HTML5 Client Side Data Encryption - What are my options?

Asked 13 years, 7 months ago Modified 8 years, 6 months ago

Viewed 30k times

14

I am working on a EDIT: **mobile web app** which displays some sensitive information and requires a login which stores the members username and password in a HTML5 Session. The username and password are currently stored in an un-encrypted state for the reason that we need to use this username and password on each page load to access the clients remote web-service.

EDIT: After a security review our client raised the following concern:

"There is the potential that Session Storage information can get stored on disk (e.g. on a browser crash). For this reason no sensitive information should be stored unencrypted in session storage. User ID’s and session tokens can be stored since session timeouts are implemented however storing of passwords/PINs is not recommended."

What would be the best/most secure method of encrypting and decrypting sensitive data stored client-side?

Thanks!

javascript web-applications html encryption

Share

Improve this question

Follow

edited May 12, 2011 at 10:01

asked May 12, 2011 at 9:37

TGuimond

5,487 ● 6 ● 43 ● 51

Secure against what? Client-side attacks? In-transit attacks? The answer will be very different depending on this. – Piskvor left the building May 12, 2011 at 9:42

@Piskovar- There was a particular concern raised by a member of the clients security team which was "There is the potential that Session Storage information can get stored on disk (e.g. on a browser crash). For this reason no sensitive information should be stored unencrypted in session storage. User ID’s and session tokens can be stored since session timeouts are implemented however storing of passwords/PINs is not recommended." – TGuimond May 12, 2011 at 9:45

9 Answers

Sorted by: Highest score (default)

▲

11

Hi instead of storing the username and password, can you not create some sort of "session" with the remote server and instead transmit an authentication token?

Storing a username and password anywhere in the client side gives me the shivers.

Perhaps of looking for ways of storing the username / password safely, look for ways of removing the need to store it at all.

However of course I'm saying this without knowing the full background... I'm guessing there is a good reason to need to store the username / password.

Share Improve this answer Follow

answered May 12, 2011 at 9:51
Alex KeySmith
17.1k ● 11 ● 82 ● 157

1 The reason that we require the username/password for each page load is that we have to use it to load data from a remote web-service on every page load. Our clients arent willing to budge on this requirement :(– TGuimond May 12, 2011 at 9:59

@TGuimond A tricky problem, does the web-service have any other authentication methods available? Could you authenticate using Windows Authentication instead? – Alex KeySmith May 12, 2011 at 10:41

8

For anyone stumbling upon this question, Stanford has a crypto project over at http://crypto.stanford.edu/sjcl/. I have not used it myself in production, but am busy investigating it and so far it looks promising. Hope this helps someone.

Share Improve this answer

Follow

answered Sep 20, 2012 at 9:07

Tash Pemhiwa

7,685 ● 4 ● 46 ● 51

3

David Dahl, a Firefox engineer, has a prototype Firefox extension, domcrypt (repository on github), that provides Javascript access to Firefox's NSS (Network Security Services) APIs. Since Chrome also uses NSS, providing the same API is probably straightforward for it as well.

He's pushing Mozilla to evolve it a bit more for eventual inclusion within Firefox; we'll see what happens.

Share Improve this answer

Follow

answered May 12, 2011 at 9:53

Samat Jain

16.3k ● 4 ● 22 ● 13

@David Dahl: I completely forgot to mention that its a web app for Mobile Browsers, so we are restricted to smart phone browsers. Apologies. – TGuimond May 12, 2011 at 10:02

2

See this HTML5 Web DB Security

> client-side encryption libraries aren't mature or tested well enough

...but it's been a year ago, so that could be false already

✓

Share Improve this answer

Follow

edited May 23, 2017 at 11:53

Community Bot

1 ● 1

answered May 12, 2011 at 9:41

František Žiačik

7,614 ● 1 ● 36 ● 61

▲

2

▼

Was researching this topic myself recently. I think by now we do have some proven JS encryption libraries see [here]() and [here]().

Now the question is where to store the key. Storing it on the client side would be the same as storing the data with no encryption at all. And having the user enter the key all the time would defeat the purpose.

Maybe you could ask your server to generate a new key whenever you create a new session. (Make sure to use HTTPS when making this request). If the session expires, the user has to enter username/password again and it would be encrypted using the new token. To decrypt the key you have to make a (secure) request to your server (passing in your session id) to request the key, which then can be used to decrypt username and password.

Now this still leaves open the usual vulnerabilities such as cross side scripting or session hijacking, but at least the user password is not stored in clear text on the client side.

What do you think?

Share Improve this answer

Follow

edited Jun 20, 2020 at 9:12

Community Bot

1 ● 1

answered Jul 13, 2011 at 22:43

user832834

61 ● 3

2

More recent browser versions should support Web Crypto API.

[1. See the live test page if you browser works](#)
[2. The w3c Webcrypto API description](#)
[3. Mozilla Developer Network Info on WebCrypto API](#)

Share Improve this answer

Follow

answered Jun 10, 2016 at 14:46

phil soady

11.3k ● 5 ● 54 ● 99

0

I work on an [application](#) that faces the same problem. Security is important for this application because it allows users to build personal trees (or nested lists) and to store them on the cloud.

My solution is to encrypt the password stored on the client side with another password generated by the server for each user.

Share Improve this answer

answered Feb 19, 2014 at 0:16

Follow

telepath
1 ● 1

-1

I have to say if your creating a session data 1 is that not,- stored on the server not client side thus no one sees the session data or at least it should be done that way via asp, or php, ect so have the app require internet and retrieve the info from a web server and don't store it on the client side. 2 if this does deal with client side like dealing with streaming a video, or images or you have to create some files on the client side storing the key on the clients mobile device is the only way. Thus either have the key with a short ttl to decrypt the data, the key given through some form of authentication or certificate, or a key installed from your main office and encrypt the device in case they loose it. I not found and encrypt function I like to suggest yet for you.

Share Improve this answer

Follow

answered May 31, 2013 at 6:54

justaguest1000
1

-1

Storing sensitive user credentials are really not a good design. Instead generate a authenticated token from server using, say, sprint framework. You can then store the same in localstorage using the Web DB Security module.

Share Improve this answer

answered Apr 5, 2016 at 7:15

Follow

Tanmoy Roy

29 ● 1 ● 4