JWTs Suck

(for web auth and basically everything else)

@rdegges

@oktadev

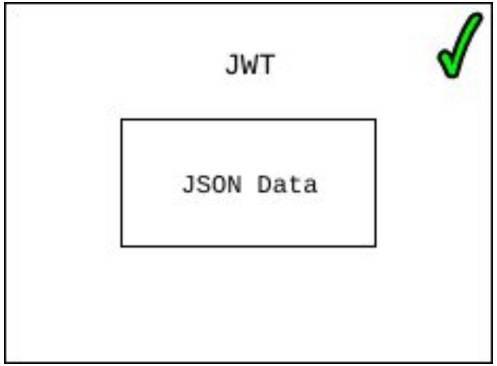
Randall Degges

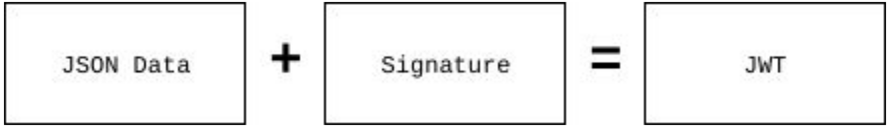
Chief Hacker @ Okta

Python / Node / Go

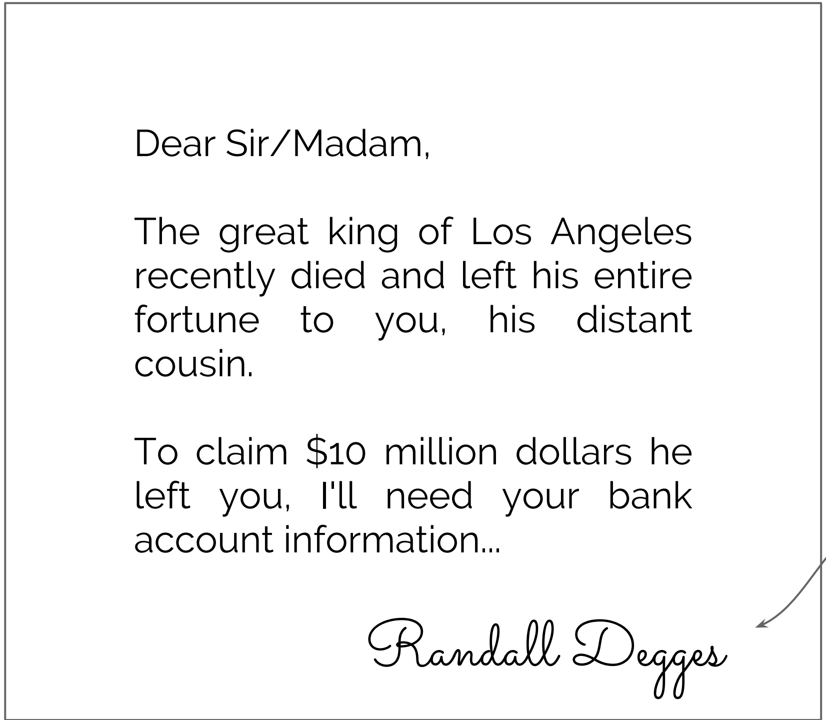
What are JWTs?

- JSON data
- Cryptographically signed
- Not encrypted
- Not special





What’s a Cryptographic Signature?



Dear Sir/Madam,

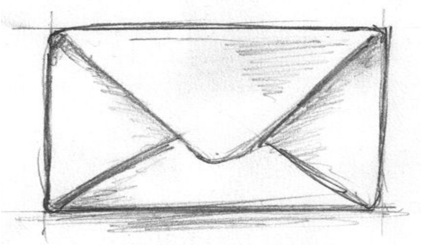
The great king of Los Angeles recently died and left his entire fortune to you, his distant cousin.

To claim $10 million dollars he left you, I'll need your bank account information...

Randall Degges

What Do JWTs Actually Do?

Prove that some JSON data can be trusted.



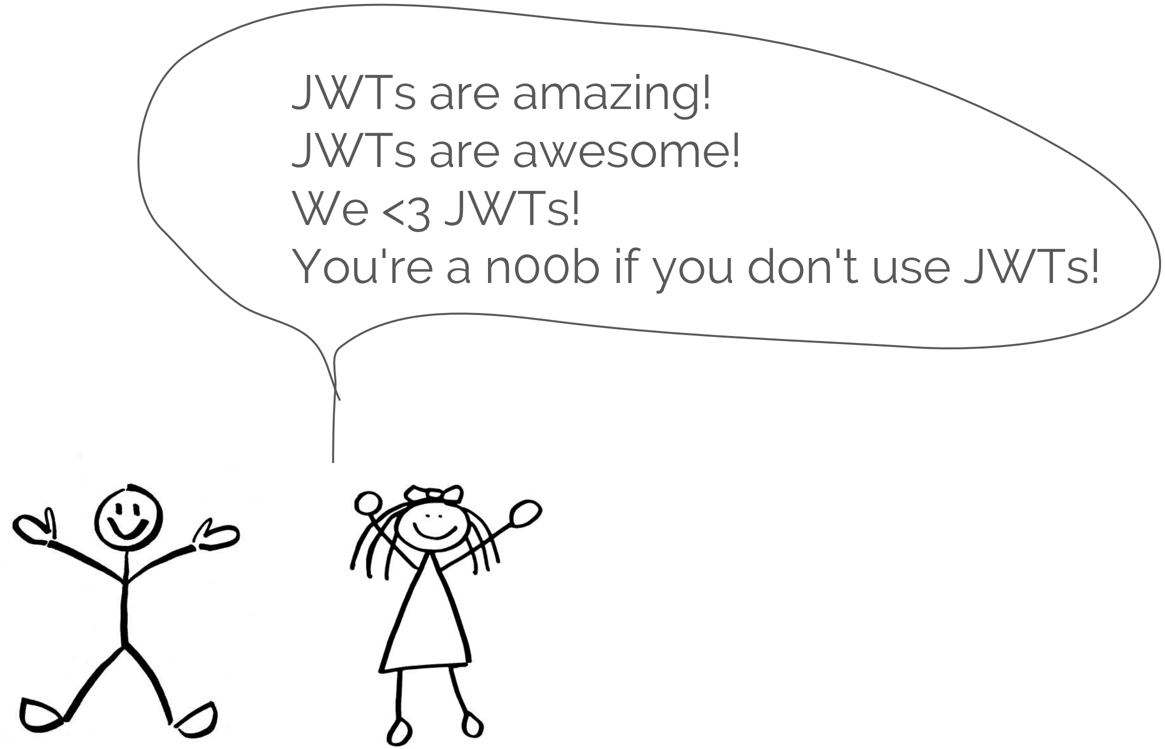
How Do People Typically Use JWTs?

As identity proof

How JWTs are Most Commonly Used

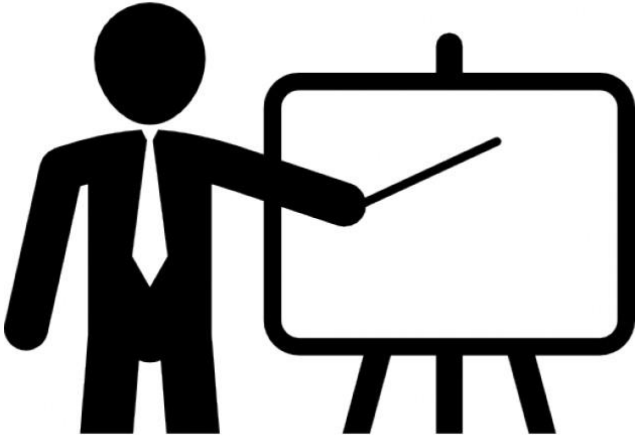
- ➔ User sends credentials to website to login
- ➔ Website validates credentials, generates JWT
- ➔ Website sends response to browser containing JWT
- ➔ Browser then stores JWT in localStorage
- ➔ Browser pulls JWT out of localStorage and sends it to website for subsequent requests

What happens when you Google JWTs?



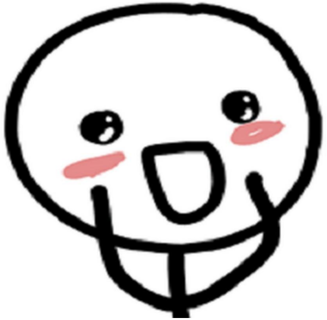
JWTs are amazing!
JWTs are awesome!
We <3 JWTs!
You're a n00b if you don't use JWTs!

Everyone is wrong.



I FEEL LIKE I'M TAKING
CRAZY PILLS
quickmeme.com

Everyone has forgotten how *amazing* session cookies actually are.



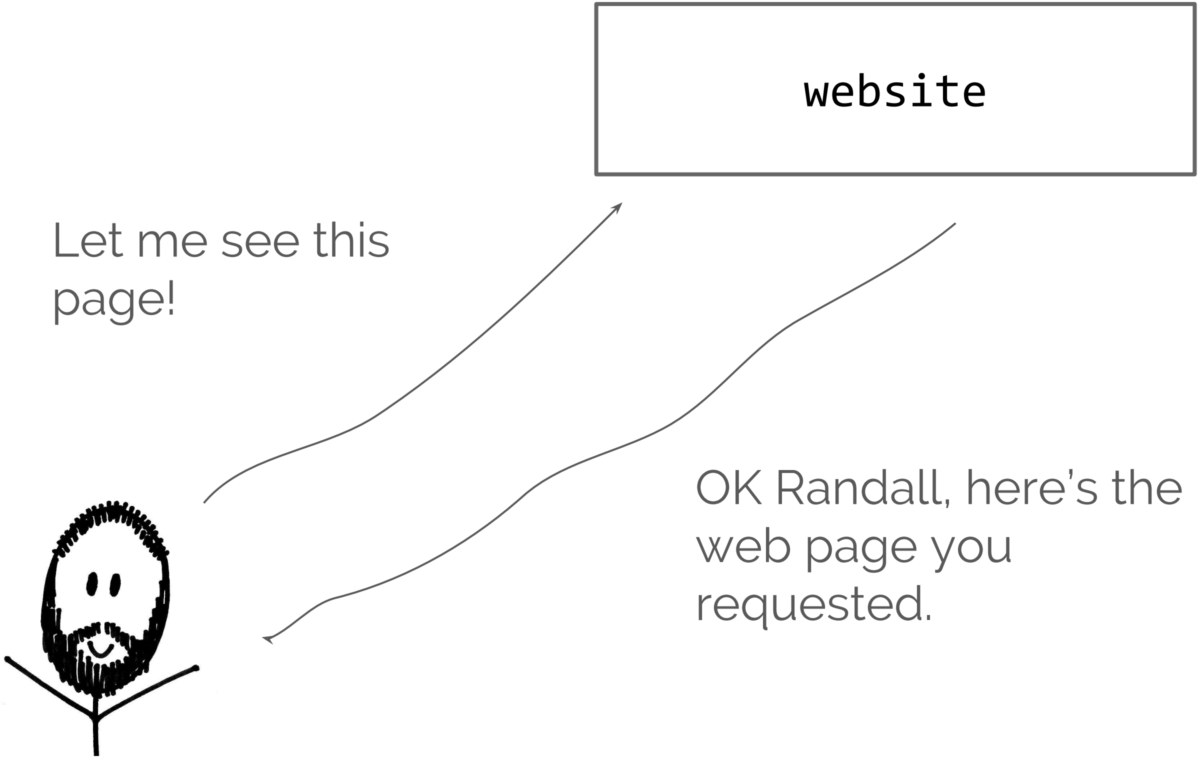
Let’s define some terms…

Term: Stateless JWT

Definition:

