



Adobe Commerce Site Audit

August 15, 2023

Prepared By

Ryan Hoerr
Adobe Commerce Software Architect
ParadoxLabs, Inc.

Overview

_____ has contracted ParadoxLabs to audit its ecommerce web presence at _____. To that end, ParadoxLabs has performed a comprehensive site audit to evaluate the website's current status, identify problems and risks, and provide recommendations.

This audit will encompass security, performance, health, best practices, and other factors relevant to a smoothly-running Adobe Commerce website and _____.

Security

Software

Your website is running Adobe Commerce (On-premise), version 2.4.5. That's a fairly recent version, but is missing multiple security patches. The latest Adobe Commerce version is 2.4.6. Urgent attention should be given to upgrading Adobe Commerce to 2.4.5-p4, and then to 2.4.6-p2 upon further validation of compatibility of the 2.4.6 version with the site themes, extensions, and custom code.

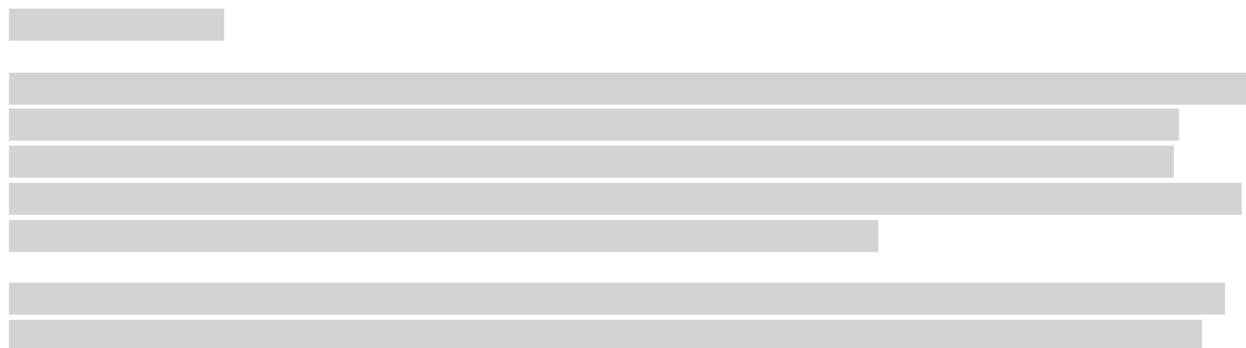
Your server is running PHP version 8.1, which is the current recommended version for Adobe Commerce. Typically upgrading sites to PHP 8.1 from older versions is a major undertaking due to language changes, so it is encouraging to see the site is running smoothly with it already. That being said, during the course of code analysis we found that a previous development partner shortcut this process by suppressing all error messages that normally come from PHP 8.1, without necessarily fixing the underlying errors. We can continue with this error suppression for the time being, but in the near future it will be necessary to perform the code maintenance and cleanup to ensure your site is actually in alignment with PHP 8.1+, and then remove that error suppression. This can be done after urgent site fixes are resolved.

You have regular site malware scanning in place via Sansec eComscan, including immediate alerts to your staff and development partners upon any issues being found. This is very good for detection of vulnerabilities and of any hacks that might occur.

You also have all your ecommerce domains running behind Cloudflare (which includes CDN and WAF services). That helps block attacks and suspicious traffic before they even reach your web servers.

Admin Panel

Your admin panel does not appear to have any particular protections in place. This is problematic as the admin panel is the single greatest source of Adobe Commerce hacks and vulnerabilities.



Hosting

Take care when authorizing third parties to access your servers, especially production, as each one is an additional point of vulnerability.

Codebase

There are no maliciously modified core files, no known vulnerable modules, no publicly-accessible backups, and no other apparent indicators of the site being compromised.

One file in the site's custom modules should be examined in detail to ensure it is not a security risk by use of PHP's unserialize function:

Configuration

Your credit card payment methods are

That means your frontend checkout is compliant to PCI DSS level SAQ A, but your admin checkout is only compliant to

PCI DSS level SAQ D and is considered fully in scope for PCI compliance. The admin CC payment form is an area for possible improvement, especially if your staff or affiliates enter a lot of admin orders.

Summary

Your security situation is in good shape overall. With an upgrade and small adjustments, you should be in very good standing against typical Adobe Commerce attacks.

