

Forum:[Hack Forums](#)

Thread: [ViewMy.PM - Upload and view your private messages online! Fast, secure, and FREE!](#)

'Snorlax - January 23, 2014, 11:09 am

[ViewMy.PM](#) is a site where you can upload your exported MyBB private messages and view them at all time!

It works for every MyBB site out there, as long as you can export the messages as .csv!

The user passwords are encrypted with SHA-256 and a salt. Your passwords will therefore be secure!

The CSV file names are encoded with many different characters, so people will not be able to guess the name of the file and steal your messages!

To export your messages on Hack Forums, you simply go to <https://hackforums.net/private.php?action=export> and do this: <https://puu.sh/6vrzc.png>

Basically select .csv at the bottom and disregard date! That way you will get all the private messages!

A HUGE thanks to my buddy [1n9i9c7om](#) for coding the user, upload, and PHP backend system! Without him this would not have been released!

FeaturesUpload .CSV files and name them

Read private messages on-the-go

Delete .CSV files

Search between messages quickly

.CSV manager

User system

Image previews

Again a HUGE thanks to [1n9i9c7om](#) for making the backend PHP stuff!

Known bugs [\(Click to View\)](#) When you are using the search feature, there is a slight chance that the first message (latest message of your PMs) will be on top

If you have the LastPass plugin installed, there is a chance your messages can look like this:

<https://puu.sh/6vqf7.png> - Currently only when you see an email

1n9i9c7om - January 23, 2014, 11:10 am

Finally you released it. :3

Don't worry about your passwords or whatever... passwords are hashed with a salt, the website is secure and nobody cares about your PMs :3

Only you can view your PMs, so enjoy. ;)

If you find any bugs, report them. :)

Cryptic™ - January 23, 2014, 11:30 am

This is good, but what would make it even better is if u made it look like HFES's pretty PMs.

Or if you had an option to change the PM style, so people can choose if they want the default, or pretty pm.

'Snorlax - January 23, 2014, 11:39 am

(Jan 23, 2014 12:30 PM)Cryptic™ Wrote: [\[CITE\]](#) This is good, but what would make it even better is if u made it look like HFES's pretty PMs.

Or if you had an option to change the PM style, so people can choose if they want the default, or pretty pm.

I can look into that! Should not be a problem ;)

OldFag - January 23, 2014, 11:41 am

Yes I will download my private messages from here and upload them somewhere else so I can view them.

'Snorlax - January 23, 2014, 11:43 am

(Jan 23, 2014 12:41 PM)OldFag Wrote: [\[CITE\]](#) Yes I will download my private messages from here and upload them somewhere else so I can view them.

I can feel a large amount of irony in that post.

A lot of people (like myself), like to store PMs a place where they can be read easily.

Therefore I made this site, so you do not have to view them in a bad way through Notepad or Excel!

Cryptic™ - January 23, 2014, 11:45 am

(Jan 23, 2014 12:41 PM)OldFag Wrote: [\[CITE\]](#) Yes I will download my private messages from here and upload them somewhere else so I can view them.

Well you do have a point, a lot of people would be comfortable if nothing get's stored on the server. So people can upload the file, site reads the file, displays it, deletes the file.

If people reload/close the browser, they will have to do it all over again.

I'm pretty sure more people will like it that way.

Maybe Snorlax can make a guest only mode, so ppl can upload the file, see it in their browser, and as soon as they close their browser or leave the page, it will all be gone.

If people want to store them on the server in their user account, it's their choice.

? BoxyBabee ? - January 23, 2014, 11:46 am

This is pretty fuckin' awesome.

Thanks for releasing this, I know I'll use it in the future.

'Snorlax - January 23, 2014, 11:48 am

(Jan 23, 2014 12:45 PM)Cryptic™ Wrote: [\[CITE\]](#) Well you do have a point, a lot more people would be comfortable if nothing get's stored on the server. So people can upload the file, site reads the file, displays it, deletes the file.

If people reload/close the browser, they will have to do it all over again.

I'm pretty sure more people will like it that way.

Maybe Snorlax can make a guest only mode, so ppl can upload the file, see it in their browser, and as soon as they close their browser or leave the page, it will all be gone.

If people want to store them on the server in their user account, it's their choice.

What point would that make? If your account gets hacked through the site, they might as well hack your Hack Forums account.

You cannot even view the PMs if you get access to the server, because you would not know who they are from.

1n9i9c7om - January 23, 2014, 11:50 am

(Jan 23, 2014 12:41 PM)OldFag Wrote: [\[CITE\]](#) Yes I will download my private messages from here and upload them somewhere else so I can view them.

(Jan 23, 2014 12:45 PM)Cryptic™ Wrote: [\[CITE\]](#) Well you do have a point, a lot more people would be comfortable if nothing get's stored on the server. So people can upload the file, site reads the file, displays it, deletes the file.

If people reload/close the browser, they will have to do it all over again.

I'm pretty sure more people will like it that way.

Maybe Snorlax can make a guest only mode, so ppl can upload the file, see it in their browser, and as soon as they close their browser or leave the page, it will all be gone.

If people want to store them on the server in their user account, it's their choice.

One reason for this site is, that when you run out of PM space, you can store your PMs there, so you won't loose them.

But... of course it'd be possible to make it so that you upload it, read the PMs and delete it after that. We could add this as a guest mode -- but there's not much difference between uploading and deleting the CSV, except that you don't have to register. :P

What won't be possible is to prove that we really won't save the uploaded PMs, but seriously: Why should we? There's no need for us to read your PMs, we have better things to do. ;)

'Snorlax - January 23, 2014, 11:55 am

Or we could password protect all the CSV files to your account. Then you can only access it on the site if you enter your login password.

How does that sound?

1n9i9c7om - January 23, 2014, 11:56 am

(Jan 23, 2014 12:55 PM)Snorlax Wrote: [\[CITE\]](#) Or we could password protect all the CSV files to your account. Then you can only access it on the site if you enter your login password.

How does that sound?

Or - even better - an encryption key?

They'd enter it when they upload the file, and they have to enter it again to view the file.

We just have to prove that we aren't storing the key somewhere then. ?

'Snorlax - January 23, 2014, 11:58 am

(Jan 23, 2014 12:56 PM)1n9i9c7om Wrote: [\[CITE\]](#) Or - even better - an encryption key?

They'd enter it when they upload the file, and they have to enter it again to view the file.

We just have to prove that we aren't storing the key somewhere then. ?

Encrypt the key with SHA256 and a salt, then check if the encryption key they enter matches the one stored.

Like the login system basically.

1n9i9c7om - January 23, 2014, 12:01 pm

(Jan 23, 2014 12:58 PM)Snorlax Wrote: [\[CITE\]](#) Encrypt the key with SHA256 and a salt, then check if the encryption key they enter matches the one stored.

Like the login system basically.

No.

Encrypt the file with a custom encryption key chosen by the user.

Then, when they wanna open a CSV, they'll be forced to enter the encryption key, otherwise it'd be impossible to open it.

So even we won't be able to read them, much safe, very secure, such customer.

'Snorlax - January 23, 2014, 12:03 pm

(Jan 23, 2014 01:01 PM)1n9i9c7om Wrote: [\[CITE\]](#) No.

Encrypt the file with a custom encryption key chosen by the user.

Then, when they wanna open a CSV, they'll be forced to enter the encryption key, otherwise it'd be impossible to open it.

So even we won't be able to read them, much safe, very secure, such customer.

I am sure there is some way you can encrypt a file when the file is uploaded. In the whole uploading process.

Well I do not know. I suck at PHP D:

Nas - January 23, 2014, 12:03 pm

What would be cool if you added it on a userscript on HackForums. A page that looks just like HF and there will be a PM folder where you can store all your PM's but it wont really go in your PM space.

SIM-1166170 - January 23, 2014, 12:06 pm

Seems neat and cool. Good work 1n9i9c7om and 'Snotlax! ?

?XilluX - January 23, 2014, 12:10 pm

So yeah its quite a good Site, but if I register you are able to see my PM's, I have sent.

