University of BRISTOL

Systems Security

COMSM1500

University of BRISTOL

Web Security

Client side

bristol.ac.uk

At the beginning of time…

At the beginning of time…

- The web was simple

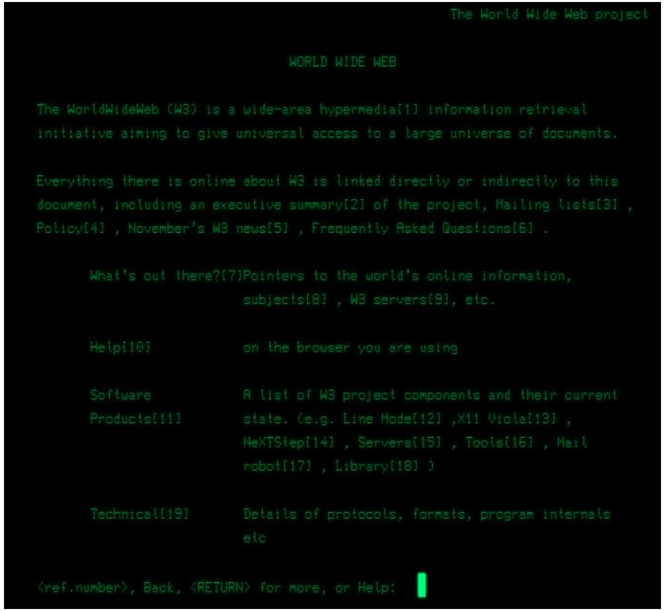
At the beginning of time…

- The web was simple
- A server, a browser

At the beginning of time…

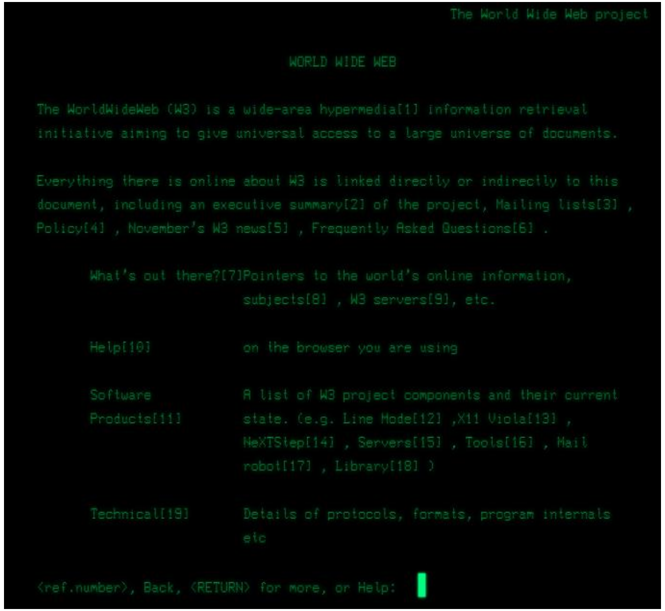
- The web was simple
- A server, a browser
- The browser displayed the content sent by the server

At the beginning of time

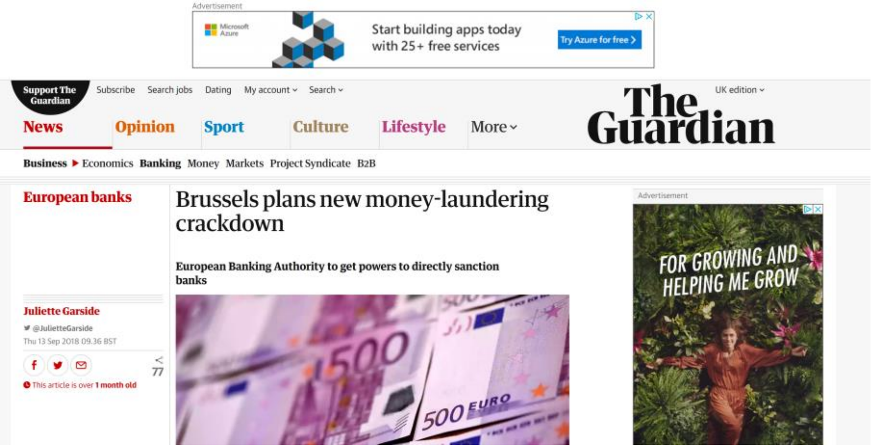


```
                                                  The World Wide Web project

                              WORLD WIDE WEB

   The WorldWideWeb (W3) is a wide-area hypermedia[1] information retrieval
   initiative aiming to give universal access to a large universe of documents.

   Everything there is online about W3 is linked directly or indirectly to this
   document, including an executive summary[2] of the project, Mailing lists[3] ,
   Policy[4] , November's W3 news[5] , Frequently Asked Questions[6] .

         What's out there?[7]Pointers to the world's online information,
                             subjects[8] , W3 servers[9], etc.

         Help[10]            on the browser you are using

         Software            A list of W3 project components and their current
         Products[11]        state. (e.g. Line Mode[12] ,X11 Viola[13] ,
                             NeXTStep[14] , Servers[15] , Tools[16] , Mail
                             robot[17] , Library[18] )

         Technical[19]       Details of protocols, formats, program internals
                             etc

   <ref.number>, Back, <RETURN> for more, or Help:
```

… and now



```
                                              The World Wide Web project

                             WORLD WIDE WEB

The WorldWideWeb (W3) is a wide-area hypermedia[1] information retrieval
initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this
document, including an executive summary[2] of the project, Mailing lists[3] ,
Policy[4] , November's W3 news[5] , Frequently Asked Questions[6] .

       What's out there?[7]Pointers to the world's online information,
                           subjects[8] , W3 servers[9], etc.

       Help[10]            on the browser you are using

       Software            A list of W3 project components and their current
       Products[11]        state. (e.g. Line Mode[12] ,X11 Viola[13] ,
                           NeXTStep[14] , Servers[15] , Tools[16] , Mail
                           robot[17] , Library[18] )

       Technical[19]       Details of protocols, formats, program internals
                           etc

<ref.number>, Back, <RETURN> for more, or Help:
```



Brussels plans new money-laundering crackdown

European Banking Authority to get powers to directly sanction banks

Juliette Garside

@JulietteGarside

Thu 13 Sep 2018 09.36 BST

This article is over 1 month old

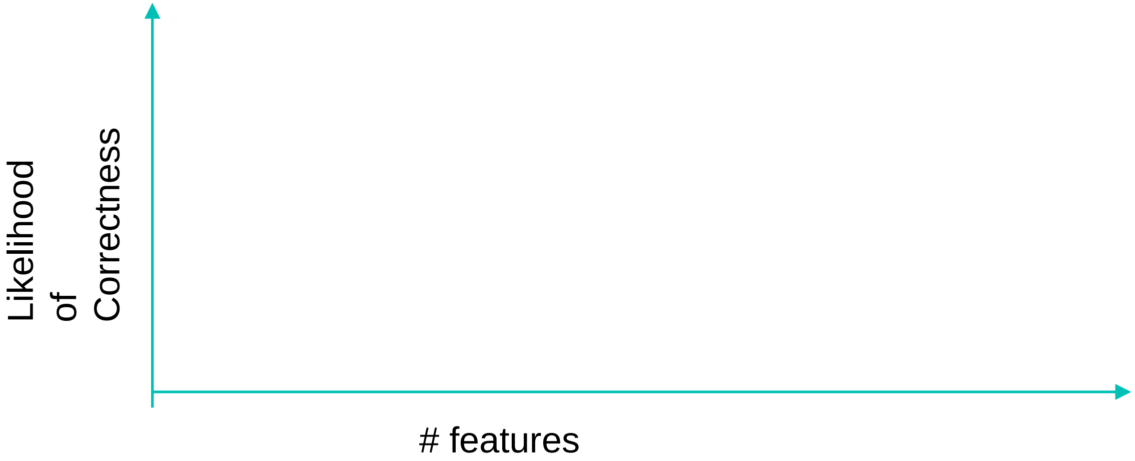
Feature rich browsers

- JavaScript
- DomModel
- AJAX
- Web sockets
- Multimedia
- Geolocation
- Many more features…

