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
Register
TOO MUCH
INFO!
Purpose for collection of personal information (principle one)

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?
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

Gather only the information you need

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

xc3511 + 65d184854bc0aa x 1 iteration
(\sim 20 \ \mu s) \rightarrow \text{b6618740c7a775800e292f74b3cd27c7...}

... 

xc3511 + 65d184854bc0aa x 10000 iterations
(\sim 200 \ \text{ms}) \rightarrow \text{fed559ccbc2dd83d10e57133702fa812...}
Use slow hashes with unique salts
Registration Page

- Gather only the information you need
- Hash your passwords (unique salt, slow algorithm)
- Encourage highly entropic passwords
Encouraging strong passwords

• Lots of misconceptions about how to choose a password
  o Basketball1991!
  o qwER43@
  o 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
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.

https://xkcd.com/936/
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

Gather only the information you need

Hash your passwords (unique salt, slow algorithm)

Encourage highly entropic passwords

Discourage Automated Signups
Preventing spammers from signing up...
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 **0.7 USD 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-Captcha** 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?
Login Page
Let people use password managers
<input type="password" onpaste="return false;">
Ben Woodward @Sacro
@BritishGas please can you remove 'onpaste="return false"' from password confirmation, it breaks @LastPass the ability to paste passwords.

British Gas Help @BritishGasHelp

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

@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

Likes: 154
Do not disable “paste” functionality in password fields
Before the Login

Let people use password managers

Password Reset
<table>
<thead>
<tr>
<th>ID</th>
<th>Username</th>
<th>Reset Token</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>mattcotterellnz</td>
<td>9cdfb439c7...</td>
<td>2017-02-28 00:00</td>
</tr>
</tbody>
</table>

✉ "Please click https://bank.geek.nz/reset/9cdfb439c7..."

🔒 GET https://bank.geek.nz/reset/9cdfb439c7...

🔒 HTTP 200 <change_password.html>
Be careful of social engineering, authenticate user through their email address
Before the Login

Let people use password managers

Password Reset

Always use type="password" for password fields
Well, duh? Right?
May be handled differently in the browser’s memory

Can still be styled

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

Changes behaviour in some situations (such as autocomplete)
“...‘secure text input’ is way more than just drawing bullets on screen... don’t try to fake it...” - @jnadeau
During the Login

Secure data in transit
Use HTTPS *everywhere*, and not just when sending sensitive data.
During the Login

Secure data in transit

Mitigate session hijacking/fixation
You should totally click “https://bank.geek.nz/(s(eW91IGhhdmUgdG9vIG11Y2ggdGltZSBvbiB5b3VyIGhhbmRz))/Account/FreeMoney/”
MITM

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

$ ./geekbank

MI

🍪
Use HTTPS **everywhere**, and expire session cookies after every login/logout
During the Login

- Secure data in transit
- Mitigate session hijacking/fixation
- Rate limit brute force attempts
POST https://bank.geek.nz/Account/Login <"password">

POST https://bank.geek.nz/Account/Login <"123456">

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

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

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

POST https://bank.geek.nz/Account/Login <"$yourPetsName>
Block IPs, not accounts. Challenge accounts with CAPTCHAs.
During the Login

- Secure data in transit
- Mitigate session hijacking/fixation
- Rate limit brute force attempts
- Two Factor Authentication
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: OWASPday2017!
Two Factor Token: (blank)

Ensure user-controlled redirects go to a domain you control
After the Login

Open Redirects

Security Questions
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!

@mattcotterellnz
@mattcotterellnz
@ mattcotterellnz