The Key Threats and Risks That Third-Parties Create to Websites

Third-party apps on websites present potential threats and risks that may affect the security and privacy posture of your website. For your customers, your website is the front end of your organization.

In today's digitally connected world, websites play a major part in almost every company's success, and yours is no different. Websites often integrate third-party tools to make themselves more dynamic and interactive, and for offering smooth connectivity to their customers.

These third-party tools and apps also play a vital role in generating revenue for your website. If you examine any given website today, you will find dozens of these tools. We use them for advertising and digital marketing, user engagement, widgets, chatbots, social media tools, analytics, cloud storage, trackers, developer frameworks, and lots more.

The Risk of Using Third-Party Apps

No one can deny the benefits that these third-party apps provide. They bring better functionality for your customers and allow your organization to monetize its business and generate more revenues.

Who are we?
We're a cyber-security company that helps organizations mitigate security and privacy risks resulting from third-party components installed in their websites

Visit our website:
www.reflectiz.com

Who are we?
We're a cyber-security company that helps organizations mitigate security and privacy risks resulting from third-party components installed in their websites

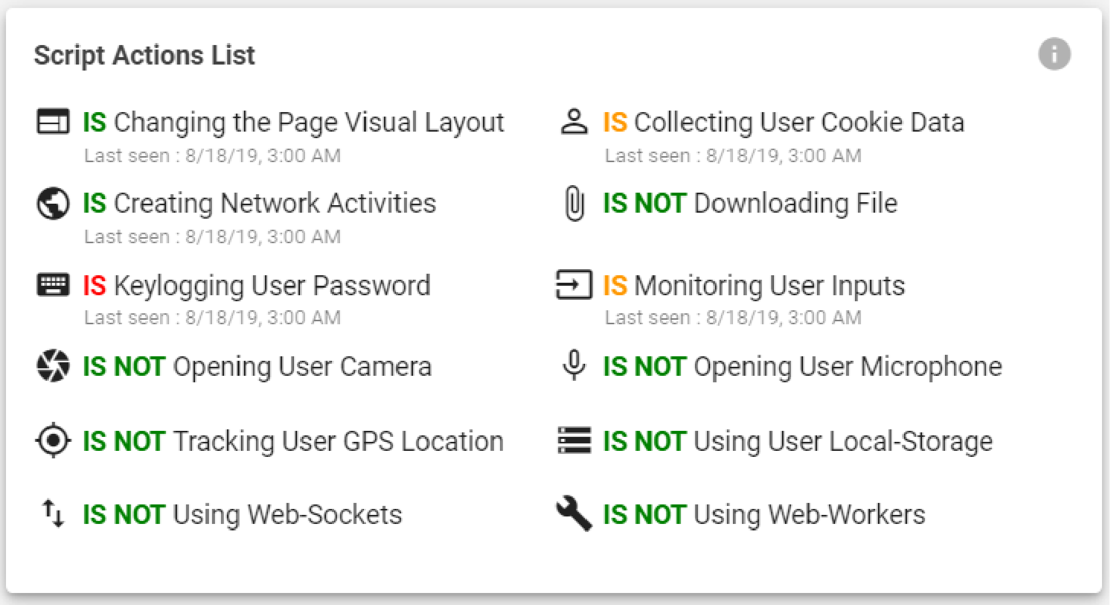
Visit our website:
www.reflectiz.com

However, these apps also present significant security risks and privacy threats to the users' data. Yes, you might have been using an Intrusion Prevention Systems (IPS) or a Web Application Firewall (WAF) to protect your website from web-based attacks. But these controls alone are simply not enough for end-to-end security of the web applications on a website. Standard web security solutions like IPS or WAFs can help protect the communication between the end-user and your servers. However, they are not as effective when it comes to third-party web apps. Why? Because for these apps, the client-side is responsible for the connections with the third-party vendors, and your IPS or WAFs' protection mechanism simply doesn't function on that environment. In fact, the end-user generates communications with dozens of global locations, but websites have minimal capabilities to monitor it within their existing security products. And this is a problem!