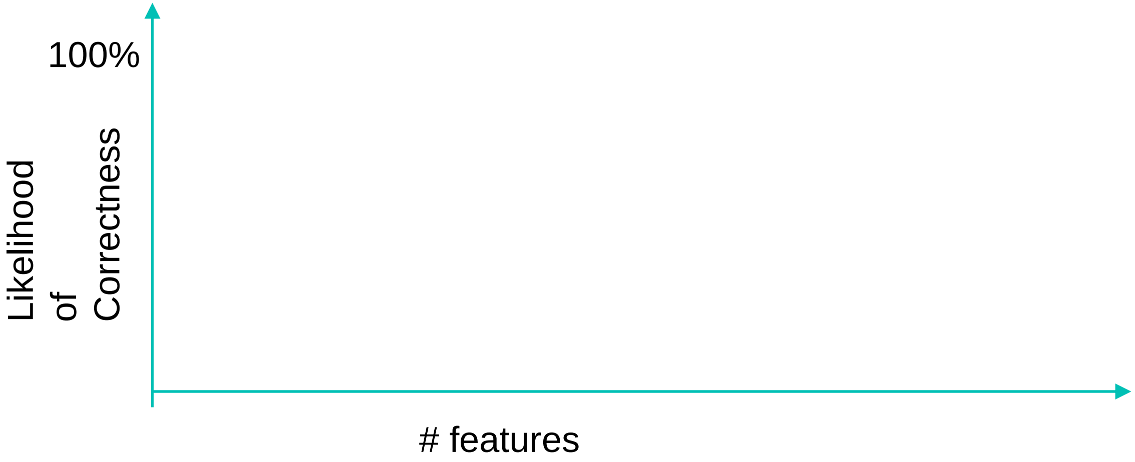
Feature rich browsers

- JavaScript
- DomModel
- AJAX
- Web sockets
- Multimedia
- Geolocation
- Flash (we learned it was bad)
- Many more features…

