



Building the ultimate login and signup

OWASP New Zealand Day 2017

```
$ whoami
```

```
PS> $env:username
```

Matt Cotterell

- Security Engineer @ Fairfax Media (stuff.co.nz and friends)
- Previously Orion Health
- ~5 years professional .NET developer, been dabbling in it for nearly 10 years now!
- Security focus in web tech, particularly around authentication and authorisation flows



mattcotterellnz



mattcotterellnz



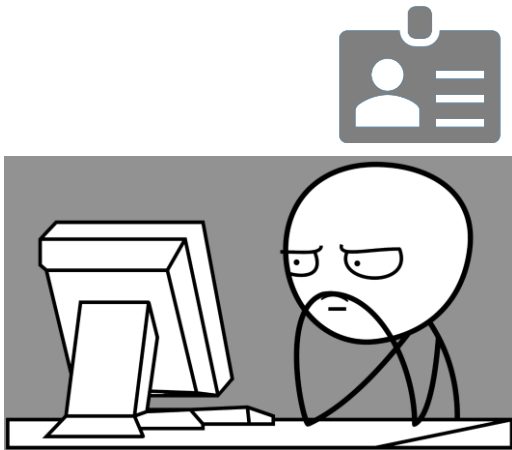
@mattcotterellnz

Overview



- Registration
 - Get only what you need
 - Protecting passwords in the database
 - Getting your users to choose good passwords
 - Preventing spam accounts
- Before the login
 - Password Managers
 - Use OS/Browser features
 - Password Reset
- During the login
 - Securing data in transit
 - Session hijacking/fixation
 - Dealing with brute forcing attempts
 - Protecting your users with two factor authentication
- After they're logged in
 - Open Redirects
 - Security Questions

Registration Page



- Identifier (username)
- Authentication credential (password)
- Other stuff (email, name, phone etc)



Registration Page



**Gather only the
information you need**



Register.

Create a new account.

Username

Password

Confirm password

I'm not a robot



reCAPTCHA
[Privacy](#) - [Terms](#)

Register

TOO MUCH

INFO!

Privacy Act & codes

[Home](#) / [Privacy Act & codes...](#) [Privacy principles](#) / [Purpose for collecti...](#)

[Introduction](#)[The Privacy Act](#)[Privacy principles](#)[Purpose for collection](#)[Source of information](#)[What to tell an individual](#)[Manner of collection](#)[Storage and security](#)[Access](#)[Correction](#)[Accuracy](#)[Retention](#)

Purpose for collection of personal information (principle one)

[Print](#) | [Email this page](#)

Personal information shall not be collected by any agency unless -

- (a) the information is collected for a lawful purpose connected with a function or activity of the agency; and
- (b) the collection of the information is necessary for that purpose.

Agencies need to carefully consider the purpose for which they collect personal information. If an agency defines its purpose too narrowly, it may be unable to use information in the way that it wants to in the future. But, if its purposes are too broad, they risk becoming meaningless - the agency could be collecting information it has no real need for and people could be confused.

Having a clearly defined purpose will make it much easier for an agency to respond to its obligations under the other principles of the Act.

If you're collecting personal information, check these questions:

- 1) Do I have a lawful purpose for collecting this information?
- 2) Is that purpose connected with one of my agency's functions or activities?
- 3) Do I really need to collect this information to achieve that purpose?



Pwned websites

Breached websites that have been loaded into this service



Qatar National Bank


In July 2015, the Qatar National Bank suffered a data breach which exposed 15k documents totalling 1.4GB and detailing more than 100k accounts with passwords and PINs. The incident was made public some 9 months later in April 2016 when the documents appeared publicly on a file sharing site. Analysis of the breached data suggests the attack began by exploiting a SQL injection flaw in the bank's website.