Sulfer - January 23, 2014, 12:12 pm

Nice this looks great :) will make an account ounce I get home. Thanks again :)

'Snorlax - January 23, 2014, 12:12 pm

(Jan 23, 2014 01:10 PM)?XilluX Wrote: [\[CITE\]](#) So yeah its quite a good Site, but if I register you are able to see my PM's, I have sent.

I would have access to a bunch of csv files, but I would not know which one would be you. I cannot even log in as you, because your password is hidden.

It is like trusting Facebook, forum owners, and so on that they will not read your private messages.

(Jan 23, 2014 01:03 PM)-Nas Wrote: [\[CITE\]](#) What would be cool if you added it on a userscript on HackForums. A page that looks just like HF and there will be a PM folder where you can store all

your PM's but it wont really go in your PM space.

Well yeah... Thing is just that I would still have to store them somewhere.

Maybe in future I will create an userscript for the site. We will see.

1n9i9c7om - January 23, 2014, 12:19 pm

(Jan 23, 2014 01:03 PM)Snorlax Wrote: [\[CITE\]](#) I am sure there is some way you can encrypt a file when the file is uploaded. In the whole uploading process.

Well I do not know. I suck at PHP D:

That's actually what I'm talking about. It encrypts the file and to open it, you have to enter the key you used to encrypt it.

Nothing saved.

To Cryptic and everyone who's interested - I'll talk with Snorlax about the guest access thingy tomorrow. :)

Tyl3r Durd3n - January 23, 2014, 12:20 pm

Looks cool if u don't like privacy i guess?

1n9i9c7om - January 23, 2014, 12:21 pm

(Jan 23, 2014 01:20 PM)Tyl3r Durd3n Wrote: [\[CITE\]](#) Looks cool if u don't like privacy i guess?

You didn't read anything in this thread, did you? ???

We would be ABLE to read PMs, but the CSV files have random file names after the upload - we don't know who uploaded which one.

Also, do you think we have no better things to do than reading PMs that are most likely random chats anyways?

It's like trusting any other site. They could even log your password. They could sell your data. They could basically do everything.

chrisman0091 - January 23, 2014, 12:23 pm

I personally think this is VERY cool and was personally thinking about this concept the other day(not creating it, couldnt to save my life haha). One cool feature(more of adding on to one I read earlier in thread) would be a userscript for HF itself, which could add a button in PMs next to export saying "export to ViewMy.PM" or similar, to automatically do it, and then you could add a button with the other links on top of page(Home, Contact, Upgrade, etc.) that leads to the login page. Which would just make using this more convenient for the overall HF use with this(:

1n9i9c7om - January 23, 2014, 12:26 pm

(Jan 23, 2014 01:23 PM)chrisman0091 Wrote: [\[CITE\]](#) I personally think this is VERY cool and was personally thinking about this concept the other day(not creating it, couldnt to save my life haha). One cool feature(more of adding on to one I read earlier in thread) would be a userscript for HF itself, which could add a button in PMs next to export saying "export to ViewMy.PM" or similar, to automatically do it, and then you could add a button with the other links on top of page(Home, Contact, Upgrade, etc.) that leads to the login page. Which would just make using this more convenient for the overall HF use with this(:

I agree - it'd be cool. 'Snorlax is better in making userscripts than I'm, he already said he's thinking about doing this :P

?XilluX - January 23, 2014, 12:28 pm

(Jan 23, 2014 01:12 PM)Snorlax Wrote: [\[CITE\]](#) I would have access to a bunch of csv files, but I would not know which one would be you. I cannot even log in as you, because your password is

hidden.

It is like trusting Facebook, forum owners, and so on that they will not read your private messages.

Well yeah... Thing is just that I would still have to store them somewhere.

Maybe in future I will create an userscript for the site. We will see.

We all know that forum owners, especially HF does read messages. Also it is just as simple for you as checking the username and the .csv file uploaded with this account.

Or you can search through the files for special keywords than look at the quote from who to whom, if the username is not available on HF. I personally would not really trust it, but I like the good job you have done!

'Snorlax - January 23, 2014, 12:31 pm

(Jan 23, 2014 01:28 PM)?XilluX Wrote: [\[CITE\]](#) We all know that forum owners, especially HF does read messages. Also it is just as simple for you as checking the username and the .csv file uploaded with this account.

Or you can search through the files for special keywords than look at the quote from who to whom, if the username is not available on HF. I personally would not really trust it, but I like the good job you have done!

I knew trust would be the biggest issue here.

I guess we have to figure something out.

What would it take for you guys to fully trust it? Give the csv files a password only you know?

1n9i9c7om - January 23, 2014, 12:37 pm

(Jan 23, 2014 01:31 PM)Snorlax Wrote: [\[CITE\]](#) I knew trust would be the biggest issue here.

I guess we have to figure something out.

What would it take for you guys to fully trust it? Give the csv files a password only you know?

Then we'd have to prove that we're not saving the encryption key anywhere. Would be hard as well.

You can't fully prove everything, a bit trust is always needed. ;) But I can understand everybody who is worried about the privacy, something HAS to be done. :P

?XilluX - January 23, 2014, 12:40 pm

No the thing is you can do this easily offline with other tools, where you don't have to upload it, but honestly why do I actually I care ? I don't actually need this though.

'Snorlax - January 23, 2014, 12:42 pm

(Jan 23, 2014 01:40 PM)?XilluX Wrote: [\[CITE\]](#) No the thing is you can do this easily offline with other tools, where you don't have to upload it, but honestly why do I actually I care ? I don't actually need this though.

Some input to improve it would be nice though.

Offline tool has been made. Price is 5 dollars though. I would rather make this and share it for free.

?XilluX - January 23, 2014, 12:43 pm

Alright here comes my input to improve: just change the style everything else is awesome.

chrisman0091 - January 23, 2014, 12:44 pm

Personally I trust this from your post count, awards, rep, and all the HQ stuff I've seen from you. Though not everybody can be randomly trusting so I can understand the worries. Though I also don't see the need to PM very sensitive info, might just be me though!

'Snorlax - January 23, 2014, 12:48 pm

(Jan 23, 2014 01:43 PM)?XilluX Wrote: [\[CITE\]](#) Alright here comes my input to improve: just change the style everything else is awesome.

The style... Hmm. I might change it around a bit. Not sure what to improve though.
I could make a theme changer.

(Jan 23, 2014 01:44 PM)chrisman0091 Wrote: [\[CITE\]](#) Personally I trust this from your post count, awards, rep, and all the HQ stuff I've seen from you. Though not everybody can be randomly trusting so I can understand the worries. Though I also don't see the need to PM very sensitive info, might just be me though!

Thank you very much! I completely agree with you.

I am not some scum who would go and read other people's PMs. I cannot see a reason for it to be honest.

chrisman0091 - January 23, 2014, 12:53 pm

(Jan 23, 2014 01:48 PM)Snorlax Wrote: [\[CITE\]](#) The style... Hmm. I might change it around a bit. Not sure what to improve though.

I could make a theme changer.

Thank you very much! I completely agree with you.

I am not some scum who would go and read other people's PMs. I cannot see a reason for it to be honest.

Yeah, not much you could get out of PMs imo...

Also for the style, I think maybe he means something along the lines of CSS additions.

Eeluminati - January 23, 2014, 12:58 pm

(Jan 23, 2014 12:43 PM)Snorlax Wrote: [\[CITE\]](#) I can feel a large amount of irony in that post.

A lot of people (like myself), like to store PMs a place where they can be read easily.

Therefore I made this site, so you do not have to view them in a bad way through Notepad or Excel!
I don't see why people can't just put their PM's in a notepad rather than uploading them to another members site?

Fishy/10

Tyl3r Durd3n - January 23, 2014, 12:58 pm

(Jan 23, 2014 01:21 PM)1n9i9c7om Wrote: [\[CITE\]](#) You didn't read anything in this thread, did you?
???

We would be ABLE to read PMs, but the CSV files have random file names after the upload - we don't know who uploaded which one.

Also, do you think we have no better things to do than reading PMs that are most likely random chats anyways?

It's like trusting any other site. They could even log your password. They could sell your data.

