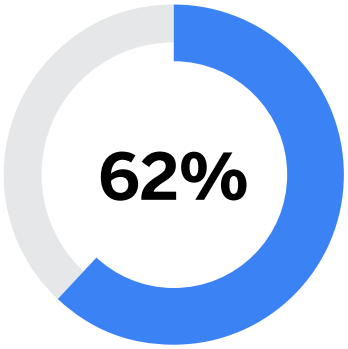
TALA

Taking the risk out of digital transformation

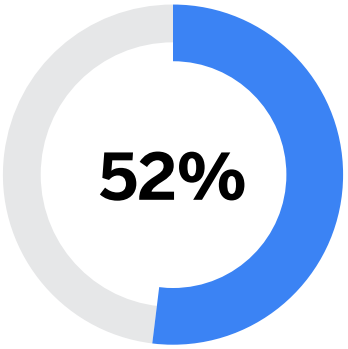
– turning web security into a business enabler

You've invested significant resources into delivering a rich customer experience online. Analytics and metrics help to continually tune that experience. But what if that same rich experience is putting your business and customers at risk?

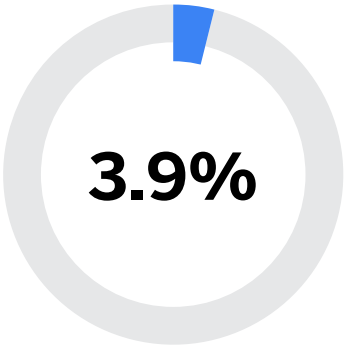
When it comes to online transactions, trust is everything.
Whether you're a financial services provider or a retailer, healthcare specialist, media outlet or marketing business, nothing tests customer relationships like a data breach:



62% of consumers **aren't confident their personal data is secure** with retailers.[1]



52% of customers who experienced fraud on their card said it left them with a **negative perception of the retailer** - even when it wasn't the retailer's fault.[2]



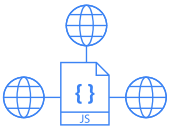
Breaches caused **customer turnover** of 3.9% in 2019.[3]

The challenge for all businesses embracing digital transformation is that the trust ecosystem inevitably involves third parties: the products and service providers behind the chatbots, analytics tools, marketing services and many of the rich user experiences that businesses love to use.

These third-party integrations are capable of capturing and processing user data - often without website owner authorization or control. Breaches originating from a third party – such as the website supply chain – cost companies significantly more on average[4], emphasizing the need for companies to closely vet the security of companies they do business with, align security standards, and actively monitor third-party access.

The complexity of this ecosystem is growing all the time:

The average website relies on **33 third parties**.