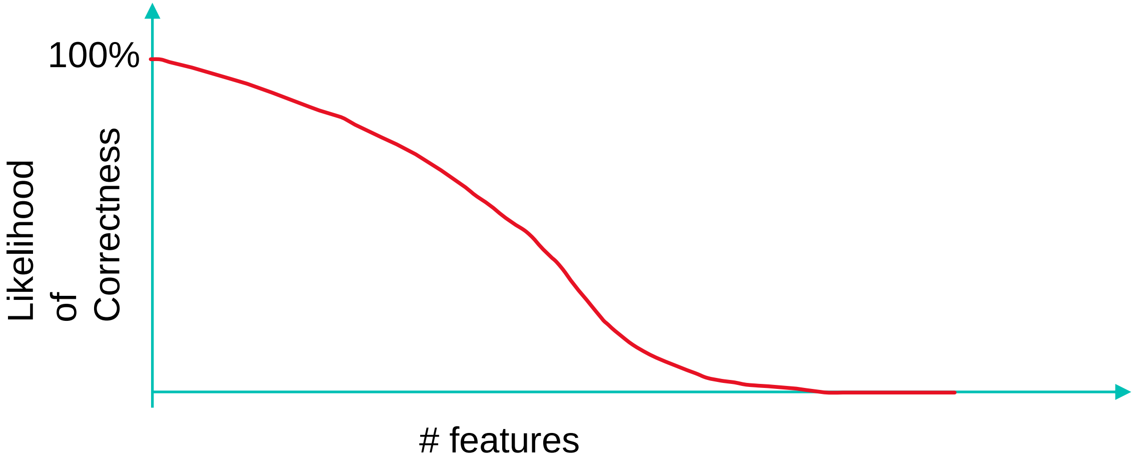
We learned



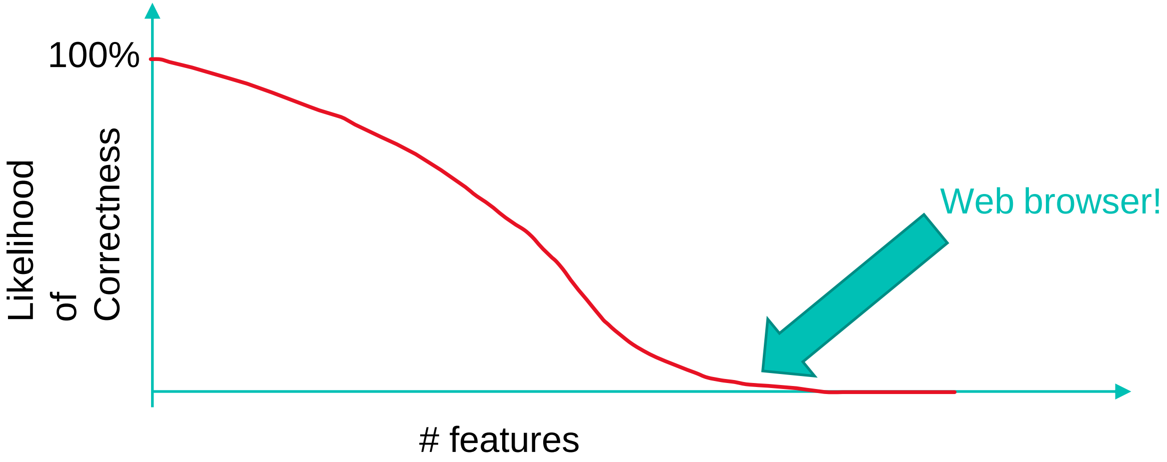
We learned



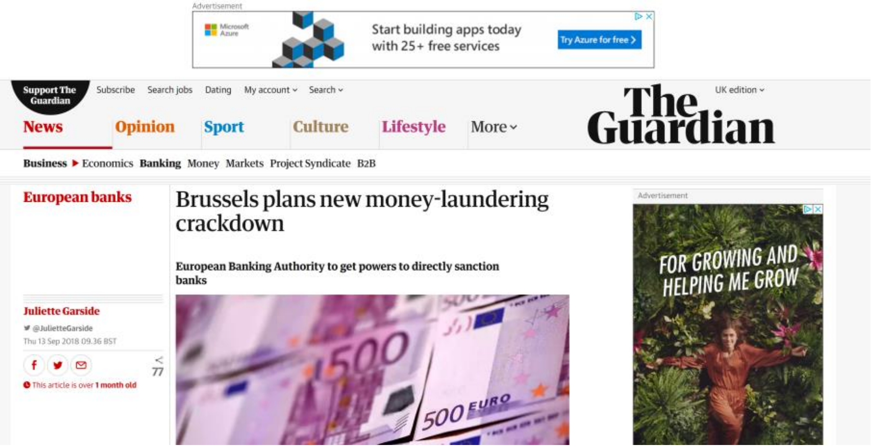
We learned



We learned



What’s on a website



European banks

Brussels plans new money-laundering crackdown

European Banking Authority to get powers to directly sanction banks

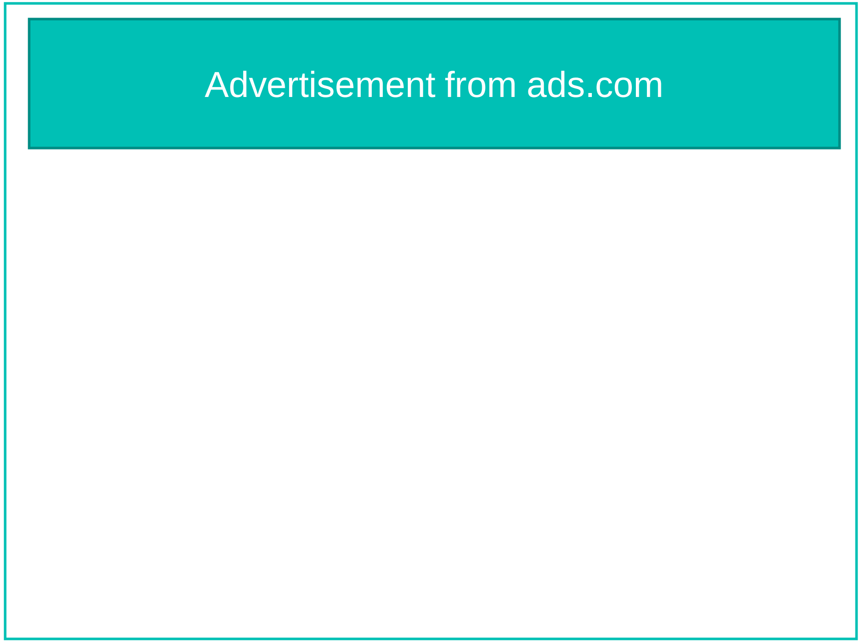
Juliette Garside

@JulietteGarside

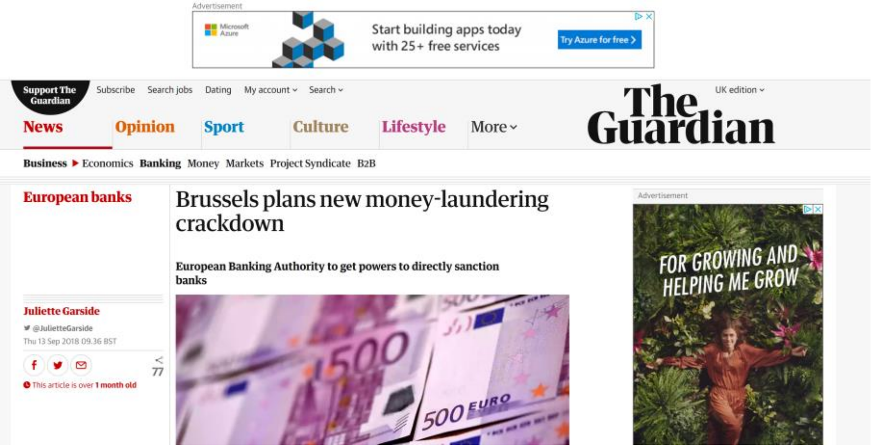
Thu 13 Sep 2018 09.36 BST

This article is over **1 month old**

What’s on a website



Advertisement from ads.com



European banks

Brussels plans new money-laundering crackdown

European Banking Authority to get powers to directly sanction banks

Juliette Garside

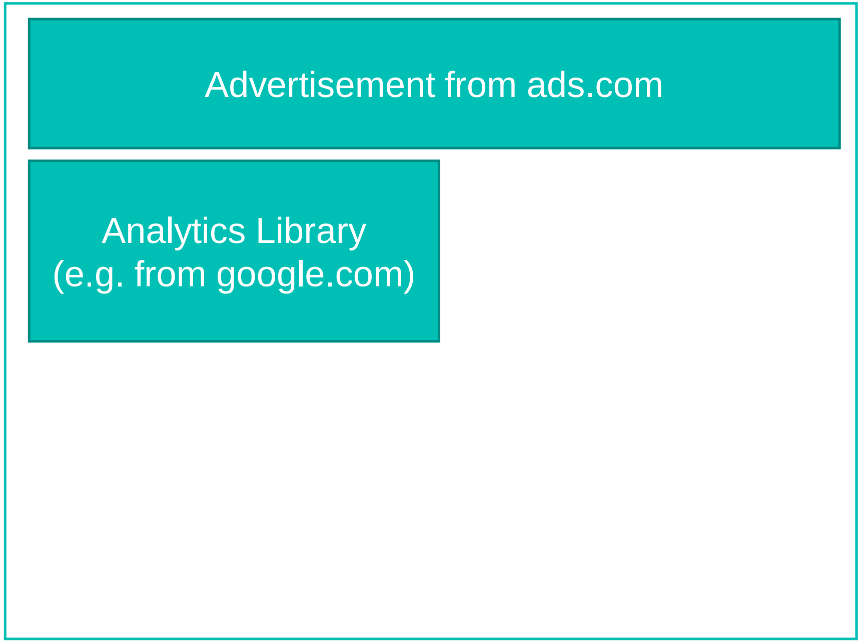
@JulietteGarside

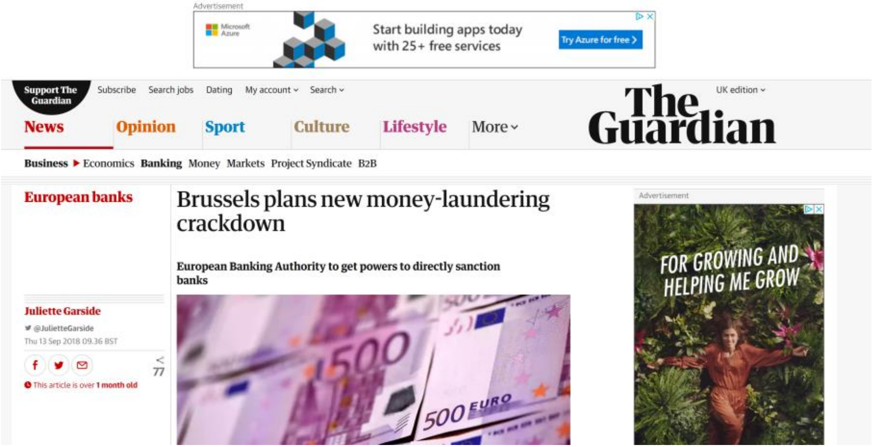
Thu 13 Sep 2018 09.36 BST

77

This article is over 1 month old

What’s on a website





Start building apps today with 25+ free services

European banks

Brussels plans new money-laundering crackdown

European Banking Authority to get powers to directly sanction banks

Juliette Garside

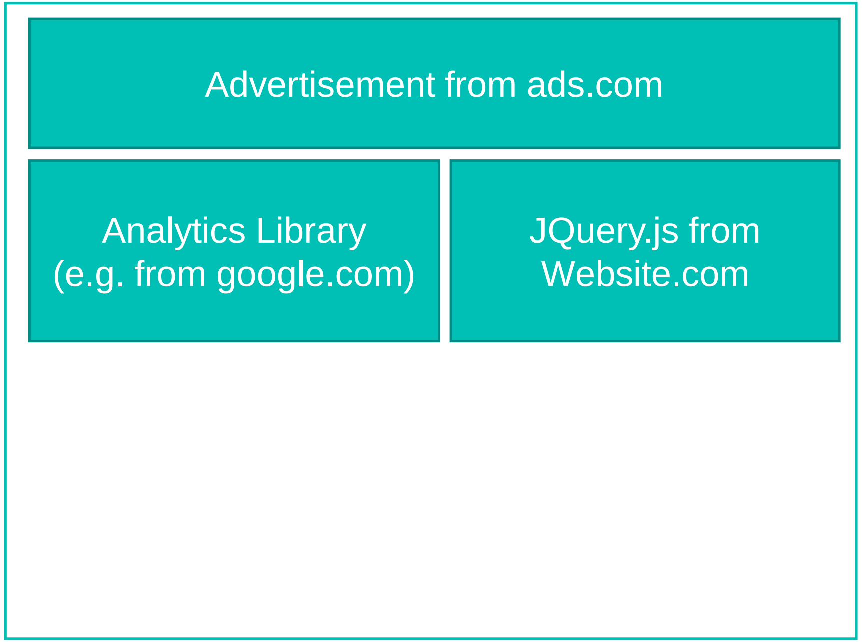