A JWT that is entirely self-contained, and holds all user information necessary to complete a transaction within it. EG: userName, firstName, lastName, email, etc…

Validates token… OK!



website

It looks like your name is Randall Degges, and your email is r@rdegges.com

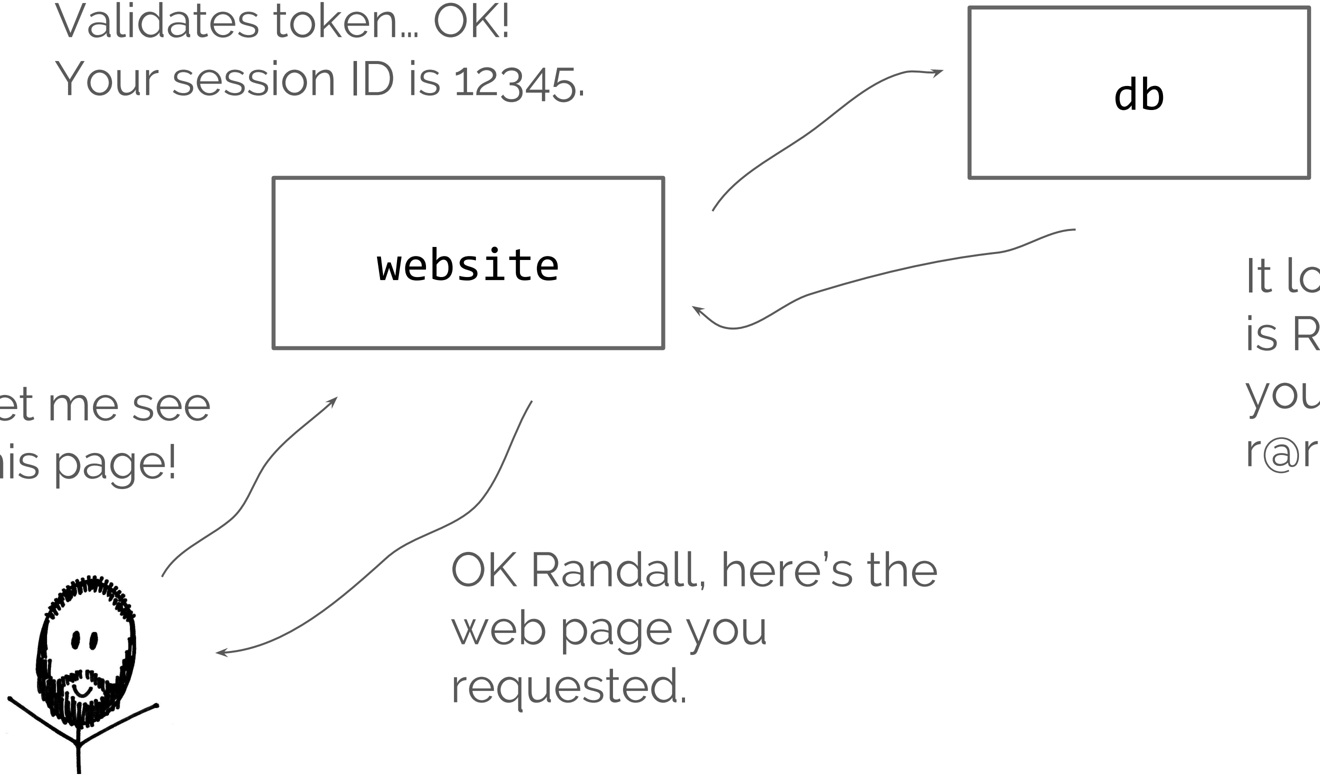
Let me see this page!

OK Randall, here’s the web page you requested.

Term: Stateful JWT

Definition:

A JWT that only contains a session ID. All user data is stored server-side and retrieved from a database.



Let me see this page!

Validates token… OK!
Your session ID is 12345.

Who is the user with
session ID 12345?

Session ID 12345 is
Randall Degges. Here
you go.

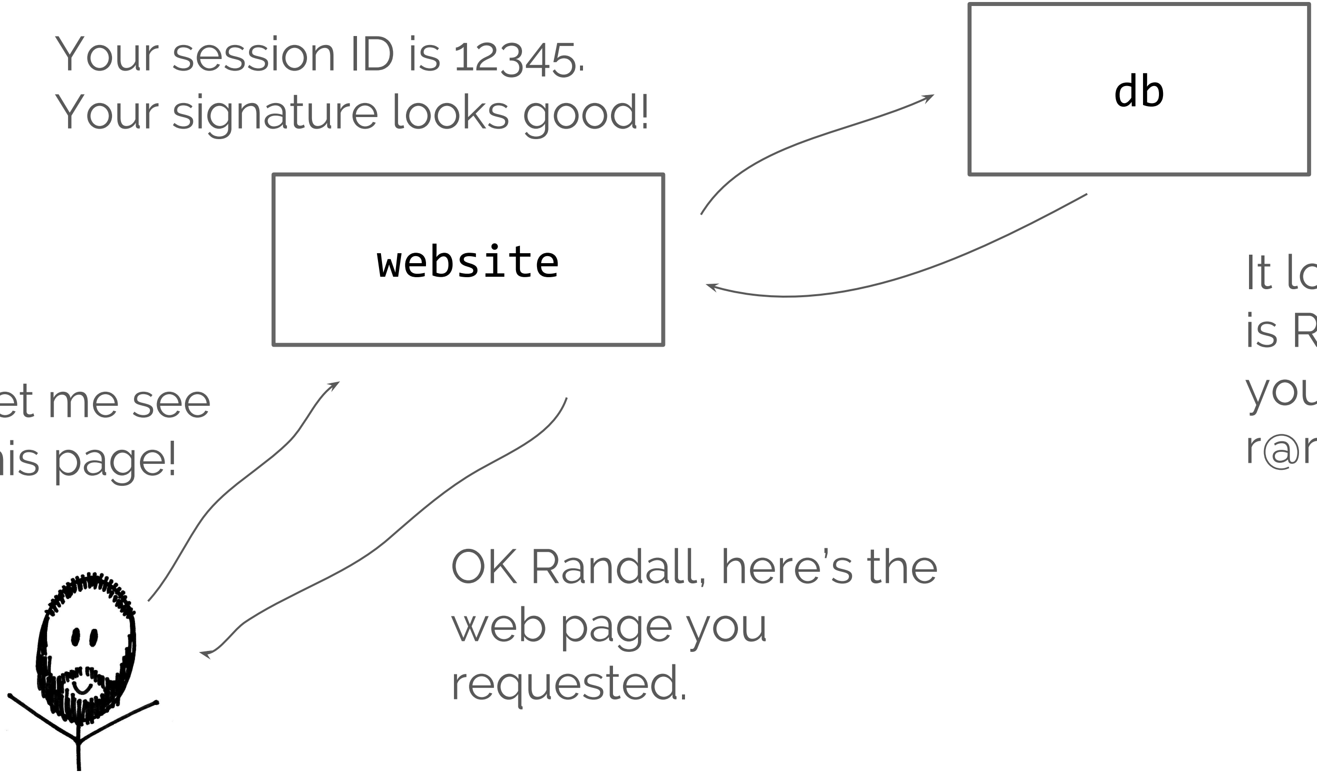
It looks like your name
is Randall Degges, and
your email is
r@rdegges.com

OK Randall, here’s the
web page you
requested.

Term: Session Cookie

Definition:

A cryptographically signed session identifier stored in a cookie. All user data is stored server-side and retrieved from a database.



Let me see this page!

Your session ID is 12345. Your signature looks good!

Who is the user with session ID 12345?

Session ID 12345 is Randall Degges. Here you go.

It looks like your name is Randall Degges, and your email is r@rdegges.com

OK Randall, here’s the web page you requested.

BONUS: What’s the difference between a Session Cookie and a Stateful JWT?

¯\_(ツ)_/¯

- They’re both cryptographically signed
- They both contain a session identifier (12345)

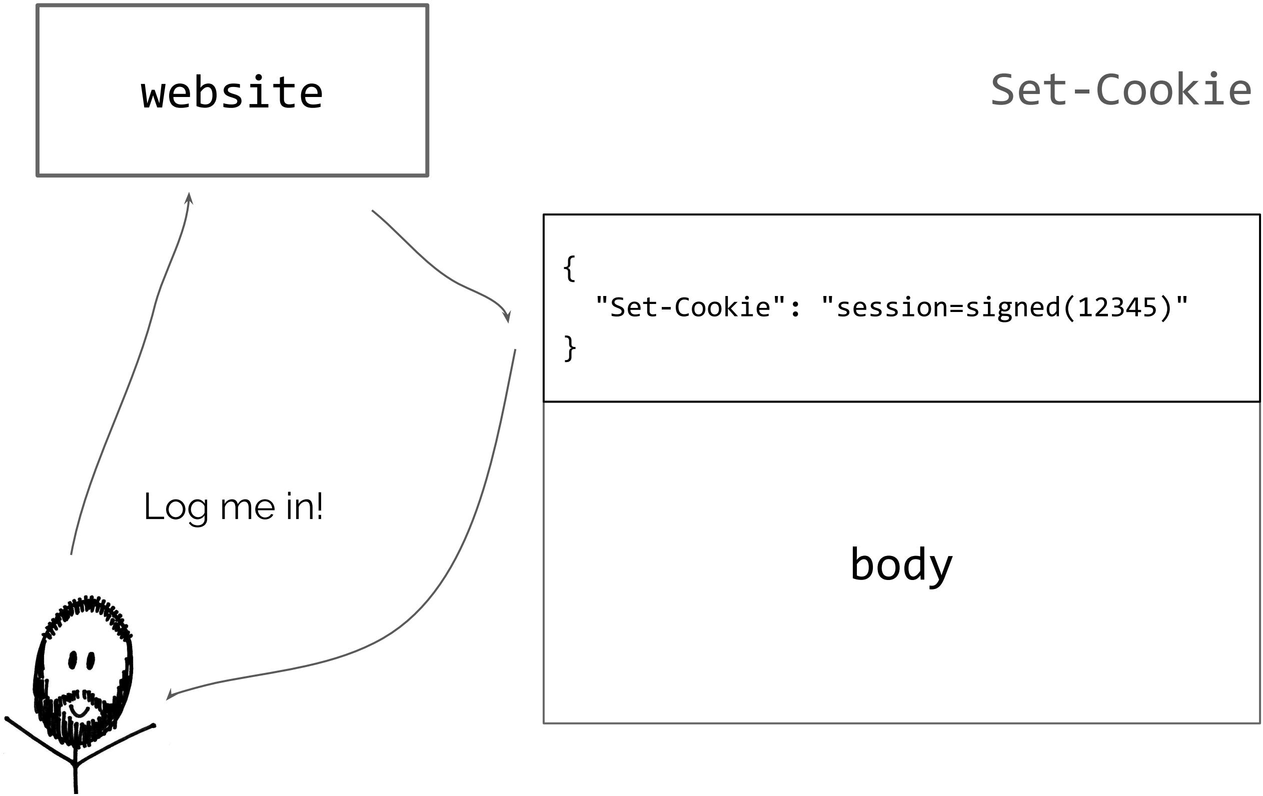
- **One uses the JWT format (JSON) and one is just a simple string**

Term: Cookies

Definition:

An HTTP header field that allows you to store or retrieve key/value data, set data expiration times, and apply various other data integrity rules. Caps out at ~4k.