Quality

General Comments

The bad news is your codebase is not in great shape. There are numerous indicators of your site being maintained in a fairly questionable manner over the years, including untracked modifications to core and vendor module files; clutter from duplicated file backups; use of ObjectManager; and substantial code performance problems.

We also discovered in the course of onboarding and audit that your site was connected to the Adobe Commerce Marketplace account of a seemingly unrelated merchant. That broke all package management and ability to update your site until the problem was identified and resolved.

The good news is that every one of these problems can be fixed with care and good development practices.

Codebase



Government	Percentage
Current government	55%
Previous government	45%

Government	Percentage
Current government	85%
Previous government	15%

[illegible]



Code Issue of Note: PHP 8.1 compatibility

One of the modified core files is related to PHP 8.1 compatibility, as mentioned in the security review. A previous developer achieved PHP 8.1 compatibility for the site by suppressing all PHP 8.1 deprecation and type conflict errors. That's a cheap solution to the problem, but not a sustainable one.

./app/bootstrap.php:

```
//error_reporting(E_ALL);  
error_reporting(E_ALL & ~E_DEPRECATED & ~E_STRICT);
```

Code Issue of Note: Composer installation

The current composer configuration fails to install due to a dependency conflict:

```
$ composer2 install  
Installing dependencies from lock file (including require-dev)  
Verifying lock file contents can be installed on current platform.  
Your lock file does not contain a compatible set of packages. Please run composer update.
```

Problem 1

Code Issue of Note:

Code Issue of Note:

Modules

Logs

There are many exceptions being logged in system.log that should be evaluated and fixed where possible. This includes instances of:

Configuration

All caches are enabled, and settings look generally good. Your site uses [redacted] to optimize caching of public pages (FPC) and static files, with [redacted] on top.

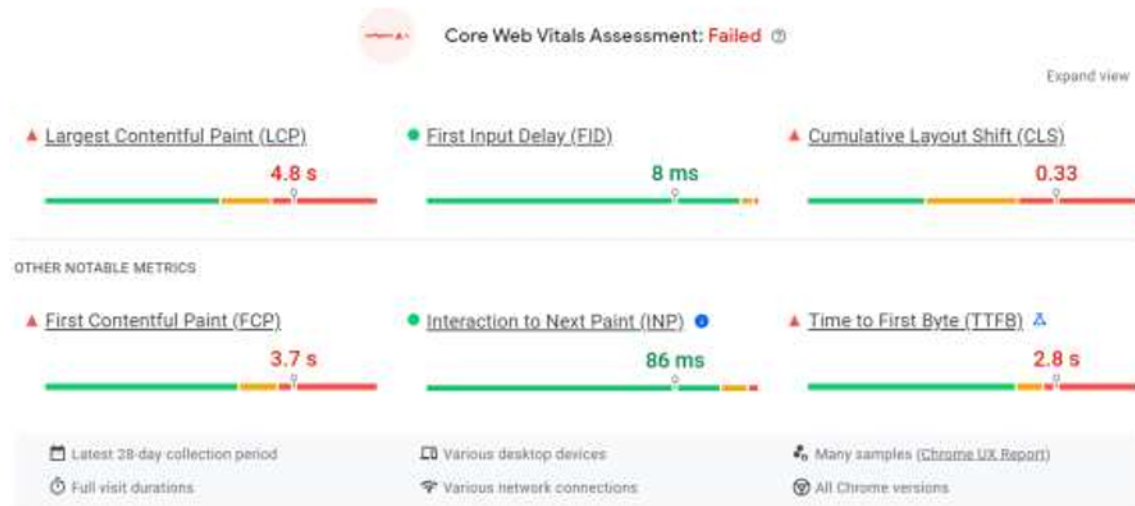
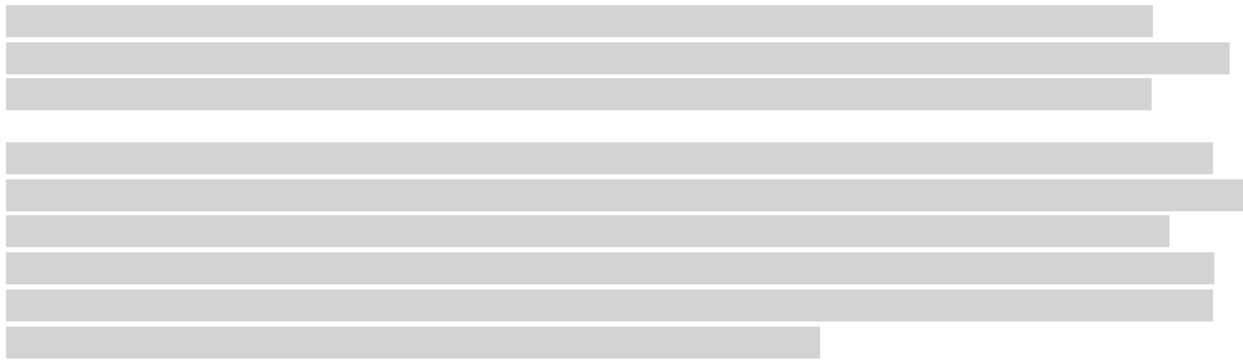
During evaluation, we observed some admin page loads would redirect to the dashboard abruptly. This may indicate an issue with [redacted]

