Adobe® Magento Commerce Security Best Practices Guide

Table of Contents

Overview

This guide details several features and techniques designed to help protect your installation of Adobe® Magento Commerce from security incidents. Although there is no single way to eliminate all security risks, there are many steps you can take to harden your installation and make it a less attractive target for bad actors.

Anyone responsible for a Adobe® Magento Commerce installation and/or developing applications for the Magento Commerce solution should read this guide in its entirety in order to understand how to establish and maintain a secure environment. This guide is also relevant for customers using Adobe Commerce Cloud, which contains Magento Commerce plus other Adobe Experience Cloud services, including Adobe Experience Manager.

Please note: The recommendations and procedures in this guide only apply to Adobe® Magento Commerce version 2.3.x and later. It is always important to use the latest version to ensure that your site is protected with the most up-to-date security features and security patches.

Shared Responsibility Model

Adobe® Magento Commerce relies on a shared responsibility model, which places certain security responsibilities on the customer and others on Adobe. The basic division of responsibilities is included here.

Customer

The customer is responsible for the security of their Magento Commerce environment, including:

- Ensuring a secure configuration and coding of the application
- Applying Adobe-released patches immediately upon release
- Implementing security monitoring best practices, including penetration testing and vulnerability scans, as well as any activities required to achieve compliance with any security standards as may be relevant in the context of the customer's business
- Managing and monitoring any and all access to customer information, including:
  - Issuance of login credentials to access customer assets and web properties
  - The system and related accounts like the magento.com account, marketplace account (if different, or cloud accounts
  - Any other accounts that might be used to compromise the application

The customer may perform these activities in-house or enlist the services of an Adobe solution integrator partner.

The customer is responsible for the PCI-DSS compliance of the customized application and their internal processes. In particular, the customer is responsible for configuring and using Magento Commerce in a manner that complies with the customer's PCI-DSS obligations.

Adobe

Adobe is responsible for the following as part of Magento Commerce deployments:

- Server-level patching
- Operating the necessary services to deliver Magento Commerce
- Vulnerability testing of the out-of-the-box application
- Operational and performance monitoring
- Incident response (more information on Adobe's incident response process available here)
- Ongoing technical support
- Ensuring that the customer infrastructure is available in accordance with SLA
- Managing server firewall configurations and perimeter firewall configurations (security groups)
- Maintaining PCI certification as a merchant service provider for the Adobe infrastructure

Adobe also follows industry best practices for security and compliance in its ongoing application development, operations, and response to security incidents affecting our infrastructure.

Adobe® Magento Commerce Architecture

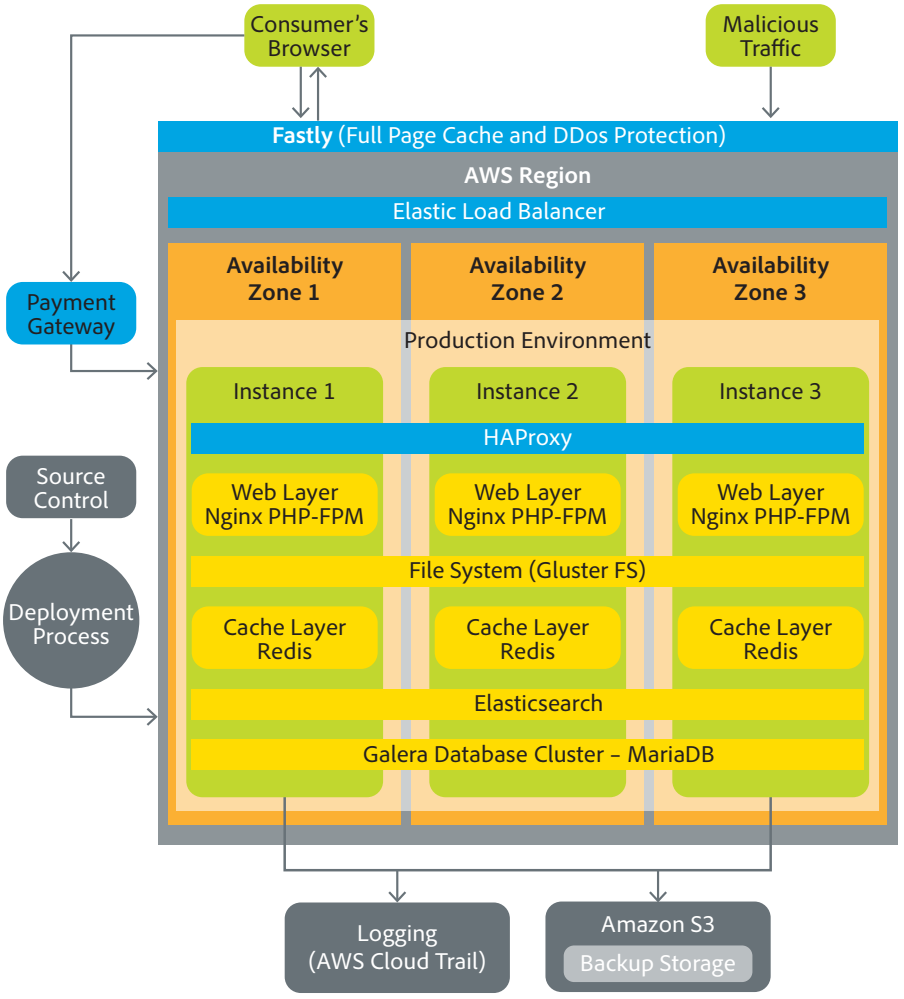

Figure 1: Adobe® Magento Commerce solution architecture

Magento Commerce Data Flow

Adobe relies on content delivery networks (CDNs), such as Fastly, to optimize content flow between users and the Magento Commerce environment. All user traffic should be secured using HTTPS, either using a shared SSL certification included with the Magento Commerce solution (and hosted on the Fastly CDN) or the customer's own SSL certificate. If the customer chooses the latter option, acquisition and management of this certificate to support HTTPS traffic is the customer's responsbility. Customers can contact their Adobe representative for additional assistance.