Creating Cookies



website

Log me in!

```
{
  "Set-Cookie": "session=signed(12345)"
}
```

body

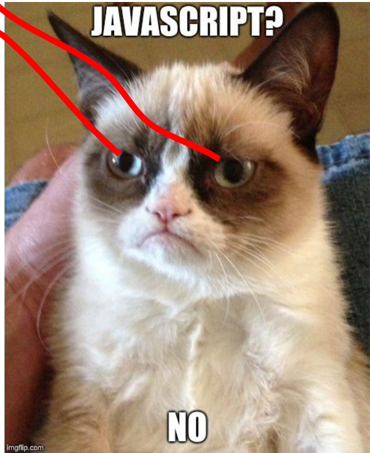
```
Set-Cookie: a=b; c=d; e=f
```

NOTE: Required Cookie Flags

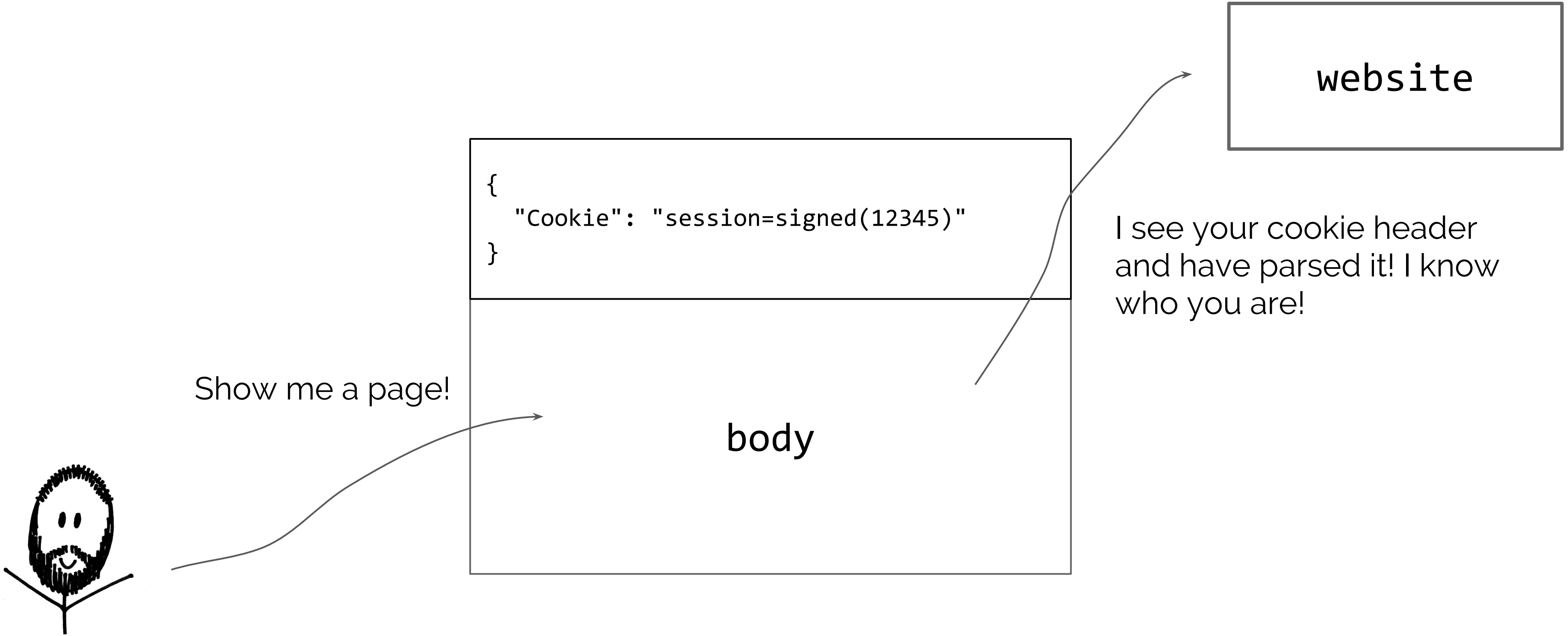
```
Set-Cookie: a=b; HttpOnly;
 SameSite=strict; secure;
```

No nasty cross-origin cookie sharing!

SSL only!



Reading Cookies



```
{
  "Cookie": "session=signed(12345)"
}
```

Show me a page!

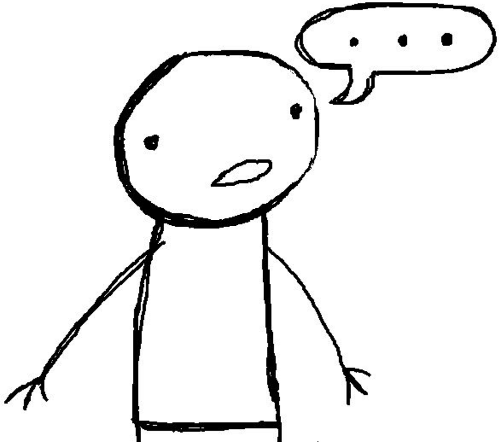
I see your cookie header and have parsed it! I know who you are!

Term: Local Storage

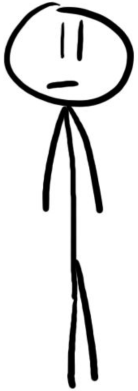
Definition:

A Javascript API that allows a user to store data in a browser that is accessible only via Javascript. Also known as “session storage”. Widely considered to be an alternative to using cookies to store session data.

Myths about JWTs



JWTs are Easier to Use



JWTs:

- First spec draft: Dec 27, 2012
- Began gaining adoption / marketing: mid 2014
- Requires additional tools, libraries, and knowledge to function (developer effort required)

Session Cookies:

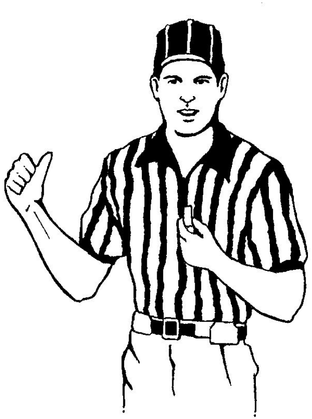
- Every web framework since 1990s
- Requires 0 effort to use

Score

JWTs

Session Cookies

0



1

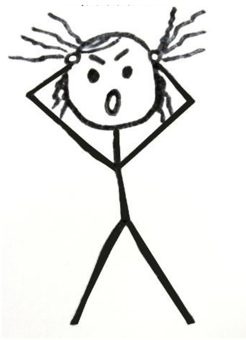
JWTs are More Flexible

JWTs

```
{
  “sessionId”: “12345”,
  “email”: “r@rdegges.com”,
  “firstName”: “Randall”,
  “lastName”: “Degges”
}
```

Session Cookies

```
sessionId=12345;
email=r@rdegges.com;
firstName=Randall;
lastName=Degges
```



JWTs are More Flexible

JWTs

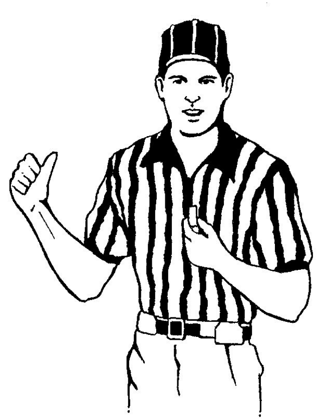
```
{
  “userId”: “12345”,
  “email”: “r@rdegges.com”,
  “firstName”: “Randall”,
  “lastName”: “Degges”,
  “iat”: “123456789”,
  “exp”: “987654321”
}
```

Session Cookies

```
userId=12345;
email=r@rdegges.com;
firstName=Randall;
lastName=Degges;
Expires=xxxx;
```

Score

JWTs	Session Cookies
0	2



JWTs are More Secure

JWTs

Good:

- Cryptographically signed
- Can be encrypted (JWE)

Bad:

- Complex spec / crypto :(
- Multiple vulnerabilities found in last three years
- Vastly different support in libraries

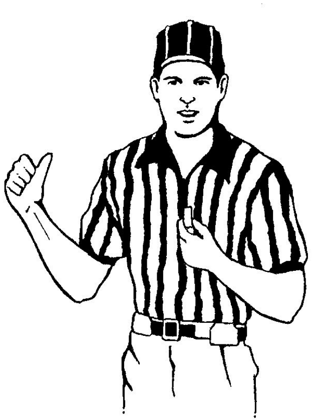
Session Cookies

Good:

- Cryptographically signed
- Can be encrypted
- Been around since ~1994
- Well vetted, battle tested
- 0 complexity in the spec
- No vulnerabilities in like… forever
- Identical library support everywhere

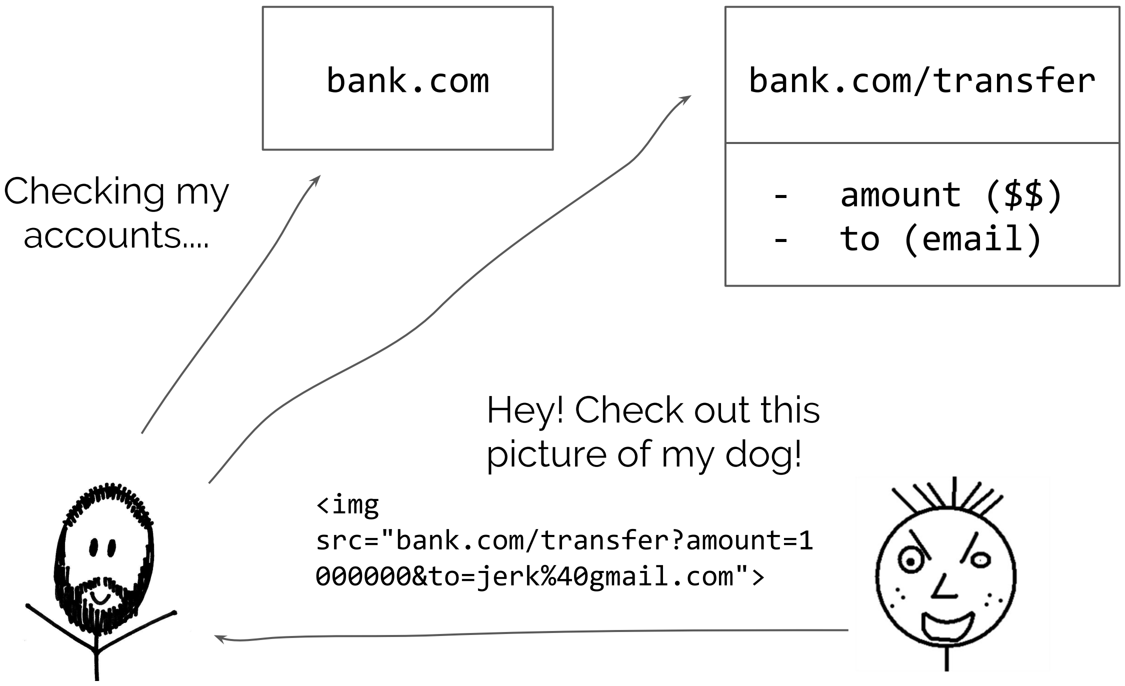
Score

JWTs	Session Cookies
0	3



JWTs Prevent CSRF

DETOUR! What is CSRF?



bank.com

bank.com/transfer

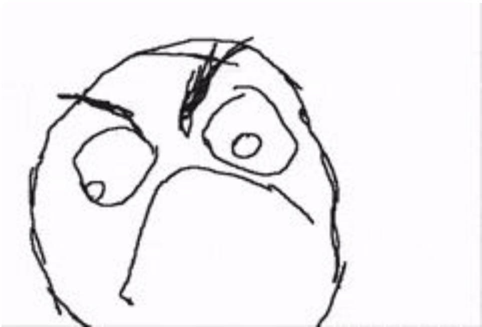
- amount ($$)
- to (email)

Checking my accounts....

