Developer Induction

Agenda

Time	Topic
30 mins	Welcome and introductions
30 mins	Introduction to the DSP
2 hours	Hands on with the DSP
1 hour	Continuous integration with Drone
45 mins	Lunch
30 mins	Securing applications in the Home Office
1 hour	Accessibility

The Central Team

Who are we?

Developers and DevOps Engineers

Why do we exist?

Our aim – to enable delivery teams to deliver higher quality software and services more quickly

- We're still researching how best to do this, but have done a lot already
- Generally we will be looking at:
  - Central services, products, libraries, and tooling
  - Supporting projects to use these services, and align to best practice
  - Supporting consistently high quality recruitment

What have we done?

- DevOps team are more established, and delivered a number of services
  - Hosting platform
  - Gitlab
  - Monitoring with Sysdig
  - Logging with ELK
  - Artifactory
  - CI
  - Keycloak authentication

What have we done?

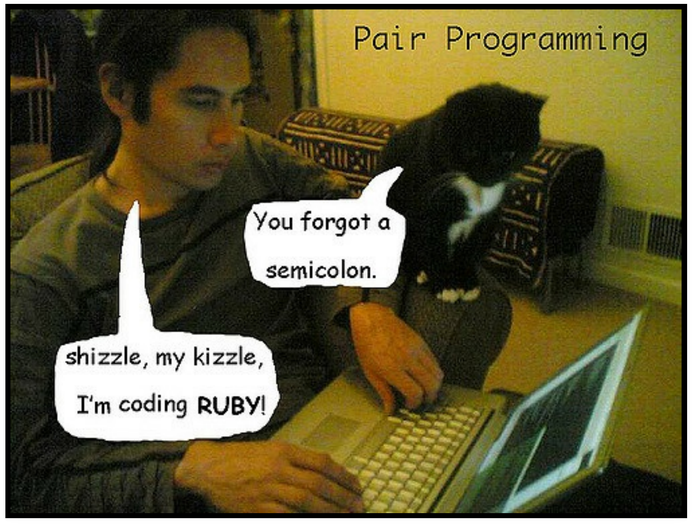
- More recently, together we have delivered
  - Documentation for the platform
  - Developer inductions
  - Drone CI improvements and guidance
  - Survey tools research and recommendation
  - Security scanning tools initial research

What's next?

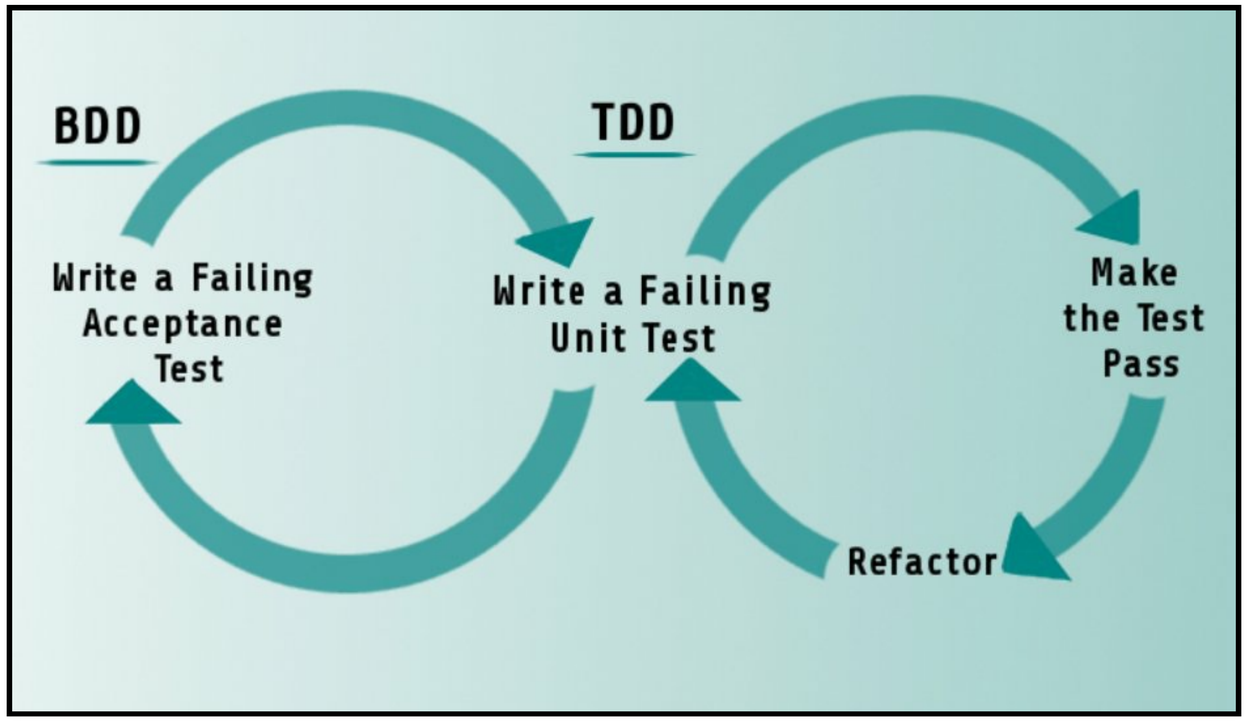
- Find out what's next on our kanban boards
  - Central Team - Dev
  - Central Team - DevOps
- But generally…
  - More user research...
  - Dashboards for project teams

How do developers in the Home Office work?

