feroot

The Ultimate Guide to

Client-Side Security

EXECUTIVE SUMMARY

In a world in which commerce, business, and information are driven almost exclusively by the internet, protecting both consumers and data is critical.

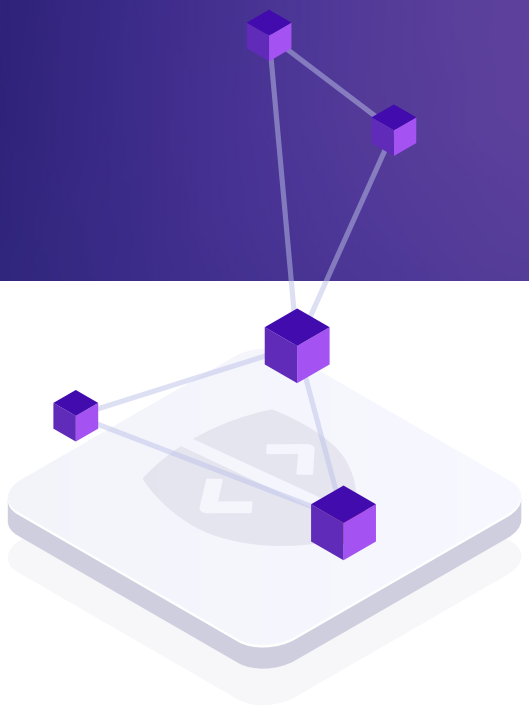
The Ultimate Guide to Client-side Security" provides organizations with a guide for understanding how modern websites and web applications work within the context of client-side interactions and the dangers inherent in the client-side coding structures that underpin website functionality. The content examines a wide range of concerns and issues, from the basic vulnerabilities and flaws that exist in commonly used code, such as JavaScript, to the types of threats and attacks that are increasingly targeting organizations that deliver goods and services to businesses and consumers via websites and applications.

Client-side threat detection and response is crucial to protecting businesses today, particularly as threats continue to advance and expand. While modern websites and the JavaScript code that powers them can offer businesses an opportunity for phenomenal growth, the applications and plugins used to drive the client-side also introduce tremendous risk by creating a demonstrable security gap during end-user engagement.

It is no longer enough to simply secure the perimeter and server side with tools like firewalls. Organizations must protect their front end or “client side” if they want to ensure growth and consumer safety.

To download the full 55-page e-book, please **click here.**

E-book Highlights



The Importance of Client-side Security

Consumers today expect a seamless and safe website experience, with minimal or no risk.

The client side is the entry point for all web interactions and must be made as secure as possible.

As companies expand investment in the end-user digital experience, client-side attacks have been increasing in both size and cost. This creates a unique opportunity for threat actors to take advantage of end-user activities.

Client-side security protects end users from incidents, vulnerabilities, and attacks that occur within an end user's browser or "front end."

The Dangers of JavaScript

While JavaScript is the most commonly used code for client-side web behavioral elements, it is also extremely vulnerable to attack, since it is easy for hackers and other threat actors to input query strings into forms to access, steal, or contaminate protected data.

JavaScript risk is further complicated by the fact that it does not have security permissions built into it.

Many websites are assembled using third- and fourth-party JavaScript code that is not vetted and may contain unintentional vulnerabilities or intentionally malicious code that can easily facilitate client-side attacks.

The Front End (Client Side) Must Be Protected

- The front end or “client side” drives the user experience—from graphics and colors to buttons, forms, and navigation menus.

  Front-end/client-side frameworks include:

  - Angular JS
  - React JS
  - Bootstrap
  - jQuery

- Front-end logic is becoming more prevalent in order to fully facilitate the end user’s digital journey.
- As front-end logic becomes more common, threat actors are targeting it to identify additional ways to maliciously engage with businesses and end users.