Hey! Check out this picture of my dog!

```
<img
src="bank.com/transfer?amount=1
000000&to=jerk%40gmail.com">
```

OK! Transfer received!
Sending 1 million dollars to
jerk@gmail.com!



JWTs Prevent CSRF

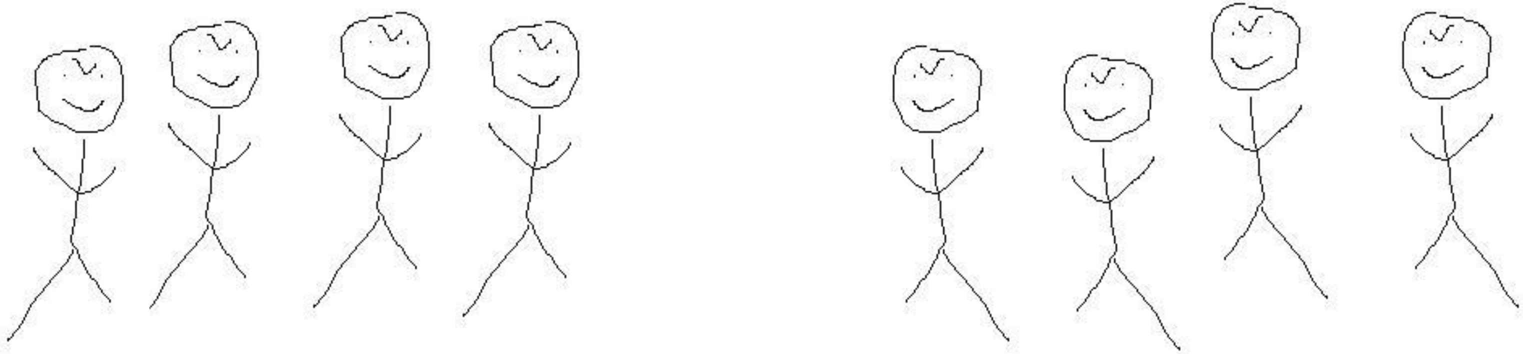
Cookies

- You are still susceptible to CSRF

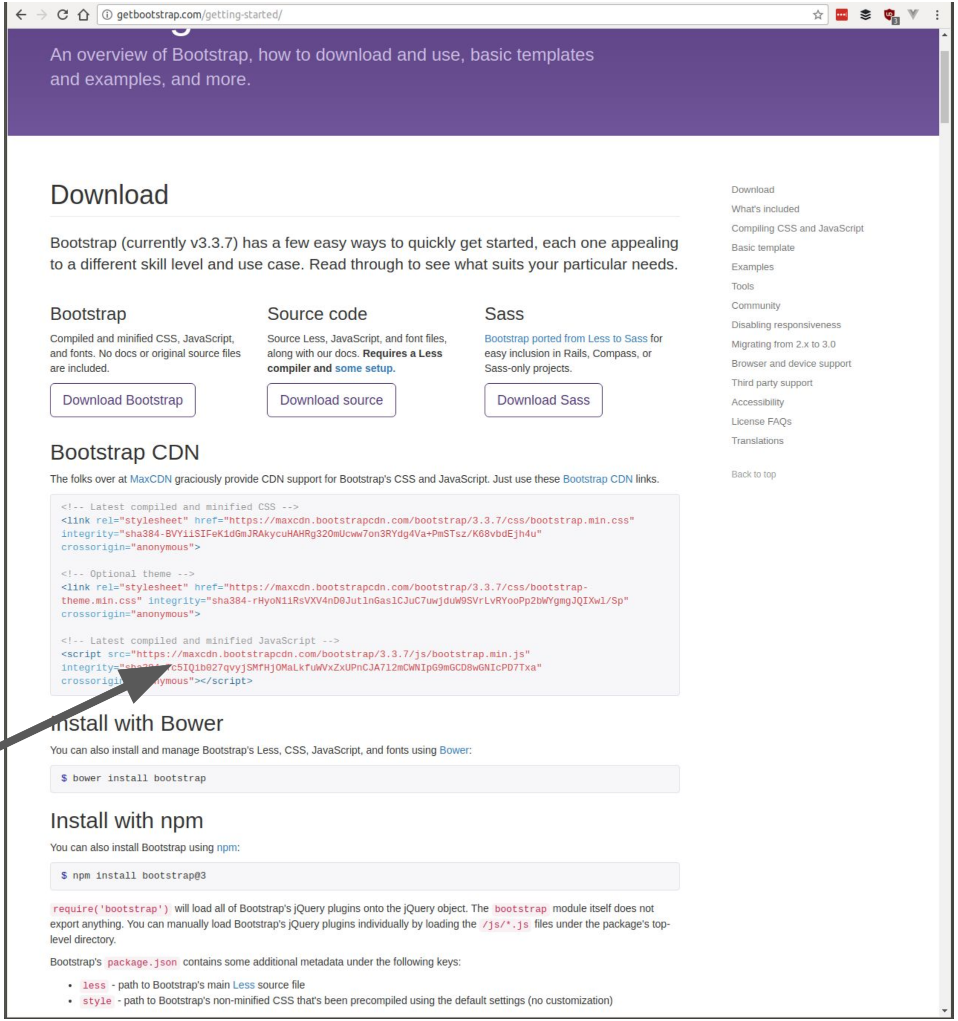
Local Storage

- You are safe from CSRF, but have opened yourself up to a much greater attack vector… XSS

CSRF is trivial to fix. XSS… Not so much.



Bad News



An overview of Bootstrap, how to download and use, basic templates and examples, and more.

Download

Bootstrap (currently v3.3.7) has a few easy ways to quickly get started, each one appealing to a different skill level and use case. Read through to see what suits your particular needs.

Bootstrap

Compiled and minified CSS, JavaScript, and fonts. No docs or original source files are included.

Download Bootstrap

Source code

Source Less, JavaScript, and font files, along with our docs. **Requires a Less compiler and some setup.**

Download source

Sass

Bootstrap ported from Less to Sass for easy inclusion in Rails, Compass, or Sass-only projects.

Download Sass

Bootstrap CDN

The folks over at MaxCDN graciously provide CDN support for Bootstrap's CSS and JavaScript. Just use these Bootstrap CDN links.

```
<!-- Latest compiled and minified CSS -->
<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css"
integrity="sha384-BVYiiSIFeK1dGmJRAkycuHAHRg32OmUcww7on3RYdg4Va+PmSTsz/K68vbdEjh4u"
crossorigin="anonymous">

<!-- Optional theme -->
<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap-
theme.min.css" integrity="sha384-rHyoN1iRsVXV4nD0JutlnGaslCJuC7uwjduW9SVrLvRYooPp2bWYgmgJQIXwl/Sp"
crossorigin="anonymous">

<!-- Latest compiled and minified JavaScript -->
<script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"
integrity="sha384-Tc5IQib027qvyjSMfHjOMaLkfuWVxZxUPnCJA7l2mCWNIpG9mGCD8wGNIcPD7Txa"
crossorigin="anonymous"></script>
```

Install with Bower

You can also install and manage Bootstrap's Less, CSS, JavaScript, and fonts using Bower:

```
$ bower install bootstrap
```

Install with npm

You can also install Bootstrap using npm:

```
$ npm install bootstrap@3
```

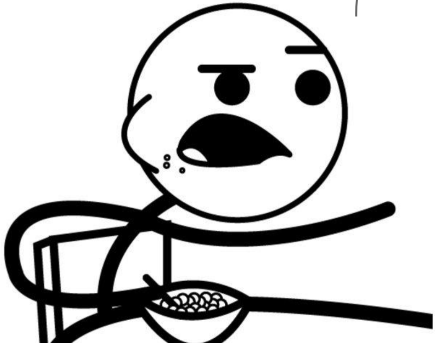
`require('bootstrap')` will load all of Bootstrap's jQuery plugins onto the jQuery object. The `bootstrap` module itself does not export anything. You can manually load Bootstrap's jQuery plugins individually by loading the `/js/*.js` files under the package's top-level directory.

Bootstrap's `package.json` contains some additional metadata under the following keys:

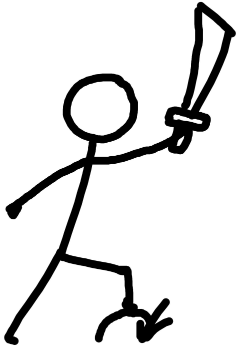
- `less` - path to Bootstrap's main Less source file
- `style` - path to Bootstrap's non-minified CSS that's been precompiled using the default settings (no customization)

Back to top

But… I just won’t use third party JS on my site… So I can still be secure!



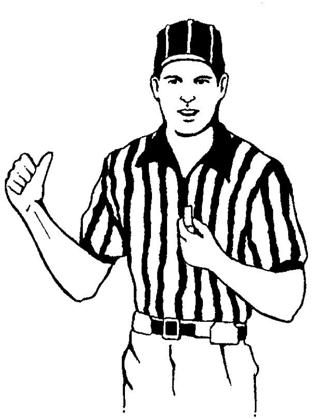
“… In other words, any authentication your application requires can be bypassed by a user with local privileges to the machine on which the data is stored. **Therefore, it's recommended not to store any sensitive information in local storage.**”



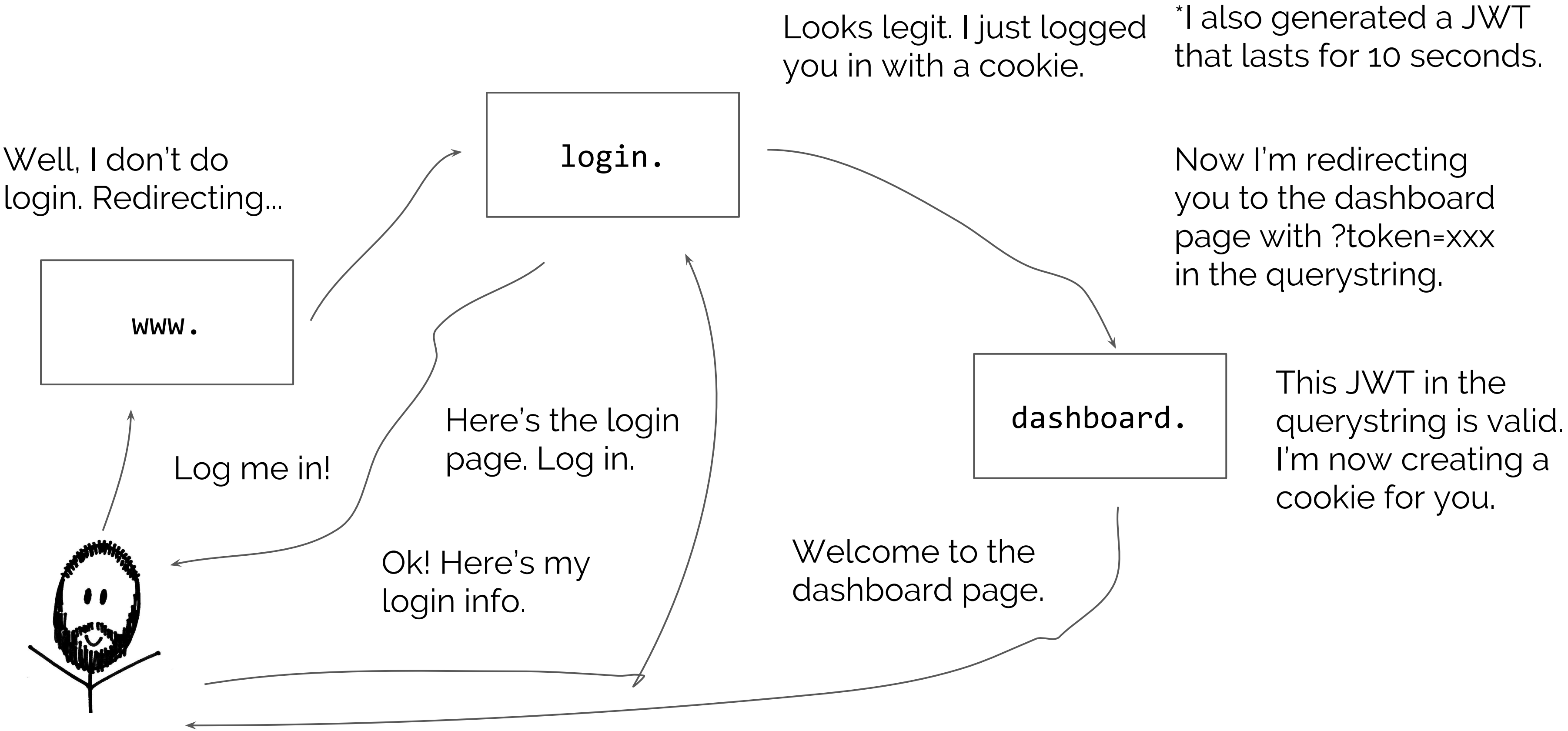
- OWASP (Open Web Application Security Project)