@JulietteGarside

Thu 13 Sep 2018 09.36 BST

77

This article is over 1 month old

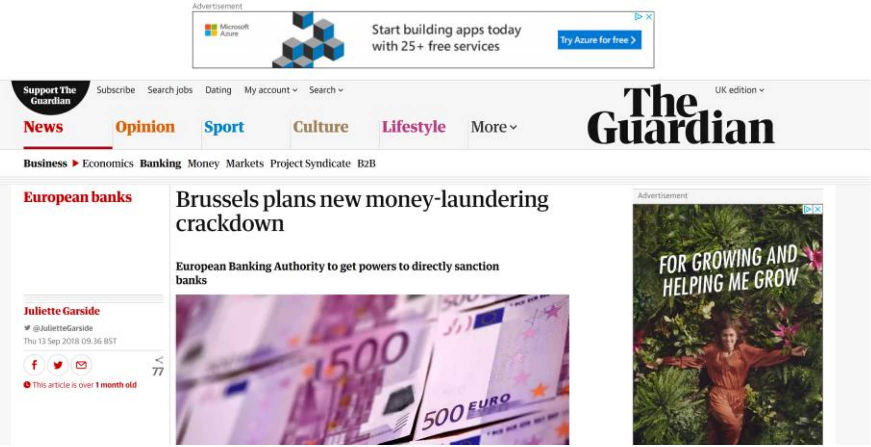
What’s on a website



Advertisement from ads.com

Analytics Library (e.g. from google.com)

JQuery.js from Website.com



European banks

Brussels plans new money-laundering crackdown

European Banking Authority to get powers to directly sanction banks

Juliette Garside

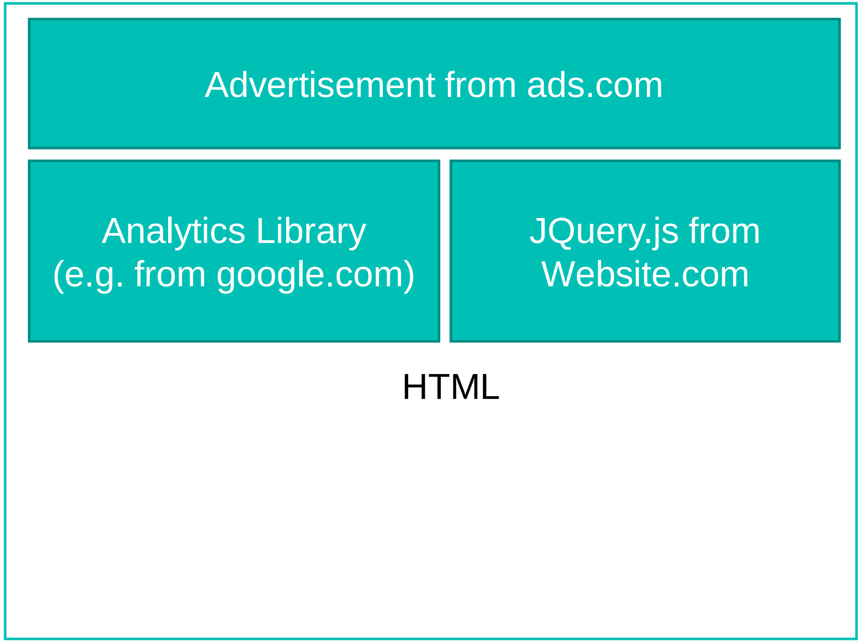
@JulietteGarside

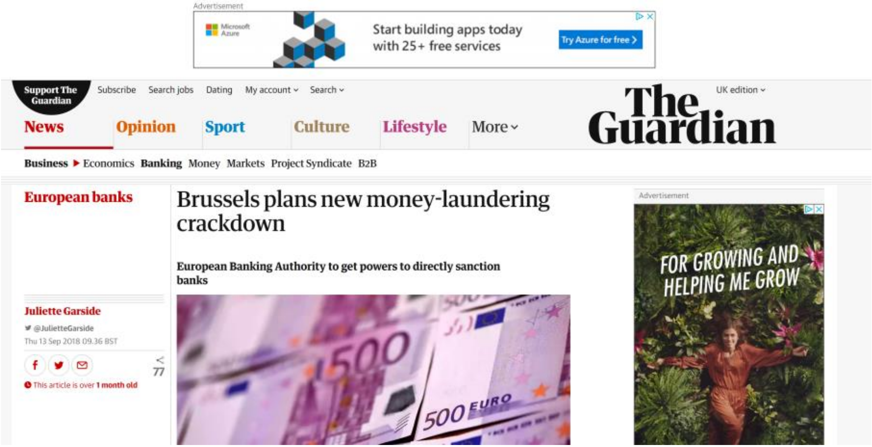
Thu 13 Sep 2018 09.36 BST

77

This article is over 1 month old

What’s on a website


Advertisement from ads.com
Analytics Library (e.g. from google.com)
JQuery.js from Website.com
HTML



European banks

Brussels plans new money-laundering crackdown

European Banking Authority to get powers to directly sanction banks

Juliette Garside

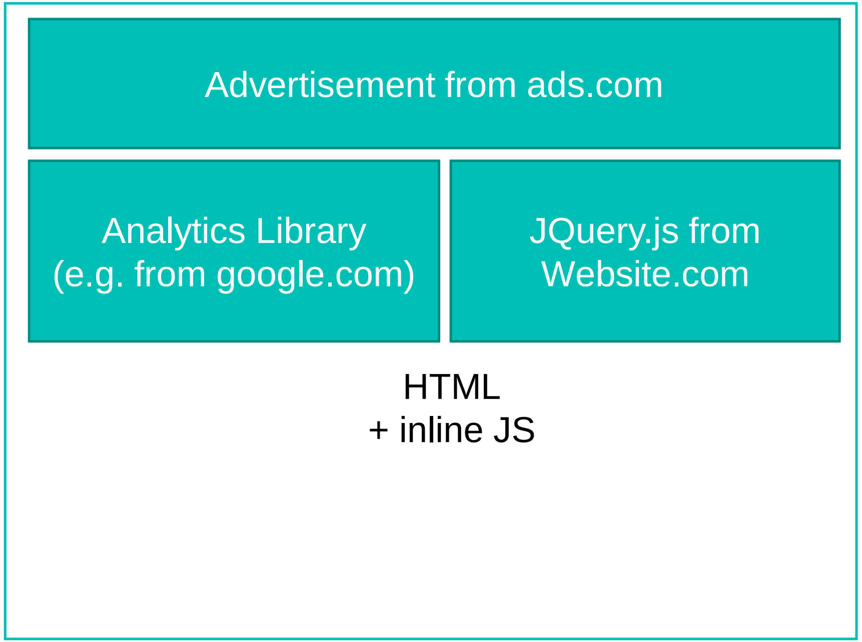
@JulietteGarside

Thu 13 Sep 2018 09.36 BST

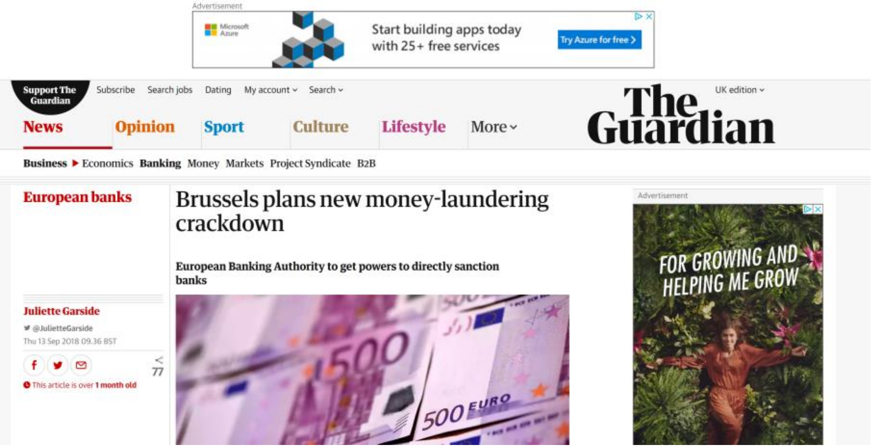
77

This article is over 1 month old

What’s on a website



Advertisement from ads.com
Analytics Library (e.g. from google.com)
JQuery.js from Website.com
HTML + inline JS



