uses the Yii framework and these settings are used by YII.

A full example return array looks like this:

```
return array(
  'components' => array(
      'db' => array(
        'connectionString' =>
'mysql:host=localhost;port=3306;dbname=example_ls_db;',
        'emulatePrepare' => true,
        'username' => 'example-ls-db',
        'password' => '12345',
        'charset' => 'utf8',
        'tablePrefix' => 'ls__',
      ),
```

```
'request' => array(
        'enableCsrfValidation' => true,
        'hostInfo' => 'https://www.example.com/',
        'csrfCookie' => array('domain' => 'www.example.com'),
),
     'session' => array (
        'cookieParams' => array(
          'secure' => true, // use SSL for cookies
          'httponly' => true, // Cookies may not be used by other protocols
- experimental
          'domain' => 'www.example.com',
        ),
      ),
      'urlManager' => array(
        'urlFormat' => 'path',
        'rules' => array(
      ),
    'showScriptName' => true,
    ),
  ),
  'config'=>array(
    'debug'=>0,
    'debugsql'=>0, // Set this to 1 to enanble sql logging, only active when
debug = 2
  )
);
```

Settings in .htaccess

Edit the file `.htaccess` in the LimeSurvey root directory and add this line to prevent frame based attacks:

```
Header append X-Frame-Options DENY
```

From:
https://gemstracker.org/wiki/ - **GemsTracker**

Permanent link:
https://gemstracker.org/wiki/doku.php?id=userzone:limesurvey_security_settings&rev=1488198775

Last update: **2020/03/12 12:08**