openresty / encrypted-session-nginx-module

encrypt and decrypt nginx variable values

59 commits 1 branch 3 releases 3 contributors

branch: master encrypted-session-nginx-module / +

Merge pull request #6 from bloodyKnuckles/patch-1 ...

agentzh authored on Jul 12, 2014 latest commit 387f23a837

src	fixed more warnings from the Microsoft C compiler. thanks Edwin Cleto…	a year ago
t	added (passing) tests for using "encrypted_session_expires" with "if".	2 years ago
util	feature: added debugging logs for expiration times during encryption …	2 years ago
.gitignore	updated .gitignore a bit.	2 years ago
README	Typography tweaks.	7 months ago
config	bugfix: the -lssl option broke nginx linking when --with-openssl=DIR …	3 years ago
valgrind.suppress	suppressed a valgrind false positive in libdl.	11 months ago

README

```
Name
    encrypted-session-nginx-module - encrypt and decrypt nginx variable values

    *This module is not distributed with the Nginx source.* See the
    installation instructions.

Status
```

```
    This module is production ready.

Synopsis

    # key must be of 32 bytes long
    encrypted_session_key "abcdefghijklmnopqrstuvwxyz123456";

    # iv must not be longer than 16 bytes
    #   default: "deadbeefdeadbeef" (w/o quotes)
    encrypted_session_iv "1234567812345678";

    # default: 1d (1 day)
    encrypted_session_expires 2; # in sec

    location /encrypt {
        set $raw 'text to encrypted'; # from the ngx_rewrite module
        set_encrypt_session $session $raw;
        set_encode_base32 $session; # from the ngx_set_misc module

        add_header Set-Cookie 'my_login=$session';  # from the ngx_headers module

        # your content handler goes here...
    }

    location /decrypt {
        set_decode_base32 $session $cookie_my_login; # from the ngx_set_misc module
        set_decrypt_session $raw $session;

        if ($raw = '') {
            # bad session
        }

        # your content handler goes here...
    }

Description
    This module provides encryption and decryption support for
    nginx variables based on AES-256 with Mac.

    This module is usually used with the ngx_set_misc module
    ( http://github.com/agentzh/set-misc-nginx-module )
    and the standard rewrite module's directives.
```

```
    This module can be used to implement simple user login and ACL.

    Usually, you just decrypt data in nginx level, and pass the uncrypted
    data to your FastCGI/HTTP backend, as in

       location /blah {
              set_decrypt_session $raw_text $encrypted;

              # this directive is from the ngx_set_misc module
              set_escape_uri $escaped_raw_text $raw_text;

              fastcgi_param QUERY_STRING "uid=$uid";
              fastcgi_pass unix:/path/to/my/php/or/python/fastcgi.sock;
       }

    Lua web apps running directly on ngx_lua can call
    this module's directives directly from within Lua code:

       local raw_text = ndk.set_var.set_decrypt_session(encrypted_text)

Directives
    encrypted_session_key
        set the key for the cipher (must be 32 bytes long)

    encrypted_session_iv
        set the init vector used for the cipher (must be no longer than 16 bytes)

    encrypted_session_expires
        set expiration time difference (in seconds)

        For example, consider the config

            encypted_session_expires 1d;

        When your session is being generated, ngx_encrypted_session will plant
        an expiration time (1 day in the future in this example) into the the
        encrypted session string, such that when the session is being decrypted
        later, the server can pull the expiration time out of the session and
        compare it with the server's current system time. No matter how you
        transfer and store your session, like using cookies, or uri args,
        or whatever.
```

```
        People may confuse this setting with the expiration date of http
        cookies. This directive simply controls when the session gets expired;
        it knows nothing about http cookies. Even if the end user intercepted
        this session from cookie by himself and uses it later manually, the
        server will still reject it when the expiration time gets passed.

    set_encrypt_session

    set_decrypt_session

Installation
    This module is bundled and enabled by default in the ngx_openresty bundle:

        http://openresty.org

    Alternatively, you can install this module with the official Nginx source code
    distribution like this:

    1. Grab the nginx source code from nginx.org (<http://nginx.org/ >), for
        example, the version 1.2.7 (see nginx compatibility),

    2. Grab the NDK module from GitHub:
        http://github.com/simpl/ngx_devel_kit

    3. and then build the source with this module:

        wget 'http://nginx.org/download/nginx-1.2.7.tar.gz'
        tar -xzvf nginx-1.2.7.tar.gz
        cd nginx-1.2.7/

        # Here we assume you would install you nginx under /opt/nginx/.
        ./configure --prefix=/opt/nginx \
            --add-module=/path/to/ngx_devel_kit \
            --add-module=/path/to/encrypted-session-nginx-module

        make
        make install

    Download the latest version of the release tarball of this module from
    encrypted-session-nginx-module file list
    (<http://github.com/agentzh/encrypted-session-nginx-module/tags >).
```

```
    OpenSSL should not be disabled in your Nginx build.

Compatibility
    The following versions of Nginx should work with this module:

    *   1.2.x (last tested: 1.2.7)

    *   1.1.x (last tested: 1.1.5)

    *   1.0.x (last tested: 1.0.11)

    *   0.9.x (last tested: 0.9.4)

    *   0.8.x (last tested: 0.8.54)

    *   0.7.x >= 0.7.46 (last tested: 0.7.68)

    Earlier versions of Nginx like 0.6.x and 0.5.x will *not* work.

    If you find that any particular version of Nginx above 0.7.44 does not
    work with this module, please consider reporting a bug.

Report Bugs
    Although a lot of effort has been put into testing and code tuning,
    there must be some serious bugs lurking somewhere in this module. So
    whenever you are bitten by any quirks, please don't hesitate to

    1.  send a bug report or even patches to <agentzh@gmail.com>,

    2.  or create a ticket on the issue tracking interface
        (<http://github.com/agentzh/encrypted-session-nginx-module/issues >)
        provided by GitHub.

Source Repository
    Available on github at agentzh/encrypted-session-nginx-module
    (<http://github.com/agentzh/encrypted-session-nginx-module >).

ChangeLog

Test Suite
    This module comes with a Perl-driven test suite. The test cases
```

```
    (<http://github.com/agentzh/encrypted-session-nginx-module/tree/master/test/t/ >
    ) are declarative
    (<http://github.com/agentzh/encrypted-session-nginx-module/blob/master/test/t
/sanity.t >)
    too. Thanks to the Test::Base
    (<http://search.cpan.org/perldoc?Test::Base >) module in the Perl world.

    To run it on your side:

        $ cd test
        $ PATH=/path/to/your/nginx-with-encrypted-session-module:$PATH prove -r t

    Test::Nginx (<http://search.cpan.org/perldoc?Test::Nginx >) is used by
    the test scaffold.

    You need to terminate any Nginx processes before running the test suite
    if you have changed the Nginx server binary.

    Because a single nginx server (by default, "localhost:1984") is used
    across all the test scripts (".t" files), it's meaningless to run the
    test suite in parallel by specifying "-jN" when invoking the "prove"
    utility.

    Some parts of the test suite requires modules rewrite, and echo
    to be enabled as well when building Nginx.

TODO

Getting involved
    You'll be very welcomed to submit patches to the author or just ask for
    a commit bit to the source repository on GitHub.

Author
    Yichun "agentzh" Zhang (章亦春) *<agentzh@gmail.com>*

Copyright & License
    Copyright (c) 2009-2013, Yichun Zhang (agentzh) <agentzh@gmail.com>, Cloud
Flare Inc.

    This module is licensed under the terms of the BSD license.

    Redistribution and use in source and binary forms, with or without
```

```
    modification, are permitted provided that the following conditions are
    met:

    *   Redistributions of source code must retain the above copyright
        notice, this list of conditions and the following disclaimer.

    *   Redistributions in binary form must reproduce the above copyright
        notice, this list of conditions and the following disclaimer in the
        documentation and/or other materials provided with the distribution.

    THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS
    IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
    TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
    PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
    HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
    SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED
    TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
    PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
    LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
    NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
    SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

See Also
    * NDK: http://github.com/simpl-it/ngx_devel_kit
    * ngx_set_misc module: http://github.com/agentzh/set-misc-nginx-module
```