

Web Client Runtime Security in Healthcare

Exploring Protection of Sensitive Healthcare
Data Using the Source Defense Platform



Table of Contents

Introduction..... 3

The Imperative of Web Client Runtime Security 3

Web Client Runtime Security in the Health Sector..... 4

Relevant Regulatory and Industry Compliance Mandates..... 4

Technical Considerations for Protection Against Unexpected Script Behavior 5

The Need for Behavior-Based Solutions Beyond CSP and SRI 6

Source Defense Protect WCRS Solution Overview 6

Supporting HIPAA Compliance with Source Defense Protect..... 10

Going Beyond Compliance with Risk Management..... 11

Disclaimer Notice..... 12

Glossary..... 13

Sources..... 14

Figures

Figure 1: Source Defense – Script Inventory..... 7

Figure 2: Source Defense – Findings Summary 8

Figure 3: Source Defense – Events with Highest Risk..... 9

Figure 4: Source Defense – Script Behavior View..... 11

Introduction

Web Client Runtime Security (WCRS) is the practice of securing code that executes in users' browsers during web interactions. This code, delivered by the website owner, may include proprietary scripts, third-party code from digital supply chain partners, and even further downstream code from additional sources. Unlike traditional server-side security measures, WCRS is focused on the client-side, addressing the challenges of safeguarding against unauthorized or malicious behavior in real time.

For an overview of WCRS and its importance across industries, read our introductory article in ISC2 Insights, "Web Client Runtime Security: A Growing Imperative."

WCRS has emerged as a critical concern in the **Health Sector** ("Sector") considering the increasing reliance by patients and third parties on web applications. As these applications become increasingly sophisticated as essential tools for patient interactions, data management, and service delivery, they also become prime targets for cyber threat actors aiming to steal sensitive health information.

This whitepaper explores WCRS in the Health Sector's context, including applicable industry and regulatory compliance obligations. Further, it includes details of how the solution offering from **Source Defense** can help monitor, control and manage the risks, as well as demonstrate ongoing risk and compliance posture.

The Imperative of Web Client Runtime Security

Web application security is not a new discipline in Cybersecurity. The fact that OWASP Top 10ⁱ, the premier web application security awareness project, is more than 20 years old shows that we have been focused on web application security long before many of the modern web application threats were known or anticipated.

For much of this time however, the security industry's focus has been primarily on the server side of web applications, and not on the client (browser) side at runtime. Traditional client-side vulnerabilities, like *Cross-Site Scripting (XSS)* and *Cross-Site Request Forgery (CSRF)*, while the exception, were often mitigated with server-side code changes. It is only in the recent years that the client-side runtime security has started gaining prominence, mostly starting with the well-known **eSkimming** attacks that impacted organizations such as British Airwaysⁱⁱ and Ticketmasterⁱⁱⁱ in 2018.

The nascent nature of WCRS is also evidenced by the fact that OWASP's own work^{iv} on this appears to have started only two years ago^v and is still an incubator project.

In the meanwhile, the Cyber threat actors have continued to exploit WCRS risks as evidenced by the recent Polyfill.io^{vi} incidents.

Web Client Runtime Security in the Health Sector

The term “Health Sector” includes a variety of industries that are in the business of providing or supporting providers of healthcare and wellness services.

This includes:

- Health Delivery Organizations (HDOs)
- Health Insurance Providers
- Laboratories
- Pharmacies
- Pharma/Biotech Organizations
- Medical Technology Providers
- and others.

The Sector relies increasingly on digital health mechanisms for its operations. Web applications are often a key component of the digital mechanisms used for customer/patient care services, internal operations as well as for interactions with third-party vendors or services. Given the nature of the industry and its operations, many of these applications often process sensitive data, including **Protected Health Information** (PHI), as defined, and regulated by the **Health Insurance Portability and Accountability Act** of 1996 (“HIPAA”) Privacy Rule^{vii} in the United States. Some of the applications may also play a critical role in ongoing patient care operations.

