Sandboxing Trackers with Tracking Protection

Steven Englehardt
@s_englehardt
Tracking Protection
Manchester City 2-1 Sunderland: Former Manchester United defender Paddy McNair scores late own goal to gift first Premier League victory to Pep Guardiola

- Late Paddy McNair own goal handed Manchester City a win in Pep Guardiola’s first match in charge
- An equaliser from Jermain Defoe had looked like denying Guardiola in the Premier League opener
- Sub McNair, signed from Manchester United this week, headed into his own net after 87 minutes
- New City boss had made an immediate impact at City by dropping Joe Hart and Yaya Toure

By ROB DRAPER FOR THE MAIL ON SUNDAY
PUBLISHED: 12:41 IST, 13 August 2016 | UPDATED: 15:01 IST, 13 August 2016

At the end, the Etihad Stadium roared with the kind of enthusiasm you might expect when greeting one of the world’s finest and most iconic coaches. Poor Paddy McNair, brought on to safeguard the score, had just headed into his own goal within four minutes of his debut, and City finally had their breakthrough.

Jesus Navas crossed the ball. Vito Mannone flicked it away from the feet of Kelechi Iheanacho and McNair simply could not react quick enough to avoid nodding home from close range. The clock read 87 minutes and City fans sang with gusto, as though they finally believed a Messiahic figure was about to lead them to the promised land. And so it will be recorded that the Pep Guardiola era began with a win.

And, after the years of anticipation, it was really Guardiola on the touchline, finally overseeing a Premier League match. There was the familiar expensive, well-cut suit and the distinctive bald head, bobbing up and down as he waved his arms in excitement and exasperation in equal measure. On the pitch, the look was not quite so good.
Manchester City 2-1 Sunderland: Former Manchester United defender Paddy McNair scores late own goal to gift first Premier League victory to Pep Guardiola

- Late Paddy McNair own goal handed Manchester City a win in Pep Guardiola's first match in charge
- An equaliser from Jermain Defoe had looked like denying Guardiola in the Premier League opener
- Sub McNair, signed from Manchester United this week, headed into his own net after 87 minutes
- New City boss had made an immediate impact at City by dropping Joe Hart and Yaya Toure


At the end, the Etihad Stadium roared with the kind of enthusiasm you might expect when greeting one of the world’s finest and most iconic coaches. Poor Paddy McNair, brought on to safeguard the score, had just headed into his own goal within four minutes of his debut, and City finally had their breakthrough.

Jesus Navas crossed the ball, Vito Mannone flicked it away from the feet of Kelechi Iheanacho and McNair simply could not react quick enough to avoid nodding home from close range. The clock read 87 minutes and City fans sang with gusto, as though they finally believed a Messianic figure was about to lead them to the promised land. And so it will be recorded that the Pep Guardiola era began with a win.

And, after the years of anticipation, it was really Guardiola on the touchline, finally overseeing a Premier League encounter. In the end, it was a night of great theatre – and Guardiola, thankfully, will not be remembered for the wrong reasons.
Here's The Thing With Ad Blockers

We get it: Ads aren’t what you’re here for. But ads help us keep the lights on. So, add us to your ad blocker’s whitelist or pay $1 per week for an ad-free version of WIRED. Either way, you are supporting our journalism. We’d really appreciate it.
Forbes

QUOTE OF THE DAY

“The rewards in business go to the man who does something with an idea.”
- William Benton

Hi again. Looks like you’re still using an ad blocker. Please turn it off in order to continue into Forbes’ ad-light experience.
Facebook will start bypassing adblockers on desktop browsers

- Users of mobile adblockers will continue to experience an ad-free version
- Decision ‘takes a dark path against user choice’, Adblock Plus warns
Can sandbox trackers instead of block them?
Can sandbox trackers instead of block them?

No :(
1. Make a new third-party cookie blocking mode

From Non-Trackers
1. Make a new third-party cookie blocking mode

+ No stateful tracking in 3rd party iframes
1. Make a new third-party cookie blocking mode

+ No stateful tracking in 3rd party iframes
+ No cookies with `<script src…>` embeds
1. Make a new third-party cookie blocking mode

+ No stateful tracking in 3rd party iframes
+ No cookies with `<script src…>` embeds
+ Less breakage than other cookie blocking
1. Make a new third-party cookie blocking mode

- No stateful tracking in 3rd party iframes
- No cookies with `<script src…>` embeds
- Less breakage than other cookie blocking

- `<script src…>` DOM access

From Non-Trackers
1. Make a new third-party cookie blocking mode

+ No stateful tracking in 3rd party iframes
+ No cookies with `<script src…>` embeds
+ Less breakage than other cookie blocking

- `<script src…>` DOM access
- Active content can still fingerprint
1. Make a new third-party cookie blocking mode

+ No stateful tracking in 3rd party iframes
+ No cookies with `<script src…>` embeds
+ Less breakage than other cookie blocking

- `<script src…>` DOM access
- Active content can still fingerprint
- Will encourage fingerprinting

From Non-Trackers
2. Block cookies and use iframe sandbox


2. Block cookies and use iframe sandbox

+ No fingerprinting in iframes
+ Restrict plugin use, modal dialogs, top-level navigation, etc
2. Block cookies and use iframe sandbox

+ No fingerprinting in iframes
+ Restrict plugin use, modal dialogs, top-level navigation, etc

Not enough trackers are embedded in iframes.
3. Block active content and sandbox iframes

Built a prototype to test this...
3. Block active content and sandbox iframes

Built a prototype to test this...

breakage is still too high!
3. Block scripts and sandbox iframes

- Google, Facebook, Twitter all require or recommend first-party script access
- 2 out of 10,000 sites iframe Doubleclick
- 209 out of 10,000 sites iframe Facebook
Blocking with Tracking Protection
Sandboxing with Tracking Protection
Guten Abend!
Ihr Wetter für heute in Berlin

bis 21°C leicht bewölkt

Zur Tagesvorhersage

Aussichten

weiterlesen

Empfehlungen der Redaktion

Blocking with Tracking Protection
Guten Abend!
Ihr Wetter für heute in Berlin

Aussichten

Sandboxing with Tracking Protection
4. Sandbox active content and sandbox iframes

G'.prototype

Main Page

Tracking Sandbox
4. Sandbox active content and sandbox iframes

Define *tracking wrappers* for interactions across the sandbox boundary
What do Google scripts do?
What do Google scripts do?

<iframe
    onload = "...
    id = "aswift_0"
    width = "300"
    height = "250"
> </iframe>
What do Google scripts do?

```javascript
var i = this.id,
    s = window.google_iframe_oncopy,
    h = s & amp; & amp;
    s.handlers, h = h & amp; & amp;
    h[i], w = this.contentwindow, d;
    d = w.document
    if (h & amp; & amp; d & amp; & amp;
        `...
        w.location.replace(h)
    }
}
Tracking scripts require inline javascript access

- Google iframes with `onload` -- 10% of sites
- Iframes with `javascript: src urls` -- 20% of sites
- Insert inline scripts into first-party -- 18% of sites
Sandboxing Javascript is infeasible

- Breakage still too high
- Requires support for inline javascript
  - Inline function rewriting
  - Function reflection from sandbox to main page
- **Sandbox design will change as scripts change**
Thank you!

Joint work with Tanvi Vyas (my mentor!) and Eric Rescorla

Thanks to my manager Steve Workman, the Security Engineering team, and the University team!

Contact me:

singlehardt.com
@s_englehardt