The Dangers of Third-party Scripts

- When building websites and web functionality, developers rarely write code from scratch. Instead, they leverage pre-written code pulled from open-source communities, such as GitHub.
- A modern web application contains, on average, over 20 third- and fourth-party scripts as part of the user experience.
- In addition to offering ready-made functionality, third- and fourth-party code also gives developers access to the creativity and ingenuity of other developers.
- Unfortunately, vulnerabilities and coding errors are common in third- and fourth-party scripts. Many flaws are unintentional, but present risk, nonetheless. Others are intentional and malicious, with threat actors often purposely creating vulnerable and dangerous code and then promoting it to unsuspecting developers.

Risks Related to Authentication, Authorization, and Tokenization

- Many processes, such as authentication, authorization, and tokenization that previously existed on the heavily protected server side, have moved to the less protected and more vulnerable client side.
- Broken access controls are one of the biggest risks to web applications today and currently reside in the number one spot in the OWASP Top 10.

Common Client-side Threats

The client-side threats targeting organizations today include:

- Cross-site Scripting
- DOM-based XSS
- Directory Traversal or Path Traversal
- E-skimming
- Magecart
- E-commerce Platform Skimming
- Drive-by Web Skimming
- Trusted Cloud-hosted Platform Skimming
- Anti-forensic, Self-cleaning, and Stealth Data Skimming
- JavaScript Injection
- SQL Injection
- XML Entity Injection
- Formjacking
- Side loading & Chain loading
- JavaScript Sniffing
- Broken Link Hijacking
- Server-side Request Forgery
- Cross-site Request Forgery

Industries at Risk

Industries at high and moderate risk for client-side attacks, particularly e-skimming, include:

- Financial Services and Banking
- Insurance
- Healthcare and Medical
- E-commerce and Retail
- Travel and Hospitality
- Communications, Social Media, and Content Producers
- Cryptocurrency Exchanges and Blockchain
- Real Estate
- Technology and Cybersecurity
- Distribution and Transportation
- Education
- Entertainment

Security Approaches for JavaScript and Client-side Attacks

- Cyber defense frameworks that can help defend and mitigate threats and attacks include Lockheed Martin's Cyber Kill Chain™.

Seven primary tools are used to secure the client side:

- Web application firewalls (WAFs)
- Content security policies (CSPs)
- Penetration testing and assessments (vulnerability and security)
- Client-side vulnerability scanning
- Code scramblers and obfuscators
- Client-side attack surface monitoring
- JavaScript security permissions

Each of these seven tools presents both benefits and downsides to the client-side security process. Unfortunately, a number of these tools are time consuming to manage and not particularly effective when it comes to providing comprehensive protection.

The two most beneficial, secure, and easy-to-manage, client-side security tools are client-side attack surface monitoring and JavaScript security permissions.

Threat Detection & Prevention on the Client-side

- To maximize detection and protection, organizations are encouraged to develop an inventory of web assets and document all scripts that operate on a website or within web applications.
- Organizations are also encouraged to review code and processes for vulnerabilities and misconfigurations, perform assessments on scripts and coded loaded into the browser, and regularly test web applications.
- Priority detection and prevention tips include the use of security control integrity monitoring and change detection automation systems, as well as the implementation of client-side intrusion detection solutions.
- Organizations are also encouraged to apply a layered security strategy or 'defense-in-depth' to websites and web applications.

The Importance of Collaboration

Cybersecurity professionals should work with all business teams, particularly application development, marketing, privacy and compliance, and product security (as applicable) to:

- Build strong relationships.
- Understand current or emerging privacy trends or regulations and apply them within a cybersecurity context.
- Promote a secure business mission, remove friction in the customer journey, and facilitate success for the business.
- Develop a strong security architecture.

Recovering from a Client-side Attack

If a breach happens, organizations are advised to:

- Calmly and logically assess the threat/attack.
- Contain the breach.
- Investigate the situation.
- Shut down/block any malware, malicious scripts, or backdoors.
- Identify the point of origin for the attack.
- Engage fully in the recovery process.

To prepare for future attacks, organizations should:

- Learn as much as they can about the types of threats and the attack environment.
- Scan for and identify vulnerabilities.
- Regularly test defenses.

To download the full e-book, please click here.