Score

JWTs	Session Cookies
0	4



JWTs Are Better for Cross Domain



Log me in!

Well, I don’t do login. Redirecting…

Here’s the login page. Log in.

Ok! Here’s my login info.

Looks legit. I just logged you in with a cookie.

*I also generated a JWT that lasts for 10 seconds.

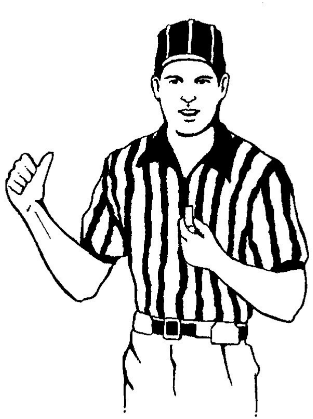
Now I’m redirecting you to the dashboard page with ?token=xxx in the querystring.

This JWT in the querystring is valid. I’m now creating a cookie for you.

Welcome to the dashboard page.

Score

JWTs	Session Cookies
0	5

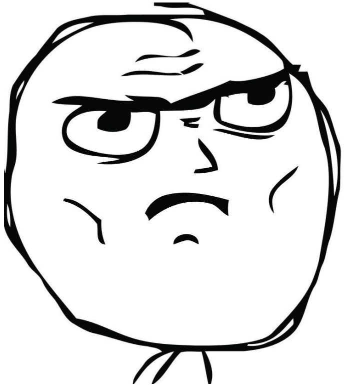


JWTs are More Efficient

```
JWT({ sessionId: 'aKF271L99Q47Zy9Ds9lCefuizH9wuTjVewxH4yaL' })     // 179 bytes
signed(aKF271L99Q47Zy9Ds9lCefuizH9wuTjVewxH4yaL)                   // 64 bytes
```

~3x larger

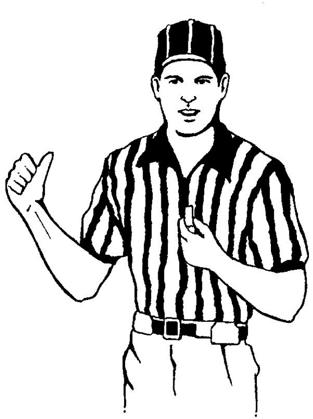
BUT...



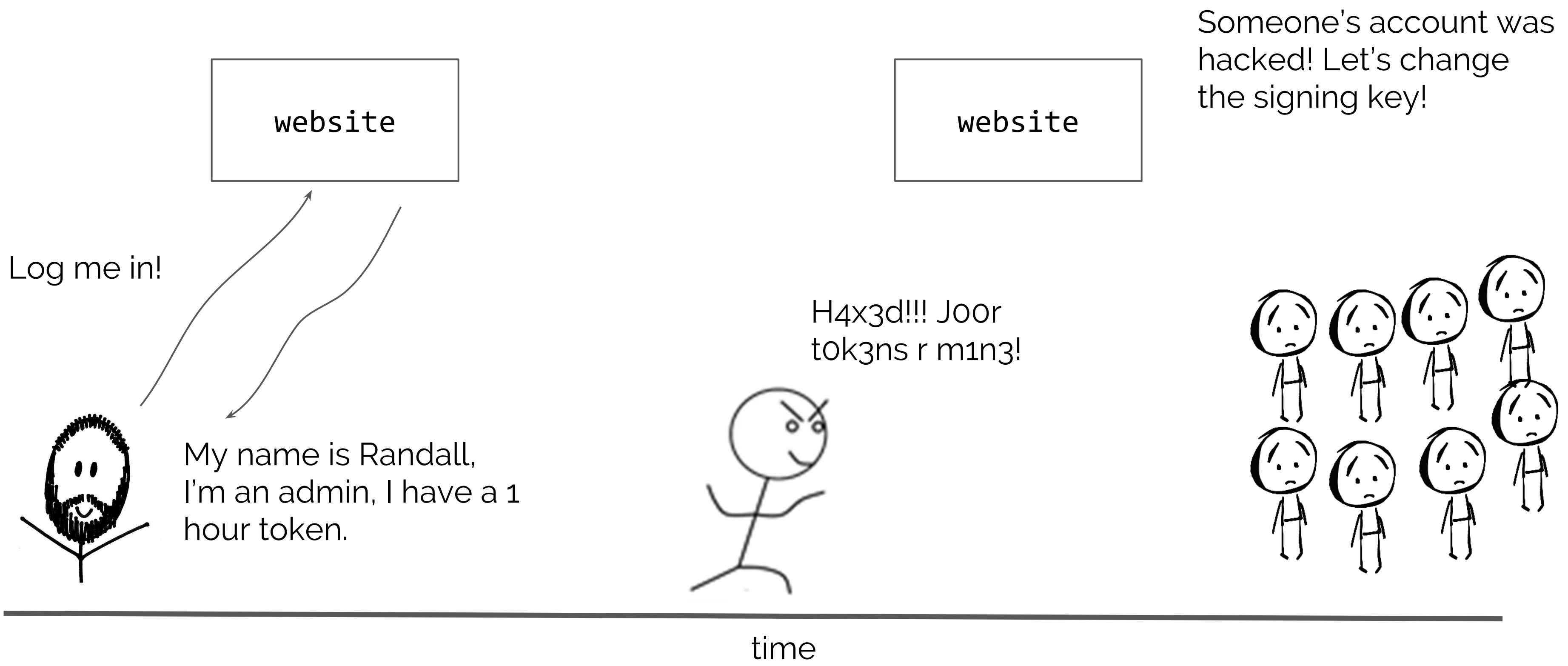
~10x -> 100x!

Score

JWTs	Session Cookies
0	6



JWTs Are Easy to Revoke



Log me in!

website

My name is Randall,
I’m an admin, I have a 1
hour token.

H4x3d!!! J00r
t0k3ns r m1n3!

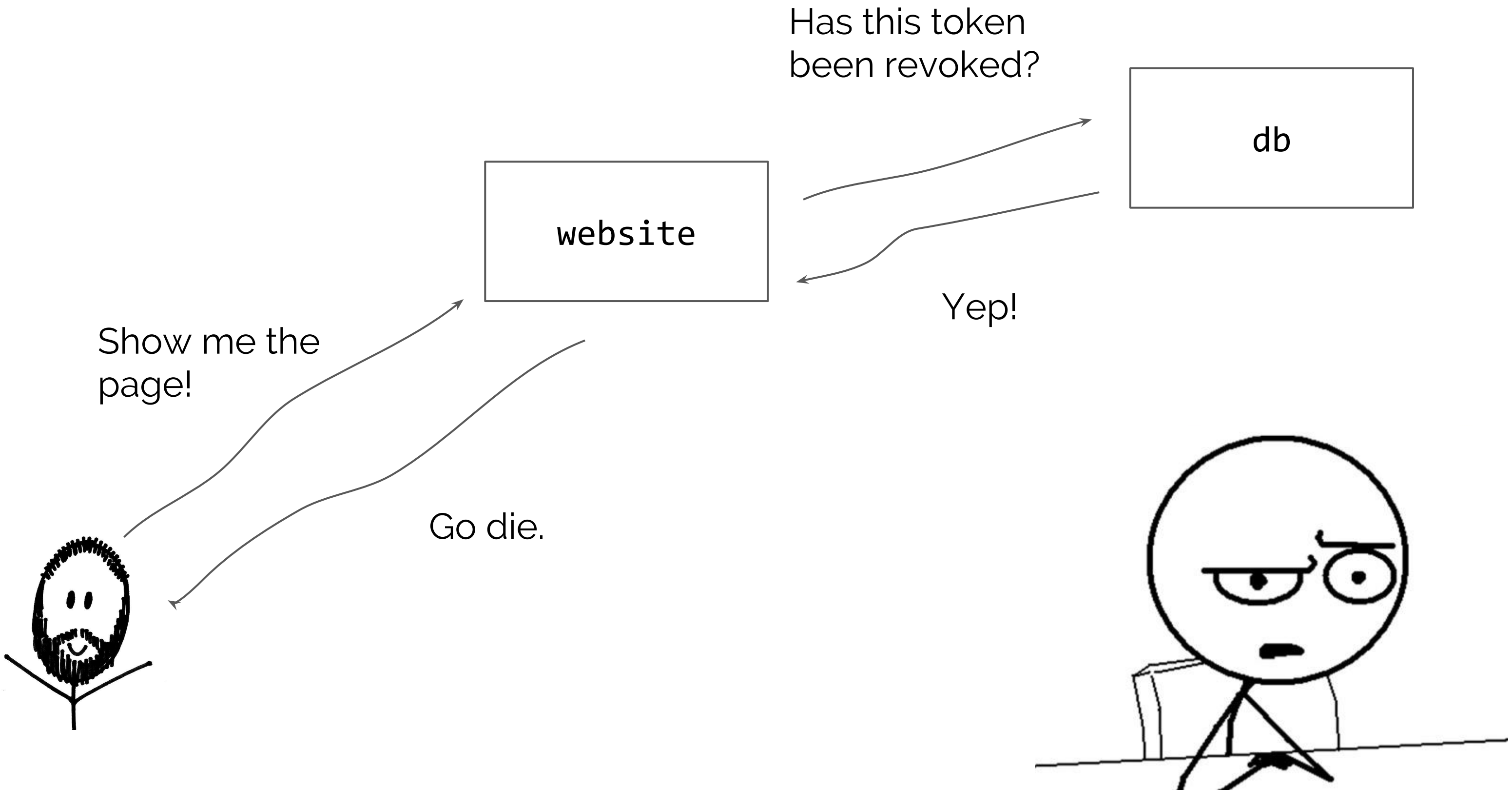
website

Someone’s account was
hacked! Let’s change
the signing key!

time

Randall, you are a n00b! If I want to invalidate an individual JWT I can just use a revocation list!!