The admin order and product grids are very slow to load in data. [redacted]

Performance

Metrics



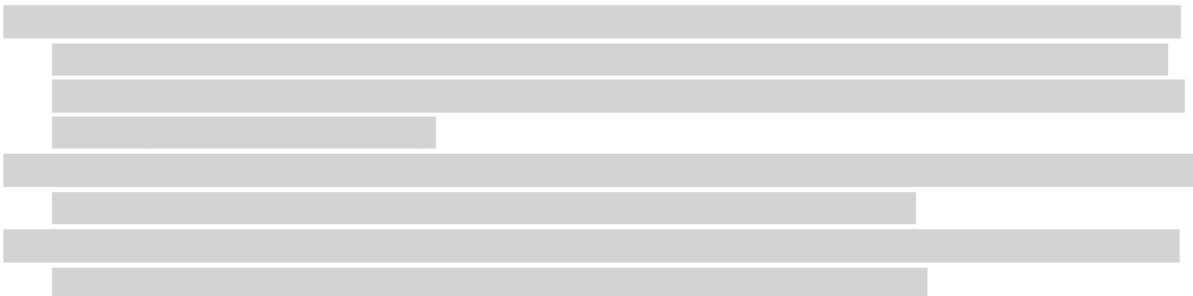


Once the server response times are improved, reducing the layout shift should be the next priority. This means ensuring elements on each page move as little as possible while the page loads in. The biggest culprits of this are usually account buttons, banner messages, and sliders.

Reviewing New Relic performance metrics, your overall average response time (including all uncached request types and AJAX) is 1550 ms. Your average total load time is 6.6 seconds. Both of these are much too high. Product pages are graciously covered by FPC and so this time is only a factor for the first load of each product, but still a product's uncached response time is in the area of 4.6 to 5.2 seconds.

Category pages appear to be entirely uncovered by FPC, and show a response time consistently around 4 seconds.

Doing a deep performance audit of several page types from New Relic data showed the following issues:



[Redacted content]

Configuration

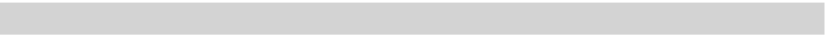
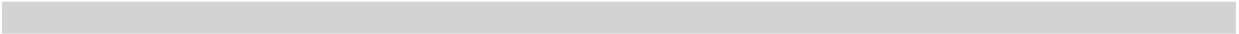
[Redacted content]

Monitoring

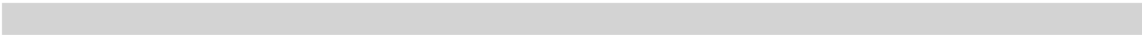
[Redacted content]

Whatever the situation, there are clear opportunities for improvement we have identified, and we will help you to resolve them and get your site performing to a point you're happy with.

Frontend

Your site theme is custom built on 


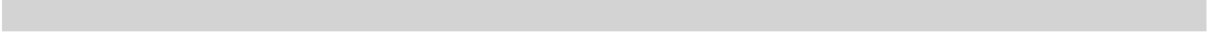
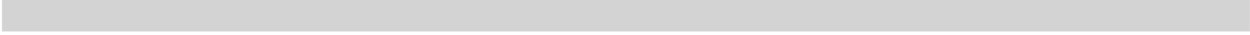










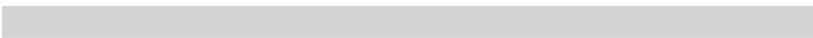


Looking Forward









With regards,

The team at ParadoxLabs