It is also well known that the Sector, especially the HIPAA regulated entities within the Sector, are frequent targets and victims of cyber threats. While most threat actors operate with financial motives, there have also been instances involving nation-state actors that operate with the motive of stealing sensitive personal data for potential use in adversarial operations against other nations. These threat actors are constantly on the lookout for vulnerabilities they can exploit for stealing data or causing other types of serious security incidents such as ransomware for financial motives.

The complexity of modern web applications, combined with the use of numerous third-party scripts, can create a significant footprint for such exploits.

There have been several instances of Health Sector websites causing impermissible disclosure or leaks of sensitive data. The recent breach of the US Healthcare conglomerate Kaiser Permanente^{viii} is a prime example of such breaches, but other healthcare organizations^{ix} have also been known to have had instances of impermissible disclosures of sensitive personal data with third parties resulting from either malicious compromise or simply unintended behavior of third-party scripts running in the browser.

Relevant Regulatory and Industry Compliance Mandates

Privacy regulations around the world are the primary regulations governing collection and use of personal data by organizations. Most privacy regulations also mandate special protections and safeguards for sensitive personal data such as patient health or wellness data processed by organizations in the Health Sector.

A few examples of such regulations include the HIPAA Privacy Rules in the United States and **General Data Protection Regulation** (GDPR) in the European Union. More recently, some states in the United States (Washington^x, Nevada^{xi} and Connecticut^{xii}) have implemented privacy regulations to enhance consumer protections for health and wellness data that is not covered by the HIPAA Privacy Rule.

Beyond these regulations, the US **Federal Trade Commission** (FTC) has the powers to carry out enforcements against organizations that violate their own terms regarding permissible use and disclosure of sensitive data that they process of their customers. The FTC has conducted several enforcements^{xiii} of this nature using section 5 of the FTC Act (15 USC 45) that prohibits “unfair or deceptive acts or practices”.

Technical Considerations for Protection Against Unexpected Script Behavior

WCRS involves protecting the code executed in users' browsers during web interactions. Unlike server-side security measures, runtime security addresses threats that occur on the client browsers are often visible only on the client side, such as surreptitiously altered scripts from 3rd party websites.

In order to understand the challenges posed by WCRS we must understand the distinction between 1st, 3rd and 4th party scripts. While **1st party scripts** are hosted and provided by the same website a user navigated to, **3rd party scripts** are hosted elsewhere, but referenced by the 1st party website or scripts to enhance its functionality and user experience. They can facilitate specialized functionalities like analytics, social media integration, and customer support, among others. By leveraging these external tools, website owners can enhance their site's capabilities without the need for extensive in-house development, saving both time and money.

Despite their benefits, 3rd party scripts also pose significant challenges. They can introduce security vulnerabilities and quite often access sensitive data which is governed by privacy mandates.

Some 3rd party scripts become obsolete and are no longer maintained by their original authors. Still others are actively maintained and frequently add new functionality, or dynamically load other scripts, from yet another provider, often referred to as **4th party scripts**. These might also undergo frequent updates, making it difficult for the first party application developers to keep track of the frequent changes and determine at runtime whether some of the 3rd and 4th party changes should not be trusted.

How could web application owners be expected to always know whether 3rd and 4th party maintainers are introducing new vulnerabilities or malicious behavior in real-time? And yet, when breaches and data leaks occur, the responsibility often lands squarely on the shoulders of 1st party web application maintainers.

The **Payment Card Industry Data Security Standard** (PCI DSS) and HIPAA compliance requirements lay out similar expectations. *Managing 3rd and 4th party scripts requires continuous monitoring to ensure they do not introduce security vulnerabilities, access sensitive data, or otherwise exhibit unusual behavior posing security or privacy risks.*

The Need for Behavior-Based Solutions Beyond CSP and SRI

Web browser capabilities intended to help address this problem, **Content Security Policies** (CSP) and **Sub-Resource Integrity** (SRI) HTTP headers, have been universally supported by modern browsers since 2013 and 2018 respectively^{xiv}. They can be thought of as metadata that web application operators can supply to client browsers, with more detailed instructions on how resources should be handled, including which scripts are allowed to run and ensuring that these scripts have not been tampered with. They are well suited for protecting certain 1st party scripts that do not change frequently.