OK, OK



Has this token been revoked?

db

website

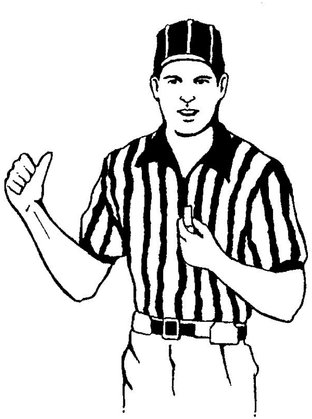
Yep!

Show me the page!

Go die.

Score

JWTs	Session Cookies
0	7



JWTs are Easier to “Scale”

JWTs

Good

- Can be validated locally without any necessary external DB access

Bad

- This only applies to stateless JWTs, not stateful JWTs
- Requires more bandwidth on every request

Session Cookies

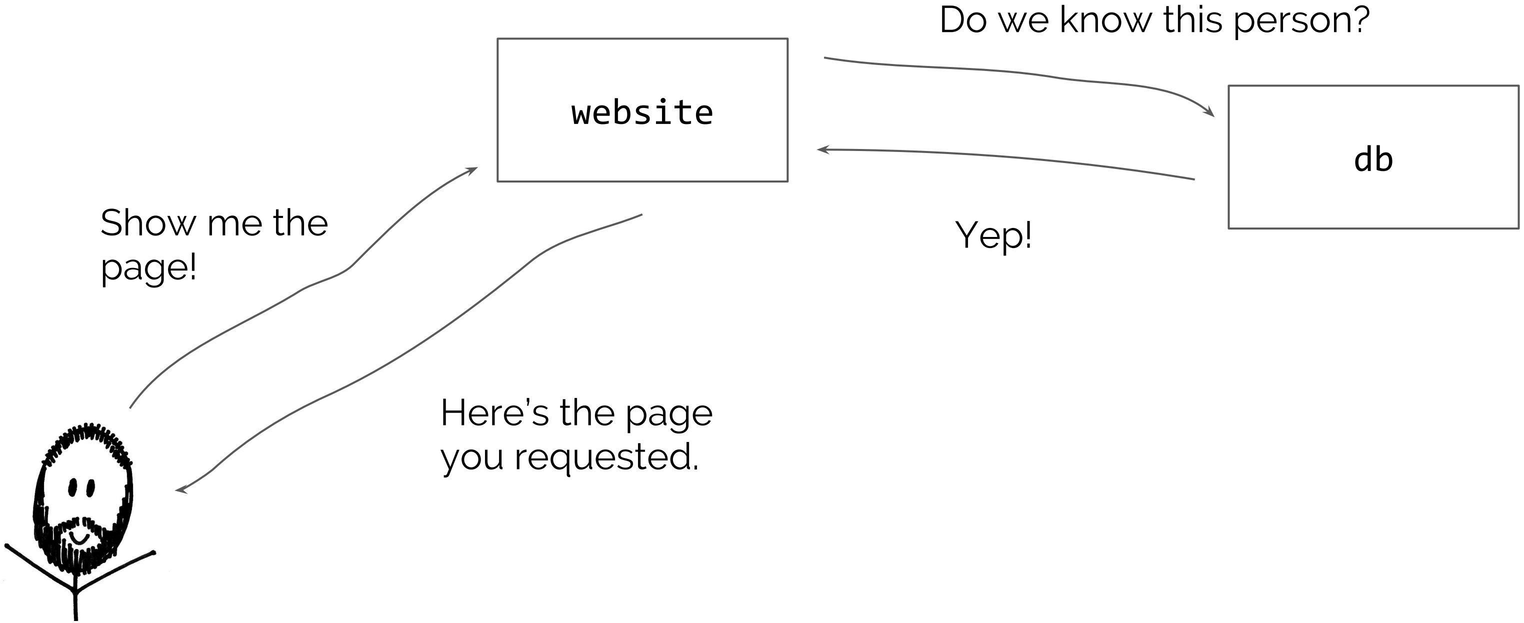
Good

- Can use different types of session caches to speed up access server-side (including local memory)
- Requires less bandwidth for users

Bad

- Always requires some sort of DB / cache to retrieve data

Session Scaling (basic)



Do we know this person?

website

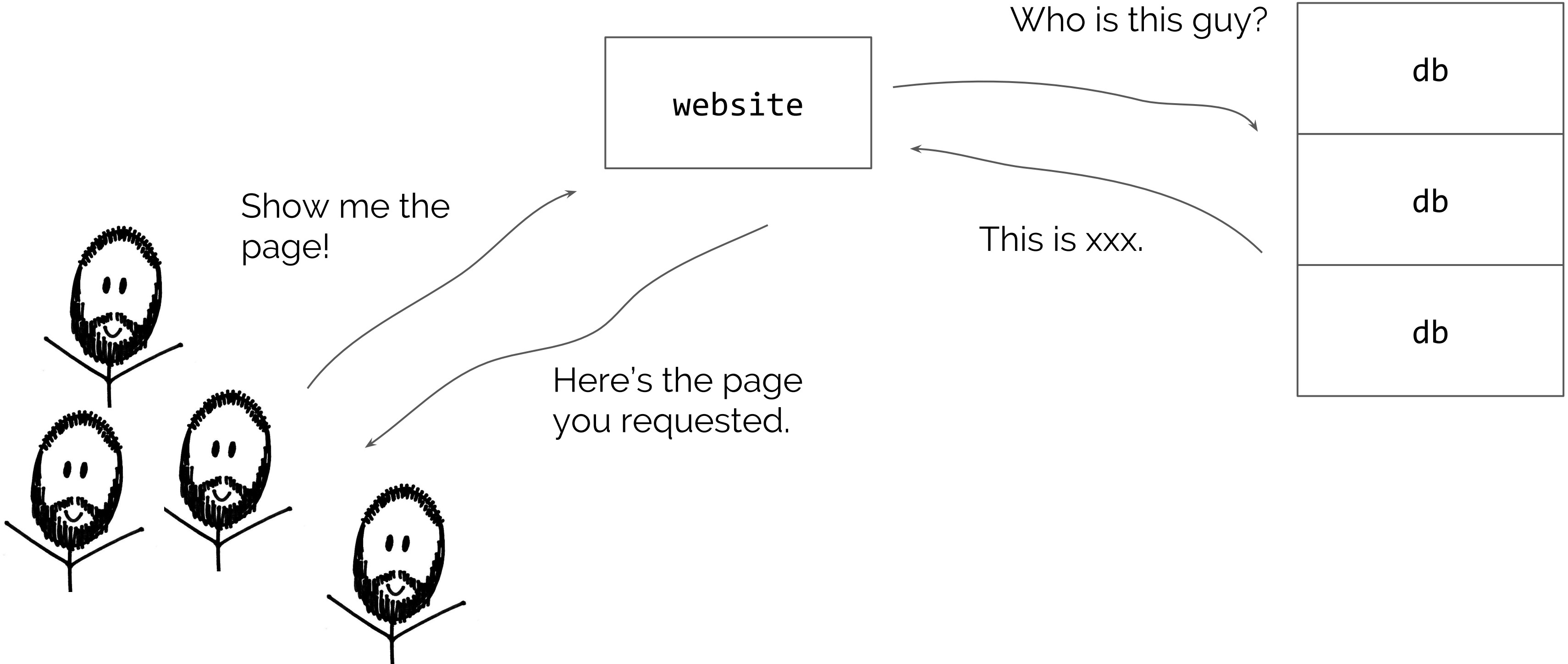
db

Show me the page!

Yep!

Here’s the page you requested.

Session Scaling (advanced)



Who is this guy?

website

db

db

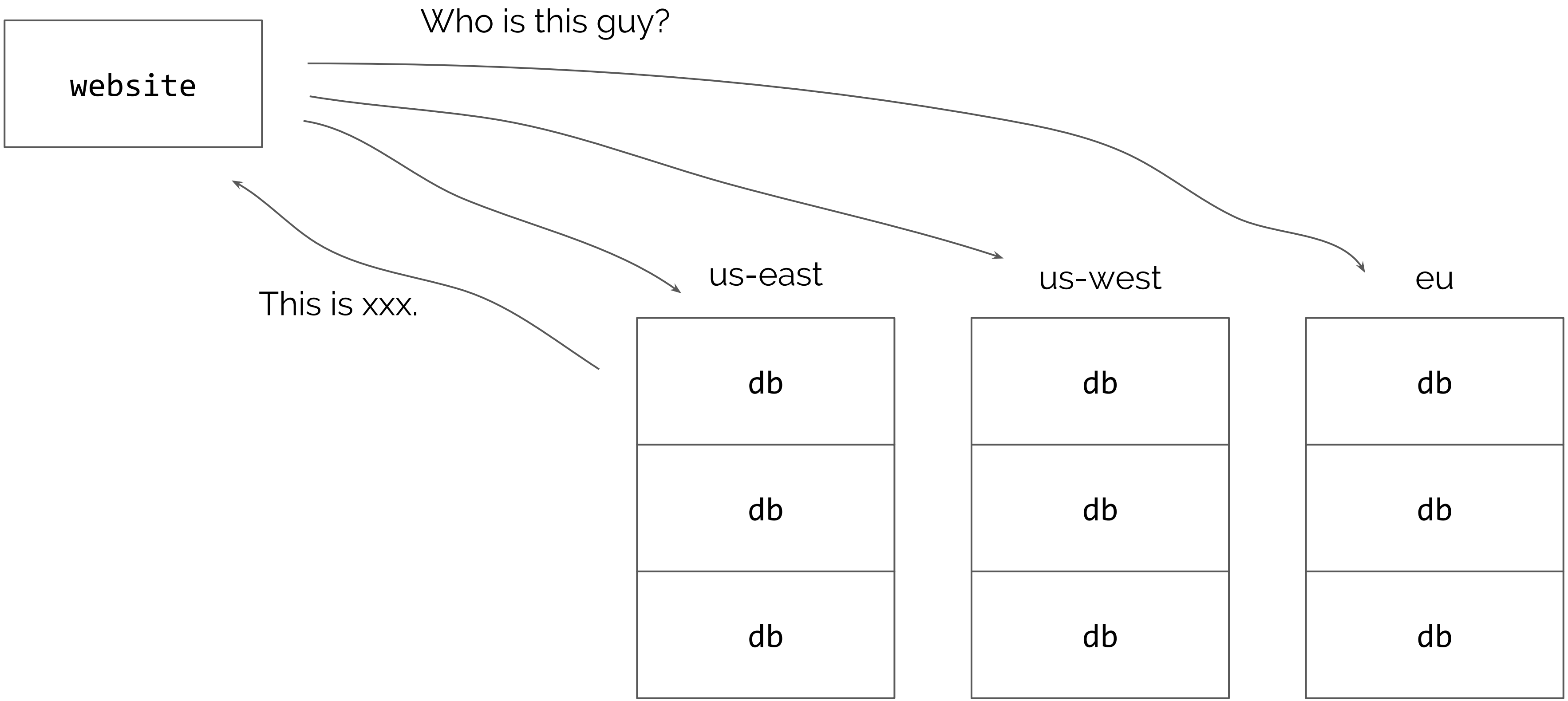
db

Show me the page!

This is xxx.

Here's the page you requested.

