Website Risk Assessment

Understand the risk to your website from Shadow Code vulnerabilities, including digital skimming/Magecart attacks, PII harvesting, watering hole attacks and open source vulnerabilities.

Prepared for	**Wine Co**
Website URL	**https://wines.pxcdshop.com/checkout.html**
Date Analyzed	**October 5, 2020**

Overview

Total number of Scripts Found	First-party Scripts	Third-party Scripts
32	6	26

81% of your website scripts are third-party.

70% of the scripts on a typical website are third-party.

Third-party scripts introduce unknown risks into your web applications. These scripts are loaded directly from the third-party CDN to your user's browser and do not pass through your web application firewalls. Hackers often target commonly used third-party scripts to inject malicious Shadow Code into your website. This code can skim personal information from your site including passwords and credit card numbers, or modify your page to send users to fake checkout sites, resulting in client-side data breaches and Magecart attacks

Website Security Controls

SSL/TLS Encryption	Yes
Content Security Policy	No
X-Frame-Options	Same Origin
Strict-Transport-Security	No

Controls such as Content Security Policy (CSP) are often used to prevent cross-site scripting attacks on websites. While an effective tool in some cases, they need to be frequently updated as third-party scripts are added or removed from your site. Code injection attacks can take place even with a CSP in place through one of the trusted domains. Continuous monitoring of client-side scripts will alert you to such attacks which can then be mitigated by modifying the CSP rules.

Open Source Vulnerabilities Found

jQuery 3.4.1 - outdated

Open source libraries are commonly used in most modern web applications. While they enable development teams to innovate and deploy code faster, they can introduce unknown Shadow Code vulnerabilities into your web application. These vulnerabilities can be exploited by hackers to inject malicious scripts that skim sensitive personal data from your websites, including passwords and credit card numbers. While software composition analysis can help you identify vulnerable libraries during the deploy phase, continuous client-side monitoring will detect and stop attempts to exploit these vulnerabilities.

Third Party Scripts Found on Your Website

https://www.domain.com/ws/r2/

https://www.googleadservices.com/pagead/conversion_async.js

https://d.impactradius-event.com/A74466-7450-478e-9797-c9d4ea25869d1.js

https://assets.adobedtm.com/launch-ENf18281e271074772b32cb3388047efe9.min.js

https://www.domain.com/ruxitagentjs_ICA27SVfghjqrux_10181191119154660.js

ttps://bkstr.scene7.com/s7viewers/html5/js/MixedMediaViewer.js

https://edge1.certona.net/cd/929deaf8/www.bkstr.com/scripts/resonance.js

https://ajax.googleapis.com/ajax/libs/jquery/1.4.2/jquery.min.js

https://request.eprotect.vantivcnp.com/eProtect/js/eProtect-iframe-client3.min.js

https://www.domain.com/0.9d619562295ceaeb4b73.chunk.js

https://www.domain.com/9.e513e4f904d3ace5ca90.chunk.js

https://assets.adobedtm.com/4083eeeaedf7/b1c7c9cd4e3b/d8addece3ed3/EX6d4765cee8d946ba84f6c5670e4b0503-libraryCode_source.min.js

https://www.google-analytics.com/analytics.js

https://www.googletagmanager.com/gtag/js?id=AW-1035649345

https://googleads.g.doubleclick.net/pagead/viewthroughconversion/1035649345/

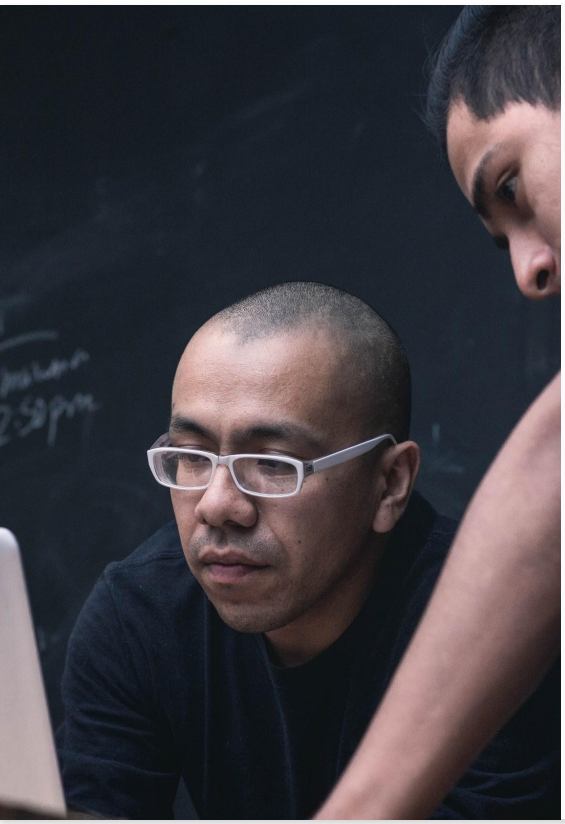
https://googleads.g.doubleclick.net/pagead/viewthroughconversion/973763668/

https://assets.adobedtm.com/4083eeeaedf7/b1c7c9cd4e3b/d8addece3ed3/RC2c92d9899f54484f9843e07b578f87cb-source.min.js

https://assets.adobedtm.com/4083eeeaedf7/b1c7c9cd4e3b/d8addece3ed3/RC30425ac0b3844805a0ff4d0b85933c17-source.min.js

https://assets.adobedtm.com/4083eeeaedf7/b1c7c9cd4e3b/d8addece3ed3/RCd120051abe174c46814cd6c7cd7c08c2-source.min.js

https://assets.adobedtm.com/4083eeeaedf7/b1c7c9cd4e3b/d8addece3ed3/RC3ed2c914024a4b05a2b0e101df615d33-



Get a Detailed Risk Analysis of Your Website

PerimeterX Code Defender is a client-side application security solution that continuously protects your website from digital skimming, formjacking and Magecart attacks, stopping data breaches and reducing your risk of non-compliance. Using a lightweight JavaScript Sensor, Code Defender can continuously analyze your website for third-party risk, open source vulnerabilities, PII access and data exfiltration attempts. Get a detailed analysis of your website with our complimentary 15 day trial.

Request a Free Trial

About PerimeterX

PerimeterX is the leading provider of application security solutions that keep your business safe in the digital world. Delivered as a service, the company's Bot Defender, Code Defender, and Page Defender solutions detect risks to your web applications and proactively manage them, freeing you to focus on growth and innovation. The world's largest and most reputable websites and mobile applications count on PerimeterX to safeguard their consumers' digital experience. PerimeterX is headquartered in San Mateo, California and at www.perimeterx.com.

perimeterx

www.perimeterx.com