THE THREAT OF
JAVASCRIPT SKIMMING

How Malicious Actors are Using Client Side Code to Steal Sensitive Data
CONTENTS

Introduction to JavaScript Skimming 3
The Issue with JavaScript 5
How Can You Prevent JavaScript Skimming? 6
About SecurityMetrics 7
INTRODUCTION TO JAVASCRIPT SKIMMING

Over the years, the payment card industry has focused on securing point of sale (card present) transactions. The addition of EMV and P2PE has improved the security of card present transactions. Software installed on payment terminals has to meet compliance standards and be audited for security.

E-commerce transactions are completely different. Page analytics, marketing automation, digital advertising applications, and other programs and software give merchants fantastic amounts of business intelligence. However, this data collection wouldn’t be tolerated in a point of sale environment without many kinds of compensating controls locking down where and how those communications are happening, yet they are all allowed in an e-commerce environment. This has led to numerous skimmers that exploit the trust relationship between the application and third party, such as malicious ads served by a trusted ad network. And with the improvements in security to card present transactions, more and more attackers are turning to e-commerce and other digital ways to steal sensitive information.

As web sites become more sophisticated web developers are forced to move away from traditional server-side processing architecture to client-side JavaScript architecture. The benefits of JavaScript architectures are numerous, but one of the serious downsides is the ease of adding JavaScript libraries to compromises a website.

In the past developers programmed their own source code. However, with so many readily available and free JavaScript libraries we are seeing a shift where web developers are using open source libraries that are often not checked for proper security protocols.
New Content Delivery Networks (CDN) are now readily available that provide free JavaScript libraries hosted on other third-party websites. These JavaScript libraries are easy to use, but businesses must rely on CDN provider’s security. If CDN JavaScript libraries are compromised, then all websites using those libraries may also be compromised.

Web developers can create engaging websites faster if they use shopping cart software. However, shopping cart software has many thousands of lines of intricate code, which allows JavaScript compromises to be hidden safely from traditional security tools like vulnerability assessment scans, file integrity monitors, and web application firewalls.

The massive success behind JavaScript skimming attacks lies in their ability to hide in plain sight in static environments.

Traditional tools used to catch the exfiltration of sensitive information out of the network can not detect such requests that occur in the context of the client’s browser. This is the function of SecurityMetrics’ Shopping Car Monitor, it detects all requests that are made from the browser and alerts on any that were not expected.
THE ISSUE WITH JAVASCRIPT LIBRARIES

JavaScript libraries (e.g., node.js, angular.js) were created to control the flow of the website and make developing a website easier for the programmer. But they may introduce problems like single page web applications, where customers think they’re visiting dozens or even hundreds of different pages when, in reality, the code is all the same and the JavaScript just delivers the relevant information to them. Essentially, this makes the homepage the same code as their checkout page. SecurityMetrics forensic analysts have seen hackers taking advantage of these situations over and over again.

Aaron Willis, Principal Security Analyst at SecurityMetrics, found a case where the Apache caching module allowed attackers to upload malicious images that had php code in them. This allowed the attacker to add code to the website via the image upload. It’s easy to look at an image upload component and not see anything dangerous. It’s just an image after all. But utilizing the vulnerability, the attackers were able to upload full pages of code and take complete control of the website.

We’ve also seen cases where companies have a single page website and they add a WordPress blog. That blog is a plugin that now has direct access to the cart page because of the configuration of the website. If websites are not architected and configured for security, it is likely that vulnerabilities exist to give hackers access to the shopping cart environment.

From our experience helping e-Commerce website owners, third party plugins can introduce serious security issues. These plug-ins are as equally dangerous as the JavaScript libraries. Programmers often don’t realize the security complexities of interconnected website components.

JavaScript has evolved so much that programmers have become overwhelmed trying to keep up with the newest methods of using the development language. This leads them to take shortcuts and not fully vet their implementations or not perform proper security tests on their applications and websites. Any data, even trusted data input from internal sources should be reviewed, sanitized and treated as if it could have malware.
HOW CAN YOU PREVENT JAVASCRIPT SKIMMING?

If you hire a security consultant, they’ll check your static code on your server, but they won’t check the browser experience of the site. Malware, antivirus, and vulnerability scanners typically just check the main page of a site. They’ll find the malware if it’s installed on the homepage, not if it manifests pages into a session. These more recent attacks target that very scenario.

For example, the malware is only installed on a checkout page and is only visible or only fires when a CVV field has been modified. Meaning, the malware is invisible to any kind of check (e.g., vulnerability scan, anti-virus) except a check that is actually mocking a real life purchase. The attackers want their malware to lay dormant and hide until they know credit card information is present.

These attacks may be triggered when a person puts in their credit card details, and if you don’t run your solution right at that exact moment, you may never see the malware. You might never see that any information was stolen.

SecurityMetrics WIM technology helps prevent these skimming attacks by running right at that precise moment—and checking what scripts are present at that time.
ABOUT SECURITYMETRICS

We help customers close data security and compliance gaps to avoid data breaches. We provide managed data security services and are certified to help you achieve the highest data security and compliance standards.

We are a PCI certified Approved Scanning Vendor (ASV), Qualified Security Assessor (QSA), Certified Forensic Investigator (PFI), and Managed Security provider with 20 years of data security experience.

From local shops to some of the world’s largest brands, we help all businesses achieve data security through managed services, compliance mandates (PCI, HIPAA, GDPR), and security assessments (HITRUST consulting and assessments). We have tested over 1 million systems for data security and compliance. We are privately held and are headquartered in Orem, Utah, where we maintain a Security Operations Center (SOC) and 24/7 multilingual technical support.
LEARN HOW SECURITYMETRICS’ WIM TECHNOLOGY CAN PROTECT YOU FROM JAVASCRIPT SKIMMING

Learn More