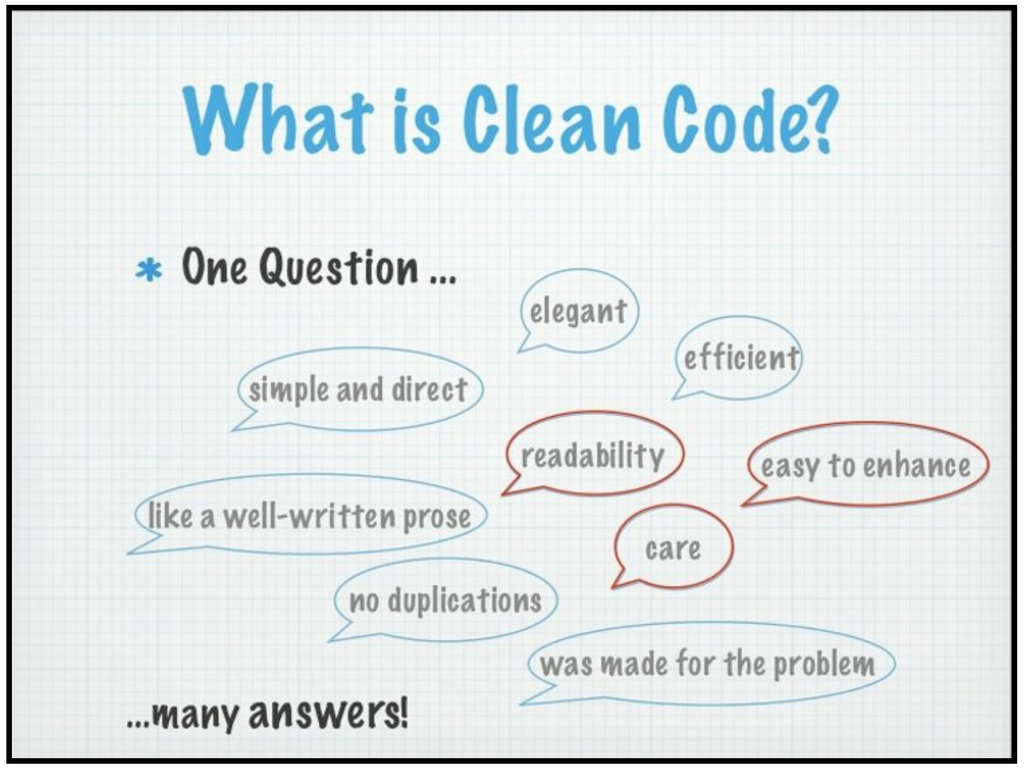
Pair programming



BDD and TDD


BDD
TDD
Write a Failing Acceptance Test
Write a Failing Unit Test
Make the Test Pass
Refactor

Clean Code


What is Clean Code?
One Question ...
elegant
efficient
simple and direct
readability
easy to enhance
like a well-written prose
care
no duplications
was made for the problem
...many answers!

Branching

- Protect your master branch
  - No force pushing to master
  - Reviews required on PRs before they can be merged
- Develop each story on a new branch
- Merge to master regularly to avoid merge hell

Expectations

- Understand the platform
- Responsible for security
- Responsible for documentation
- Collaborating with others to complete stories
- Reach out to other teams, identify opportunities to share best practice and re-use components
- Publicise libraries and services
- Up to 20% of time on non-project work
- Participate in away days

In return you get...

- To work with really good people
- Flexible working
- To use interesting tech
- To work with other professions
- An opportunity to give back to wider Home Office, Cross Government, and beyond...

The technology we use

- Java 8, Scala, or Javascript
- Java – Spring, Dropwizard
- Scala – Play, Spray
- Javascript
  - Back end – node, express
  - Front end – angular, react
- Docker
- Kubernetes

The HO technology stack

More detail on the technology stack is kept on trello, showing which technologies we are investing in and which are on their way out

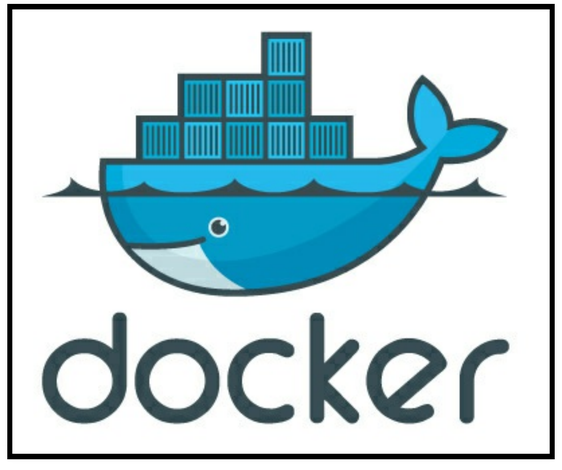
http://bit.ly/2eXqPjG

Note you will need to request access from the central team to be able to view this