They could basically do everything.If a user uploads a file nothing is stored? Not even the transfer logs?

And yes if u could make money selling the data there is not a doubt in my mind you would read them I know i certainly would. Also most sites are under some sort of agreement when it comes to personal data.

Not bashing thread or site it will help out alot of people I personally just dont like data mining .

Squidward - January 23, 2014, 1:00 pm

Hmm, this is some shady shit right here.

'Snorlax - January 23, 2014, 1:06 pm

(Jan 23, 2014 01:58 PM)Eeluminati Wrote: [\[CITE\]](#) I don't see why people can't just put their PM's in a notepad rather than uploading them to another members site?

Fishy/10

Because reading the PMs through notepad or Excel is really frustrating.

(Jan 23, 2014 01:58 PM)Tyl3r Durd3n Wrote: [\[CITE\]](#) And yes if u could make money selling the data there is not a doubt in my mind you would read them I know i certainly would. Also most sites are under some sort of agreement when it comes to personal data.

Well you are a scum then. That is the difference between you and me.

I would be happy to make an agreement. I will not read the files. Adding an agreement will not make it less fishy.

(Jan 23, 2014 02:00 PM)Squidward Wrote: [\[CITE\]](#) Hmm, this is some shady shit right here.

Feel free not to use the site then. I am not forcing anyone to use it.

Obfuscated userscripts are more fishy to be honest. They can access everything on your HF profile FYI. That is one of the reasons why I do not obfuscate my many many userscripts.

Illuminati™ - January 23, 2014, 1:27 pm

(Jan 23, 2014 12:41 PM)OldFag Wrote: [\[CITE\]](#) Yes I will download my private messages from here and upload them somewhere else so I can view them.

(Jan 23, 2014 01:20 PM)Tyl3r Durd3n Wrote: [\[CITE\]](#) Looks cool if u don't like privacy i guess?

I don't want to be a dick or something but honestly I have never laughed this much over something that I've read on the Internet. Oh god I love HF douches.

killerxknight - January 23, 2014, 5:26 pm

Dosen't work for me i export my Pm to .CSV Format but when import it to Viewmypm i get this

Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator, root@localhost and inform them of the time the error occurred, and anything you might have done that may have caused the error.

More information about this error may be available in the server error log.

'Snorlax - January 23, 2014, 10:00 pm

(Jan 23, 2014 06:26 PM)killerxknight Wrote: [\[CITE\]](#) Dosen't work for me i export my Pm to .CSV Format but when import it to Viewmypm i get this

Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator, root@localhost and inform them of the time the error

occurred, and anything you might have done that may have caused the error.

More information about this error may be available in the server error log.

Hmm odd. Try another browser. I am not getting this error.

killerxknight - January 23, 2014, 11:29 pm

(Jan 23, 2014 11:00 PM)Snorlax Wrote: [\[CITE\]](#) Hmm odd. Try another browser. I am not getting this error.Could i Show you this on TV maybe you know a way to fix it?

'Snorlax - January 23, 2014, 11:46 pm

(Jan 24, 2014 12:29 AM)killerxknight Wrote: [\[CITE\]](#) Could i Show you this on TV maybe you know a way to fix it?

I really have no clue why it will not work. It has worked for everyone else.

Try another browser and report back! :)

killerxknight - January 23, 2014, 11:54 pm

(Jan 24, 2014 12:46 AM)Snorlax Wrote: [\[CITE\]](#) I really have no clue why it will not work. It has worked for everyone else.

Try another browser and report back! :)Firefox And Chrome Both don't work So. I Can give you my TV Details and you can see me upload .CSV again and trying to browse my pms?

'Snorlax - January 24, 2014, 12:02 am

(Jan 24, 2014 12:54 AM)killerxknight Wrote: [\[CITE\]](#) Firefox And Chrome Both don't work So. I Can give you my TV Details and you can see me upload .CSV again and trying to browse my pms?

Can you try one last time? I am checking the apache error log, but I am not getting anything.

killerxknight - January 24, 2014, 12:09 am

(Jan 24, 2014 01:02 AM)Snorlax Wrote: [\[CITE\]](#) Can you try one last time? I am checking the apache error log, but I am not getting anything.Just Tried it again and still receiving this error?

'Snorlax - January 24, 2014, 12:15 am

(Jan 24, 2014 01:09 AM)killerxknight Wrote: [\[CITE\]](#) Just Tried it again and still receiving this error? Really odd.. Really. I see nothing out of the ordinary.

How big is your file?

killerxknight - January 24, 2014, 12:17 am

(Jan 24, 2014 01:15 AM)Snorlax Wrote: [\[CITE\]](#) Really odd.. Really. I see nothing out of the ordinary. How big is your file?The File is 181 KB with like 250+ Pms

'Snorlax - January 24, 2014, 12:18 am

(Jan 24, 2014 01:17 AM)killerxknight Wrote: [\[CITE\]](#) The File is 181 KB with like 250+ Pms If you would not mind, please try and send me the file in a PM.

I will not look at the file. I am not sure what would happen if you password protect it, but feel free to try.

g0han - January 24, 2014, 12:19 am

No offense but i think you should think a bit more about the design of the site ? A little logo on the left and background pattern instead of solid colour would do wonders, PM me if you need some GFX Ill gladly do it for free

Other than that nice site and idea!

Insanity? - January 24, 2014, 12:21 am

This will be very useful to most users, thanks for the great share man!

'Snorlax - January 24, 2014, 12:21 am

(Jan 24, 2014 01:19 AM)instxgram Wrote: [\[CITE\]](#) No offense but i think you should think a bit more about the design of the site :D A little logo on the left and background pattern instead of solid colour would do wonders, PM me if you need some GFX Ill gladly do it for free

Other than that nice site and idea!

I am not looking for fancy graphics. I was going for a notepad look, and I think I hit it pretty good. Selector on the left and content on the right.

http://sdsblog.files.wordpress.com/2010/04/l_640_480_7ae7f8b1-06e5-4195-8391-558980a262b8.jpg

This is what I was going for ;)

killerxknight - January 24, 2014, 12:23 am

(Jan 24, 2014 01:18 AM)Snorlax Wrote: [\[CITE\]](#) If you would not mind, please try and send me the file in a PM.

I will not look at the file. I am not sure what would happen if you password protect it, but feel free to try.I've Sent you the Pm.CSV containing my pms.

'Snorlax - January 24, 2014, 1:50 am

(Jan 24, 2014 01:23 AM)killerxknight Wrote: [\[CITE\]](#) I've Sent you the Pm.CSV containing my pms. Looked into it and I fixed the issue. It was a PHP mistake, which I fixed by letting Javascript take care of it.

My mate and I will look into inserting the CSV content into the database and then encode it. Then people will have their privacy all by themselves.

Zyzz™ - January 24, 2014, 1:52 am

Cool site but you should work more on the design tbh.

'Snorlax - January 24, 2014, 1:56 am

(Jan 24, 2014 02:52 AM)Zyzz™ Wrote: [\[CITE\]](#) Cool site but you should work more on the design tbh. I personally like the design. So unless I get some more information about what to change, I am not going to worry about it ;)

Give me some constructive criticism! ;)

Trafz - January 24, 2014, 2:30 am

Well damn, it appears we are back in the 90s.

'Snorlax - January 24, 2014, 2:43 am

(Jan 24, 2014 03:30 AM)Trafz Wrote: [\[CITE\]](#) Well damn, it appears we are back in the 90s. What is that supposed to mean? I am not really sure.

Uhm... While fixing the security I accidentally truncated the wrong table. So your uploads are gone, which I cannot do anything about.. Sorry.

It will not happen again.

1n9i9c7om - January 24, 2014, 5:22 am

(Jan 24, 2014 03:43 AM)Snorlax Wrote: [\[CITE\]](#) What is that supposed to mean? I am not really sure. He was talking about the design ?

(Jan 24, 2014 02:50 AM)Snorlax Wrote: [\[CITE\]](#) Looked into it and I fixed the issue. It was a PHP mistake, which I fixed by letting Javascript take care of it.
Mind sending me a PM telling me what was wrong? ?

