

Forum:[Hack Forums](#)

Thread: [SecurePaste.net - AES encrypted paste and file hosting - Completely open source, too!](#)

observers.watch - September 14, 2012, 8:55 pm

[SecurePaste](#)

Still working on the file storage. File encryption works right now, but I haven't put a page in for actually retrieving your uploaded files yet. Sorry, it'll be done in an hour or so and I'll edit the thread accordingly.

Also, if you're interested in the source of any page, click the "src?" down at the bottom. It's a quine, it prints it's own (unformatted, unfortunately) source. (Source will be formatted later with the GeSHi syntax highlighting library.)

Feel free to make any suggestions for new features that you'd like!

How paste storage/retrieval works:

Storage:

User enters paste data, password, and Captcha

Paste data is AES-256 encrypted with the user's provided password (done via PHPseclib)

Encrypted data is converted to base64 (to solve compatibility issues with the characters that encrypted shit comes out as)

Base64'd data is stored in a MySQL DB

Retrieval:

User gets a link to a paste

User enters a password

If the password is correct, proceed. If not, they're shown an error.

Base64 data is retrieved from database and converted into encrypted text

Password is used to decrypt plaintext

Plaintext is shown to user

How file storage/retrieval will work once fully implemented:

Storage:

User enters a file, a password, and fills out a Captcha

File is moved to an alternate directory and given a 32 character random name (file extension is kept)

in-tact)

File's contents are read using `file_get_contents()`, then that data is encrypted with the provided password

The data is converted into base64 (again, for compatibility reasons with MySQL)

The data + some info about the file is stored in the MySQL DB for retrieval later

Retrieval:

User is given a link to a file

User enters password; if the password is correct, proceed to 3

Data from MySQL DB is decoded and then decrypted with the pass the user provided

Data is assembled into a file with a random name (but the appropriate extension)

User is linked to that file

120 seconds after the download link is clicked, the file given to the user is deleted (But can be recreated again under a different name if the user enters the password again, of course)

GreyPhantom - September 19, 2012, 2:12 am

A Chinese Website. :3

You are kidding right?

observers.watch - September 19, 2012, 1:26 pm

(Sep 19, 2012 02:12 AM)GreyPhantom Wrote: [\[CITE\]](#) A Chinese Website. :3

You are kidding right?

What are you talking about? Did you go to securepaste.com or something? Cause my site is securepaste.net.

GodlikeGuy - September 21, 2012, 8:57 am

This is actually really good, I prefer Obin though.

PhineasPhreak - September 21, 2012, 2:36 pm

Bookmarked but not really sure when I will ever need an encrypted paste.

badbrains - September 21, 2012, 10:12 pm

You should upgrade to MySQLi or PDO. MySQL 4 is outdated and soon to be removed from the PHP extensions.

observers.watch - September 25, 2012, 4:46 am

Anybody got any other features they'd like to see on the site? I need something to do with my time.

Thanksgiving - September 25, 2012, 4:47 am

Wait like the 2nd person to post said... a Chinese website really? Imfao!

observers.watch - *September 28, 2012, 8:48 pm*

Just overhauled several pages on the site, and added a full login and registration system with email verification! :D Site looks much better now.