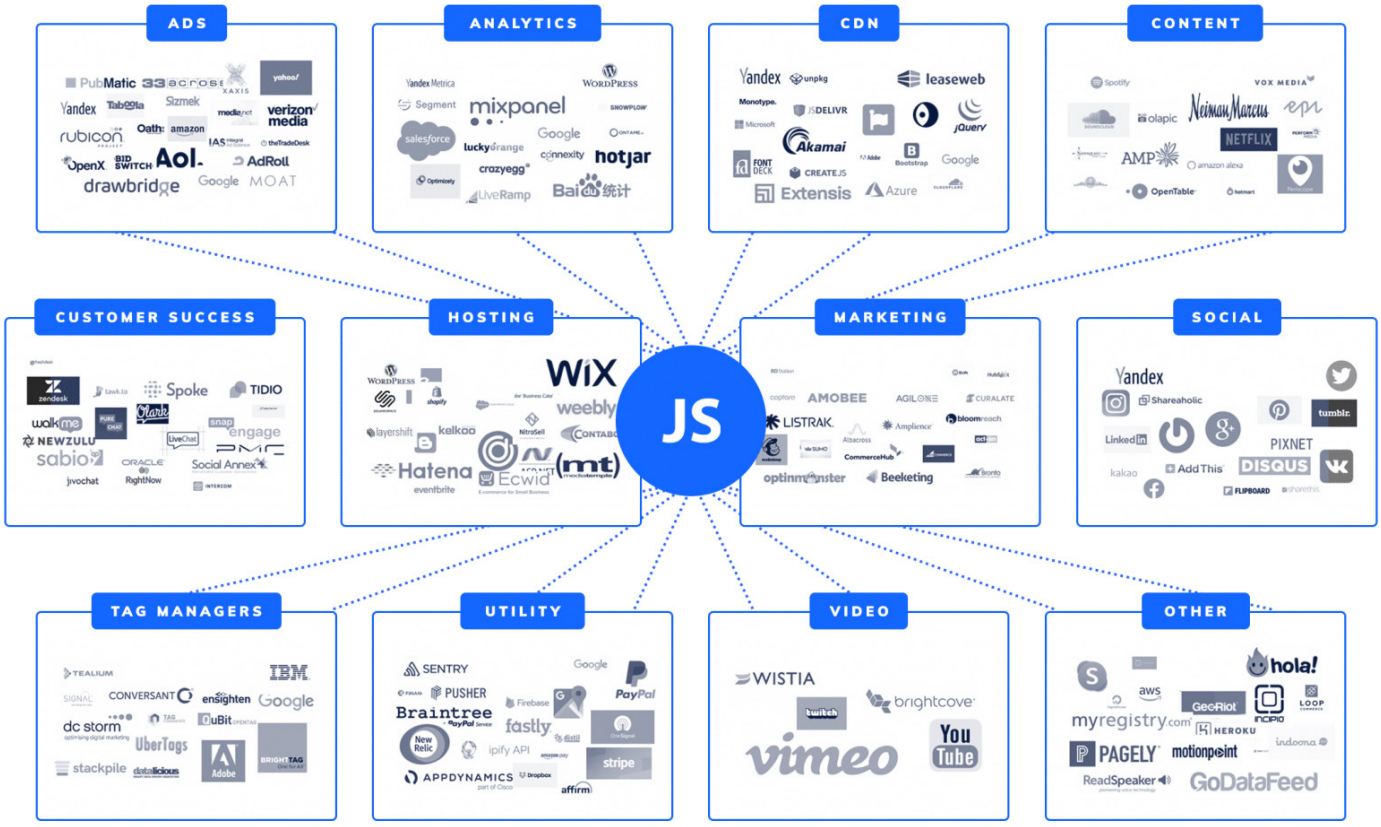
63% of JavaScript code executed in the browser is **written and/or managed by third parties**.

Source: State of the Web Report 2019

1. https://www.digitalcommerce360.com/2019/01/15/why-all-data-breaches-pose-a-threat-to-retailers-customer-experience/
2. https://www.digitalcommerce360.com/2019/01/15/why-all-data-breaches-pose-a-threat-to-retailers-customer-experience/
3. IBM: Cost of a Data Breach 2019
4. https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

TALA

99% of websites globally include multiple client-side vulnerabilities that leave them open to attackers: The average website relies on 33 third party services.



How prevalent are client-side attacks?

↑78%
increase in website supply chain attacks

↑10X
more sensitive data than intended

$230M
largest GDPR fine for a data breach tied to Magecart

TALA

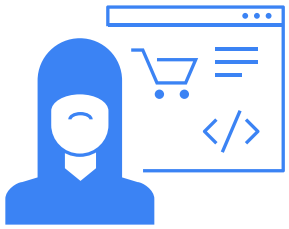
Let's take a look at some of the most common vulnerabilities and exploits through the lens of some very high-profile attacks, and what they mean in real terms for your business or marketing efforts. Then we'll show you how you can mitigate them - for good.

Magecart (formjacking)

'Magecart' isn't a specific piece of malware, it's an umbrella term to describe the 12+ different cybercriminal gangs using card-skimming, code injections and other data exfiltration techniques to steal user data (including payment card details) from business websites. It's sometimes called 'formjacking.'

The reason you've probably heard of Magecart is because it's responsible for multiple high-profile attacks belonging to huge global brands: British Airways, Macy's, Ticketmaster, NewEgg, OXO and thousands of others (at least). Magecart skimmers have been detected on over two million global websites, with supply chain attacks (i.e. third party code hosted on a website) causing a significant spike in breaches and detections[6]. In the Macy's attack, the cybercriminals actually customized code specifically for the retailer's website. Credit card information was stolen from customer wallets and new registrations. When the news broke, Macy's stock took an 11% hit in October 2019.

The British Airways attack used cross-site scripting (XSS) to steal 565,000 credit cards - at a cost of $230m in fines. What made this attack unusual was that the criminals exploited BA's own code on their site - it was crafted to blend in carefully with BA's normal payment set up. This is what makes Magecart so powerful for attackers: it's not just a third-party attack, it can also strike as a first party, as British Airways discovered.