In spite of the most stringent tests and checks, third-party services can infiltrate your systems without requiring any permission from your website. This blind spot in your website security infrastructure can end up compromising your software platforms and data, leading to severe consequences.

There are three major types of risks that third-party apps and services can pose to your website:

- Supply Chain Attacks
- Third-Party Vendor Errors
- Privacy Breaches and Regulation Issues



Script Actions List

IS Changing the Page Visual Layout
Last seen : 8/18/19, 3:00 AM

IS Collecting User Cookie Data
Last seen : 8/18/19, 3:00 AM

IS Creating Network Activities
Last seen : 8/18/19, 3:00 AM

IS NOT Downloading File

IS Keylogging User Password
Last seen : 8/18/19, 3:00 AM

IS Monitoring User Inputs
Last seen : 8/18/19, 3:00 AM

IS NOT Opening User Camera

IS NOT Opening User Microphone

IS NOT Tracking User GPS Location

IS NOT Using User Local-Storage

IS NOT Using Web-Sockets

IS NOT Using Web-Workers

Script actions description screen. This case refers to a real e-commerce website, describing both potential and actual activities that a third-party or a fourth-party script can perform.
Source: a sample client's dashboard, refSec by Reflectiz

Supply Chain Attacks

Supply chain attacks happen when hackers penetrate systems through an external partner or service provider and gain access to your systems and data. Every organization, ranging from Walmart and Ford to Samsung and Dell, has a massive supply chain working for them down the line. These suppliers and service providers have access to the most confidential information of your customers, as well as to your security systems. Not every organization in your supply network deploys the best security measures. Cybercriminals take advantage of this aspect and tamper with your systems or the automated manufacturing process of your product in a production unit by installing hardware-based spying components. On the web environment, this becomes even more critical, as all your vendors are being loaded to your page when the users are browsing your website semi-automatically. To demonstrate – it's like embedding a vendor's straight inline into your code. You will not do it with usual outbound suppliers, but on your website, you don't have a choice. They are there!