Advertisement

Microsoft Azure

Start building apps today with 25+ free services

Try Azure for free ›

Support The Guardian

Subscribe Search jobs Dating My account ⌄ Search ⌄

UK edition ⌄

The Guardian

News Opinion Sport Culture Lifestyle More ⌄

Business ▶ Economics **Banking** Money Markets Project Syndicate B2B

European banks

Brussels plans new money-laundering crackdown

European Banking Authority to get powers to directly sanction banks

Juliette Garside

@JulietteGarside

Thu 13 Sep 2018 09.36 BST

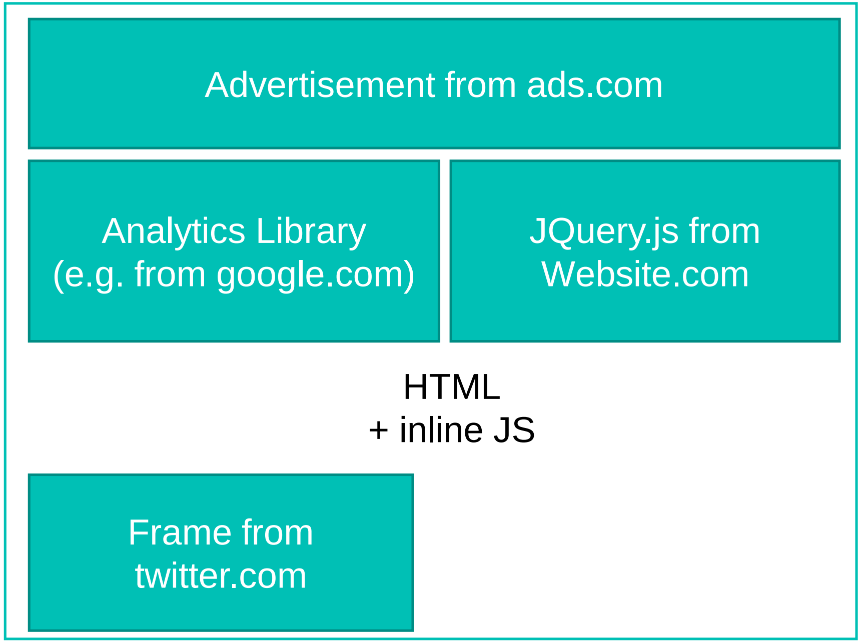
77

This article is over **1 month old**

Advertisement

FOR GROWING AND HELPING ME GROW

What’s on a website



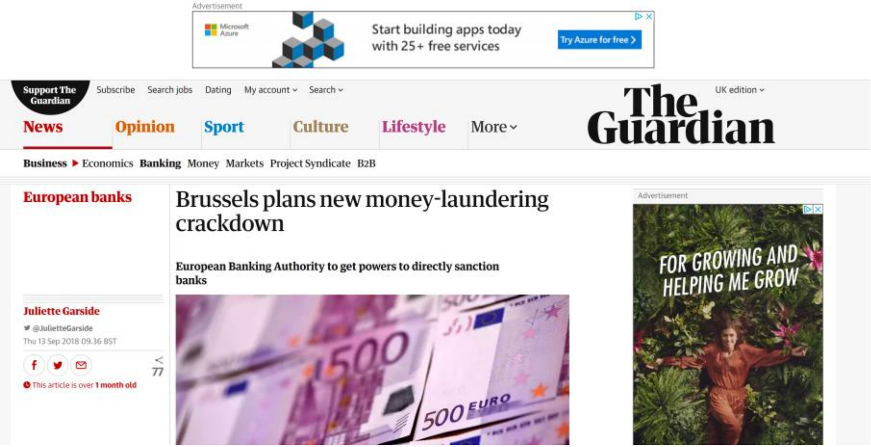
Advertisement from ads.com

Analytics Library
(e.g. from google.com)

JQuery.js from
Website.com

HTML
+ inline JS

Frame from
twitter.com



European banks

Brussels plans new money-laundering crackdown

European Banking Authority to get powers to directly sanction banks

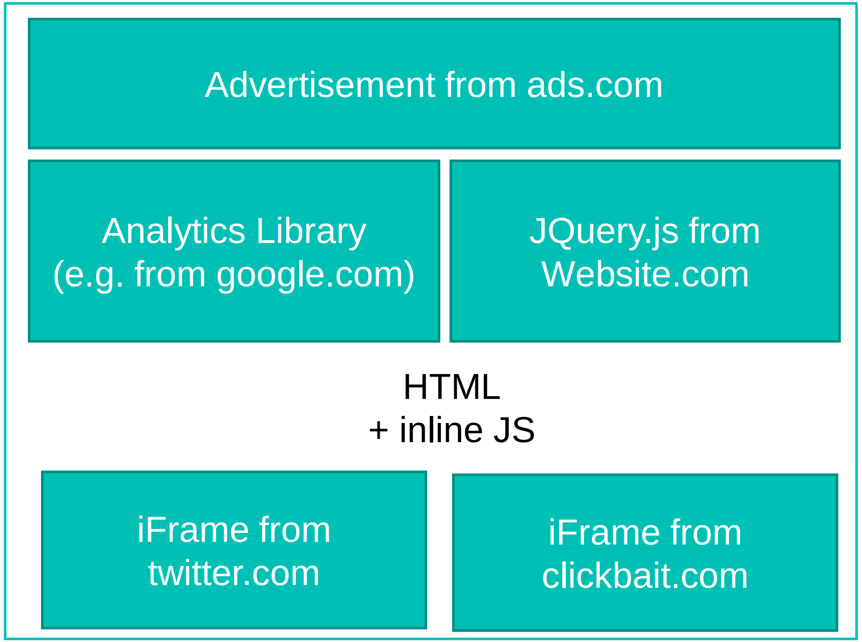
Juliette Garside

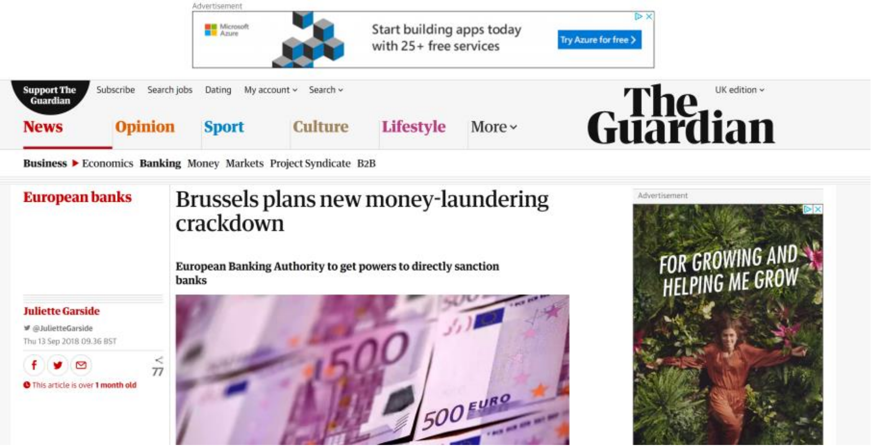
@JulietteGarside

Thu 13 Sep 2018 09.36 BST

This article is over 1 month old

What’s on a website


Advertisement from ads.com
Analytics Library (e.g. from google.com)
JQuery.js from Website.com
HTML + inline JS
iFrame from twitter.com
iFrame from clickbait.com



Brussels plans new money-laundering crackdown

European Banking Authority to get powers to directly sanction banks

Juliette Garside

@JulietteGarside

Thu 13 Sep 2018 09.36 BST

77

This article is over 1 month old

Same origin policy

How should we control how things interact?