(Jan 24, 2014 02:50 AM)Snorlax Wrote: [\[CITE\]](#) My mate and I will look into inserting the CSV content into the database and then encode it. Then people will have their privacy all by themselves. Every PM in a row or did you mean "save the contents of the CSV in a string and encrypt it, then save it"? ?

'Snorlax - January 24, 2014, 7:59 am

(Jan 24, 2014 06:22 AM)1n9i9c7om Wrote: [\[CITE\]](#) He was talking about the design ?

Mind sending me a PM telling me what was wrong? ?

Every PM in a row or did you mean "save the contents of the CSV in a string and encrypt it, then save it"? ?

1. Oh damn. It is classic though!
2. IM'd!
3. Every PM in a row yes.

Guys: So far I have successfully imported a CSV file into the database and encrypted EVERY message using XOR.

The encryption key (you decide) is not stored anywhere, and the messages cannot be decrypted unless it is being brute forced.

Your messages will therefore be hidden like this:

That is 14 messages. If you have the XOR key you can decrypt the message. I will make some changes on the site with my mate [Doctor Blue](#), and we will implent this in the near future.

To be absolutely clear: I, or anybody else, will not be able to view your messages without knowing your encryption key. There is no way I would be able to do that.

Your messages will be safe with me.

iKinky - January 24, 2014, 1:46 pm

(Jan 24, 2014 01:19 AM)instxgram Wrote: [\[CITE\]](#) No offense but i think you should think a bit more about the design of the site ? A little logo on the left and background pattern instead of solid colour would do wonders, PM me if you need some GFX Ill gladly do it for free

Other than that nice site and idea!

It's not like he's making people pay for it, I don't really think the aesthetics are a big deal as long as it works.

badbrains - January 24, 2014, 2:11 pm

(Jan 23, 2014 12:43 PM)Snorlax Wrote: [\[CITE\]](#) I can feel a large amount of irony in that post.

A lot of people (like myself), like to store PMs a place where they can be read easily.

Therefore I made this site, so you do not have to view them in a bad way through Notepad or Excel!

To be honest, I don't think this will ignite. It is more safe to keep your private messages on the website they belong to, and it doesn't really make it any easier to view them.

edit: I see that you are encrypting private messages. I still don't think this makes reading PMs any easier. It's good as an archive, though. Is that what it's intended purpose is?

chrisman0091 - January 24, 2014, 2:13 pm

(Jan 24, 2014 03:11 PM)Wolf Haley Wrote: [\[CITE\]](#) I think you mean sarcasm.

To be honest, I don't think this will ignite. It is more safe to keep your private messages on the website they belong to, and it doesn't really make it any easier to view them.

edit: I see that you are encrypting private messages. I still don't think this makes reading PMs any easier. It's good as an archive, though. Is that what it's intended purpose is? No, he is right. Sarcasm is another word for verbal irony, which is what it really is.

OT: Personally I think it IS easier to read than just opening it in Notepad like normal. And keeping PMs on-site isn't always an option, as PM boxes fill (especially for people who aren't upgraded).

badbrains - January 24, 2014, 2:17 pm

(Jan 24, 2014 03:13 PM)chrisman0091 Wrote: [\[CITE\]](#) No, he is right. Sarcasm is another word for verbal irony, which is what it really is.

OT: Personally I think it IS easier to read than just opening it in Notepad like normal.
Yes, you are right. My mistake ?
I should have thought about it more.

'Snorlax - January 24, 2014, 2:17 pm

(Jan 24, 2014 03:13 PM)chrisman0091 Wrote: [\[CITE\]](#) No, he is right. Sarcasm is another word for verbal irony, which is what it really is.

OT: Personally I think it IS easier to read than just opening it in Notepad like normal. And keeping PMs on-site isn't always an option, as PM boxes fill (especially for people who aren't upgraded).
Well we are a few people who disagree then! ;)

(Jan 24, 2014 03:11 PM)Wolf Haley Wrote: [\[CITE\]](#) I think you mean sarcasm.

To be honest, I don't think this will ignite. It is more safe to keep your private messages on the website they belong to, and it doesn't really make it any easier to view them.

edit: I see that you are encrypting private messages. I still don't think this makes reading PMs any easier. It's good as an archive, though. Is that what it's intended purpose is?
The purpose was to upload and store your archives, and then view them globally wherever you go. The messages will be even more secure than on HF.
Imagine if your VMP (ViewMyPM) account got hacked. The hacker would have to know the encryption key for your archives, and without it, it is worthless.

badbrains - January 24, 2014, 2:20 pm

(Jan 24, 2014 03:17 PM)Snorlax Wrote: [\[CITE\]](#) Well we are a few people who disagree then! ;)

The purpose was to upload and store your archives, and then view them globally wherever you go. The messages will be even more secure than on HF.

Imagine if your VMP (ViewMyPM) account got hacked. The hacker would have to know the encryption key for your archives, and without it, it is worthless.

Can you have multiple keys for different inboxes (CSVs from different websites)?

'Snorlax - January 24, 2014, 2:22 pm

(Jan 24, 2014 03:20 PM)Wolf Haley Wrote: [\[CITE\]](#) Can you have multiple keys for different inboxes (CSVs from different websites)?

That is what I would like to achieve. So far it is still in development, so a lot could change (such as better encryption).

badbrains - January 24, 2014, 2:25 pm

(Jan 24, 2014 03:22 PM)Snorlax Wrote: [\[CITE\]](#) That is what I would like to achieve. So far it is still in development, so a lot could change (such as better encryption).

Okay. Another thing I would like to point out is that I was not prompted to enter any encryption key. That leads me to believe that they are decrypted by the server.

Another issue: XSS. Look at this.

'Snorlax - January 24, 2014, 2:41 pm

(Jan 24, 2014 03:25 PM)Wolf Haley Wrote: [\[CITE\]](#) Okay. Another thing I would like to point out is that I was not prompted to enter any encryption key. That leads me to believe that they are decrypted by the server.

Another issue: XSS. Look at this.

It has not been released, so there is no encryption system yet.

Hmm... I did do htmlspecialchars() and stripslashes()... Hmm.

badbrains - January 24, 2014, 2:47 pm

(Jan 24, 2014 03:41 PM)Snorlax Wrote: [\[CITE\]](#) It has not been released, so there is no encryption system yet.

Hmm... I did do htmlspecialchars() and stripslashes()... Hmm.
Oh. That sucks.

Don't bother with stripslashes().
Just use htmlentities().

VodkaNik - January 24, 2014, 2:50 pm

Tbh, most people will not use this simply because of how easy it is to take down. P.s I don't mean ddos.

'Snorlax - January 24, 2014, 2:50 pm

(Jan 24, 2014 03:47 PM)Wolf Haley Wrote: [\[CITE\]](#) Oh. That sucks.

Don't bother with stripslashes().
Just use htmlentities().
Well yeah. I do not know. I did not create the backend stuff.

Any idea why XSS is possible then? ?

(Jan 24, 2014 03:50 PM)VodkaNik Wrote: [\[CITE\]](#) Tbh, most people will not use this simply because of how easy it is to take down. P.s I don't mean ddos.

Then what do you mean? Please elaborate.

Johnny Ramone - January 24, 2014, 2:51 pm

Are the PMs encrypted on the server?

badbrains - January 24, 2014, 2:54 pm

(Jan 24, 2014 03:50 PM)Snorlax Wrote: [\[CITE\]](#) Any idea why XSS is possible then? ?
No, I did not create the back end stuff. ? Probably just a small error.

'Snorlax - January 24, 2014, 2:55 pm

(Jan 24, 2014 03:51 PM)P?lpF?c??? Wrote: [\[CITE\]](#) Are the PMs encrypted on the server?
Not yet. So unless somebody gets access to your account, your PMs will be safe.

Read this: <https://hackforums.net/showthread.php?tid=4015844&pid=37898990#pid37898990>

(Jan 24, 2014 03:54 PM)Wolf Haley Wrote: [\[CITE\]](#) No, I did not create the back end stuff. ?
Probably just a small error.
Most likely. I hope so. Thanks for pointing out.