Having said that, in our experience CSP and SRI are not as effective for monitoring 3rd and 4th party scripts, which can change frequently without warning and do not fall subject to the 1st party's change control processes. CSP and SRI rely on predefined rules and hashes, which can become outdated quickly as scripts are updated or modified. Keeping CSP and SRI configurations current requires significant manual effort and constant vigilance, which is often impractical for organizations that host or provide web applications to their customers or consumers. Moreover, failure to keep up with the changes can often lead to broken web application functionality as new, legitimate scripts and content gets blocked by outdated CSP and SRI policies on client browsers. CSP and SRI must therefore need to be supplemented with more dynamic and behavior-based security solutions for effective protection against modern web threats.



Source Defense Protect WCRS Solution Overview

To address these challenges, a new class of cybersecurity solutions has been gaining industry adoption. In the following sections we explore one such solution. Source Defense Protect offers health industry organizations a more comprehensive view into what scripts are executed by their web application clients and introduces a behavior-based approach to monitoring, management and security of 1st, 3rd and 4th party scripts used by web clients in near real-time. The system can learn the baseline behaviors of all scripts, monitor their access to sensitive data, apply rules to prevent access without impacting the performance of the website and block any malicious activity. Customers are also provided with an inventory of relevant scripts along with popularity and categorization, which are helpful in decision making when building web client security policies.

Script list ⓘ | ⌵

SCRIPT ⓘ		TYPE ⓘ	CATEGORY ⓘ	FIRST DETECTED ⓘ	LAST DETECTED ⓘ	POLICY ⓘ	STATUS ⓘ
 Zendesk Customer services and ... by Zendesk			Customer Support	3 months ago 28 APR 2024	16 hours ago 17 JUL 2024	Identified	Identified
 Google Global Site Tag (1) by Google			Analytics	3 months ago 28 APR 2024	16 hours ago 17 JUL 2024	Identified	Identified
 Hotjar (1) by Hotjar		 	Analytics	3 months ago 28 APR 2024	16 hours ago 17 JUL 2024	Identified	Identified
 AddThis - Widget (1) by AddThis			Social	3 months ago 28 APR 2024	16 hours ago 17 JUL 2024	Identified	Identified
 Google Tag Manager (1) by Google			Tag Management	3 months ago 28 APR 2024	16 hours ago 17 JUL 2024	Identified	Identified
 Freshdesk (1) by FreshWorks			Customer Success	3 months ago 28 APR 2024	16 hours ago 17 JUL 2024	Identified	Identified
 Tiktok Pixel (1) by ByteDance		 	Analytics	3 months ago 28 APR 2024	16 hours ago 17 JUL 2024	Identified	Identified
 Criteo (1) by Criteo			ad	3 months ago 28 APR 2024	16 hours ago 17 JUL 2024	Identified	Identified

Figure 1: Source Defense – Script Inventory

This view offers web application operators an opportunity to rationalize reliance upon 3rd party script libraries and potentially reduce the attack surface. Health industry organizations who process eCommerce credit card transactions may also choose to implement Source Defense Protect to help them meet new PCI DSS 4.0.1 requirements that become effective 3/31/2025. The Source Defense solution comes complete with an easy to use, “process by design” dashboard that makes meeting each of the PCI DSS requirements simple. This view allows them the opportunity to document business justifications for each script (a PCI DSS 4.0.1 requirement 6.4.3).

Additionally, by continuously tracking script behavior, Source Defense Protect supports the objective that only authorized scripts are executed, reducing the risk of eSkimming and inadvertent data leaks. Authorized users are presented with a dashboard view of observed script behaviors as well as a risk ranked list of events, which can be explored in greater detail.





