


How to protect global variables (window) from being overwritten


Asked 1 year, 6 months agoActive 1 year, 6 months agoViewed 72 times

▲

0

▼





I am currently working on a project where security is very important. By default, all global variables/properties like `Promise` or even `crypto` can be overwritten.

Is there a way to protect them from being overwritten?

Example:

```
window.crypto.getRandomValues = () => { return [1] }  
window.crypto.getRandomValues(new Uint32Array(1))[0] // 1
```

My first thought was to use `Object.freeze()` to lock the object, but one can simply overwrite the `Object.freeze` method so it does nothing.

We are already very selective of the dependencies we use, but I would still like to make sure that those variables can not be overwritten. Or at least detect if they were overwritten.

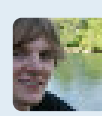
javascript

typescript

security

sharefollow

asked May 29 '19 at 8:37



Andreas Gassmann

5,46642338

2

It's the user's own browser - in the end, they can run whatever code they want, and they may monkeypatch whatever they want as well. – [CertainPerformance](#) May 29 '19 at 8:39

maybe only eslint rule [eslint.org/docs/rules/no-global-assign](#) – [Vadim Hulevich](#) May 29 '19 at 8:45

If the user wants to do that himself I can live with it. But I want to prevent other libraries to interfere with mine. So if locking the global variables is not possible, is there a way to "sandbox" the different dependencies? I read the proposal about `realms`. I think this would be what I'm looking for, but it's not ready yet. – [Andreas Gassmann](#) May 29 '19 at 8:56

add a comment


1 Answer


ActiveOldestVotes

▲

1

▼





Disclaimer: All this is just a rough outline, not thoroughly tested. I'm sure there are more problems to solve.

[freezing](#) the window-object is no option, this would just cause problems, but maybe Objects like `window.crypto`?

But you can re-define properties to be no longer changeable, even on the window-object

```
function freezeProp(target, propertyName) {  
  const { value, get = () => value, set = () => void 0, ...desc } = Object.getPrototypeOf(target).defineProperty(target, propertyName, { ...desc, get, set, configurable: false });  
}  
  
freezeProp(window, "crypto");
```

But these methods only work out if you can ensure that you are the first script to run.

Detecting if some methods have been changed is also just possible if you have a reference to them; and we're back at being the first script to run.


But if you're not sure wether the global scope has been spoiled, why not get a fresh window-object?

```
window.crypto.getRandomValues = () => {  
  return [1]  
};  
  
const secure = (() => {  
  let iframe = document.createElement("iframe");  
  document.body.appendChild(iframe);  
  const contentWindow = iframe.contentWindow;  
  document.body.removeChild(iframe);  
  return contentWindow;  
})();  
  
var a = window.crypto.getRandomValues(new Uint8Array(1));  
console.log(a);  
  
var b = secure.crypto.getRandomValues(new Uint8Array(1));  
console.log(b);
```

sharefollow

edited May 29 '19 at 9:43

answered May 29 '19 at 9:38



Thomas

7,8411815


You came to the same conclusion as I. You have to ensure to be the *first* to freeze/lock objects, before someone else can overwrite anything. Your solution seems to work for crypto, but for example "Proxy" and "Promise" can still be overwritten. My initial thought would be to create `const safeProxy = Proxy` and lock it's properties, so you can always rely on safeProxy being there and in it's original form. BTW, your last approach with the iframe doesn't work, because one can simply overwrite the `document.createElement` function :). – [Andreas Gassmann](#) May 29 '19 at 10:29

add a comment


Your Answer


B


I





























Sign up or log in

 Sign up using Google

 Sign up using Facebook

 Sign up using Email and Password

Post Your Answer

By clicking "Post Your Answer", you agree to our [terms of service](#), [privacy policy](#) and [cookie policy](#)

Post as a guest


Name


Email

Required, but never shown


Not the answer you're looking for? Browse other questions tagged [javascript](#) [typescript](#) [security](#) or [ask your own question](#).


The Overflow Blog


 How to write an effective developer resume: Advice from a hiring manager

 Podcast 290: This computer science degree is brought to you by Big Tech

Featured on Meta

 "Question closed" notifications experiment results and graduation

 MAINTENANCE WARNING: Possible downtime early morning Dec 2/4/9 UTC (8:30PM...)

 Congratulations VonC for reaching a million reputation

Related

6359

How do I remove a property from a JavaScript object?

1113

How does the SQL injection from the "Bobby Tables" XKCD comic work?

1470

How do you use a variable in a regular expression?

1344

How should I ethically approach user password storage for later plaintext retrieval?

2221

How can I determine if a variable is 'undefined' or 'null'?

8841

How can I remove a specific item from an array?


715


How do you explicitly set a new property on 'window' in TypeScript?


5743


How do I return the response from an asynchronous call?


Hot Network Questions


 Is the source important for fair use?


 What does "blaring YMCA — the song" mean?


 Figures as a one column panel with same x axis but changing y axis


 Do PhD students sometimes abandon their original research idea? If so, how do they cope with it?


 MC Cable through double 2x4 top plate


 The pronunciation of Eta (η)


 Choose Snapping Point?


 Figuring out from a map which direction is downstream for a river?


 What does "中" as an independent verb means?

 Why does C9 sound so good resolving to D major?

 BJT and signal source

 Nested Undersets

 Question feed



STACK OVERFLOW

QuestionsJobsDeveloper Jobs DirectorySalary CalculatorHelpMobile

Disable Responsiveness

PRODUCTS

TeamsTalentAdvertisingEnterprise

COMPANY

AboutPressWork HereLegalPrivacy PolicyContact Us

STACK EXCHANGE NETWORK

TechnologyLife / ArtsCulture / RecreationScienceOther

BlogFacebookTwitterLinkedInInstagram

site design / logo © 2020 Stack Exchange Inc; user contributions licensed under cc by-sa. rev 2020.11.30.38071