The secret to Magecart's success:

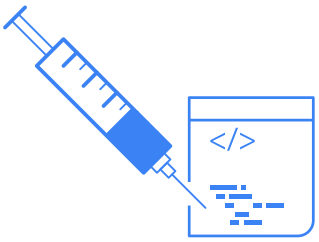
What makes this technique so effective is that these attacks can go undetected for months or even years. Everything happens in the browser (the 'client-side'). It doesn't impede the transaction in any way, so the customer carries on, the retailer receives their payment and no one spots anything. Until they do.

6. https://www.darkreading.com/endpoint/magecart-skimmers-spotted-on-2m-websites/d/d-id/1336011

TALA

Content/Ad Injection

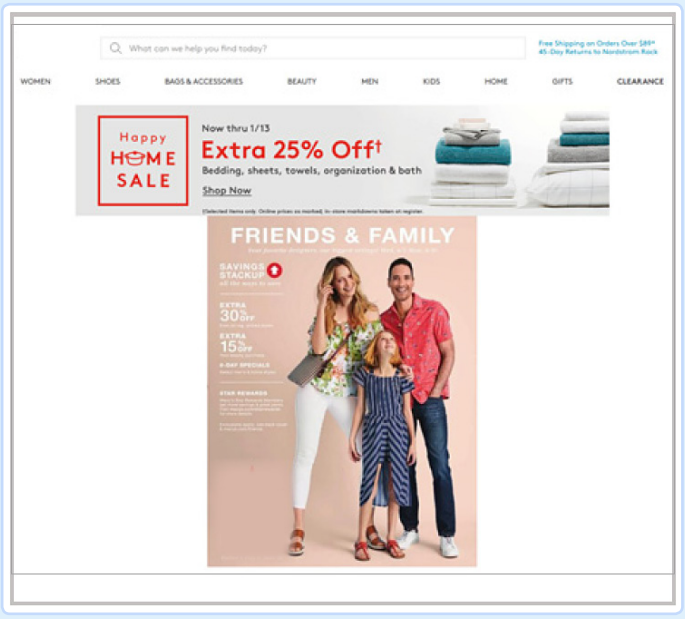
You've invested a lot of time into refining the user experience on your e-commerce website. You've optimized everything to attract your target audience, all the way through the special offers, but you're losing business to competitors. You dig a little deeper and find that when your customers visit your site, unapproved malicious or competitive ads are being displayed to them. They're clicking for what looks like a better deal - and you're losing business.



You've experienced a content injection attack. In this instance, it's known as a 'competitor ad injection' but the unwanted ads can serve malware or entice users to undesirable sites (called 'clickjacking', which we'll talk about a little later). Google estimates that 17% of Windows binaries and 38% of Chrome extensions injected ads[7]; an estimated 10-15% of online web traffic is hijacked or subjected to injection attacks, with as many as 70% of these ads carrying offers from direct competitors.

The average invalid traffic volume per North American internet user is projected to increase 57% through 2023 - twice the growth of genuine ad traffic over the same timeframe[8]. With an estimated 80% of display ads bought by automated systems in 2019[9], the threat posed by complex and often opaque supply chains is growing - advertisers displaying a million ads over a 24-hour period are likely to pay for more than 100,000 ads before any issue is detected[10].

Malicious or competitive, non-approved ads can be served to end-users. As this mocked-up screenshot shows, the website the end user is browsing to (retailer.com) is serving ads for a competitor (retailer-competitor.com)



7. Google et al: Ad Injection at Scale
8. Traffic Guard & Juniper Research
9. R. Benes: Agency Pros Say Fraud is Biggest Threat to their Budgets.
10. Traffic Guard & Juniper Research