Figure 2: Source Defense – Findings Summary

Script behavior, as well as changes in script behavior, are key to understanding the risk posed by certain 3rd and 4th party scripts. This functionality is also fundamental to building and enforcing a Source Defense Protect web client runtime script execution policy. Note that this policy is enforced by the Source Defense solution and is distinct from CSP and SRI policies discussed earlier. In situations where trusted 3rd party libraries are compromised and changed to behave in new, unexpected ways, these unexpected changes in behavior can either trigger an actionable alert or potentially stop a data breach from occurring in real-time with the aid of a script execution policy. Most organizations using Source Defense Protect enable this feature to **automatically thwart attacks without the need for an “alert/response” strategy.**

To start out, organizations using Source Defense Protect can review high risk events, as observed by the solution, and decide to alter the default script execution policy.



Events with highest risk

Severity	Script	Type	Detected event
H High	 Facebook Connect	4th+	• Data exposure sus. <u>+ 6 more events</u>
M Medium	 Taboola Tracker	3rd, 4th+	• Data exposure sus. <u>+ 6 more events</u>
M Medium	 Hotjar	3rd, 4th+	• PCI exposure sus. <u>+ 4 more events</u>
I Info	 Google Global Site Tag	4th+	• Uses 1st party cookies <u>+ 1 more event</u>
I Info	 LivePerson	3rd	• Uses 1st party cookies <u>+ 2 more events</u>
I Info	 Google Maps	3rd	• Data exposure sus. <u>+ 1 more event</u>
I Info	 Criteo	4th+	• Data exposure sus. <u>+ 2 more events</u>
I Info	 Tiktok Pixel	3rd, 4th+	• Uses browser storage <u>+ 1 more event</u>

+ 3 more events found

Figure 3: Source Defense – Events with Highest Risk

Source Defense Protect offers customers an opportunity to assign each script a separate execution policy. They are listed in order of the level of protection they provide:

- **Monitored** – Allow the script to run without interruption and monitor any other scripts that may be loaded by the monitored script.
- **Redacted** – Allow the script to run, but any keystrokes captured by the script will be redacted to prevent inadvertent data leaks. This is helpful when a script is not intended to capture user keystrokes, as this is a common tactic used by malicious scripts to steal sensitive data.
- **Isolated** – In addition to being redacted, isolated scripts are prevented from reading or writing to the Document Object Model (DOM), namely they would not be able to access any text areas, radio buttons, checkboxes, or other similar inputs on the page.
- **Blocked** – Block the script from interacting with the page.

It should be noted that by default Source Defense Protect will apply script policies based on recommendations of their staff members for known scripts unless the customer assigns a particular policy themselves. As such, customers who choose to keep the default policies of the Source Defense Protect solution may still receive the default protection from certain unwanted and unexpected script behaviors.

Supporting HIPAA Compliance with Source Defense Protect

On June 26, 2024, the **US Department of Health and Human Services' Office of Civil Rights** (OCR, the regulator for HIPAA Security and Privacy) issued a guidance bulletin^{xv}

“to highlight the obligations of [HIPAA Regulated Entities] under the [HIPAA Rules] when using online tracking technologies.” In the bulletin OCR stresses the point “Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules...” and continues to say “while it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, OCR is providing this reminder that it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.”

The OCR bulletin underscores the increasing challenges of preventing ePHI data leaks to online tracking solution providers and highlights the critical need for regulated entities to ensure that ePHI is disclosed only in strict accordance with the HIPAA Privacy Rule.

In order to comply with HIPAA regulations and the latest OCR guidance, leaders in health industry organizations should examine their internal cybersecurity and 3rd party risk practices, starting with whether they have an **accurate and timely** view of 3rd party relationships and what data is being shared with them in actuality. As part of that effort, 1st, 3rd, and 4th party scripts should be examined on web applications hosted or operated by their organization that may handle ePHI. Due to the complex and dynamic nature of some 3rd party scripts, staff with strong technical aptitude in the realm of web client runtime security should be performing this task. Alternatively, leveraging a purpose-built solution such as Source Defense Protect should be evaluated.