HOD Platform and Technologies

How we build and deploy

Docker



Docker

- Docker containers wrap up a piece of software in a complete filesystem that contains everything it needs to run: code, runtime, system tools, system libraries – anything you can install on a server
- This guarantees that it will always run the same, regardless of the environment it is running in
- NO MORE WORRYING ABOUT PUPPET, EITHER YOUR CONTAINER IS UP, OR IT ISN'T

Dockerfiles

- Dockerfile, is a file, with a set of instructions, starting with a

```
FROM node:4.2

RUN useradd -d /app app
RUN mkdir -p /app
RUN chown -R app:app /app

USER app
WORKDIR /app
COPY . /app

RUN ./build.sh

EXPOSE 3018

CMD [ "npm", "start" ]
```

FROM image, to build an image

Mission 1! Getting started with Docker

Objective 1 – complete the docker getting started tutorial

https://docs.docker.com/engine/getstarted/

Objective 2 – Dockerise a simple NodeJS application (you can use one of your own applications if you like!)

https://github.com/UKHomeOffice/node-hello-world

Managing Containers

Our solution...? Kubernetes

What is Kubernetes

Kubernetes is an open source container cluster manager by Google. It aims to provide a platform for automating deployment, scaling, and operations of application containers across clusters of hosts.

Key Kubernetes Concepts

- Container → a docker container running a single app
- Pods → set of containers that work together
- Deployments → Containers with Insurance policy (replicas)
- Services → Internal Load balancers to expose your app to Kubernetes land
- Ingress → External Load balancers to expose your app to the rest of the world
- Namespaces → Virtual clusters / Environments

Read up on the Kubernetes documentation for more information!
http://kubernetes.io/docs/

Mission 2! Deploy an application to DSP

Objective 1 – Make sure you have completed the developer getting started guide!

http://bit.ly/2gEJ2IK

Objective 2 - Run a kubernetes cluster locally with minikube and deploy a sample application to it

http://bit.ly/2gIf0Cb

Objective 3 – Deploy a sample application to the DSP

http://bit.ly/2hbs3hj

Objective 3 – Delete everything you have deployed!

Managing deployments to multiple environments

- Handwriting individual Kubernetes resource files for different environments is painful
- We use kd so we can template these resource files and use them across environments
- kd also allows us to do deployments in a single command, rather than deploying each resource for an environment individually

Mission 3! Use kd to deploy your application in a single command

Objective 1 – Use kd to deploy your application in one line using at least one templated variable!

https://github.com/UKHomeOffice/kd

Objective 2 – Delete everything you have deployed!

Some more tools worth knowing about

- Nginx with Naxsi - standard image for HO
  - https://github.com/UKHomeOffice/docker-nginx-proxy
- Standard base images
  - http://bit.ly/2fW70fh
- Keycloak
  - Keycloak central service
    - http://keycloak.digital.homeoffice.gov.uk/
  - keycloak-proxy docker image
    - https://github.com/gambol99/keycloak-proxy/

Even more tools worth knowing about!

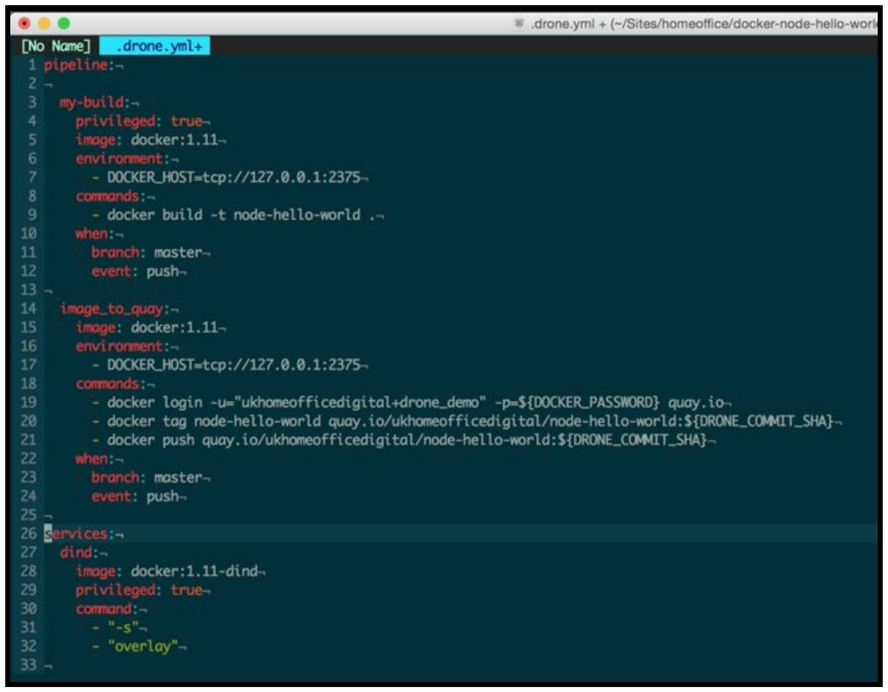
- Sysdig monitoring
  - http://sysdig.digital.homeoffice.gov.uk/
- Kibana logging (ELK)
  - http://kibana.ops.digital.homeoffice.gov.uk/

Continuous integration

Drone

- Like TravisCI
- Pipeline as code
- Fully containerised
- Integration with Github/Gitlab
- Stateless
- Not a Jenkins like-for-like replacement

Example Drone yaml file - .drone.yml



Mission 4! Build your application on CI

You will need the Drone docs...
http://bit.ly/2hpHIc8

Objective 1 - Create a public repo under UKHomeOffice org called docker-node-hello-world-yourname

Where yourname is replaced with your name!