Session Scaling (super advanced)

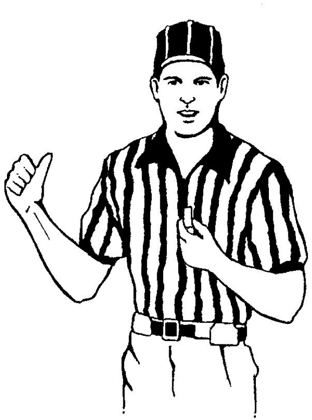


Score

JWTs

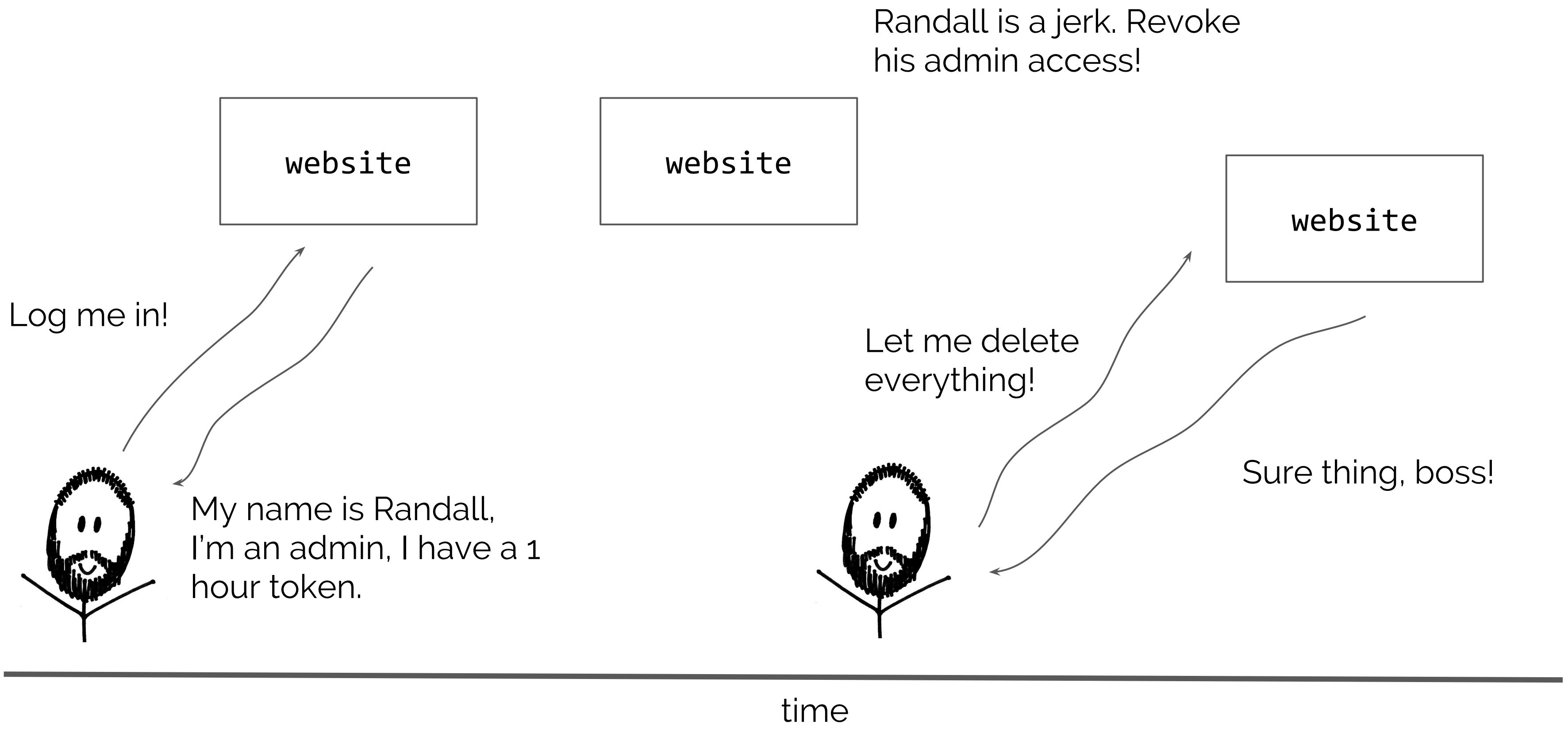
Session Cookies

0



8

JWTs Are Secure By Design



Log me in!

website

My name is Randall,
I'm an admin, I have a 1
hour token.

website

Randall is a jerk. Revoke
his admin access!

Let me delete
everything!

website

Sure thing, boss!

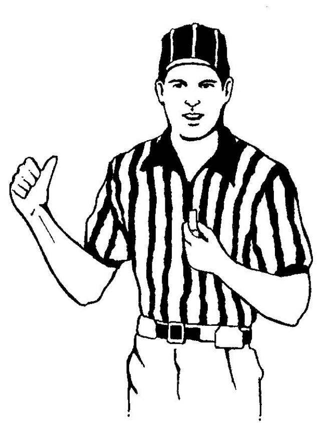
time

Score

JWTs

Session Cookies

0



9

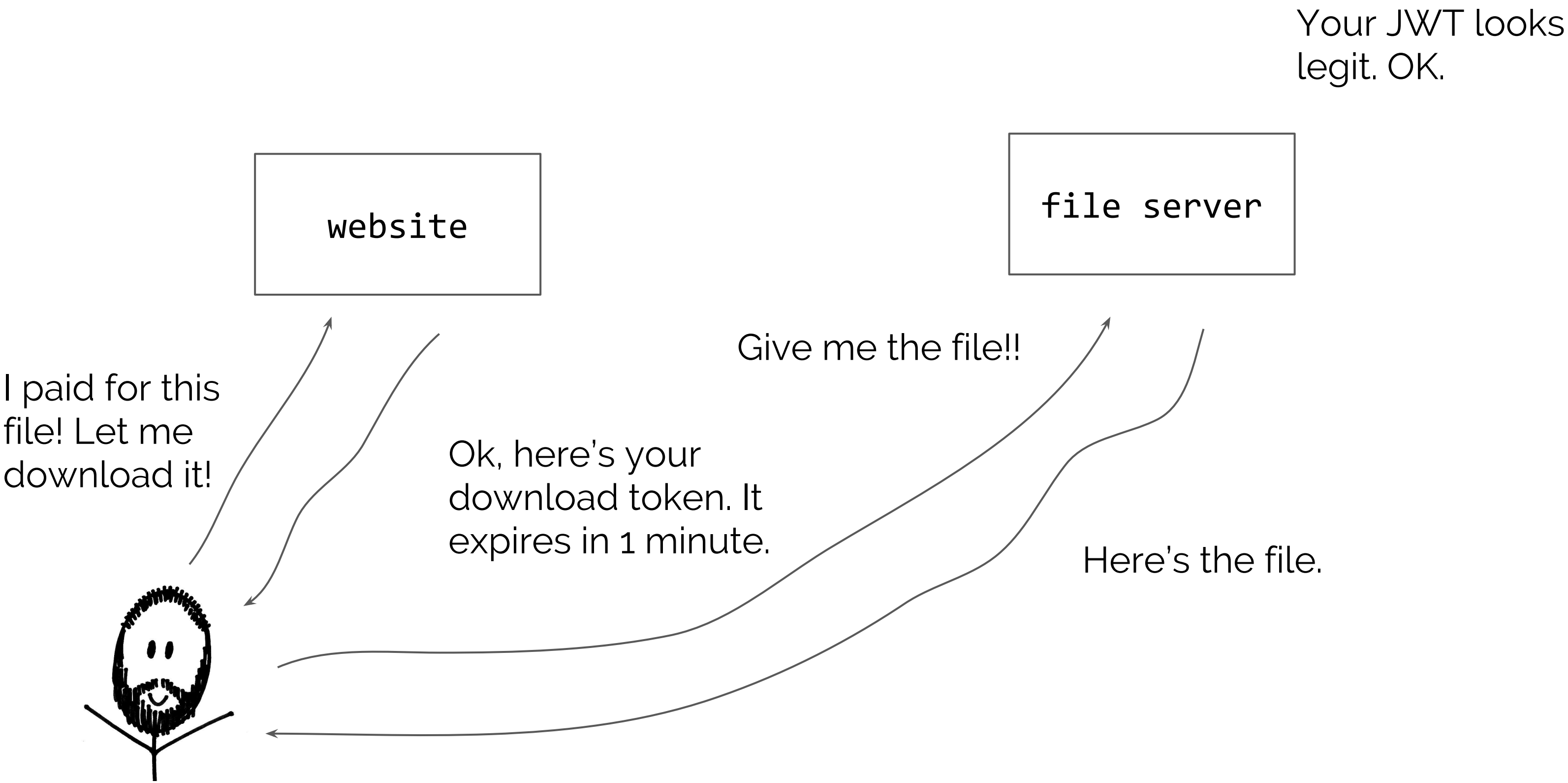
So how should I use JWTs then, you jerk?

Rules for Using Tokens

1. They should have a **short lifespan** (few seconds)
2. They should only be used a **single time**

PROTIP: Don't use JWTs though. There are better, safer, more modern standards for tokens now (e.g., PASETO).

JWT Use Cases



I paid for this file! Let me download it!

website

Ok, here’s your download token. It expires in 1 minute.

Give me the file!!

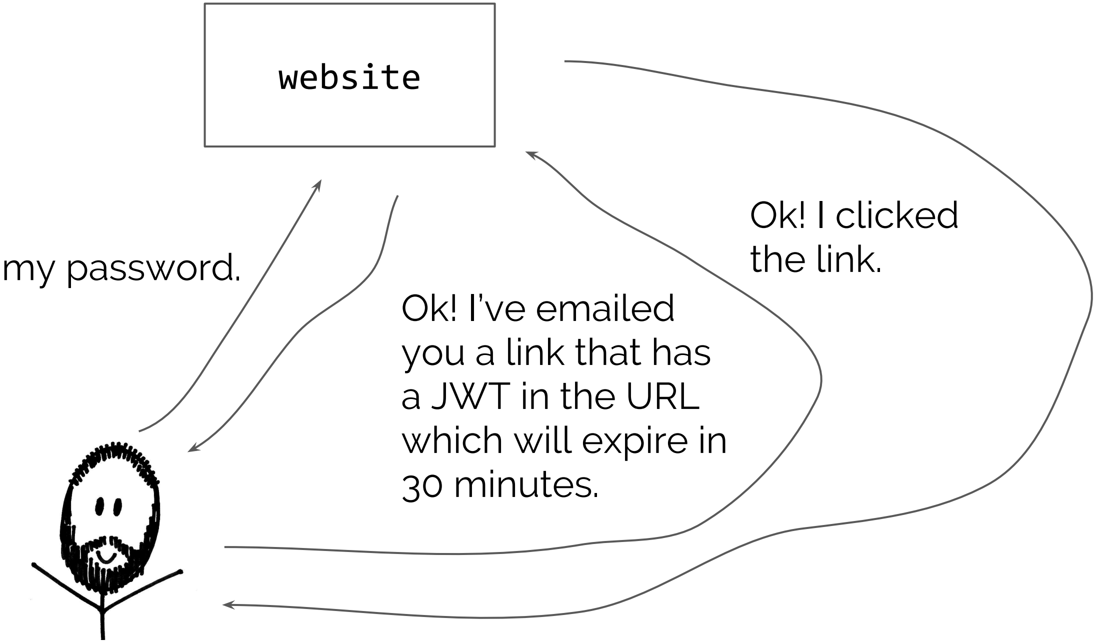
file server

Your JWT looks legit. OK.

Here’s the file.

JWT Use Cases (cont)

This JWT looks legit. I suppose I'll let you reset your password.