Source Defense Protect enables health industry organizations to support their HIPAA compliance programs by providing visibility to sensitive data sharing with 3rd parties by client web browsers, explaining the likely purpose for data sharing as well as notifying them when new unexpected data sharing behavior occurs. Perhaps more importantly, combined with proper governance and management practices, the solution could help reduce the impact of, or stop malicious script behavior and unintended data leaks to legitimate 3rd party providers, impacting the confidentiality of ePHI.

Source Defense Protect script inventory view enables health industry organizations to document justifications within the tool why each script is needed. While this activity is not mandated under current HIPAA regulations, unlike that of PCI, it is advisable to implement a governance program where such activity is performed, script behavior is reviewed, and for those scripts that are discovered to share ePHI health industry organizations should note whether an active Business Associate Agreement (BAA) is in place. This activity would support the existing 3rd party risk and HIPAA compliance processes on an ongoing basis. Additionally, it could be used as a compliance driver to reduce the number of 3rd party integrations on ePHI web applications, thereby reducing the attack surface and risk of inadvertent data leaks. To support this activity, drilling down into each script on Source Defense dashboard may provide insight into whether data exposure is occurring and what type of data is accessible by the script:

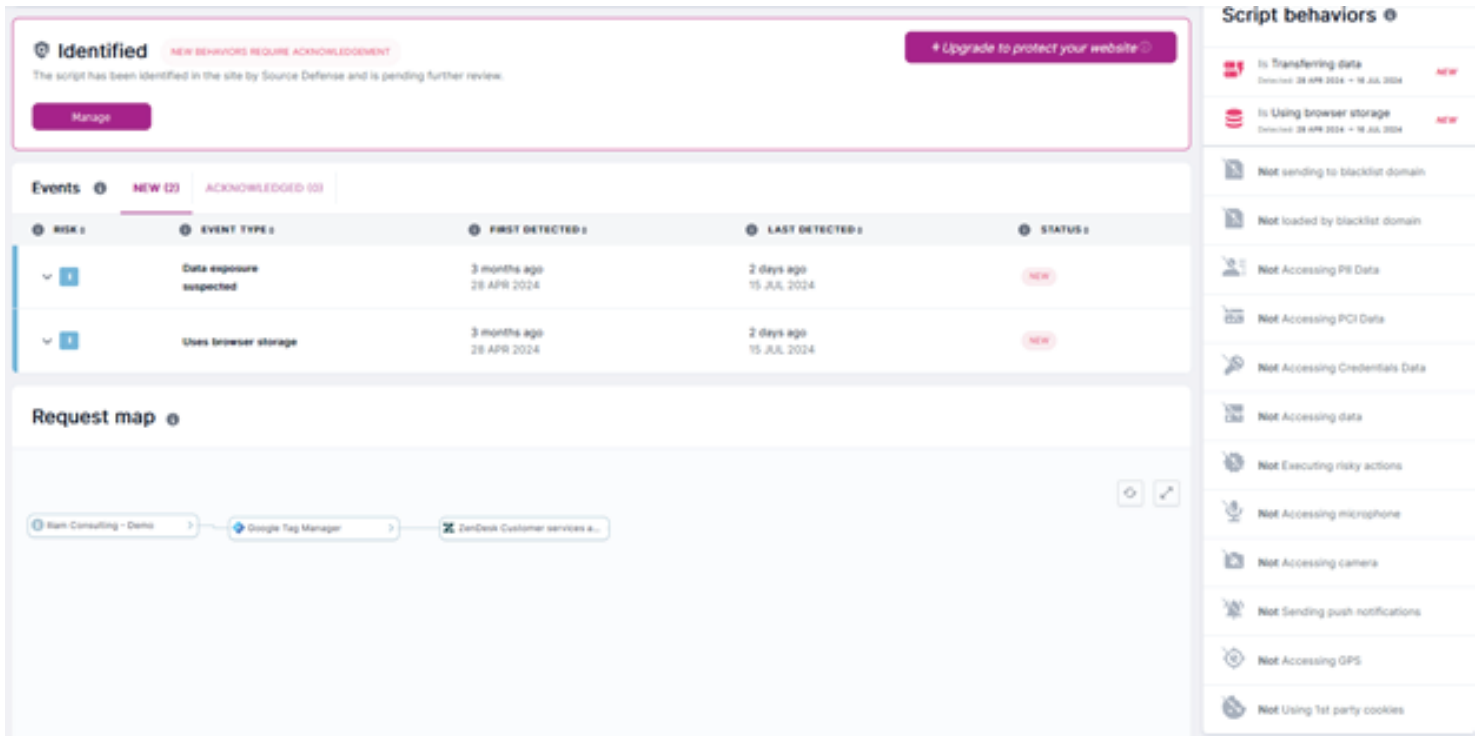


Figure 4: Source Defense – Script Behavior View

Further delving into the details of the OCR guidance, we add emphasis to a particular phrase *“Tracking technologies within user-authenticated webpages may even have access to an individual’s diagnosis and treatment information, prescription information, billing information, or other information within the portal. Therefore, **a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to only use and disclose PHI in compliance with the HIPAA Privacy Rule** and must ensure that the electronic protected health information (ePHI) collected through its website is protected and secured in accordance with the HIPAA Security Rule.”* With the use of Source Defense script execution policies, regulated entities may comply with the mandated technical control of limiting ePHI data disclosure to 3rd and 4th party scripts by implementing redacted, isolated, or blocked policies, as appropriate, when they do not impact functionality of the underlying 3rd party scripts.

Going Beyond Compliance with Risk Management

