



E-Commerce Website Security Audit

Sample Report

Copyright @ 2021

Overview

This report provides an **overview of the main security threats** to your E-commerce website. It focuses specifically on threats to the **client-side** (i.e., everything that takes place on the browser or end-user device).

Client-side threats are especially important to E-commerce businesses because **cyber attackers are actively targeting client-side security weaknesses**. These weaknesses are **not** fixed by commonly used security layers such as Web Application Firewalls.

A prime example of one of these threats is **Magecart** web skimming attacks, which covertly leak credit card data whenever a client makes a purchase on your website, often remaining undetected for months. The Magecart attack on British Airways, for example, **leaked over 400,000 credit cards** and resulted in a **\$30 million GDPR fine**.

The  Register®

{* SECURITY *}

British Airways fined £20m for Magecart hack that exposed 400k folks' credit card details to crooks

Fri 16 Oct 2020 // 12:15 UTC

This report is divided into two sections. The first one provides an **overview** of the key security threats and the second one provides **technical details** of the analysis of the main security threats to your E-commerce website.

Key Security Threats

Customer Hijacking

A significant portion of your website's users are not having a seamless experience due to security problems. Your **third-party services** might be serving **malicious code** and [leading your visitors to malware](#). This completely **disturbs the user experience** and **compromises your brand's reputation**. Your users may also be using price comparison tools and browser extensions that **display pop-ups** and redirect them to competitor websites.

Assets

468 Total assets being loaded in your web app.

211 Assets that come from 3rd-parties.

80 Total domains loading assets in your web app.

Associated risk:

Are you aware and in control of all these assets? What is the risk of a compromised 3rd party script affecting your Web Application and customers?

Session Hijacking

5% Average user sessions affected by hijacking.

\$10M Estimated average annual revenue lost to hijacking.

Associated risk:

Are you aware of how much revenue you're losing to hijacking every year?

Your Customer Hijacking Risk: **High**

Data Leakage

The average website today runs 35 different third-party components. Each of these can be compromised and **breach your website without your awareness**. These leaks stay active for weeks or even months before being detected, resulting in massive data breaches.

Below, you will find an overview of key metrics and, on the following pages of this report, we present a detailed technical breakdown of these findings.

Domains

97 Total domains receiving data from your web app.

98% Percentage of these domains that are 3rd-party.

Associated risk:

Are you aware of all these destinations, and monitoring for new unexpected destinations?

Poisoning Events

4 Poisoning events detected on forms.

8 Poisoning events detected on network events.

Associated risk:

Form poisoning allows untrusted code to collect data from your forms. Network poisoning allows untrusted code to intercept data.



Your Data Leakage Risk: High

Report

During this session, our Embedded Agent (EA) collected insights about the session and delivered reports to a backend of ours in the form of Occurrences. These single JSON objects contain detailed information about the activity such as:

- **DOM Tamperings**
- **Code / Native API Poisoning**
- **Network Requests**
- **Inventory with Classification**

On the full report, you can expect high-level tables such as the one below:

Type	Total
Critical - XMLHttpRequest Send	8 
Critical - Form Submit	3 
Other click events	466
Critical - button click	70
Other keyboard/mouse events	9

Plus, it will contain several other tables and graphs with detailed information on specific detections such as **code/native API poisoning**, **source domains**, **destination domains**, **resources/scripts**, **breakdown of scripts** into first and third party, and a **digested overview of the critical issues**.

Inventory

With our Inventory feature, you get an overview of **every resource and network asset** that has been loaded or performs changes on the web page. The table below displays how many third-party assets are being loaded, broken down by domain:

Resource	Count
s.w.org	2
res.cloudinary.com	3
cdn.segment.com	1
cc.swifttype.com	1
ads.avct.cloud	1
s7.addthis.com	2
cdn.cookie law.org	6
cdn.ampproject.org	4
static.intercomassets.com	1
js.intercomcdn.com	2
intercom.io	3
gstatic.com	2
googleoptimize.com	1
doubleclick.net	2
www.google.com	1
www.googletagmanager.com	1

The table below displays a sample shortlist of the inventory:

Resource	Third-Party	Domain
s.w.org/images/example.svg	YES	s.w.org
res.cloudinary.com/js/example.js	YES	res.cloudinary.com
cdn.segment.com/js/example.js	YES	cdn.segment.com
cc.swifttype.com/js/example.js	YES	cc.swifttype.com
ads.avct.cloud/js/example.js	YES	ads.avct.cloud
s7.addthis.com/js/example.js	YES	s7.addthis.com
cdn.cookielaw.org/js/example.js	YES	cdn.cookielaw.org
cdn.ampproject.org/js/example.js	YES	cdn.ampproject.org
static.intercomassets.com/js/example.js	YES	static.intercomassets.com
js.intercomcdn.com/js/example.js	YES	js.intercomcdn.com
intercom.io/js/example.js	YES	intercom.io
gstatic.com/js/example.js	YES	gstatic.com
googleoptimize.com/js/example.js	YES	googleoptimize.com
doubleclick.net/js/example.js	YES	doubleclick.net
www.google.com/js/example.js	YES	www.google.com
www.googletagmanager.com/js/example.js	YES	www.googletagmanager.com
your-website.com/content/js/script.js	NO	your-website.com
static.your-website.com/shared/example1.js	NO	static.your-website.com
assets.your-website.com/shared/example2.js	NO	assets.your-website.com
assets.your-website.com/shared/example3.js	NO	assets.your-website.com

You can clearly see multiple assets loaded from third-party domains that were present in the session. We also map out all Resource Assets that correspond to the Domains or URIs responsible for generating events that triggered a detection by WPI's monitoring, such as **DOM mutations** (e.g. adding a script to a page or modifying an attribute in a form) and **poisoning** of native browser functions (e.g. modifying the function of an onSubmit event).

Contact Us

If you want to know more about how Jscrambler can help you protect your E-commerce platform, don't hesitate to contact us.

hello@jscrambler.com

+1 650 999 0010

The Gartner logo, consisting of the word "Gartner" in a bold, blue, sans-serif font, with a registered trademark symbol (®) to the right.

Jscrambler is the leader in Client-Side Application Security

Recognized in **Gartner's Market Guide for Online Fraud Detection**

And in **Gartner's Market Guide for In-App Protection**