Compromised data: Bank account numbers, Banking PINs, Customer feedback, Dates of birth, Financial transactions, Genders, Geographic locations, Government issued IDs, IP addresses, Marital statuses, Names, Passwords, Phone numbers, Physical addresses, Security questions and answers, Spoken languages

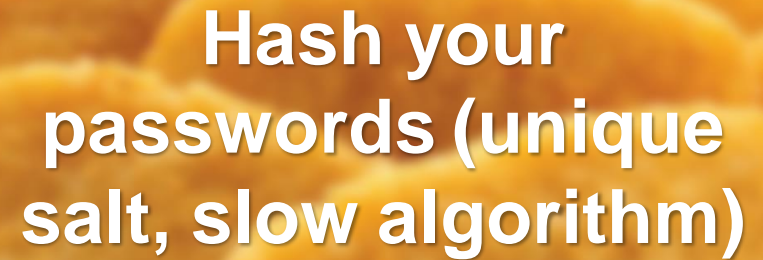
Gather only the information you need,
otherwise it is an unnecessary liability



Registration Page

A close-up, slightly blurred photograph of a cat's face, showing its eyes and whiskers. The image is used as a background for the first text box.

**Gather only the
information you need**

A close-up photograph of golden-brown french fries, used as a background for the second text box.

**Hash your
passwords (unique
salt, slow algorithm)**

Password Hashing 101



xc3511 -> 3ffa611f12317c42f7847ed69640052c

...

xc3511 -> 3ffa611f12317c42f7847ed69640052c

xc3511 -> 3ffa611f12317c42f7847ed69640052c

xc3511 -> 3ffa611f12317c42f7847ed69640052c

xc3511 -> 3ffa611f12317c42f7847ed69640052c

xc3511 -> 3ffa611f12317c42f7847ed69640052c

xc3511 -> 3ffa611f12317c42f7847ed69640052c



Password Hashing 101 - Take 2

xc3511 + 65d184854bc0aa

-> beae75e6fc616d3ddda5bf56dd938220

...

xc3511 + d001ba500ac588

-> df1a4e33ba017bf414bbb37545293404

xc3511 + bf414bbb37df1a

-> afc1996b95d611ba11ae907a329df1b2

Password Hashing 101 - Take 2 3

xc3511 + 65d184854bc0aa x 1 iteration

(~20 μ s) -> b6618740c7a775800e292f74b3cd27c7...

...

xc3511 + 65d184854bc0aa x 10000 iterations

(~200 ms) -> fed559ccbc2dd83d10e57133702fa812...

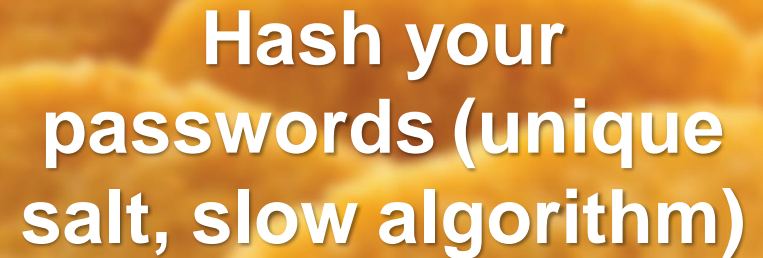
A photograph of several golden-brown, breaded chicken nuggets arranged on a white plate. In the background, a clear glass salt shaker with a silver top is visible. A dark horizontal banner is overlaid across the middle of the image, containing white text.

Use slow hashes with unique salts

Registration Page

A close-up photograph of a cat's face, showing its eyes and whiskers, used as a background for the first text box.

Gather only the information you need

A close-up photograph of golden-brown french fries, used as a background for the second text box.

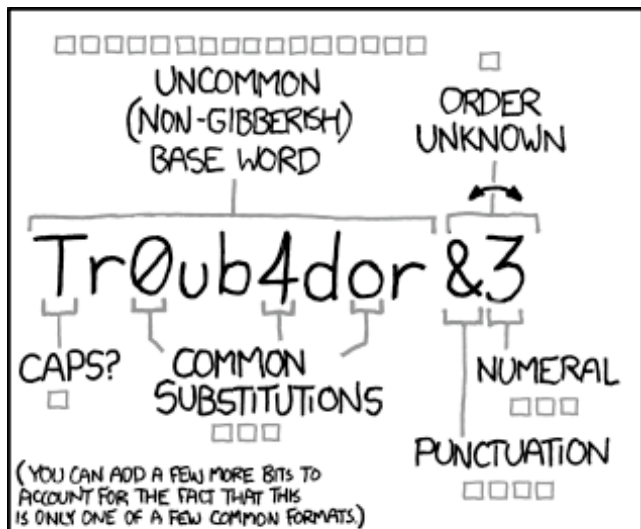
Hash your passwords (unique salt, slow algorithm)

A blurred, colorful background with shades of yellow, orange, and blue, used as a background for the third text box.