Do you mind sending me that code you used in a PM?

badbrains - January 24, 2014, 2:58 pm

(Jan 24, 2014 03:55 PM)Snorlax Wrote: [\[CITE\]](#) Not yet. So unless somebody gets access to your account, your PMs will be safe.

Read this: <https://hackforums.net/showthread.php?tid=4015844&pid=37898990#pid37898990>

Most likely. I hope so. Thanks for pointing out.

Do you mind sending me that code you used in a PM?

I imagine any HTML would work. But this is what it was in particular.

```
<iframe src=""></iframe>
```

Null Byte - January 24, 2014, 3:14 pm

Hm, I don't like the thought of my PMs being unencrypted and readable by anyone... I'm no expert in encryption but perhaps you could encrypt our passwords with our hashed password as the key (use new salt of course). I don't know. I just think security should be the #1 priority here.

BTW, do you guys have a github for this? Open source would be great.

'Snorlax - January 24, 2014, 3:20 pm

(Jan 24, 2014 03:58 PM)Wolf Haley Wrote: [\[CITE\]](#) I imagine any HTML would work. But this is what it was in particular.

```
<iframe src=""></iframe>
```

Looking into it. I found the issue! ;)

(Jan 24, 2014 04:14 PM)DogeCoin Wrote: [\[CITE\]](#) Hm, I don't like the thought of my PMs being unencrypted and readable by anyone... I'm no expert in encryption but perhaps you could encrypt our passwords with our hashed password as the key (use new salt of course). I don't know. I just think security should be the #1 priority here.

BTW, do you guys have a github for this? Open source would be great.

Unfortunately not. It is closed for now.

The encryption will be safe. Nobody will be able to decrypt your messages unless you use a bad password like 123.

Look up XOR ;) It will be secure. Trust me.

Null Byte - January 24, 2014, 3:24 pm

(Jan 24, 2014 04:20 PM)Snorlax Wrote: [\[CITE\]](#) Unfortunately not. It is closed for now.

The encryption will be safe. Nobody will be able to decrypt your messages unless you use a bad password like 123.

Look up XOR ;) It will be secure. Trust me.

Oh, really? I thought you only had encryption for passwords.

So even the people who have access to the server wont be able to read the PM logs?

'Snorlax - January 24, 2014, 3:26 pm

(Jan 24, 2014 04:24 PM)DogeCoin Wrote: [\[CITE\]](#) Oh, really? I thought you only had encryption for passwords.

So even the people who have access to the server wont be able to read the PM logs?

You are absolutely right!

<https://hackforums.net/showthread.php?tid=4015844&pid=37898990#pid37898990>

Take a look at the screenshot. Some of those are regular messages starting with [quote=... and so on.

It will not be readable by anyone but you, if you know the encryption key!

Null Byte - January 24, 2014, 3:40 pm

(Jan 24, 2014 04:26 PM)Snorlax Wrote: [\[CITE\]](#) You are absolutely right!

<https://hackforums.net/showthread.php?tid=4015844&pid=37898990#pid37898990>

Take a look at the screenshot. Some of those are regular messages starting with [quote=... and so on.

It will not be readable by anyone but you, if you know the encryption key!

Thanks, but how is that encryption key generated? Via our password?

'Snorlax - January 24, 2014, 3:42 pm

(Jan 24, 2014 04:40 PM)DogeCoin Wrote: [\[CITE\]](#) Thanks, but how is that encryption key generated? Via our password?

You enter an encryption key for your uploads, and then you would have to enter that key to unlock the messages (I guess unlocking to the session would be okay).

Okay so the XSS has been fixed. I have no idea why the first thing did not work... Do not ask me, lol.

Null Byte - January 24, 2014, 3:44 pm

(Jan 24, 2014 04:42 PM)Snorlax Wrote: [\[CITE\]](#) You enter an encryption key for your uploads, and then you would have to enter that key to unlock the messages (I guess unlocking to the session would be okay).

Okay so the XSS has been fixed. I have no idea why the first thing did not work... Do not ask me, lol.

Thanks for explaining everything, looks really HQ. BTW, I have a spare SSL cert if you want it feel free to PM me.

'Snorlax - January 24, 2014, 3:47 pm

(Jan 24, 2014 04:44 PM)DogeCoin Wrote: [\[CITE\]](#) Thanks for explaining everything, looks really HQ. BTW, I have a spare SSL cert if you want it feel free to PM me.

Oh interesting. My mate and I have our own hosting "company", so we get our certificates pretty

cheap.

I will shoot you a PM if I ever need it. Maybe we can make a deal ;) We will see.

sarciszewski - January 24, 2014, 4:51 pm

Hey, you should post the source code to github so we can evaluate it and run our own instance. Decentralized systems are very hard to backdoor ;)

Also, code auditing is a great community activity

'Snorlax - January 24, 2014, 4:55 pm

(Jan 24, 2014 05:51 PM)binary_paroxysm Wrote: [\[CITE\]](#) Hey, you should post the source code to github so we can evaluate it and run our own instance. Decentralized systems are very hard to backdoor ;)

Also, code auditing is a great community activity

It will not be open source at the moment.

sarciszewski - January 24, 2014, 4:57 pm

(Jan 24, 2014 05:55 PM)Snorlax Wrote: [\[CITE\]](#) It will not be open source at the moment.

https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle

Well, I would strongly advise everyone to not use this system until it has been open sourced. Otherwise, it's like sticking your dick into a stranger's asshole. You never know what you'll catch ;)

1n9i9c7om - January 24, 2014, 5:06 pm

(Jan 24, 2014 05:57 PM)binary_paroxysm Wrote: [\[CITE\]](#)

https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle

Well, I would strongly advise everyone to not use this system until it has been open sourced. Otherwise, it's like sticking your dick into a stranger's asshole. You never know what you'll catch ;)

So you're saying that you shouldn't use it because it's not open source? Please ask Mark Zuckerberg to release the Facebook Source. ?

--

I see where you come from, you want to be sure that the system is secure and even the people who have access to the can't read the PMS. You either trust this page or you don't, but you can't force us/'Snorlax to make it open source. ;)

sarciszewski - January 24, 2014, 5:08 pm

(Jan 24, 2014 06:06 PM)1n9i9c7om Wrote: [\[CITE\]](#) So you're saying that you shouldn't use it because it's not open source? Please ask Mark Zuckerberg to release the Facebook Source. ?

--

I see where you come from, you want to be sure that the system is secure and even the people who have access to the can't read the PMS. You either trust this page or you don't, but you can't force us/'Snorlax to make it open source. ;)Hehe. Show me my Facebook page and I'll concede your point :3

I'm glad you get it. Kerckhoff's Principle isn't as widely known as it ought to be.

Seems like you could use some help locking it down, though. I can help, but I don't contribute to closed source products. I'd be betraying years of GNU/Linux if I did ;)

1n9i9c7om - January 24, 2014, 5:13 pm

(Jan 24, 2014 06:08 PM)binary_paroxysm Wrote: [\[CITE\]](#) Seems like you could use some help

locking it down, though.

Nope. As you could see on a screenshot that 'Snorlax posted, he's already working on it. :)

'Snorlax - January 24, 2014, 5:13 pm

(Jan 24, 2014 06:08 PM)binary_paroxysm Wrote: [\[CITE\]](#) Seems like you could use some help locking it down, though. I can help, but I don't contribute to closed source products. I'd be betraying years of GNU/Linux if I did ;)

I am not interested in releasing this anytime soon. Why would I? I see no reason why I would. I could release the code for encrypting the messages (like 10-15 lines of code), but that is all you are going to get.

If you do not wish to help, that is all right. I am not asking for help, and I do not need more help.

Null Byte - January 24, 2014, 5:18 pm

(Jan 24, 2014 06:06 PM)1n9i9c7om Wrote: [\[CITE\]](#) So you're saying that you shouldn't use it because it's not open source? Please ask Mark Zuckerberg to release the Facebook Source. ?

It's funny because Facebook tracks us then sends the stuff to Big Data, advertisers, the NSA, employers, and god knows what else...