Same-origin policy

- Goal: two websites should not be able to tamper each others

Same-origin policy

- Goal: two websites should not be able to tamper each others
  - A bit vague…
  - … was easier in the early days
- Obviously bad: messing up with each other display

Same-origin policy

- Goal: two websites should not be able to tamper each others
  - A bit vague…
  - … was easier in the early days
- Obviously bad: messing up with each other display
- Obviously good: Google Map + Company Tracking

Same-origin policy

- Goal: two websites should not be able to tamper each others
  - A bit vague…
  - … was easier in the early days
- Obviously bad: messing up with each other display
- Obviously good: Google Map + Company Tracking
- More ambiguous: External JS library?

Same-origin policy

- Strategy: each resource is assigned an origin. JS can only access resource from the same origin.

Same-origin policy

- Strategy: each resource is assigned an origin. JS can only access resource from the same origin.
- Origin: scheme, domain, port
  - http://foo.com/index.html

Same-origin policy

- Strategy: each resource is assigned an origin. JS can only access resource from the same origin.
- Origin: scheme, domain, port
  - http://foo.com/index.html
  - https://foo.com/index.html 🚫 Different scheme and port

Same-origin policy

- Strategy: each resource is assigned an origin. JS can only access resource from the same origin.
- Origin: scheme, domain, port
  - http://foo.com/index.html
  - https://foo.com/index.html 🚫 Different scheme and port
  - https://bar.com:8181/... 🚫

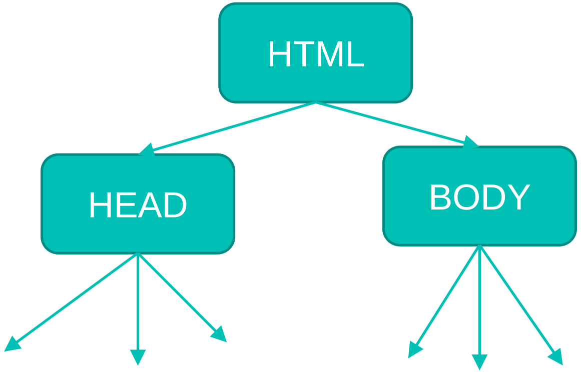
Same-origin policy

Four fundamental ideas

Same-origin policy

Four fundamental ideas

- Each origin has client side resources
  - DOM tree (JS reflection of HTML page)
  - Cookies (to maintain states)
  - DOM storage (key/value store)
  - JS namespace
  - Display area



Same-origin policy

Four fundamental ideas

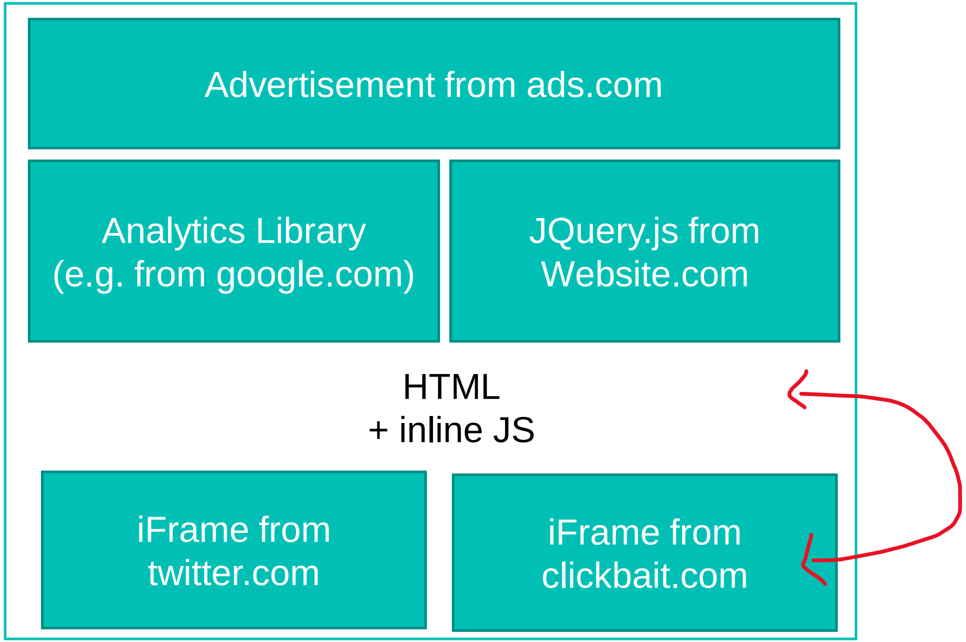
- Each origin has client side resources
- Each frame get the origin of its URL

Same-origin policy

Four fundamental ideas

- Each origin has client side resources
- Each frame get the origin of its URL
- Each JS scripts execute with the authority of its frame

Same-origin policy



Advertisement from ads.com

Analytics Library (e.g. from google.com)

JQuery.js from Website.com

HTML + inline JS

iFrame from twitter.com

iFrame from clickbait.com

JS postMessage() interface
(both side need to agree)

Same-origin policy

Four fundamental ideas

- Each origin has client side resources
- Each frame get the origin of its URL
- Each JS scripts execute with the authority of its frame
- Passive content get zero authority
  - Image
  - CCS

Why rule 4?

- Mime sniffing attack

Why rule 4?

- Mime sniffing attack
  - Old IE version trying to be helpful

Why rule 4?

- Mime sniffing attack
  - Old IE version trying to be helpful
  - Idea: server may be misconfigured and misidentifies object type!

Why rule 4?

- Mime sniffing attack
  - Old IE version trying to be helpful
  - Idea: server may be misconfigured and misidentifies object type!
  - A website link to an external image
  - IE would coerce it to for example JS script

Why rule 4?

- Mime sniffing attack
  - Old IE version trying to be helpful
  - Idea: server may be misconfigured and misidentifies object type!
  - A website link to an external image
  - IE would coerce it to for example JS script
  - Get executed with the authority of the page it is in

Why rule 4?

- Mime sniffing attack
  - Old IE version trying to be helpful
  - Idea: server may be misconfigured and misidentifies object type!
  - A website link to an external image
  - IE would coerce it to for example JS script
  - Get executed with the authority of the page it is in
- Browser are complex!
- Adding even well meaning features can have unforeseen consequences!

Frame/Window objects

- Frame get the origin of URL

OR

- A suffix of the original origin (set via document.domain)
  - e.g. X.Y.Z.com

Frame/Window objects

- Get origin of the frame URL

OR

- A suffix of the original origin (set via document.domain)
  - e.g. X.Y.Z.com
  - Y.Z.com
  - Z.com
  - A.Y.Z.com 🚫
  - .com 🚫

What could go wrong if not careful?

Hint UK

What could go wrong if not careful?