Encourage highly entropic passwords

Encouraging strong passwords

- Lots of misconceptions about how to choose a password
 - Basketball1991!
 - qwER43@!
 - T!g3r1601
 - This isn't helped by tooling
 - This isn't helped by IT industry leaders
 - This isn't helped by even our own security industry
-



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

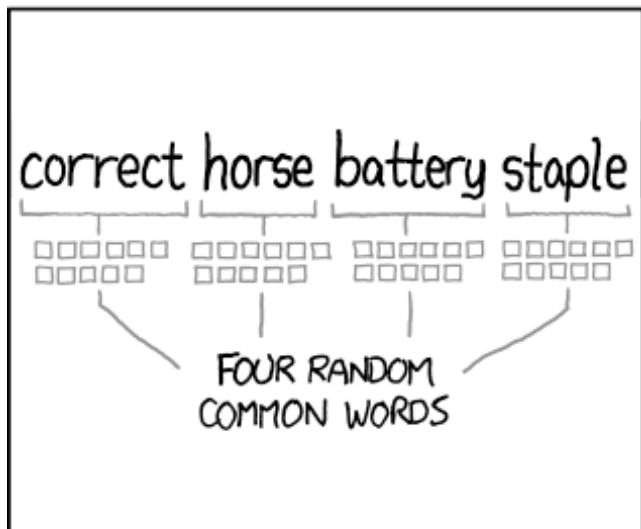
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Introducing: zxcvbn.js!



- A Javascript library that gives you an extremely easy-to-use password strength meter
- Intelligent, entropy-based strength measurements
 - Breaks the password into pieces based off dictionary words, patterns, dates, etc
- Provides recommendations on how to strengthen your passwords as you choose them
- Provides a simple 1 to 5 scoring system as you type



<https://github.com/dropbox/zxcvbn>

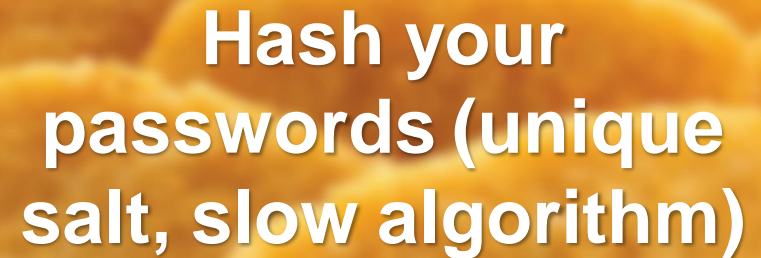


Encourage entropy over patterns,
discourage common passwords

Registration Page

A close-up photograph of a light-colored cat's face, looking slightly to the right.

Gather only the information you need

A close-up photograph of a hand holding a smartphone, with the screen displaying a registration form.

Hash your passwords (unique salt, slow algorithm)

An abstract background with a mix of yellow, blue, and red colors, resembling a colorful pattern or a close-up of a textured surface.

Encourage highly entropic passwords

A blurred background showing a crowd of people, possibly at a public event or gathering.

Discourage Automated Signups

humans Preventing spammers from signing up...



Prove you're not a robot

exposure *achieve*

Type the two pieces of text:



WORD
VERIFICATION

 &

Password (required)

Birthday (required)
March 31 1981


Human test (required)
Type in the text you see in the box below.

Sorry, your text and the image didn't match. Please try again.

Read (really!)
 I have read and agree to the [Terms of Use](#) and [Privacy Policy](#).

Security Check

Enter both words below, separated by a space.
Can't read the words below? Try different words or an audio captcha.

 auriga

Text in the box:

What's This?

Submit Cancel



8Y70IO1

Welcome!

Antigate.Com is an online service which provides real-time captcha-to-text decodings. This works easy: your software uploads a captcha to our server and receives text from it within seconds.