What I'm trying to say is that you should be very skeptical of closed source software, because you have to trust the word of the developer that it's actually private and secure. If this would go open source it would only improve your site!

Great work thus far ?

'Snorlax - January 24, 2014, 5:21 pm

(Jan 24, 2014 06:18 PM)DogeCoin Wrote: [\[CITE\]](#) It's funny because Facebook tracks us then sends the stuff to Big Data, advertisers, the NSA, employers, and god knows what else...

What I'm trying to say is that you should be very skeptical of closed source software, because you have to trust the word of the developer that it's actually private and secure. If this would go open source it would only improve your site!

Great work thus far ?

Let us say I do make it open source. What prevents me from using a modified version of the open source?

That is right. You always need to trust the developer. No matter what.

Infinity. - January 24, 2014, 7:35 pm

Don't use this ,Snorlax hax your account like this

jk, A huge vouch for my buddy here! Legitimate guy ^^

Xerif - January 24, 2014, 7:57 pm

But if I upload the exported PMs and then get a new PM, then it won't be on viewmy.pm.

Also, this thread shouldn't be in the lounge. It should be here [Website Construction](#)

Yummy - January 24, 2014, 7:58 pm

Hmm I'll consider using this. Really good program for the looks of it.

MillionaireBy30 - January 25, 2014, 2:51 am

I know you're saying trust you and all... and not trying to bash your service.. i don't know you or your reputation here... but i just wanted to comment.

it amazes me how trusting people are nowadays.

scam. - January 25, 2014, 3:40 am

Ahh so this is what you noobs were working on.

Spoiler ([Click to View](#))

Make it look better damn it!

'Snorlax - January 25, 2014, 3:42 am

(Jan 25, 2014 04:40 AM)Mael Wrote: [\[CITE\]](#) Ahh so this is what you noobs were working on.

Spoiler ([Click to View](#))

Make it look better damn it!

Tell me what to fix then, god damnit :(

scam. - January 25, 2014, 3:45 am

(Jan 25, 2014 04:42 AM)Snorlax Wrote: [\[CITE\]](#) Tell me what to fix then, god damnit :(Just the over all appeal. If you want to make it look like a notepad make like page lines, the title bar thing, etc. Right now it looks a little.... bland.

'Snorlax - January 25, 2014, 3:54 am

(Jan 25, 2014 04:45 AM)Mael Wrote: [\[CITE\]](#) Just the over all appeal. If you want to make it look like a notepad make like page lines, the title bar thing, etc. Right now it looks a little.... bland.

I was going for something like a notepad. Making the lines would make it look weird, because I do not know how I would do that without messing up the section between who wrote what.

I am probably going to do the thing Cryptic suggested the other day. Like HFES' pretty PMs. Phone texting style ;)

Automatic Coding - January 25, 2014, 4:07 am

I, in all honesty, think this is really poorly done. It requires me sending my data to your server, which, is a huge no-no. Why didn't you do it client-sided? Few examples of doing it client sided(ly):-

<http://www.html5rocks.com/en/tutorials/file/dndfiles/>

'Snorlax - January 25, 2014, 4:20 am

(Jan 25, 2014 05:07 AM)Automatic Coding Wrote: [\[CITE\]](#) I, in all honesty, think this is really poorly done. It requires me sending my data to your server, which, is a huge no-no. Why didn't you do it client-sided? Few examples of doing it client sided(ly):-

<http://www.html5rocks.com/en/tutorials/file/dndfiles/>

How are you going to view the PMs on another device then?

MillionaireBy30 - January 25, 2014, 4:22 am

honestly, ima just flat out say it.

the op is a hacker and clearly wants to read your messages. i cannot BELIEVE you guys can't see through this.

Automatic Coding - January 25, 2014, 4:27 am

(Jan 25, 2014 05:20 AM)Snorlax Wrote: [\[CITE\]](#) How are you going to view the PMs on another device then?

You don't, if you must, user remembers an encryption key, and, locally encrypts & decrypts files, so,

you only ever get an encrypted version (Refer to sites like 0bin).

Not the best, still allows you to exploit it, but, better than plaintext.

'Snorlax - January 25, 2014, 4:34 am

(Jan 25, 2014 05:27 AM)Automatic Coding Wrote: [\[CITE\]](#) You don't, if you must, user remembers an encryption key, and, locally encrypts & decrypts files, so, you only ever get an encrypted version (Refer to sites like 0bin).

Not the best, still allows you to exploit it, but, better than plaintext.

This was made so you can upload and view your private messages everywhere but also backup your messages.

No exploiting here.

1n9i9c7om - January 25, 2014, 5:18 am

(Jan 25, 2014 05:27 AM)Automatic Coding Wrote: [\[CITE\]](#) You don't, if you must, user remembers an encryption key, and, locally encrypts & decrypts files, so, you only ever get an encrypted version (Refer to sites like 0bin).

Not the best, still allows you to exploit it, but, better than plaintext.

I'm pretty sure you read the posts in this thread to realize that the encryption is already a work in progress, right?

Automatic Coding - January 25, 2014, 6:16 am

(Jan 25, 2014 06:18 AM)1n9i9c7om Wrote: [\[CITE\]](#) I'm pretty sure you read the posts in this thread to realize that the encryption is already a work in progress, right?

If you think I'm going to read 108 posts just so I can give my opinion, think again.

'Snorlax - January 25, 2014, 6:28 am

(Jan 25, 2014 07:16 AM)Automatic Coding Wrote: [\[CITE\]](#) If you think I'm going to read 108 posts just so I can give my opinion, think again.

I added the post stuff to the OP. It should be pretty visible now.

Thanks for your input though. Encryption is being worked on.

Privacy is key.

Automatic Coding - January 25, 2014, 6:33 am

(Jan 25, 2014 07:28 AM)Snorlax Wrote: [\[CITE\]](#) I added the post stuff to the OP. It should be pretty visible now.

Thanks for your input though. Encryption is being worked on.

Privacy is key.

Can I ask for the specification of the 'xor encryption' you're using? To me, it seems like there's a key space of 0xFF (One byte), E.G. 255 possible passwords. 255 possible passwords is nowhere near enough entropy to even be worth implementing, someone could crack that in under a millisecond.

RK 62 - January 25, 2014, 6:34 am

Awesome! I will look at this again once I have a web server. bookmarked

'Snorlax - January 25, 2014, 6:38 am

(Jan 25, 2014 07:33 AM)Automatic Coding Wrote: [\[CITE\]](#) Can I ask for the specification of the 'xor encryption' you're using? To me, it seems like there's a key space of 0xFF (One byte), E.G. 255

possible passwords. 255 possible passwords is no where near enough entropy to even be worth implementing, someone could crack that in under a millisecond.

I am not the guy who is doing the backend stuff, so I have no idea if it is secure. Of course I do to some degree.

PHP Code

```
<?php
function encXOR($str, $key){
    $output = "";
    for($i = 0; $i < strlen($str);$i++){
        for($j = 0; ($j < strlen($key) && $i < strlen($str)); $j++){
            $output .= $str{$i} ^ $key{$j};
        }
    }
    return $output;
}
```

That is for XOR. My friend said something about `mcrypt_encrypt()` being a lot more secure, but I have no idea. I will let him decide.

Automatic Coding - January 25, 2014, 6:45 am

(Jan 25, 2014 07:38 AM)Snorlax Wrote: [\[CITE\]](#) I am not the guy who is doing the backend stuff, so I have no idea if it is secure. Of course I do to some degree.

PHP Code

```
<?php
function encXOR($str, $key){
    $output = "";
    for($i = 0; $i < strlen($str);$i++){
        for($j = 0; ($j < strlen($key) && $i < strlen($str)); $j++){
            $output .= $str{$i} ^ $key{$j};
        }
    }
    return $output;
}
```

That is for XOR. My friend said something about `mcrypt_encrypt()` being a lot more secure, but I have no idea. I will let him decide.

Yeah, as thought, that only has a key length of 0xFF, I feared you'd do that. Honestly? If you can't implement proper encryption, don't bother. If you need help with proper encryption, feel free to post in the correct sections.

