

Forum:[Hack Forums](#)

Thread: [Cryptomsg.cf](#) | [Destroyable Messages](#) | [Disposable Shoutbox](#) | [IP Logger](#) |

Tommy Chong - October 5, 2016, 4:11 pm

This is a little project I've been working on and I'm offering it free to use for everyone. I'll be improving it over time.

Current features:

Destroyable messages

Message tracker

Disposable Shoutbox

All messages are stored encrypted in the database using Rijndael 256 encryption

IP logger with multiple domains and extensions

Steff™ Wrote: The Encryption Key is now giving along with the created message and no longer stored anywhere

(Oct 5, 2016 04:20 AM)Steff™ Wrote: [\[CITE\]](#) Added a simple IP logger with the follow links to choose from:

zippyshare.cf

fileupload.ga

imageshare.cf

4cdn.cf (based of 4chan's 4cdn.org)

With the following extensions:

.jpg, .png, .gif, .php, .html, .mp3, .mp4, .exe, .rar, .zip, .webm

Mi2414 - October 5, 2016, 4:12 pm

Interesting, posting to read over later.

Orgy - October 5, 2016, 4:14 pm

does it encrypt the message server side or client side? same question for decryption

Tommy Chong - October 5, 2016, 4:15 pm

(Oct 5, 2016 04:14 PM)Orgy Wrote: [\[CITE\]](#) does it encrypt the message server side or client side? same question for decryption
Server side ?

Orgy - October 5, 2016, 4:15 pm

(Oct 5, 2016 04:15 PM)Steff™ Wrote: [\[CITE\]](#) Server side ?

yeah fuck that

edit: follow up question: where do you store the encryption key?

SUI-3183372 - October 5, 2016, 9:23 pm

(Oct 5, 2016 04:15 PM)Orgy Wrote: [\[CITE\]](#) yeah fuck that
edit: follow up question: where do you store the encryption key?
On a separate server directly connected to the main server.

I wonder if it'd be a good idea if you could set your own key? Nah.... probably not. Too secure.

Orgy - October 5, 2016, 9:24 pm

(Oct 5, 2016 09:23 PM)Previously Known As.... Wrote: [\[CITE\]](#) On a separate server directly connected to the main server.

Ah so if the anyone takes the main box they can easily access the keys and therefore decrypt everything?

AnonymousDownload - October 5, 2016, 9:43 pm

Very interesting. If you choose the message to be destroyed upon reading, does it still have a log or a way to be viewed if someone takes the main box as Orgy theorized?

Most of whom I speak with where I'm concerned about utmost security is on these forums...so for me our HF XMPP works great.

I've been seeing most people abandon all security and just jump to skype though. Is this as commonplace as I've been seeing?

SwordofJustice - October 5, 2016, 9:56 pm

Just a suggestion for your destroyable messages, you might want to make it so that when someone clicks on the message, it redirects them to a generic url so that the message cannot be tied to anyone sending it through IMs / PMs.

Tommy Chong- - October 5, 2016, 11:07 pm

(Oct 5, 2016 09:26 PM)Yani Wrote: [\[CITE\]](#) Seems like it.

Only way of being safe with stuff like this is keeping the encryption, decryption, and key client side (javascript).

I'll be looking into this.

This is the first thing I ever actually coded so I'm sorry if it's not what you've expected.
Messages that are destroyed can't be decrypted because they simply don't exist anymore.

Tommy Chong- - October 6, 2016, 12:40 am

(Oct 6, 2016 12:33 AM)Yani Wrote: [\[CITE\]](#) I don't suggest doing anything security related if you're new to coding.

But, as it's definitely a nice project, look at how privnote handles it;

You enter your message and when you submit it to the server, javascript in the client's browser encrypts said message.

The message is sent to their servers, without any sort of encryption key that's being stored.

The key is displayed using javascript, and is added to the generated url after the # character (which is a Fragment identifier).

This key is not sent to the server, but can be accessed by javascript.

Thus the client loads the generated url and gets the message that was encrypted. The key is then used by javascript to decrypt the message.

(An extra failsafe is added to the message to make sure decryption was successful, a simple string would be perfectly fine)

This is how a safe "encrypted note" website works, and should only work.

Good luck.

Alright, thanks for taking your time to explain this

I'll take my time to look into this and implement it if I'm able to in the future.

I understand the way how I approached it isn't the most secure way, but it's better than nothing I guess.

Anyways, +1

Orgy - *October 6, 2016, 5:21 pm*

(Oct 6, 2016 12:40 AM)Steff™ Wrote: [\[CITE\]](#) I understand the way how I approached it isn't the most secure way, but it's better than nothing I guess.

Anyways, +1

I disagree. Providing a false sense of security is worse than providing no security.

Tommy Chong- *October 14, 2016, 3:16 am*

The encryption key is now given along with the encrypted message and no longer stored in any database

Tommy Chong- *November 6, 2016, 8:55 am*

Updated IP logging links as cloudflare anally penetrated me.