- .co.uk
- .ac.uk
- etc…
- https://publicsuffix.org/

Frame/Window objects

- Two frames can access each others if:
  - Both set document.domain to the same value
  - Neither has changed document.domain (and values match)
- Avoid attack from buggy subdomain

Frame/Window objects

- Two frames can access each others if:
  - Both set document.domain to the same value
  - Neither has changed document.domain (and values match)
- Avoid attack from buggy subdomain
- Nice idea to get modules in different subdomains
  - e.g. login.foo.com; payment.foo.com etc…

Cookies/AJAX/CCS

- Need to be subjected to similar origin rules

- Plugins are also a source of many nastiness
  - Used to be very trivial to write one to steal credit card number

University of BRISTOL

Some attacks

Cross Site Scripting Attack

Cross Site Scripting Attack

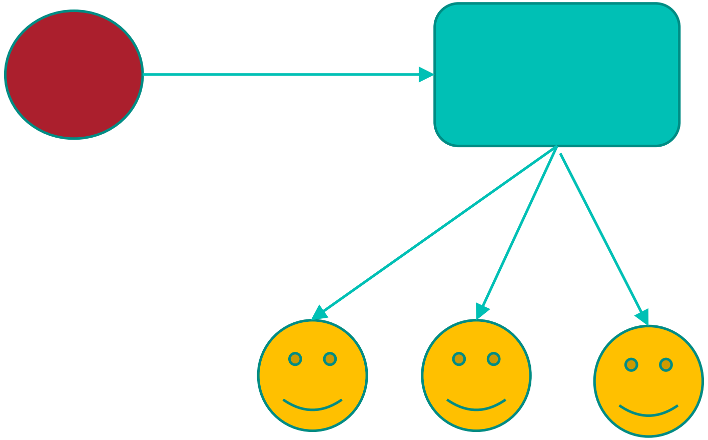
```
<html>
<head>
[…]
</head>
<body>
[…]
<p> [some user content] </p>
</body>
</html>
```

Cross Site Scripting Attack

```
<html>
<head>
[…]
</head>
<body>
[…]
<p> [some user content] </p>
</body>
</html>
```

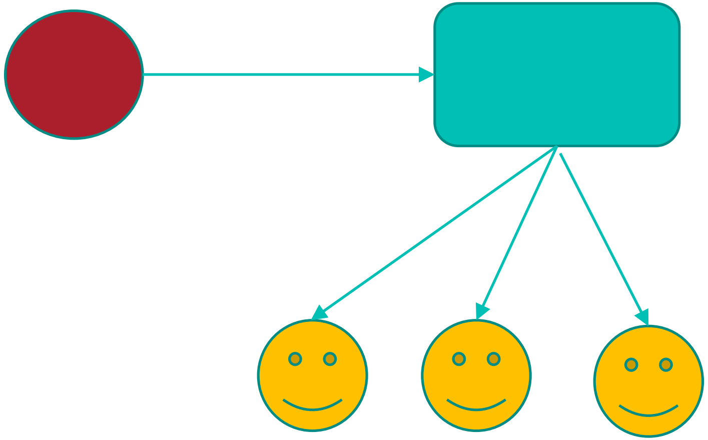
Cross Site Scripting Attack

```
<html>
<head>
[…]
</head>
<body>
[…]
<p> [some user content] </p>
</body>
</html>
```



Cross Site Scripting Attack

```
<html>
<head>
[…]
</head>
<body>
[…]
<p> </p><script>do.evil()</script></p>
</body>
</html>
```



University of BRISTOL

DNS exploit

DNS exploit

- Rely heavily on DNS security
  - Based on domain name!

DNS exploit

- Rely heavily on DNS security
  - Based on domain name!
- Approach:
  - Create a domain attacker.com

DNS exploit

- Rely heavily on DNS security
  - Based on domain name!
- Approach:
  - Create a domain attacker.com
  - User visit attacker.com

DNS exploit

- Rely heavily on DNS security
  - Based on domain name!
- Approach:
  - Create a domain attacker.com
  - User visit attacker.com
  - Browser generate DNS request to attacker.com

DNS exploit

- Rely heavily on DNS security
  - Based on domain name!
- Approach:
  - Create a domain attacker.com
  - User visit attacker.com
  - Browser generate DNS request to attacker.com
  - Attacker response is very short lived (small TTL)

DNS exploit

- Rely heavily on DNS security
  - Based on domain name!
- Approach:
  - Create a domain attacker.com
  - User visit attacker.com
  - Browser generate DNS request to attacker.com
  - Attacker response is very short lived (small TTL)
  - Attacker bind attacker.com to victim.com’s IP

DNS exploit

- Rely heavily on DNS security
  - Based on domain name!
- Approach:
  - Create a domain attacker.com
  - User visit attacker.com
  - Browser generate DNS request to attacker.com
  - Attacker response is very short lived (small TTL)
  - Attacker bind attacker.com to victim.com’s IP
  - AJAX request intended for attacker.com actually goes to victim.com

DNS exploit

- Rely heavily on DNS security
  - Based on domain name!
- Approach:
  - Create a domain attacker.com
  - User visit attacker.com
  - Browser generate DNS request to attacker.com
  - Attacker response is very short lived (small TTL)
  - Attacker bind attacker.com to victim.com’s IP
  - AJAX request intended for attacker.com actually goes to victim.com
    - Attacker has code that executes within a company internal network
    - e.g. launch a port scan into a corporate network

DNS exploit

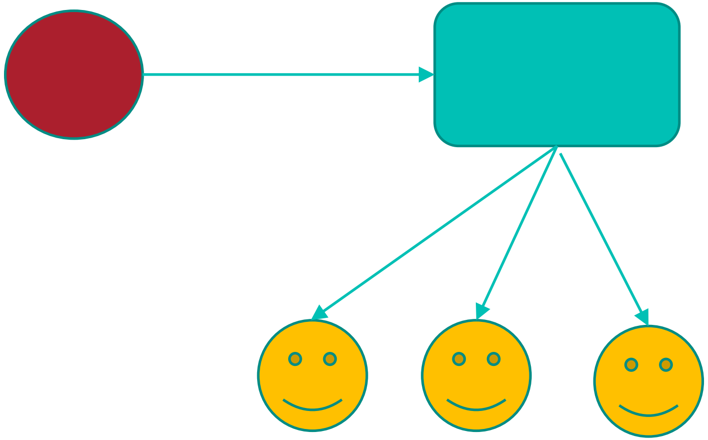
- Rely heavily on DNS security
  - Based on domain name!
- Approach:
  - Create a domain attacker.com
  - User visit attacker.com
  - Browser generate DNS request to attacker.com
  - Attacker response is very short lived (small TTL)
  - Attacker bind attacker.com to some other IP
  - AJAX request intended for attacker.com actually goes to IP
    - You can start for example a port scan into a corporate network
- FIX DNS RESOLUTION (TTL > some value)

How to avoid this?

Cross Site Scripting Attack

```
<html>
<head>
[…]
</head>
<body>
[…]
<p> </p><script>do.evil()</script></p>
</body>
</html>
```

DO SANITISE USER INPUT



Variation

- https://mydomain.com/index.html?something=<script>do.evil()</script>
  - Just get people to click on the link
- Could also get executed client side
  - *var url = new URL(url_string);*
  - *var a = url.searchParams.get("something");*

- (little game at the end of the lecture)

University of BRISTOL

Exploiting page layout

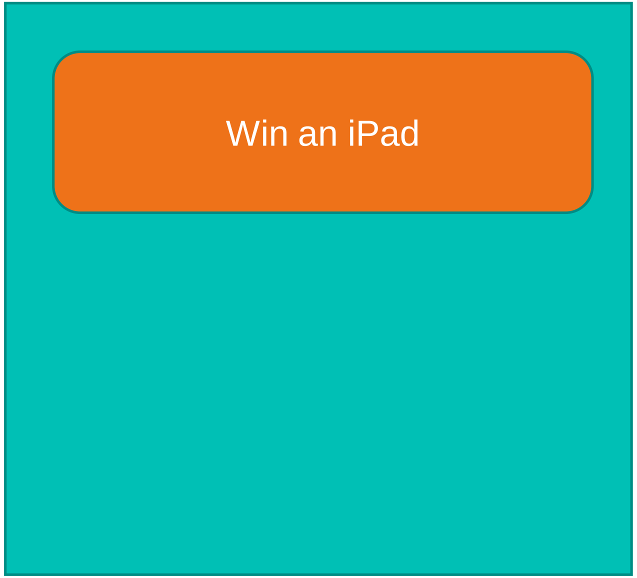
bristol.ac.uk

Exploiting page layout

- A pixel have no origin!