'Snorlax - January 25, 2014, 6:51 am

(Jan 25, 2014 07:45 AM)Automatic Coding Wrote: [\[CITE\]](#) Yeah, as thought, that only has a key length of 0xFF, I feared you'd do that. Honestly? If you can't implement proper encryption, don't bother. If you need help with proper encryption, feel free to post in the correct sections.

As I said: It is still under development. And I also said that he said something about `mcrypt_encrypt()`, which would be a lot better.

It is not done, so please do not judge it yet.

Automatic Coding - January 25, 2014, 6:59 am

(Jan 25, 2014 07:51 AM)Snorlax Wrote: [\[CITE\]](#) As I said: It is still under development. And I also said that he said something about `mcrypt_encrypt()`, which would be a lot better.

It is not done, so please do not judge it yet.

For reference, whatever the key is, it's just going to be a value from 0x00 to 0xFF (Because you're

just xoring the ASCII values of the characters together), for instance, say I had the password "S()UP3RI33tPassw0rd", right? Let's see the difference between this:-

Code package testRawr;

```
public class superPasswordEncrypt {
    public static void main(String[] args) {
        String myPassword = "S()UP3RI33tPassw0rd";
        String myText = "Super secret government data";
        for(char myChar:myText.toCharArray()) {
            int currentEncryptBlock = myChar;
            for(char myPassChar:myPassword.toCharArray()) {
                currentEncryptBlock ^= myPassChar;
            }
            System.out.print((char)currentEncryptBlock);
        }
    }
}
```

Output:-

Code ;>+<n=+-<+:n)!8+< #+ :n*/:/

And this:-

Code package testRawr;

```
public class encryptWith78 {
    public static void main(String[] args) {
        int password = 78; //Equal to "S()UP3RI33tPassw0rd", I think we can agree,
        S()UP3RI33tPassw0rd should be more secure than '78'.
        String myText = "Super secret government data";
        for(char myChar:myText.toCharArray()) {
            System.out.print((char)(myChar^password));
        }
    }
}
```

Output:-

Code ;>+<n=+-<+:n)!8+< #+ :n*/:/

And you say "Don't judge yet", but, you're the one advertising about it and posting imgaes, on top of that, YOU'RE STILL USING PHP CODE, THIS ISN'T CLIENT SIDED, MEANING IT MEANS NOTHING.

It HAS to be done in JavaScript, client-sidedly.

'Snorlax - January 25, 2014, 7:03 am

(Jan 25, 2014 07:59 AM)Automatic Coding Wrote: [\[CITE\]](#) And you say "Don't judge yet", but, you're the one advertising about it and posting imgaes, on top of that, YOU'RE STILL USING PHP CODE, THIS ISN'T CLIENT SIDED, MEANING IT MEANS NOTHING.

It HAS to be done in JavaScript, client-sidedly.

Has to be done with Javascript? What. Why is that?

I am the one advertising that it will be ENCRYPTED. I never said XOR is the one and true method we will be using for making it secure.

1n9i9c7om - January 25, 2014, 7:04 am

(Jan 25, 2014 08:03 AM)Snorlax Wrote: [\[CITE\]](#) Has to be done with Javascript? What. Why is that? Because that's the only way to prove that the encryption key isn't stored anywhere. ?

'Snorlax - January 25, 2014, 7:08 am

(Jan 25, 2014 08:04 AM)1n9i9c7om Wrote: [\[CITE\]](#) Because that's the only way to prove that the encryption key isn't stored anywhere. ?

I will be happy to release the encryption code, but I doubt you can achieve the same thing using Javascript.

I am not an expert in encryption (which is why I do not make it), but I would prefer PHP.

I guess it is up to people to decide.

VLAN - January 25, 2014, 7:16 am

Be good if you did a mobile application too in the future and introduced other software.

This is a great idea, it could kick off.

'Snorlax - January 25, 2014, 7:18 am

(Jan 25, 2014 08:16 AM)VLAN Wrote: [\[CITE\]](#) Be good if you did a mobile application too in the future and introduced other software.

This is a great idea, it could kick off.

You can view this on your phone if you want. Creating an application for each operating system would take a long time and cost a lot of money.

Han. - January 25, 2014, 7:20 am

(Jan 23, 2014 12:10 PM)1n9i9c7om Wrote: [\[CITE\]](#) nobody cares about your PMs :3

I wouldn't be so complacent about security. There's a lot of sensitive information being communicated through PMs.

'Snorlax - January 25, 2014, 7:30 am

(Jan 25, 2014 08:20 AM)Han. Wrote: [\[CITE\]](#) I wouldn't be so complacent about security. There's a lot of sensitive information being communicated through PMs.

Which is why I will make your private messages as secure as they can get.

Only you, or anyone with your encryption key and account info, will be able to view them.

Automatic Coding - January 25, 2014, 8:07 am

(Jan 25, 2014 08:03 AM)Snorlax Wrote: [\[CITE\]](#) Has to be done with Javascript? What. Why is that?

I am the one advertising that it will be ENCRYPTED. I never said XOR is the one and true method we will be using for making it secure.

Why does it have to be done in Javascript? Only client sided language that can achieve stuff like this.

(Jan 25, 2014 08:04 AM)1n9i9c7om Wrote: [\[CITE\]](#) Because that's the only way to prove that the encryption key isn't stored anywhere. ?

This. Has to be 100% client sided.

(Jan 25, 2014 08:08 AM)Snorlax Wrote: [\[CITE\]](#) I will be happy to release the encryption code, but I doubt you can achieve the same thing using Javascript.

I am not an expert in encryption (which is why I do not make it), but I would prefer PHP.

I guess it is up to people to decide.

Look at Lastpass, that's coded majority in JavaScript (Browser extensions)

Look at Blockchain, that's coded 100% in JavaScript (Everything is done locally)

Look at 0Bin, that's coded 100% in Javascript (Everything is done locally)

Etc...

(Jan 25, 2014 08:30 AM)Snorlax Wrote: [\[CITE\]](#) Which is why I will make your private messages as secure as they can get.

Only you, or anyone with your encryption key and account info, will be able to view them.

>Secure as they can get

>Using custom encryption (Not a standard like AES)

>Doing it server-sided

>Using a 0xFF (8 bit entropy) cipher key.

I'm not trying to mock you, but, seriously, do a tiny bit of research before posting, please? There are a bunch of open sourced, secure, javascript implementations of crypto related ideas on github. Hell, look at this:-

[BitAddress \(Click me!\)](#) ([Source \(Click me!\)](#)), it generates Bitcoin addresses & Private keys 100% with javascript, that's impressive, if I say so myself, but, it shows just what javascript can do.

If you want, I can link you to a bunch more sources, but, I feel you can search github on your own.

'Snorlax - January 25, 2014, 9:08 am

(Jan 25, 2014 09:07 AM)Automatic Coding Wrote: [\[CITE\]](#) Why does it have to be done in Javascript? Only client sided language that can achieve stuff like this.

This. Has to be 100% client sided.

Look at Lastpass, that's coded majority in JavaScript (Browser extensions)

Look at Blockchain, that's coded 100% in JavaScript (Everything is done locally)

Look at 0Bin, that's coded 100% in Javascript (Everything is done locally)

Etc...

>Secure as they can get

>Using custom encryption (Not a standard like AES)

>Doing it server-sided

>Using a 0xFF (8 bit entropy) cipher key.

I'm not trying to mock you, but, seriously, do a tiny bit of research before posting, please? There are a bunch of open sourced, secure, javascript implementations of crypto related ideas on github. Hell, look at this:-

[BitAddress \(Click me!\)](#) ([Source \(Click me!\)](#)), it generates Bitcoin addresses & Private keys 100% with javascript, that's impressive, if I say so myself, but, it shows just what javascript can do.

If you want, I can link you to a bunch more sources, but, I feel you can search github on your own.

Sorry I do not need advice from someone who is this blind.

Automatic Coding - January 25, 2014, 9:10 am

(Jan 25, 2014 10:08 AM)Snorlax Wrote: [\[CITE\]](#) Sorry I do not need advice from someone who is this blind.