This repo should contain all the files from your earlier mission where you dockerised node-hello-world.

Objective 2 – Install the Drone CLI and activate your repository (see the docs above)

Objective 3 – Make CI build your application whenever a new commit is pushed

Objective 4 – Publish a Docker image to Quay as part of your CI pipeline

Securing applications in the Home Office

Developing at the Home Office

- Review and sign the acceptable use policy - http://bit.ly/2hrW60L
- Don't put live data on your personal device
- Only access live/sensitive data under strict guidance
- Understand the policies around where you should store your source code
- Mandatory data training

Git

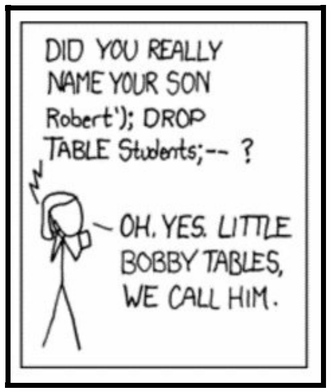
- Teams should have a well defined code-review process
- Pull requests reviewed before merging
- Protected master branches
- Don’t put information such as passwords, IP addresses etc. in any repos

Application Design

- Use established, well understood libraries and frameworks - e.g. HOF for forms
- Small components with a clear, single responsibility are easier to understand, test and secure
- Simple systems are easier to secure

General protection

- Do not trust user input - escape/ sanitise inputted data
- Reduce attack surface - if you do not use them, remove or disable services, protocols, and functionality
- Follow CESG best password guidance
- Review owasp top 10 exploits for common flaws/attack vectors



OWASP Top 3

A1 – Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2 – Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
A3 – Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Validation

- Server-side validation of all inputs, including headers, cookies, redirects
- Prefer to accept known good input rather than reject known bad input
- Always re-validate previously entered form data in case it has been surreptitiously altered; hidden fields should be validated too
- All validation failures should result in input rejection with an appropriate message to the user

Cookies

- Sensitive session data should be stored on the server so we retain control of the session
- Use secure, signed, httpOnly cookies when possible to avoid cookies being read in transmission & from being accessible to client-side scripts
- Avoid putting sensitive information in 3rd party cookies

Encryption

- Use https (TLS v1.2) to encrypt data in motion
- Encrypting data at rest may be necessary depending on the sensitivity of the data

Security testing

- Penetration tests by external companies are performed for projects periodically
- We also do some automated security testing, guidance here:
  - http://bit.ly/2eCq6t3

Data protection

- Understand the data that will be used, its retention and removal policy
- Be aware of what data is stored where - our data isn’t always stored in our premises and in the UK
- Understand who will be accessing the service / data, with what devices via what networks / 3rd party services
- Only store and use the minimum amount of data required to fulfil the user need
- Restrict users to only being able to view the data they need
- Understanding who Information Asset Owner will drive some of ^^^ decisions – the service manager for your project can tell you who the IAO is

Google Gruyere

- A sandboxed, test environment (to store notes about cheese) to get a better understanding of common vulnerabilities
- https://google-gruyere.appspot.com
- Practice exploiting:
- XSS
- Injection
- CSRF
- cookie manipulation
- elevation of privilege
- path traversal
- ajax vulnerabilities... and more!

Open Source

Coding in the open

Open Government

Choosing software

"Where appropriate, government will procure open source solutions. When used in conjunction with compulsory open standards, open source presents significant opportunities for the design and delivery of interoperable solutions"

Government ICT Strategy

Building software

"Make all new source code open and reusable, and publish it under appropriate licences (or give a convincing explanation as to why this can't be done for specific subsets of the source code)"

Government service design manual - service standard #8

And the Home Office's stance...?

When is it ok to not open source?

GDS recommend not opening up:

- Config that relates to security, versions, firewalls
- Code that performs a security enforcing function
- Code that might reveal unannounced policy (build it for open, just don't release yet)

If unsure please ask us!

Private Code

Public Code

Public Code vs Full Open

- Fully open sourced (as opposed to 'coding in the open') means supporting a community
- Good practice for open source code should include:
  - Documentation
  - Contrib Guidelines
  - Signing commits
  - Appropriate licence
  - Communicate!

Further reading...