TALA

Clickjacking

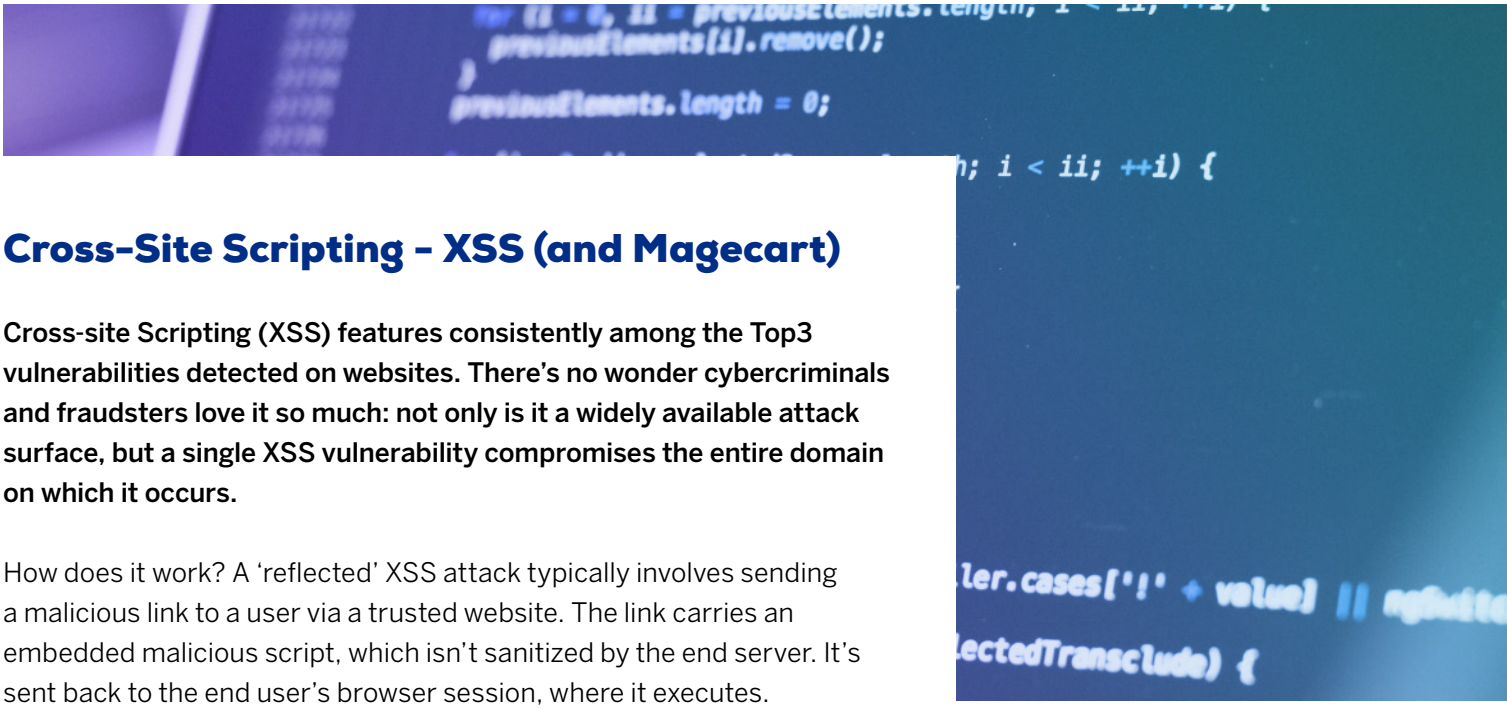
The other side of the content injection coin, unwanted ads can serve or entice users to undesirable sites - known as 'clickjacking'.

Clickjacking attacks involve tricking a user into clicking on a button, link, image or other content injection (see above) that either serves malware or diverts them to a competitor or malicious website.

It can cost trusted brands with well-earned high traffic a lot of money when they unwittingly carry the cost of traffic from injectors. As with content injection, this is all happening on the user's browser - the 'client-side' - essentially out of sight and control of any server-side controls.

How do they do it? Injection attacks often arrive via browser extensions, where users download some kind of browser enhancement that, unbeknownst to them, also includes software that can inject unauthorized ads or hijack online searches, for example. Once embedded in their browser, the attackers have control over the user's browsing experience.

The secret of content injection's success:
What makes this technique effective is the combination of end-user willingness to install browser extensions and the willingness of certain types of advertisers to pay for traffic generated by injectors. As with Magecart, everything happens in the browser, on the client-side.



Cross-Site Scripting - XSS (and Magecart)

Cross-site Scripting (XSS) features consistently among the Top3 vulnerabilities detected on websites. There's no wonder cybercriminals and fraudsters love it so much: not only is it a widely available attack surface, but a single XSS vulnerability compromises the entire domain on which it occurs.