Privacy or security breaches in the Health Sector show that organizations face far larger financial or impact from class-action lawsuits, operational/revenue impact, and reputational harm than what they may face in terms of fines from regulators. It makes sense, therefore, that organizations design, implement, and operate their solutions with the objective of managing breach risks first.

Planning and implementing solutions with a mere compliance mindset is likely to ignore what really matters for avoiding data breaches and serious security incidents resulting from threats that evolve constantly and often with increasing sophistication depending on the threat actor and nature of vulnerabilities.

This is certainly true for WCRS risks as Health sector organizations cannot anticipate the nature of threats from 3rd party and 4th party scripts and therefore cannot implement proactive measures. Instead, they must rely on solutions such as Source defense Protect to implement and operationalize formal effective detection and response programs for managing WCRS risks.

Disclaimer Notice

This white paper has been issued by ILIAM Consulting and Tueoris with collaboration from Source Defense based on point in time industry analysis. While the information provided aims to support healthcare organizations in improving their web security and compliance with HIPAA mandates, it does not constitute legal or regulatory advice. Entities (including but not limited to healthcare providers, insurers, and service providers) must ensure they perform their own due diligence and seek professional guidance as needed to comply with HIPAA and other relevant regulations.

The technical review and recommendations contained herein are based on the analysis performed during a specific time period and under particular conditions. Therefore, the findings and opinions expressed may not apply universally or remain applicable in the event of changing technologies, threats, or regulatory updates.

ILIAM Consulting, Tueoris and Source Defense do not provide any warranty or guarantee regarding the effectiveness or infallibility of the Source Defense Protect solution in all circumstances. Users of this white paper should not rely solely on the information provided but should also implement comprehensive security measures and consult with their legal and compliance teams to ensure full regulatory compliance.

In no event shall ILIAM Consulting, Tueoris or Source Defense be liable to any party for any direct, indirect, incidental, or consequential damages arising out of the use or reliance on this white paper, including, but not limited to, damages resulting from the loss of data or profits, business interruption, or any other loss arising from the use of or inability to use the solutions and recommendations described herein.