The main features are:

- Cheapest price on the market - starting from **0.7USD per 1000** images, depending on the daily volume
- Minimum payment is 1 USD, pay-per-captcha payment basis, no recurring charges.
- Average decoding speed is 15 seconds
- Pretty simple [API](#) (over HTTP) which allows you to add captcha-to-text decoding functionality to your application
- Unlimited Multi-threading. You can send as many captchas as you like in a second.
- **De-Captcher** and **Captchabot** API protocols are [completely supported](#)
- Accurate usage and payments statistics
- Never-busy-queue. We keep our captcha queue in the way to make sure that all captchas are decoded in average 15 seconds. Those who pay more receive the priority. Still the [average bid](#) is quite cheap!
- Service is provided on 24/7/365 basis since November 2007, our distributed infrastructure allows 99.9% uptime
- 100% of images decoded by human workers from [around the world](#).. This is why by using our service **you** help them to feed themselves and their families. Be sure they are very happy to earn this money!

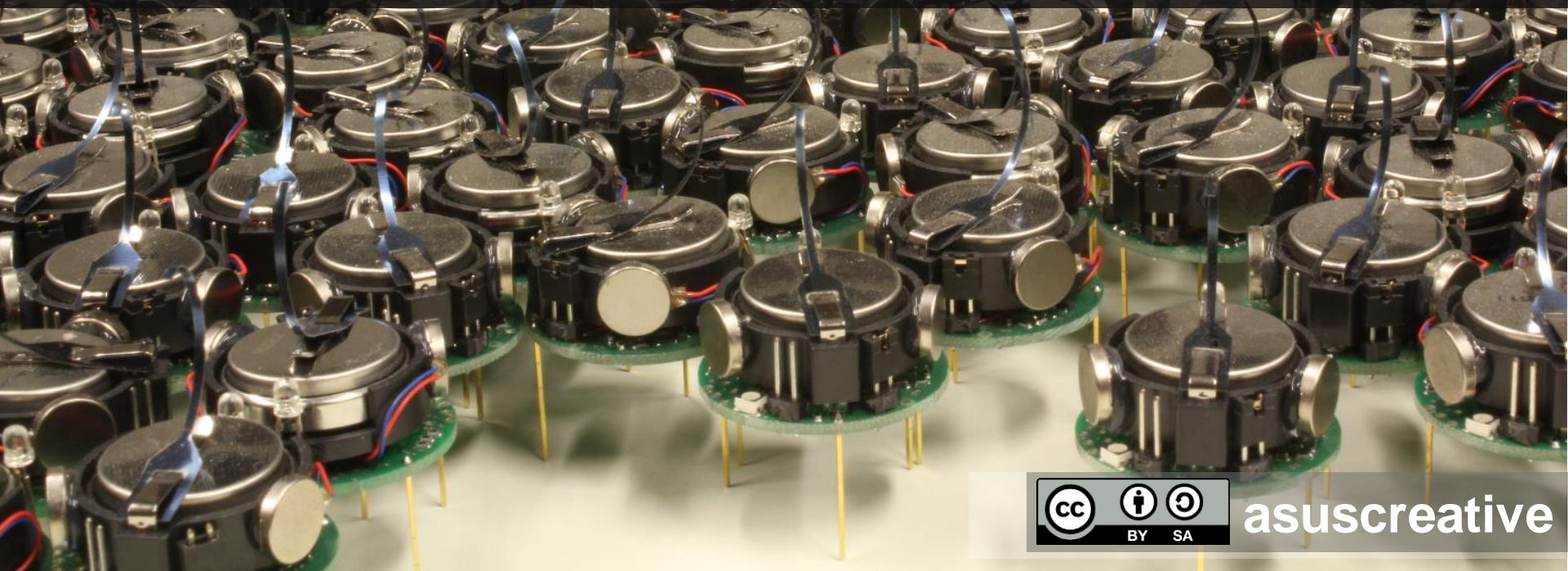
To use our system you need to pass free registration. It's easy and you'll be able to test our system for free (10 free captcha decodings).