How does it work? A 'reflected' XSS attack typically involves sending a malicious link to a user via a trusted website. The link carries an embedded malicious script, which isn't sanitized by the end server. It's sent back to the end user's browser session, where it executes.

TALA

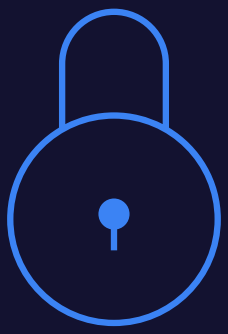
A 'persistent' attack typically happens on web applications where users enter data, through which the malicious script is injected. In these attacks, the end server stores the malicious script - and because of this, the attack executes whenever the script is fetched from the server.

Magecart groups often use XSS as a method of attack. In April 2020, researchers revealed a massive growth in XSS flaw attacks on WordPress websites, mainly targeting plug-ins. These allowed attackers to change a site's home URL to re-direct visitors to malicious/malvertising sites. In early 2020 the widely used WhatsApp platform was found to have gaps in its Content Security Policy that enabled XSS attacks capable of sending harmful code to end users via seemingly harmless messages, including customer engagement initiatives.

The secret to XSS success: Many XSS attacks rely on our tendency to click without thinking, particularly when it's a link or a message from a trusted brand, product, business or known website. Combined with the fact that a single vulnerability gives attackers access to the entire domain, and it's easy to understand the popularity of these attacks.

SECURING TODAY'S - AND TOMORROW'S - WEB

Third-party tools have transformed your online presence - but if you don't secure them, it will all be for nothing. Attacks like the ones we've just discussed not only facilitate cyberfraud and theft, but they also expose your business to inadvertent breaches of data protection regulations such as GDPR and CCPA: many businesses are unaware that otherwise legitimate apps are gathering and re-using customer data for purposes that aren't always clear.



Think about it: You're not just looking to protect your business from Magecart. You need to protect against other client-side attacks, like:

- User data leakage
- Content integrity attacks
- Ad injections
- Session re-directs
- Clickjacking
- Cross-site scripting (XSS)

The vulnerabilities might be on your website, but the point of execution for all these attacks is in your customer's web browser. And that's where you need to go to secure them. The good news is that the same experts who revolutionized and built the modern web - like Google, PayPal, W3C - saw these security flaws long before anyone else did. They not only designed security standards and controls to defend against them, they built these same controls into the browser (i.e. they're "browser-native") and web application frameworks.

Businesses that deploy these controls are using the same level of security to protect the client-side as web giants like Google, but a shockingly low number of companies take advantage of this: just 2% of U.S. Alexa 1000 websites are adequately secured against the types of attack that hit British Airways and Macy's.

TALA

HOW TALA HELPS

Tala's approach to protecting the modern web is fundamentally different from most other solutions. Like Google, the W3C and other web experts, we believe that the answer to client-side security starts in the browser. We use AI and analytics technologies to automatically implement the security standards developed by these experts - without any impact on the performance of your site.

These standards include: CSP, SRI, Referrer Policy, Feature Policy, Trusted Types and Clear-Site-Data. Together, they provide a comprehensive web security strategy, developed and built by the world's leading web innovators and experts. Who wouldn't want to secure their websites with standards developed by the best minds in the business? Leading organizations like the PCI Council and RH-ISAC recommend CSP. Here's how they can prevent the attacks we've just discussed:

Magecart/formjacking: Tala uses fine-grained CSP, along with SRI (integrity hashes) and continuous monitoring to detect these types of attacks during scanning.

Cross-site scripting/ XSS: Tala detects and prevents XSS attacks by analyzing the app, creating a list of all legitimate scripts, and whitelisting them. Malicious scripts will not be allowed to run because they won't be on the whitelist. Note: Javascript-based solutions cannot prevent XSS attacks.

Content/ad injection: Tala protects against content injection / ad injection attacks by using all the directives supported by CSP to prevent any code or markup that is injected. Tala also uses SRI to prevent any third party code modifications that could lead to content injection attacks.

Clickjacking: Tala protects against clickjacking attacks using the 'frame-ancestors' directive provided by CSP. This ensures that your website can only be embedded on whitelisted domains.

To learn more about the threats facing 99% of the world's websites, download our **Global Data at Risk - State of the Web 2020** report. You can find out more about how Tala uniquely protects against client-side attacks like Magecart and XSS without impacting on your website's performance by **booking a DEMO today!**