If you're going to resort to playground insults when I'm trying to help you, then, as you request, I just simply won't.

K.ing - January 25, 2014, 9:12 am

Legit site snorlax.

Might have to check this out.

'Snorlax - January 25, 2014, 9:20 am

(Jan 25, 2014 10:12 AM)K.ing Wrote: [\[CITE\]](#) Legit site snorlax.

Might have to check this out.

Thanks! Feel free to check it out :)

Site is working as advertised!

'An0ny - January 25, 2014, 9:22 am

I wouldn't feel trusted by uploading my PM's to a 3rd party site :3

'Snorlax - January 25, 2014, 9:30 am

(Jan 25, 2014 10:22 AM)Anony? Wrote: [\[CITE\]](#) I wouldn't feel trusted by uploading my PM's to a 3rd party site :3

No problem. I do not force people to upload their PMs. It is a simple archive system with a viewer. That is pretty much all ?

'An0ny - January 25, 2014, 10:07 am

(Jan 25, 2014 10:30 AM)Snorlax Wrote: [\[CITE\]](#) No problem. I do not force people to upload their PMs. It is a simple archive system with a viewer. That is pretty much all ?

Joke, i don't have any exclusive PM's nor do i store on exclusive stuff on HF. Very nice site my friend, my danish pølse friend.

sarciszewski - January 25, 2014, 11:07 am

(Jan 25, 2014 07:38 AM)Snorlax Wrote: [\[CITE\]](#) I am not the guy who is doing the backend stuff, so I have no idea if it is secure. Of course I do to some degree.

PHP Code

```
<?php
function encXOR($str, $key){
    $output = "";
    for($i = 0; $i < strlen($str);$i++){
        for($j = 0; ($j < strlen($key) && $i < strlen($str)); $j++){
            $output .= $str{$i} ^ $key{$j};
        }
    }
    return $output;
}
```

That is for XOR. My friend said something about mcrypt_encrypt() being a lot more secure, but I have no idea. I will let him decide.Wow.

<http://www.php.net/manual/en/function.mcrypt-encrypt.php>

<http://www.php.net/manual/en/function.openssl-encrypt.php>

Use a standard crypto library. Don't try to roll out your own, unless you're a crypto expert.

MineSQL - January 27, 2014, 11:25 pm

I'm really sorry to say this, but stating:

Quote:The user passwords are encrypted with SHA-256 and a salt Totally ruined the significance of trying to save passwords in the database. The whole reason you encrypt passwords is so if/when a database get's cracked into, the hacker will have a hard time cracking the passwords. Not now though. At least you didn't release how you hashed the salt.

Message me if you want me to remove this, I just thought I should share this with you...

'Snorlax - January 28, 2014, 12:17 am

(Jan 28, 2014 12:25 AM)MineSQL Wrote: [\[CITE\]](#) I'm really sorry to say this, but stating:
Totally ruined the significance of trying to save passwords in the database. The whole reason you encrypt passwords is so if/when a database get's cracked into, the hacker will have a hard time cracking the passwords. Not now though. At least you didn't release how you hashed the salt.

Message me if you want me to remove this, I just thought I should share this with you...
I do not see how this would matter.

http://en.wikipedia.org/wiki/List_of_hash_functions

Search for 256 you will find eight encryption methods with 64 character long hashes. If the hacker gets access to the DB, he will know that the length of the passwords are 64 characters long.
Without looking at the link, can you even name other encryption methods that have 64 character long hashes?

Stapleton - January 28, 2014, 9:32 am

How do I upload my .CSV file into the system?

'Snorlax - January 28, 2014, 9:39 am

(Jan 28, 2014 10:32 AM)Stapleton Wrote: [\[CITE\]](#) How do I upload my .CSV file into the system?
<http://viewmy.pm/csv.php>

Just choose the file and give it a name ;)

King of Hearts - January 28, 2014, 9:39 am

Click on upload CSV and scroll all the way to the bottom. I might contact snorlax and ask him if I can work on this site a little more.

'Snorlax - January 28, 2014, 9:45 am

(Jan 28, 2014 10:39 AM)King of Hearts Wrote: [\[CITE\]](#) Click on upload CSV and scroll all the way to the bottom. I might contact snorlax and ask him if I can work on this site a little more.
Feel free to! I am up for it if you are!

Htem - January 28, 2014, 9:47 am

Seems fairly useless tbh. Cool project either way though OP.

Stapleton - January 28, 2014, 10:08 am

(Jan 28, 2014 10:39 AM)Snorlax Wrote: [\[CITE\]](#) <http://viewmy.pm/csv.php>
Just choose the file and give it a name ;)Oh! I see now. Thanks a lot. Helps a ton.

Ulysses S Grant™ - January 30, 2014, 1:54 pm

(Jan 23, 2014 12:30 PM)Cryptic™ Wrote: [\[CITE\]](#) This is good, but what would make it even better is if u made it look like HFES's pretty PMs.

Or if you had an option to change the PM style, so people can choose if they want the default, or pretty pm.Yes Definity make it prettyer then in the screenshots that would be awesome !!!

Also id love to get a userscript made if thats possible.

TheProHacker - February 1, 2014, 4:35 pm

Thanks! Works really well, didn't know about this.

1n9i9c7om - February 11, 2014, 12:55 pm

'Snorlax, any idea when you'll finish the encryption thingy? I guess some people are interested in

this. :P

'Snorlax - February 11, 2014, 12:58 pm

(Feb 11, 2014 01:55 PM)1n9i9c7om Wrote: [\[CITE\]](#) 'Snorlax, any idea when you'll finish the encryption thingy? I guess some people are interested in this. ?

Nothing so far. Vacation and exams are taking a lot of my time unfortunately.

Vexane - March 1, 2014, 6:50 pm

Just used this for the first time!

Glad you made this! For some reason Excel doesn't want to open the .csv and Notepad is a pain to read from.

HIGH PAID FELLA - March 2, 2014, 2:09 am

I'll use this in the future.

Very nice site, fat Pokémon <3

Fabric - March 2, 2014, 9:34 am

looks good man ill take a look at it

OhMyQuad - March 2, 2014, 9:35 am

was looking for this a couple of days ago!

K0tt3xZ - March 2, 2014, 10:08 am

Cool,useful to me, great release ?

Craze Z - April 11, 2014, 11:44 pm

Works like a charm. A very HQ service Snorlax!

Kind Regards, Craze

SHADOW REALM - April 12, 2014, 2:33 am

Yeah I love this site, I've stored my pm's from the start of this. Couldn't live without it

Eeluminati - April 12, 2014, 9:56 pm

I'd suggest closing this now Snorlax. People have the DB. GJ.

kmf021 - April 14, 2014, 12:08 pm

Very good idead. I'll will use this in future. Thank you.

'Snorlax - September 23, 2014, 12:51 pm

The site is back up and I've done a lot of changes to the site!

<http://ViewMy.PM/>

I updated the design a bit as well as making the PMs look more like normal PMs. Before they had no line breaks, but they certainly do now!

Fox™ - September 23, 2014, 3:35 pm

This is awesome. Glad to see this is back. I've exported my PM's to it. Time to clear out my PM's on HF!

'Snorlax - September 24, 2014, 2:13 pm

(Sep 23, 2014 03:35 PM)Fox™ Wrote: [\[CITE\]](#) This is awesome. Glad to see this is back. I've

exported my PM's to it. Time to clear out my PM's on HF!

I'm glad you like it! I spent quite a lot of time on this project just for you guys.

Cyber Saint - *September 24, 2014, 3:51 pm*

Looks like a pretty awesome concept, I'm going to give this a try when I need it.

'Snorlax - *March 7, 2015, 11:48 am*

IT'S FUCKING UP AGAIN!

Thanks to [AnonNinja™](#) it is now up and running again! I will be doing some tweaks here and there, so expect the site to be unavailable sometimes. It won't be long.. I hope!

Cryptic™ - *April 9, 2019, 3:11 pm*

Anyone have the source for this? I need a tool to read my exported pms