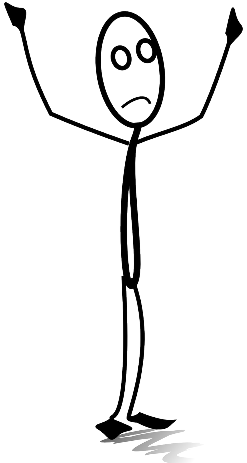
Reset my password.

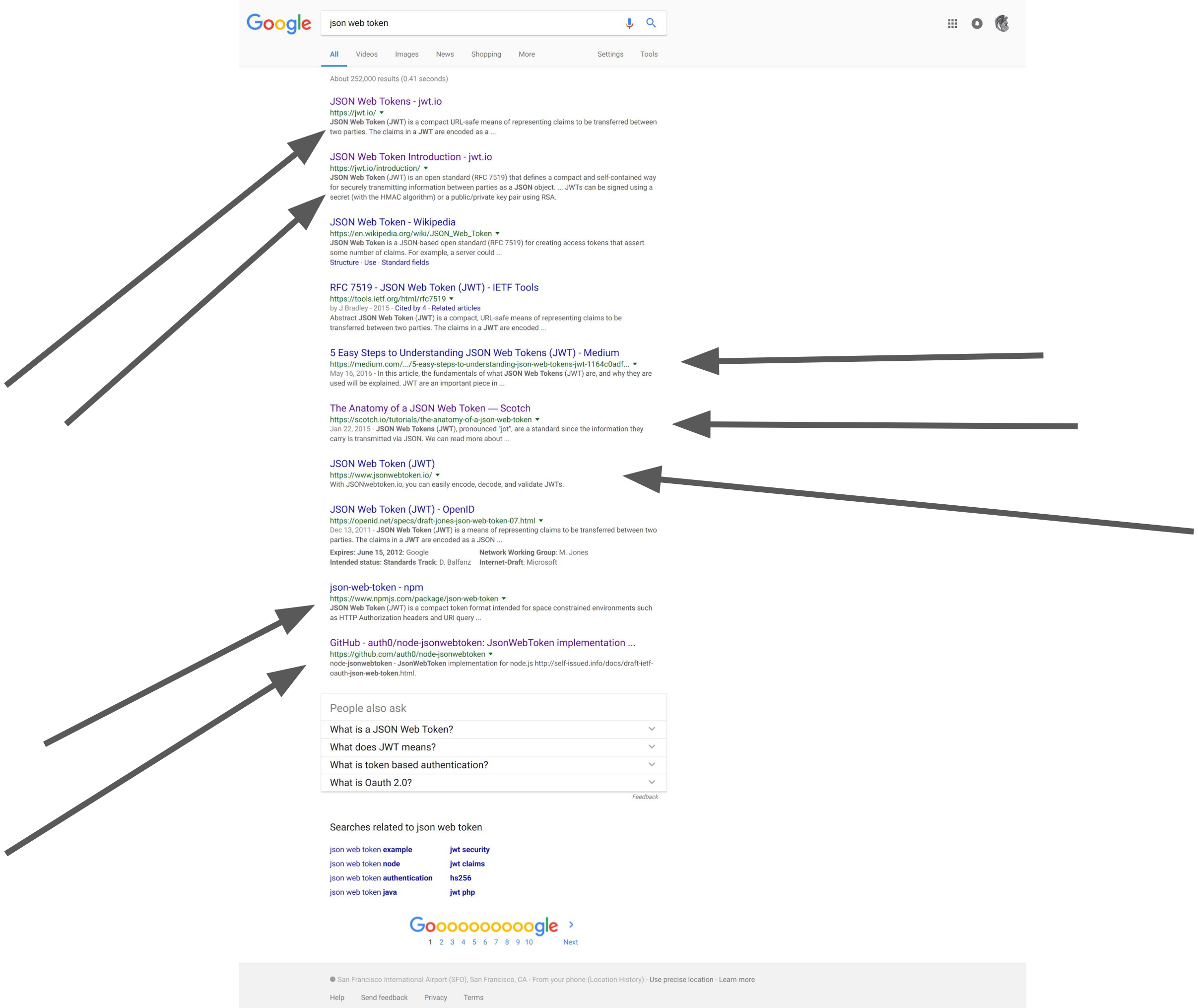
Ok! I've emailed you a link that has a JWT in the URL which will expire in 30 minutes.

Ok! I clicked the link.

Ok, your PW has been reset.

So why are JWTs so popular then?





About 252,000 results (0.41 seconds)

JSON Web Tokens - jwt.io
https://jwt.io/
JSON Web Token (**JWT**) is a compact URL-safe means of representing claims to be transferred between two parties. The claims in a **JWT** are encoded as a ...

JSON Web Token Introduction - jwt.io
https://jwt.io/introduction/
JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a **JSON** object. ... JWTs can be signed using a secret (with the HMAC algorithm) or a public/private key pair using RSA.

JSON Web Token - Wikipedia
https://en.wikipedia.org/wiki/JSON_Web_Token
JSON Web Token is a JSON-based open standard (RFC 7519) for creating access tokens that assert some number of claims. For example, a server could ...
Structure · Use · Standard fields

RFC 7519 - JSON Web Token (JWT) - IETF Tools
https://tools.ietf.org/html/rfc7519
by J Bradley - 2015 - Cited by 4 - Related articles
Abstract **JSON Web Token** (**JWT**) is a compact, URL-safe means of representing claims to be transferred between two parties. The claims in a **JWT** are encoded ...

5 Easy Steps to Understanding JSON Web Tokens (JWT) - Medium
https://medium.com/.../5-easy-steps-to-understanding-json-web-tokens-jwt-1164c0adf...
May 16, 2016 - In this article, the fundamentals of what **JSON Web Tokens** (JWT) are, and why they are used will be explained. JWT are an important piece in ...

The Anatomy of a JSON Web Token — Scotch
https://scotch.io/tutorials/the-anatomy-of-a-json-web-token
Jan 22, 2015 - **JSON Web Tokens** (**JWT**), pronounced "jot", are a standard since the information they carry is transmitted via JSON. We can read more about ...

JSON Web Token (JWT)
https://www.jsonwebtoken.io/
With JSONwebtoken.io, you can easily encode, decode, and validate JWTs.

JSON Web Token (JWT) - OpenID
https://openid.net/specs/draft-jones-json-web-token-07.html
Dec 13, 2011 - **JSON Web Token** (**JWT**) is a means of representing claims to be transferred between two parties. The claims in a **JWT** are encoded as a JSON ...
Expires: June 15, 2012: Google **Network Working Group**: M. Jones
Intended status: Standards Track: D. Balfanz **Internet-Draft**: Microsoft

json-web-token - npm
https://www.npmjs.com/package/json-web-token
JSON Web Token (JWT) is a compact token format intended for space constrained environments such as HTTP Authorization headers and URI query ...

GitHub - auth0/node-jsonwebtoken: JsonWebToken implementation ...
https://github.com/auth0/node-jsonwebtoken
node-**jsonwebtoken** - **JsonWebToken** implementation for node.js http://self-issued.info/docs/draft-ietf-oauth-**json-web-token**.html.

People also ask

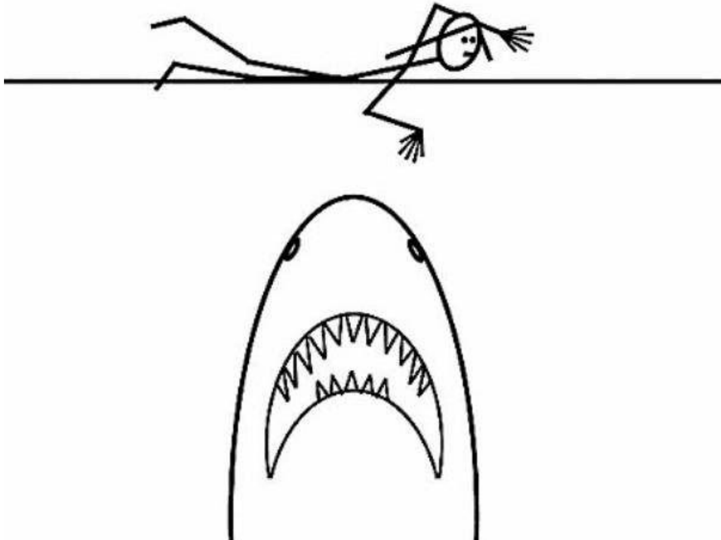
What is a JSON Web Token?
What does JWT means?
What is token based authentication?
What is Oauth 2.0?

Searches related to json web token

json web token **example**
json web token **node**
json web token **authentication**
json web token **java**
jwt security
jwt claims
hs256
jwt php

San Francisco International Airport (SFO), San Francisco, CA - From your phone (Location History) - Use precise location - Learn more

What else even is there?!



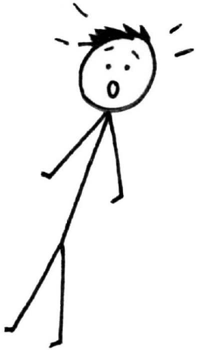
PASETO! https://paseto.io

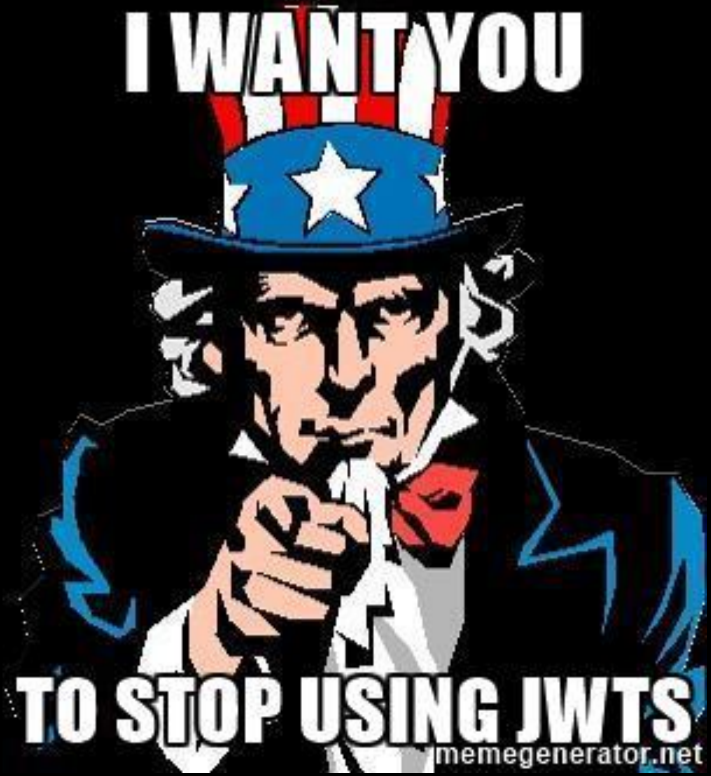
JWTs

- Lots of different options (algorithms, use cases, etc.)
- Confusing / complex spec
- Hard to implement correctly

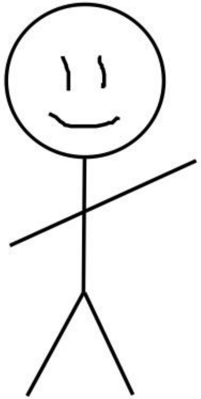
PASETO

- Two options only (local or public?)
- Simple, not confusing
- Nearly impossible to implement incorrectly




I WANT YOU
TO STOP USING JWTS
memegenerator.net

Thank you!



teespring.com/dontusejwts