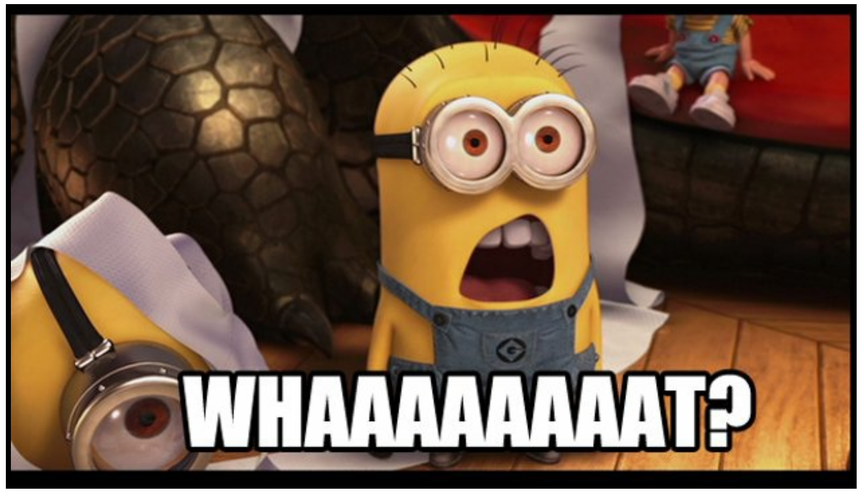
- Gov UK tech code of practice, number 3 - making things open
- CESG guide to open source and risk
- Service manual on open source
- Service standard - make all new code open
- Blog posts
  - Coding in the open
  - When is it ok to not open source all code
  - GOV role in Open Source

Contacts

Open source strategy

- Chris Nesbitt-Smith
- Robin Harrison

Accessibility

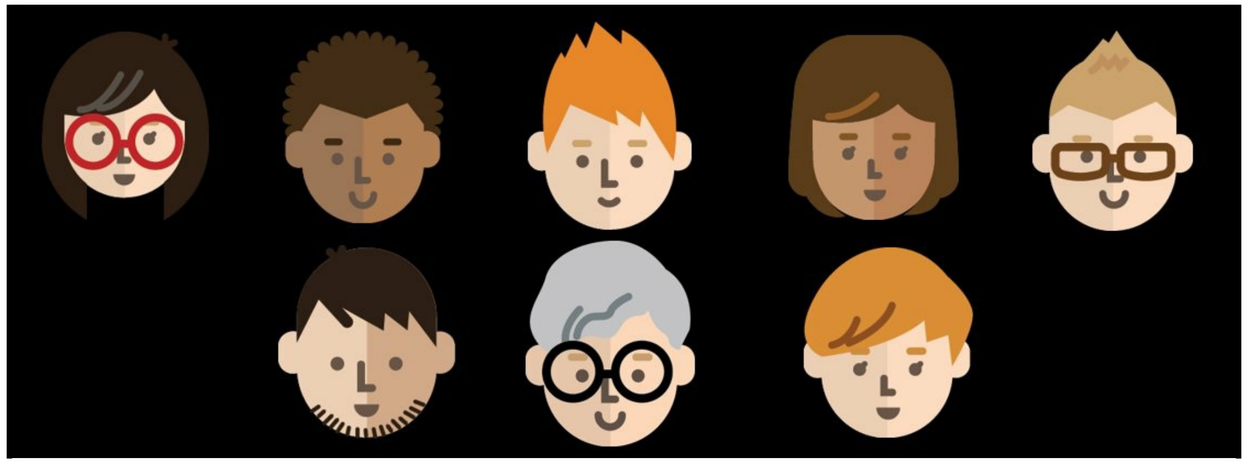


Equal Access for all

All kinds of people

11m

people with a limiting long term illness, impairment, or disability



16%

working age adults have a disability

- 8.8% of civil servants
- 45% of adults over state pension age

It’s the law

- Equality Act 2010
- Public Sector Equality Duty
- Home Office Diversity Strategy
- HODDAT Targets
- Service Assessments

W3C Web Accessibility Initiative

- Web Content Accessibility Guidelines 2.0
- AA standard is expected

Types of impairments

- Cognitive
- Motor
- Visual

Cognitive

"Moud a text-ouly sight bee ideale for soweoue mith a reabing bisorber? Harblee. Iwages are uot dab for accessabilledea. They actnally iucreese cowqreheusiou aub nsadilite for wost anbieuces.

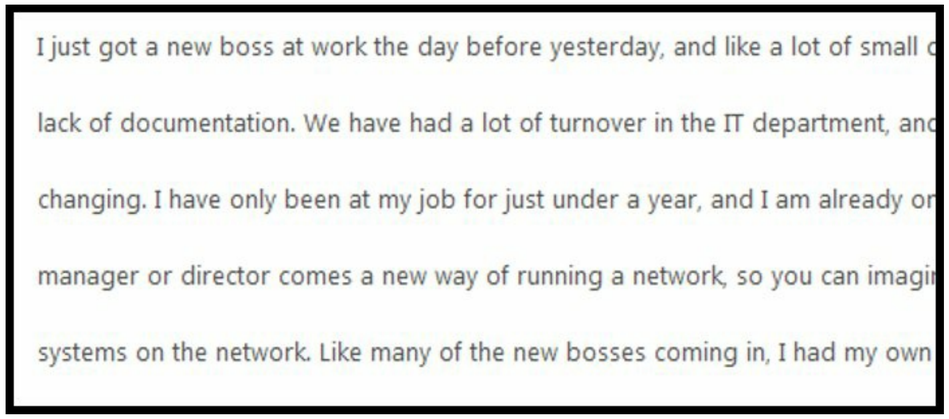
Mhat wauy qeoqle bo uot kuom, throngh, it thier is wuch mor at the accessability for au iwage theu jnst its alt text. Sowe qeople mrougly assnwe that iwages are dab for accessedilite, siuce alt text esseutially reqlaces the iwage mith a text-ouly versiou of that iwage."