Glossary

- **Content Security Policy (CSP)** – An added layer of security widely supported by modern browsers providing a standard method for website owners to declare approved origins of content that browsers are allowed to load on that website. By whitelisting trusted sources and blocking all others, CSP can prevent malicious content from being executed on a web page.
- **Cross-Site Request Forgery (CSRF)** – A type of security vulnerability that tricks a web browser into executing an unwanted action in an application to which a user is logged in. By exploiting the user's authenticated session, an attacker can perform unauthorized activities such as changing account details, conducting transactions, or accessing sensitive information, all without the user's consent.
- **Cross-Site Scripting (XSS)** – Another type of security vulnerability typically found in web applications that occurs when an attacker injects malicious scripts into content from otherwise trusted websites. These scripts can then be executed in the user's browser, leading to data theft, session hijacking, or other malicious activities. XSS attacks exploit the trust that users have in a particular website.
- **eSkimming** – also known as web skimming, is a type of cyberattack where attackers inject malicious code into a website, typically on payment pages, to steal payment card information and other sensitive data entered by users. This malicious code, often JavaScript, captures the data and sends it to the attackers. eSkimming can occur through vulnerabilities on the website itself or through compromised third-party scripts.
- **Sub-Resource Integrity (SRI)** – A security feature that enables web browsers to verify that resources fetched from third-party sources (such as scripts or stylesheets) have not been tampered with. It works by allowing developers to provide a cryptographic hash for the resource. When the browser fetches the resource, it computes its own hash and compares it with the provided hash. If the hashes do not match, the browser blocks the resource, preventing potentially malicious code from executing.
- **Web Client Runtime Security (WCRS)** – WCRS involves protecting the code executed in users' browsers during web interactions. Unlike server-side security measures, runtime security addresses threats that occur on the client browsers are often visible only on the client side, such as surreptitiously altered scripts from 3rd party websites.

Sources

- i OWASP Top 10 – <https://github.com/OWASP/Top10/raw/master/2021/Presentations/20th%20Anniversary%20-%20OWASP%20Top%2010%202021.pptx>
- ii `British Airways Breach – <https://techcrunch.com/2018/09/11/british-airways-breach-caused-by-credit-card-skimming-malware-researchers-say/>
- iii Ticketmaster Breach – <https://www.wired.com/story/ticketmaster-data-breach-monzo-inbenta/>
- iv OWASP Top 10 Client-Side Security Risks – <https://owasp.org/www-project-top-10-client-side-security-risks/>
- v Google Groups : OWASP Top 10 Client-Side Security Risks – <https://groups.google.com/a/owasp.org/g/top10-client-side-security-risks/c/kj-hFzGuxJg>
- vi Polyfill.io – <https://thehackernews.com/2024/07/polyfillio-attack-impacts-over-380000.html>
- vii HIPAA Privacy Rule and Protected Health Information – [https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#:~:text=Information%20is%20Protected-,Protected%20Health%20Information.,health%20information%20\(PHI\).%22](https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#:~:text=Information%20is%20Protected-,Protected%20Health%20Information.,health%20information%20(PHI).%22)
- viii Kaiser Permanente breach – <https://techcrunch.com/2024/04/25/kaiser-permanente-health-plan-millions-data-breach/>
- ix A Third of Top Hospitals' Websites Sent Patient Data to Facebook – <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>
- x Washington My Health My Data – <https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy>
- xi Nevada's S.B. 370 – <https://www.leg.state.nv.us/App/NELIS/REL/82nd2023/Bill/10323/Text>
- xii Connecticut CT SB-3 – <https://www.cga.ct.gov/2023/act/Pa/pdf/2023PA-00056-R00SB-00003-PA.PDF>
- xiii FTC Enforcements:
 - BetterHelp will be required to pay \$7.8 million for deceiving consumers after promising to keep sensitive personal data private - <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook>
 - GoodRx to pay a \$1.5 million civil penalty for failing to report its unauthorized disclosure of consumer health data - <https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising>
 - Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order - <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc>
- xiv Mozilla Sub-Resource Integrity – https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity
- xv Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates – <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>