CSP, the right solution for Magecart?

medium.com/reflectiz/csp-the-right-solution-for-the-web-skimming-pandemic-acb7a4414218

Idan Cohen November 29, 2020

Idan Cohen

Nov 25, 2020

.

6 min read

CSP, the Right Solution for the Web-Skimming Pandemic?

I've been asked a lot about Content Security Policy (CSP) as a possible solution for Magecart and other web-skimming attacks lately. Companies, mostly eCommerce sites, are actively looking for a way to handle this emerging threat. CSP, which is not a costly solution, has become an integral part of many security-toolboxes.

But is it the solution you really need to fight Magecart?

The Third-Party App Challenge

Modern eCommerce websites and business platforms are using dozens of external third-party apps to enhance their user engagement, site performance and conversion metrics. Third-party applications for analytics, heat-maps, ads, and chats are good examples.

Unfortunately, it's not a bed of roses. These external applications are loaded remotely and can create additional entry points for an attacker, which are not protected by any of the traditional security controls such as WAF or IPS. Risks can escalate fast, as the modern eCommerce business has to deal with cybercrime, supply-chain attacks, breaches, financial damages, accountability, reputational damage, compliance, and safety audits.

Especially since the rise of the new Magecart threat. Magecart essentially involves hacking groups that specialize in gaining unauthorized access to websites and injecting malicious code into checkout pages.And how do they gain access? By exploiting third-party applications, a common phenomenon in the eCommerce space.

Many Magecart attacks have been exposed in recent years. For example, over 10,000 online shoppers were attacked during September 2020, in what was identified as a zero-day Magento exploit (sold in the dark web markets). Almost 2,000 eCommerce websites (mainly checkout pages) were targeted with a payment-card skimmer.

This methodology is basically a malicious JavaScript (JS) code that detects sensitive user activity, such as typing of credit-card numbers, passwords or any kind of Personally Identifiable Information (PII). Shopping cart checkouts are the most desired target due to the involvement of payment details and personal information.

These attacks are evolving at a rapid pace. It's an armed battle between the evolving malicious attacks and defenders trying to block them with tools like CSP.

Content Security Policy (CSP)

Content Security Policy (CSP) is a computer security standard introduced in 2004 to combat malicious activity such as cross-site scripting (XSS), clickjacking, and other client-side code injections resulting from the execution of malicious code in trusted webpages.

Putting CSP into action requires the addition of a Content-Security-Policy HTTP header into the webpage and assigning the required values to fully control the resources end-users can load and the destinations they can go to. These elements can be scripts, pictures, videos, forms and more. By doing so, it makes it harder to pull off Magecart attacks.

In theory, if the attacker wants to load a malicious script from www.malicious.com and the CSP has been configured not to load external resource scripts, the attack will be fully blocked. However, its required to write a well planned policy to make CSP work effectively. These are a predetermined set of directives that determine what resources (fonts, images, multimedia and most importantly scripts) will be needed and used for a safe and secure browsing environment. Please visit Manisha Sangwan's article for additional details.

CSP has fought many online battles since its inception back in 2004, when it was referred to as Content Restriction. CSP was created to combat the very commonly executed XSS attacks. I won't elaborate on XSS in this article, but please check MRunal's "What is Cross-Site Scripting" article to learn more.

Unfortunately, due to the rise of these risks, CSP might not be the stand-alone solution everyone is looking for. As we'll see in the next section, Magecart and other web-skimming attacks are now gaining the upper hand.

Why is CSP Not Enough?

For starters, having a Content Security Policy is a good thing. If you have the resources to manage it, go for it. However, like any security solution, the results may vary. The best case scenario is that you may gain only partial Magecart protection, but with multiple shortcomings to deal with on a daily basis.

The Blacklist/Whitelist Approach

The first problem with CSP is that, by whitelisting a trusted domain or an app, you are whitelisting everything inside the domain, regardless of its actual behavior. That's the main problem with the blacklist / whitelist approach. You are not approving the actions and data, you are just whitelisting everything.

This issue can create three different types of attack vectors:

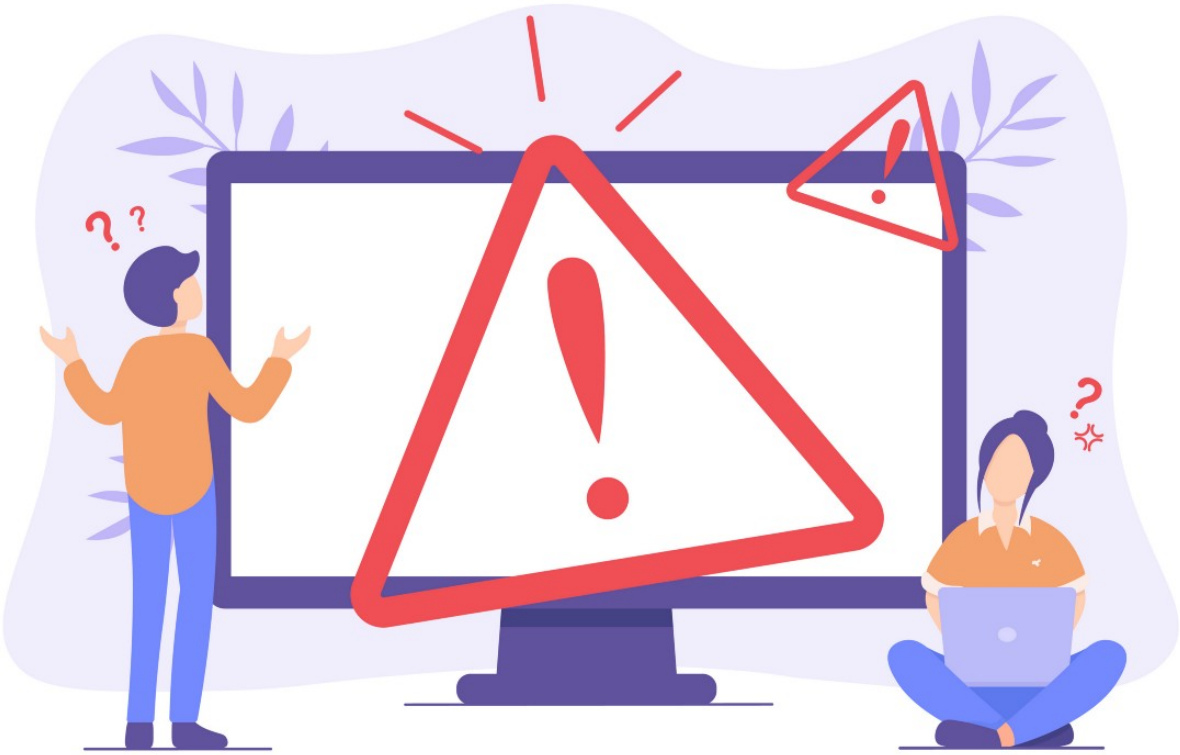
1. A third-party app breach won't be blocked by CSP. This is because the site owner has already approved the third-party domain. If the attacker can access the third-party domain, the CSP will let it run without any interference. I agree that a good CSP directives might create additional effort for an attacker in order to extract the data outside to a second unauthorized domain, but the attack will still take place leaving the attacker with enough playground to bypass it and complete the attack, as demonstrated Bhavesh Thakur's about CSP Bypass Techniques.
2. Breach the on site servers. Most of the famous Magecart attacks targeted internal unsecured servers and scripts in the organization and injected malicious code there. It's a common practice to allow scripts to be loaded from the website internal domains and bypass the entire idea of CSP. It's almost impossible to manage all the local scripts using CSP.
3. Use a common global service to extract personal data. For example, this shows that the Google Analytics API could be used to hack into eCommerce websites, and other online businesses. As Google Analytics can collect any data defined in the control panel, the attackers can just inject their own "Google Analytics" scripts to the website. It will be whitelisted by CSP, and the data will be leaked. Good luck with tracking all of the inputs being collected by dozens of third-parties using CSP.

CSP: A High maintenance solution

You might be thinking now — “Well, if CSP won’t help it all, why bother?” Yes, even with CSP, attackers can still leak data from internal and external breaches, or just exploit some online service. But I’m not saying it won’t help. CSP is a strong solution that may help block attacks or make attackers work harder, which is a good thing! Do it.

But the second problem is maybe the trickier one.

CSP is a high maintenance solution. As stated above, you need to define a whitelist and blacklist policy for the specific domain or scripts. It requires hands-on management and maintenance to achieve satisfactory results.



Let’s say you have 50 third-parties on a given website each uses several scripts and domains. Now what? You will find yourself working hard to keep it all updated and running. Some companies might have the required resources for it, but for most this is an overwhelming task. Either way, it will create a big headache, as every script change will be

blocked in production and secure your site, but the same may apply to important actions needed by the digital or marketing team. If we go beyond, CSP can also hurt the website's daily performance.

An average eCommerce website uses 50 to 60 third-party apps. Can security teams handle the risks each third-party creates continuously?

Final thoughts

CSP is still an effective weapon, but it's hard to recommend it as a stand-alone solution. It should ideally be combined with additional measures, such as discovery tools, validation tests and strict script policy to ensure reasonable resource cost .

Another interesting solution that might work better than CSP against these kinds of attacks is Subresource Integrity (SRI). It might be a better value-cost solution to battle Magecart, if done right. We will talk more about SRI in my next article. In the meanwhile, let's keep websites safe!

About me, I'm the CEO and co-founder of Reflectiz, a cybersecurity company. Reflectiz is the first website-sandbox solution that mitigates the risk of third-party apps.