[Free Signup](#)

[My Account](#)

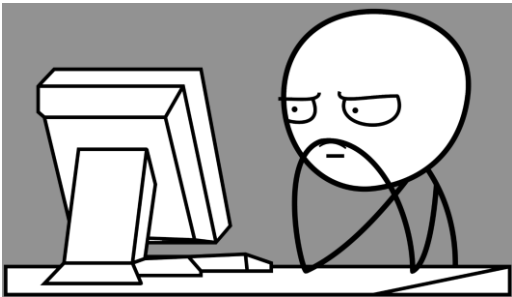


Use Google reCAPTCHA, I guess?



asuscreative

Login Page



Before the Login

A blurred image of a smartphone with a password manager app icon on the screen. The text "Let people use password managers" is overlaid on the image in white, bold font.

**Let people use
password managers**

```
<input type="password" onpaste="return false;">
```





Ben Woodward @Sacro

14 Jul 15

@BritishGas please can you remove 'onpaste="return false"' from password confirmation, it breaks @LastPass the ability to paste passwords.



British Gas Help 

@BritishGasHelp

Follow

@Sacro Hi Ben, I understand but as a business we've chosen not to have the compatibility with password managers. Thanks,
Joe

2:00 AM - 15 Jul 2015

  164  26



Pascal Hartig @passy

6 May 14

.@BritishGasHelp Disallowing pasting and therefore password managers is NOT a standard practice. It's unnecessary and dangerous.



British Gas Help 

@BritishGasHelp

Follow

@passy We'd lose our security certificate if we allowed pasting. It could leave us open to a "brute force" attack. Thanks ^Steve

9:59 PM - 6 May 2014

  507  154

Do not disable “paste” functionality in password fields



Before the Login

A hand holding a smartphone with a password manager app open, showing a list of passwords. The text "Let people use password managers" is overlaid on the image.

**Let people use
password managers**

A close-up of a person's hands typing on a keyboard. The text "Password Reset" is overlaid on the image.

Password Reset

ID	Username	Reset Token	Expires
1	mattcoterellnz	9cdfb439c7...	2017-02-28 00:00





Be careful of social engineering,
authenticate user through their email
address

Before the Login

A close-up photograph of a smartphone, likely an iPhone, with a dark screen and a silver or light-colored case. The phone is positioned diagonally.

Let people use
password managers

A photograph showing a person's hands using a green and black tool, possibly a password reset tool or a lock-picking device, on a lock. The person is wearing an orange safety vest.

Password Reset

A photograph of a computer screen displaying a login form. The focus is on a password field, which is highlighted with a red border. The text on the screen is partially obscured by the overlay text.

Always use
`type="password"` for
password fields

Well, duh? Right?