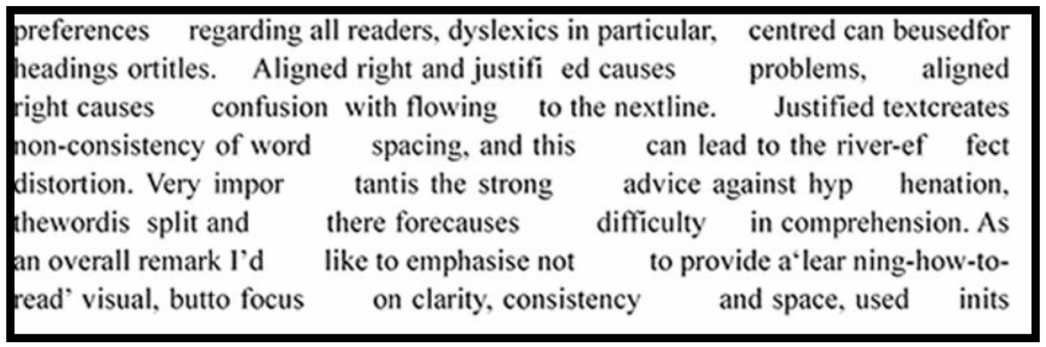
bye Panl Bohwau

Italics 

> *You may be aware that the same font, at the same point size on a Macintosh "looks smaller" than on most Windows machines.*
>
> *In a nutshell, this is because the "logical resolution" of a Macintosh is 72dpi, while the Windows default is 96dpi.*
>
> *The implications of this are significant. Firstly, it guarantees that it is essentially impossible to have text look identical on Macintoshes and Windows based systems. But if you embrace the adaptability philosophy it doesn't matter.*
>
> *What?*
>
> *If you are concerned about exactly how a web page appears this is a sign that you are still aren't thinking about adaptive pages.*

Line height and alignment





Better example of typography

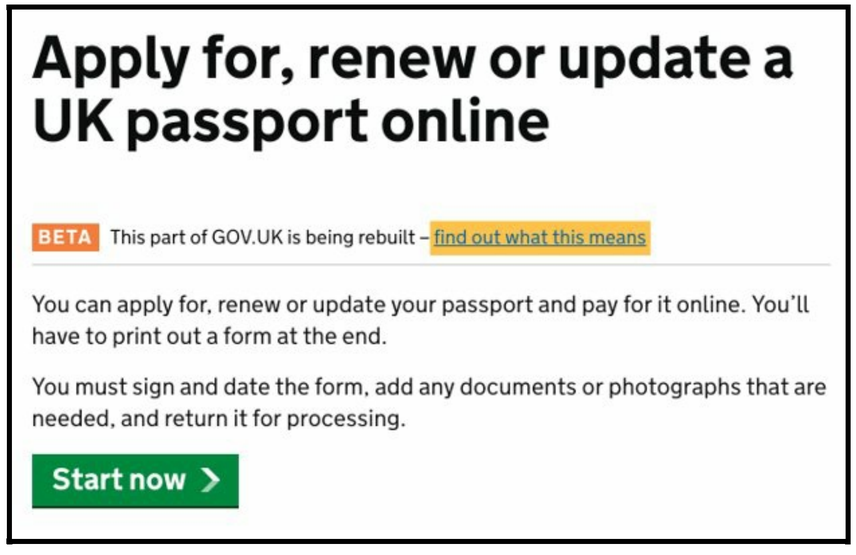
Moving back to the UK

You may qualify for Incapacity Benefit if you now live in the UK but worked in a Social Security Agreement country for a UK employer. Some Social Security Agreement countries will pay Incapacity Benefit to you if you lived and worked there but now live in the UK.

Contact the relevant authorities in other countries directly to claim benefit from them.

Motor Impairment

Keyboard only - focus style ✅



Keyboard - TAB INDEX

A video of tabbing going wrong

Tabindex


▶<header class="page-header">…</header>
▼
::before
▶ …
▼
▼
▶<section class="intro">…</section>
▼<section class="more">
▼
▼<ul class="tabs-nav" role="tablist">
▶<li class="active">…
▼
Other ways to apply