Exploiting page layout

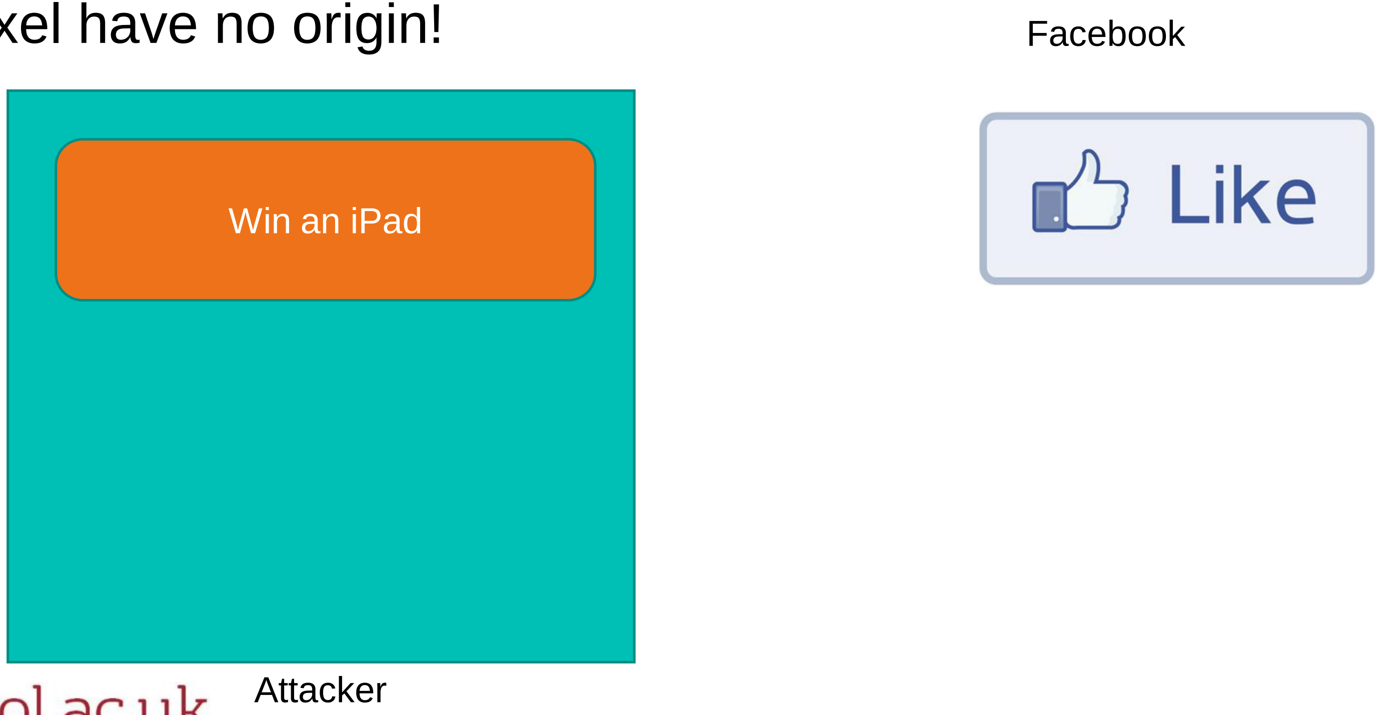
- A pixel have no origin!



Attacker

Exploiting page layout

- A pixel have no origin!



Facebook

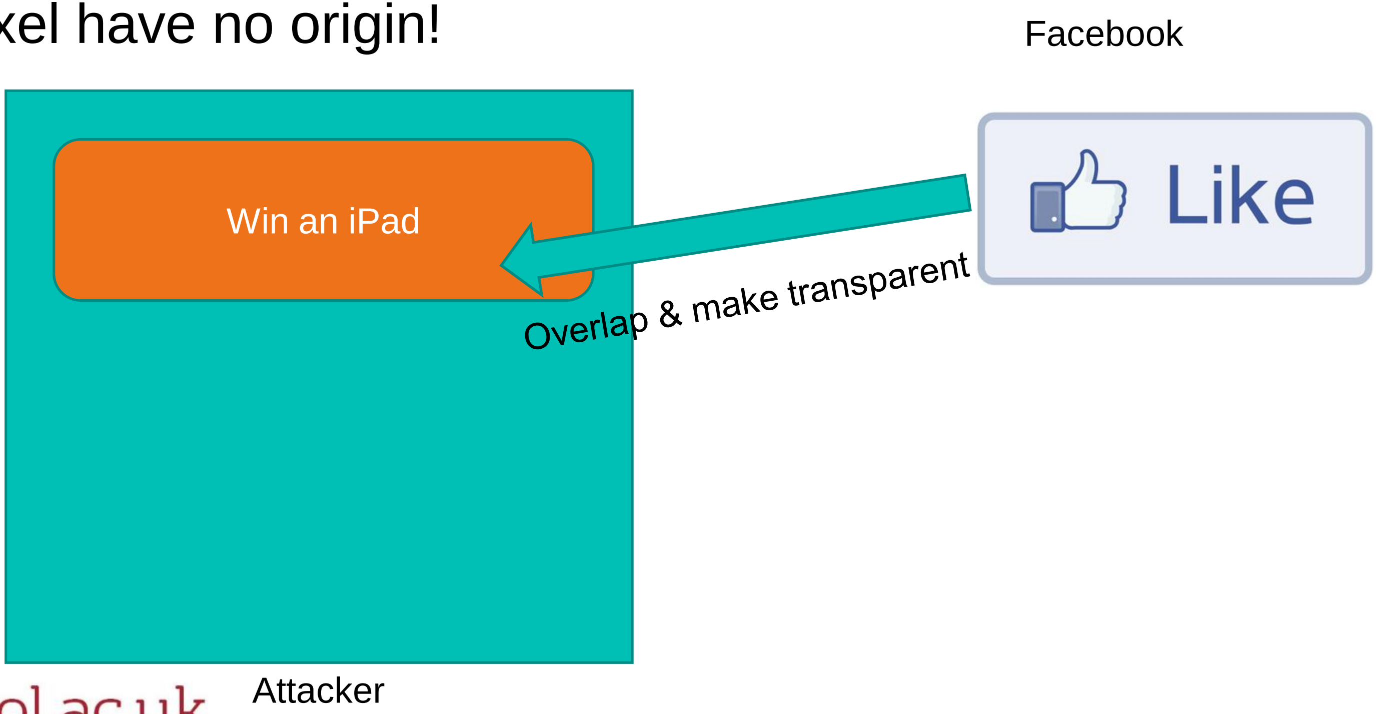
Win an iPad

Like

Attacker

Exploiting page layout

- A pixel have no origin!



Not so private, private browsing

Not so private, private browsing

- Client side privacy
  - Private browsing does not hide from network or server!

Not so private, private browsing

- Client side privacy
  - Private browsing does not hide from network or server!
- Private browsing is very leaky, leave information in e.g.:
  - DNS cache
  - RAM artefacts in page swap, hibernation files

Not so private, private browsing

- Client side privacy
  - Private browsing does not hide from network or server!
- Private browsing is very leaky, leave information in e.g.:
  - DNS cache
  - RAM artefacts in page swap, hibernation files
- Relatively trivial to recover such data with forensic tools!

Not so private, private browsing

- Client side privacy
  - Private browsing does not hide from network or server!
- Private browsing is very leaky, leave information in e.g.:
  - DNS cache
  - RAM artefacts in page swap, hibernation files
- Relatively trivial to recover such data with forensic tools!
- Possible solution? Check the Veil paper (NDSS 2018)
  - on the course github ;)

Conclusion

- Similar issue as with passwords
- Features are out there, they are used
- They are full of vulnerabilities
- However, we cannot walk back and provide something more secure
- We implement counter measure

University of BRISTOL

Thank you

Office MVB 3.26

- Google XSS game
  - https://xss-game.appspot.com