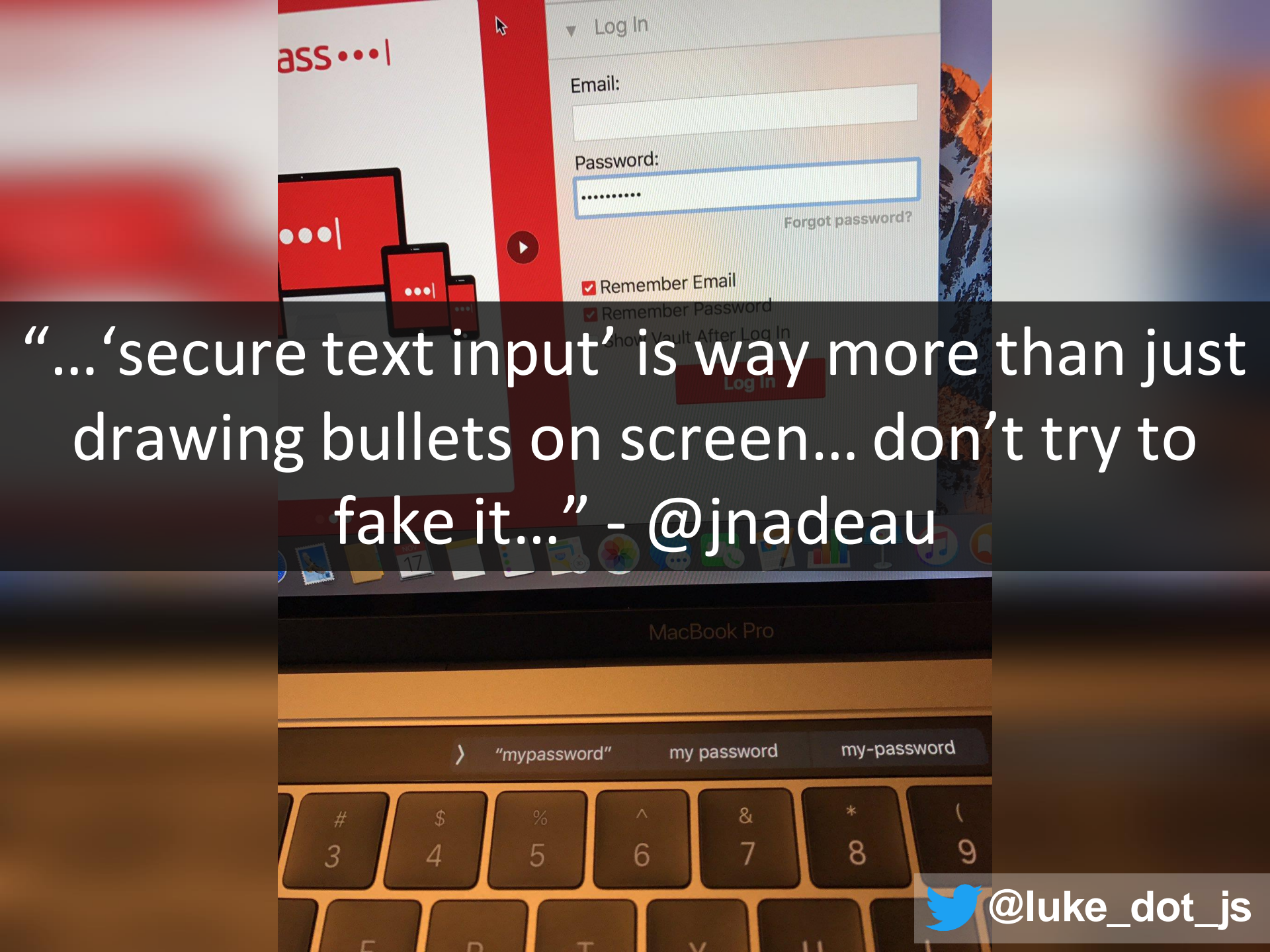
May be handled differently
in the browser's memory

Can still be styled



Changes behaviour in
some situations (such as
autocomplete)

Browser will warn users if the page
is loaded over unsecure HTTP



“...‘secure text input’ is way more than just drawing bullets on screen... don't try to fake it...” - @jnadeau



@luke_dot_js

During the Login





Use HTTPS *everywhere*, and not just when sending sensitive data



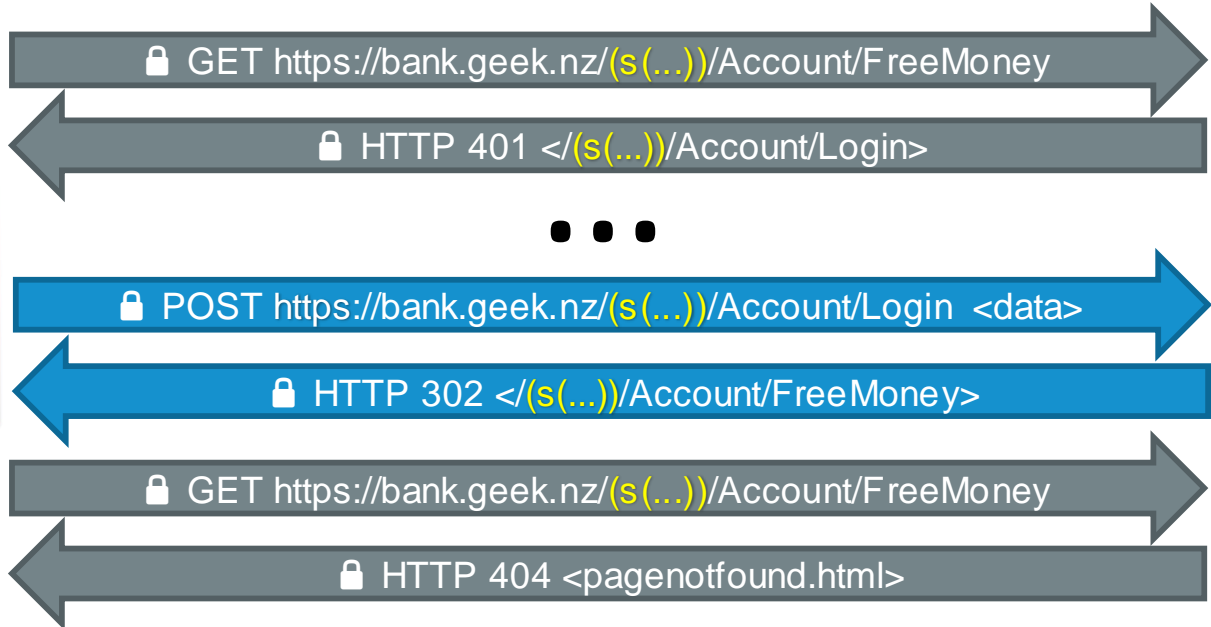
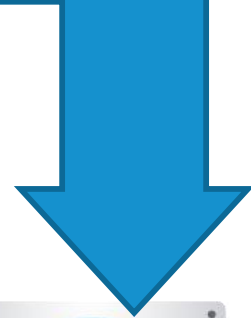
During the Login