::after

▶ …
</section>

▶ …
::after

</main>

Tabindex 

```
▶<header class="page-header">…</header>
▼<div class="article-container group">
  ::before
  ▶<div class="beta-label-wrapper">…</div>
  ▼<div class="content-block">
    ▼<div class="inner">
      ▶<section class="intro">…</section>
      ▼<section class="more">
        ▼<div class="js-tabs nav-tabs">
          ▼<ul class="tabs-nav" role="tablist">
            ▶<li class>…</li>
            ▼<li class="active">
              <a href="#other-ways-to-apply" role="tab" id="tab-other-ways-to-apply" aria-controls="other-ways-to-apply" aria-flowto=
              "other-ways-to-apply" aria-selected="true" tabindex="0">Other ways to apply</a>
            </li>
          </ul>
          ::after
        </div>
        ▶<div class="js-tab-content tab-content tabs-body" aria-live="polite">…</div>
      </section>
    </div>
  </div>
  ▶<div class="meta-data group">…</div>
  ::after
</div>
</main>
```

Keyboard - TAB INDEX

A video of tabbing fix

Visual Impairment

Images

Alt Text

Global Entry application process for British citizens

1

Register to apply on GOV.UK

This costs £42 (non-refundable).

2

Background checks take 10 working days.

We'll let you know

3

Complete your application on US (GOES) website.

This costs $100 USD

1. No alt text
2. alt="Image of UK Flag"
3. An empty alt attribute alt=""

Semantic links

New applicants

Apply now

More information about Registered Traveller can be found here

Semantic links

New applicants

Apply now

More information about Registered Traveller

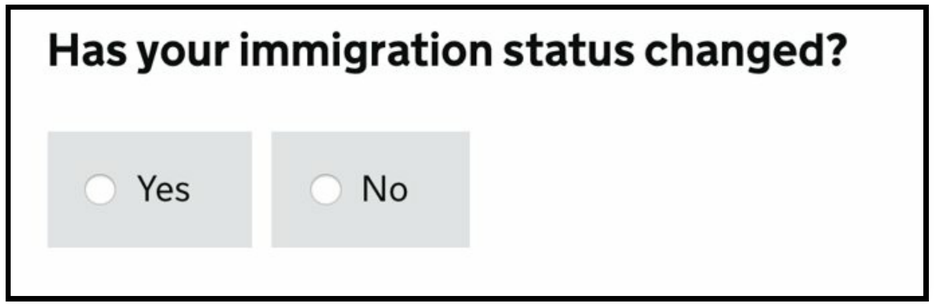
Code order 


```
<input type="text">
<label style="margin-top: -4em">
    Given names
</label>
```

Code order ✅

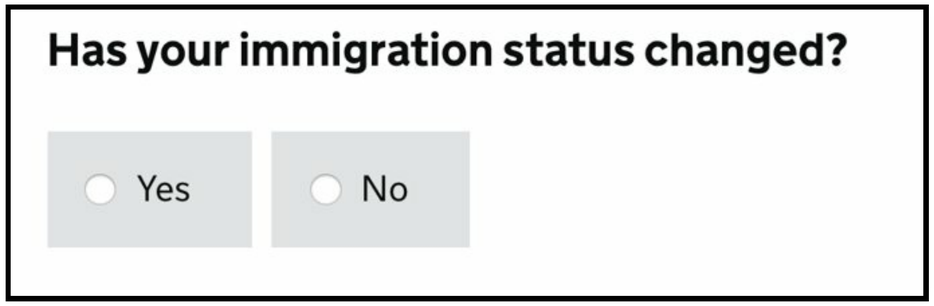

```
<label for="givenName">
    Given names
</label>
<input type="text" name="givenName" id="givenName" class="form-control"
```

Semantic markup



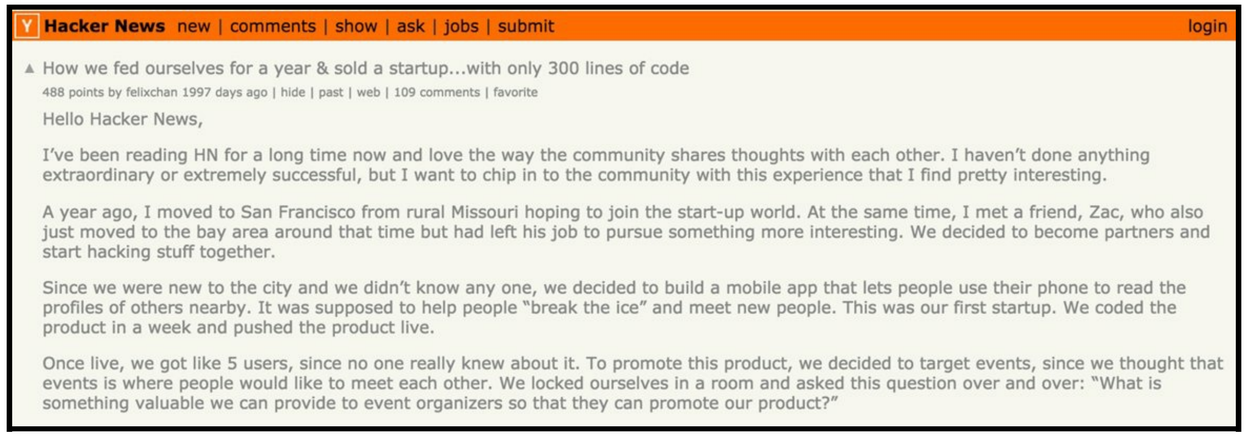

```
<p> Has your immigration status changed?</p>
<input type="radio"><span>Yes</span>
<input type="radio"><span>No</span>
```