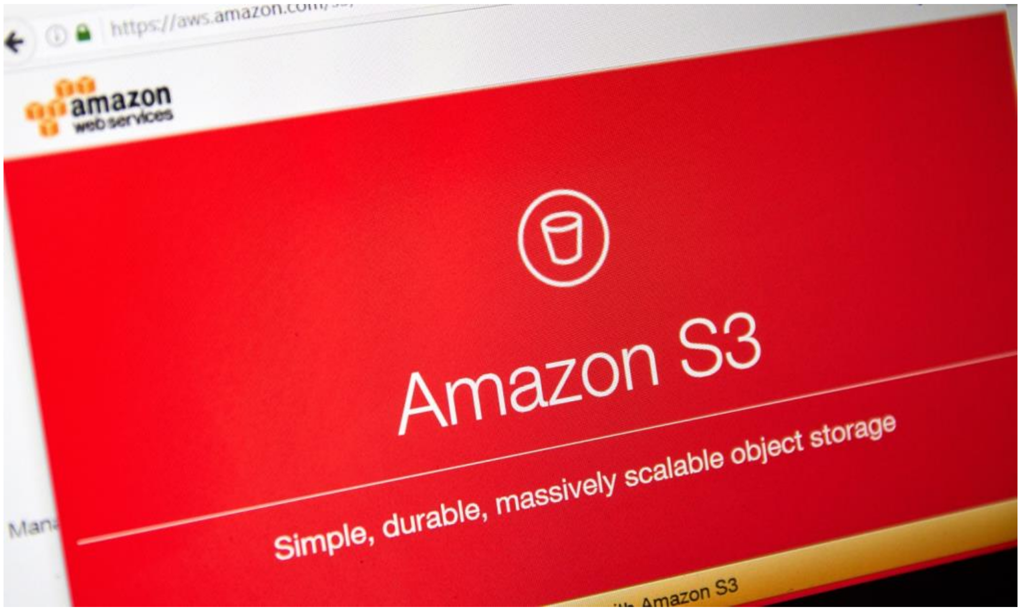
Ticketmaster Third-Party Breach Example

For example, Ticketmaster became a victim of a massive data breach between February 2018 and 23 June 2018. Confidential data of customers who used Ticketmaster website to book tickets during that period was compromised. It included name, address email address, telephone numbers, and credit card details. The malicious code was spotted on 23 June 2018, approximately four months after it started! But the damage was already done. More than 40,000 Ticketmaster customers worldwide were affected. Ticketmaster blamed Ibenta Technologies, a third-party service provider for the breach. Ibenta Technologies rejected the allegations, stating that Ticketmaster directly applied an affected JavaScript code to its payment page without informing them. They contended that they would not have advised embedding the customized script. No matter who took the blame, a severe third-party breach occurred.

It is always easy to blame a third-party, and in this case, both Ticketmaster and Ibenta Technologies were at fault. Ticketmaster should not have introduced the affected JavaScript code into the payments page without notifying Ibenta, especially when Ibenta Technologies was the third-party service provider that offered the specific customer support service. But at the same time, Ibenta Technologies should have monitored how Ticketmaster was using their services. The lack of proper communication between the two parties allowed hackers to steal vital data. To avoid such instances, websites must use a third-party monitoring mechanism, providing ability to know what each third-party is doing and means to detect any breach that could be relevant for them.

Vendor (Third Party Service Providers or Contractor) Errors

A website is connected to many third-party apps which are also developed by various vendors. Nevertheless, organizations, companies and business owners are all equally responsible for the actions of the third-party vendors. Eventually, it is their reputation that will be at stake, even if the error is on the third-party vendor's end. No matter how you look at it, it is your responsibility to ensure that everything is in order. You might expect your third-party vendor to use the same kind of security measures that you use to protect your website, but usually, this isn't the case. Therefore, monitoring your third-party vendor services becomes a crucial aspect of the proper functioning of your website. One error on their side could cause irreparable financial losses and damages to your reputation.



The Amazon S3 Bucket Example

The Amazon S3 bucket misconfiguration that was discovered in mid-2019 is an excellent example of a vendor error that caused damage to thousands of websites.

In that case, hackers scanned multiple Amazon AWS S3 buckets to detect misconfigured buckets that had remote write permission on them. The hackers scanned these S3 buckets for JavaScript files and were able to modify them. On appending the skimming code to the bottom, they could overwrite the scripts on these buckets. The reasons for this were misconfigured permissions on the S3 buckets that allowed almost anyone to overwrite information, inject the malicious code, and target dozens of websites.

The solution for the problem starts with a simple but critical understanding: that it is your reputation that is at stake. Regardless of whether there are chances of third-party errors or not, your website must have risk mitigation processes in place. Understanding the risk levels is also of prime importance. Furthermore, the stringent regulation today mandates that companies have the responsibility for their third-parties; they can't say: "It's not us; it's them."

Privacy Breaches

Organizations take different measures to protect themselves against third-party risks, usually by deploying a questionnaire or an organized process that comes before third-party integration. But even if such procedures are perfect (and they are not), third-parties commonly use other third-party apps of their own. And they bring their third-parties to your site. Hence, one data breach can lead to another down the line.

The New Privacy Sanctions

GDPR

The European Union brought a stringent privacy rule known as the General Data Protection Regulation (GDPR) into force in 2018.

reflectiz

Who are we?
We're a cyber-security company that helps organizations mitigate security and privacy risks resulting from third-party components installed in their websites

- GDPR forces companies to ensure that the method of collecting, processing, and storing customer data is secure.
- Companies can collect data only if they have a lawful reason for doing so. At the same time, the business entities cannot hold on to the data if it is not necessary.
- The business entities should inform the authorities within 72 hours of detecting a breach in their data security.

If companies fail to comply with these conditions, the European regulators can impose fines up to an amount of 4% of their annual global sales. There is a ceiling on the penalty for smaller business entities at Euro 20 million.