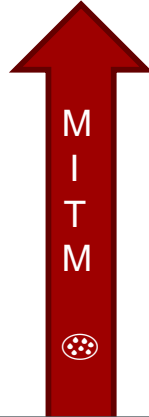





You should totally click "[https://bank.geek.nz/\(s\(eW91IGhhdmUgdG9vIG11Y2ggdGltZSBvbiB5b3VyIGhhbmRz\)\)/Account/FreeMoney/](https://bank.geek.nz/(s(eW91IGhhdmUgdG9vIG11Y2ggdGltZSBvbiB5b3VyIGhhbmRz))/Account/FreeMoney/)"

GET https://bank.geek.nz/(s(eW91IGhhdmUgdG9vIG11Y2ggdGltZSBvbiB5b3VyIGhhbmRz))/Account/StealMoney/





GET <http://bank.geek.nz/Account/FreeMoney> 



Use HTTPS everywhere, and expire session cookies after every login/logout



During the Login

A photograph of a yellow metal gate standing on a concrete path in a grassy area.

Secure data in transit

A photograph of several white, featureless masks, one of which is being held by a hand.

Mitigate session hijacking/fixation

A photograph of a row of red stop signs on a street, slightly out of focus.

Rate limit brute force attempts



POST https://bank.geek.nz/Account/Login <"aaaaf">





POST https://bank.geek.nz/Account/Login <\$yourPetsName>





Block IPs, not accounts. Challenge accounts with CAPTCHAs.

During the Login



Factors of Authentication



Knowledge

"Something you know"

- Password
- PIN



Possession

"Something you have"

- U2F Token
(*"Security Key"*)
- TOTP/HOTP token
- SIM Card
- RSA SecurID token
- Smart Card
- Your Phone/Laptop
- Physical Key



Inherence

"Something you are"

- Fingerprint Scan
 - Iris Scan
 - Facial Recognition
 - DNA
 - Voice Recognition
-



Use two *different* factors when authenticating your users

After the Login



Open Redirects



Warning: this is a malicious link!

Username: owaspday
Password: 0WASPday2017!
Two Factor Token: (blank)

<https://bit.ly/2mqAGDA>



Ensure user-controlled redirects go to a domain you control

After the Login



Factors of Authentication



Knowledge

"Something you know"

- Password
- PIN



Possession

"Something you have"

- U2F Token
- ("Security Key")
- TOTP/HOTP token
- SIM Card
- RSA SecurID token
- Smart Card
- Your Phone/Laptop
- Physical Key



Inherence

"Something you are"

- Fingerprint Scan
- Iris Scan
- Facial Recognition
- DNA
- Voice Recognition

This does not mean "something you and a bunch of other people know!"



“Although your family and friends might know the answers to [your security questions], your access number and confidential password is the protection you have to keep your banking private from them.”

Security Questions don't reliably
authenticate an individual, and are easily
predicted



Also, I'm 27 years old, I don't have a
favourite colour.

All that just to allow logins? 😞

- If you have any questions, please feel free to ask!
- I'll be around during the break...
- ...or message me on Twitter!

 **mattcoterellnz**

 **mattcoterellnz**

 **@mattcoterellnz**