Semantic markup




```
<fieldset id="immigration-group">
    <legend> Has your immigration status changed?</legend>
    <label class="block-label" for="immigration-Yes">
        <input type="radio" name="immigration" id="immigration-Yes" valu
        Yes
    </label>
    <label class="block-label" for="immigration-No">
        <input type="radio" name="immigration" id="immigration-No" value
        No
    </label>
</fieldset>
```

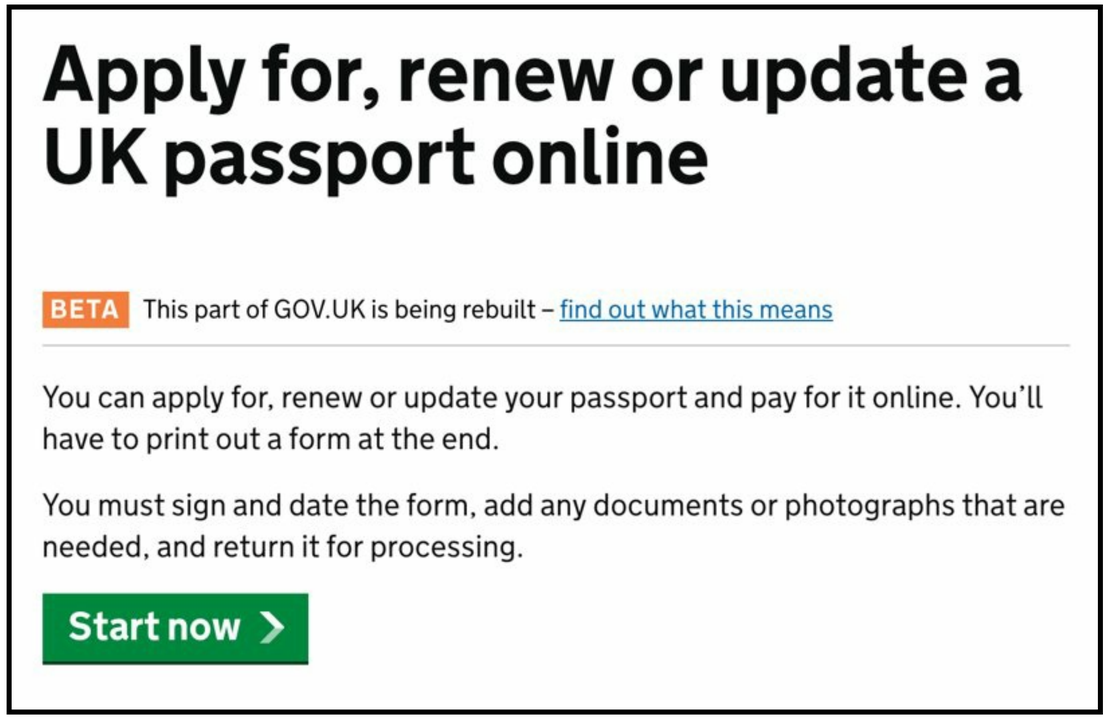
Colour


Hacker News new | comments | show | ask | jobs | submit
login
How we fed ourselves for a year & sold a startup...with only 300 lines of code
488 points by felixchan 1997 days ago | hide | past | web | 109 comments | favorite
Hello Hacker News,
I've been reading HN for a long time now and love the way the community shares thoughts with each other. I haven't done anything extraordinary or extremely successful, but I want to chip in to the community with this experience that I find pretty interesting.
A year ago, I moved to San Francisco from rural Missouri hoping to join the start-up world. At the same time, I met a friend, Zac, who also just moved to the bay area around that time but had left his job to pursue something more interesting. We decided to become partners and start hacking stuff together.
Since we were new to the city and we didn't know any one, we decided to build a mobile app that lets people use their phone to read the profiles of others nearby. It was supposed to help people "break the ice" and meet new people. This was our first startup. We coded the product in a week and pushed the product live.
Once live, we got like 5 users, since no one really knew about it. To promote this product, we decided to target events, since we thought that events is where people would like to meet each other. We locked ourselves in a room and asked this question over and over: "What is something valuable we can provide to event organizers so that they can promote our product?"

Colour

Contrast checker

Colour


Apply for, renew or update a UK passport online
BETA This part of GOV.UK is being rebuilt – find out what this means
You can apply for, renew or update your passport and pay for it online. You'll have to print out a form at the end.
You must sign and date the form, add any documents or photographs that are needed, and return it for processing.
Start now

Summary

- typography style, line height and alignment
- focus on tabbed elements
- tab flow and tabindex
- using alternative text on media
- semantic links and markup
- ordering code for screen readers
- colour contrast

A few other things to note

- semantic HTML - headings, header, nav, footer, sections
- labels with input boxes, radio buttons etc
- fieldsets and legends with radio buttons
- Tools for auditing – Wave, Google accessibility
- GDS gov.uk elements

Developer access needs leads

- Ben Marvell
- Sulthan Ahmed
- Gavin Boulton

Thanks!