CCPA

Similarly, the California Consumer Privacy Act (CCPA) protects the interests of the customers on the other side of the Atlantic Ocean. This Act provides California residents with the right to:

- Know about the data collected from them
- Know whether their data is disclosed to sold and to whom
- Deny permission to sell their personal information
- Have access to their personal data

Failure of the business entities to comply with the CCPA can result in sanctions and penalties. Companies that become victims of data theft have to pay statutory damages amounting to $100 to $750 per Californian resident. The fine for an unintentional and intentional violation is $2,500 and $7,500 respectively, for each violation.

It is crucial to understand how these third-parties are working and know their ability to modify their behavior remotely, or even install additional fourth-party (see our blog post about fourth-party code). How can the security or the privacy team in an organization know which type of data is collected, by whom, and how can they be alerted at earliest?

Visit our website:
www.reflectiz.com

British Airways Hack Example

For example, one of the most significant examples of the enforcement of GDPR is the fine of $230 million imposed on British Airways for a data breach in 2018. This breach resulted in the compromising of names, addresses, login info, credit card details, travel bookings, and other data of more than 500,000 customers. According to the British privacy watchdog, the ICO, the cause of the breach was the poor security deployed by the airline website that allowed hackers to steal such information. The breach in security permitted the hackers to direct more than half a million customers to a fraudulent page.

The enormous fine proved that the authorities are seriously monitoring the compliance to GDPR against various privacy breaches, and they do not hesitate to issue huge fines. The essential lesson in this case: a malicious JavaScript code (in this case modernizr-2.6.2.min.js script) was injected on the underlying party's website, but the penalty went straight to British Airways. Why? Because BA was unable to detect and report this incident. And once it did, it was too late.

Customer data theft

...as a matter of urgency, the theft of customer data between 22:58 BST August 21 2018 ...

With the introduction of GDPR to protect people's data, the enforcement authorities have become stringent; thereby, it resulted in the whopping fine of $230 million being imposed on British Airways. These data breaches do happen all around the world. The rules state that business organizations are accountable for any data breach caused by third-party services. The business organizations cannot wash their hands off by saying that a third-party vendor was responsible for the act. The business entities are responsible for the actions of the third-party vendors, as well. The example of British Airways is the ideal one where the airline company had to pay up for the fault of one of its service providers. Hence, it is the primary responsibility of the business organization to ensure screening of the third-party service providers to guarantee against any data breach.

Who are we?
We're a cyber-security company that helps organizations mitigate security and privacy risks resulting from third-party components installed in their websites

Visit our website:
www.reflectiz.com

How do you deal with third-party threats and risks?

The time-tested formula in risk management is to identify, assess, and mitigate third-party risks:

Identify the Risk: Taking measures that will allow you to identify potential risks is the first step towards protecting your business from third-party threats. Identification includes understanding who are the actors using your site. It also extends to identifying the location from where they are accessing it. It involves knowing what they are doing, as well. Create and manage inventory for them and conduct threat modeling.

Assess the Risk: Evaluating the risk is critical to understand the magnitude of damage it can cause to your data. Periodic assessment of the security aspects followed by your existing and erstwhile third-party service providers is vital. Perform penetration testing and dynamic code analysis by closely engaging with your third parties at all entry and exit levels, i.e., end-points. This assessment also helps you to understand the different types of risks and learn from the various sources of risks databases.

Mitigate the Risk: Mitigating the risk is the final part of the risk management exercise. Maintaining an inventory of all third-party assets is crucial. It is also imperative to review third-party service level agreements and non-disclosure agreements at periodic intervals. Regular security system audits can help in identifying, assessing, and mitigating such third-party risks. Reducing the risk levels entails employing higher levels of security such as firewalls and other security validation techniques to protect from any arising threats.

What's Next?

Third-party services and apps are integral for the functionality of your website, but it is crucial to ensure that you do not end up compromising your critical information systems and sensitive customer data. Reflectiz brings simple and zero-installation solutions to help companies and organizations mitigate privacy and security risks caused by third-party technologies installed on their websites.