Outbound communications from Magento Commerce to the user are re-encrypted after they are processed by the CDN. The CDN service supports SHA-256 certificates signed by publicly trusted certificate authorities that have a minimum key size of 2048 bits for RSA. Checkout and account pages are always served using HTTPS. The best practice is to serve all pages in a site under HTTPS.

Payment Gateway

Magento Commerce requires integration with a payment gateway to pass credit card data from the user to the payment gateway.

Extensions

The customer is responsible for verifying that any extensions to Magento Commerce either a) do not process and/or store payment information or other personally identifable information (PII), or b) that those extensions are certified as PCI-compliant if they must handle that data.

Data Storage

Adobe® Magento Commerce uses Amazon Elastic Block Store (EBS) for storage. All EBS volumes are encrypted by Amazon using the AES-256 algorithm, meaning data is encrypted at rest. Magento Commerce also encrypts data in transit between the between the CDN and users as well as between the CDN and all Magento Commerce servers. All secure communications are encrypted using TLS 1.2.

Passwords created for the various Magento Commerce system accounts are stored as hashes using Argon2id. Sensitive credentials, including those used for the payment gateway, are encrypted using AES-256. Magento Commerce does not support column-level or row-level encryption or encryption when the data is in transit, i.e., in transit between servers.

The customer can manage encryption keys from within the Magento Commerce. Keys used by the infrastructure are stored in AWS Key Management System and must be managed in Magento Commerce in order to deliver key functionality of the environment.

General Recommendations

This section provides general security best practices recommendations for all Adobe® Magento Commerce customers.

Priority Recommendations

Adobe considers the following five recommendations to be of highest priority for all customers. We recommend you implement these key best practices are part of your Magento Commerce deployment:

1. Enable two-factor authentication for your admin panel and all SSH connections.
2. Set up and use a non-default admin URL
3. Keep your code up-to-date by installing **all** patch releases from Adobe
4. Implement "lock config" and "lock env" environment variables.
5. Set up and run the Magento Commerce Security Scan service.

Select the right solution integrator and extension vendors

One of the most critical decisions a customer can make is choosing a solution integrator (SI) well-versed in security with a solid track record of dealing with security issues and proven to have secure coding practices for customizations. The solution integrator should also demonstrate adherence to secure development practices.

The customer should also consult the chosen solution integrator in selecting the most appropriate and secure extensions to Magento Commerce. Adobe recommends customers consider the following when selecting extensions to Magento Commerce:

- Only source extensions from the Magento Marketplace or through the solution integrator. If the extension is sourced through the integrator, ensure ownership of the extension license is transferrable, in case the integrator changes.
- Limit the number of extensions and vendor in order to reduce risk exposure
- If possible, review the extension code or security before integrating

Install the latest application updates and security patches

All components of the customer's installation should run the latest version of Magento Commerce available. Adobe constantly updates solution components to improve security and better protect customers against possible compromise. Using the latest version of the application as well as all current patches is the first and best line of defense against possible compromise.

Magento Commerce typically releases security updates on a quarterly basis but reserves the right to release hotfixes for major security threats based on priority and other factors. Information about our current patch and update release process is available on our website.

Develop a comprehensive disaster recovery plan

Having a disaster recovery plan in place before an incident can make can make it easier to control the damage and ensure a faster return to the normal course of business after a compromise. Even a basic plan will help get a business back on track in the event of a problem.

If a customer requires restoration of Magento Commerce due to a disaster, Adobe will provide the customer with the backup files. The customer and solution integrator, if applicable, will perform the restore.

Know the most common attacks

Below is a list of common categories of attacks that Adobe recommends all Magento Commerce customers be aware of and take measures to protect against:

- **Site defacing** — While access to the site and user accounts may be compromised, payment information often remains secure.
- **Botnets** — The customer's Magento Commerce server becomes part of a botnet that sends spam email. Although user data is not typically compromised, the customer's domain name is may be blacklisted by spam filters, preventing delivery of any email from the domain. Alternatively, the customer's site becomes part of a botnet causing a distributed denial of service (DDOS) attack on another site/s. The botnet may block inbound IP traffic to the Magento Commerce server, preventing customers from being able to shop.
- **Direct server attacks** — Data is compromised, backdoors and malware are installed, and site operations are affected. Payment information—provided that it is not stored on the server— is less likely to be compromised through these attacks
- **Silent card capture** — In this most disastrous attack, intruders install hidden malware or card capture software, or worse, modify the checkout process to collect credit card data and redirect it to another site for sale on the dark web. Such attacks can go unnoticed for extended periods of time and can result in major compromise of customer accounts and financial information.
- **Silent keylogging** — The threat actor installs keylogging code on the customer's server in order to gather admin user credentials and then perform other attacks in a non-suspicious way.

Take immediate action in the event of an attack

In the unfortunate event of a site compromise, here are some key recommendations customers may wish to follow:

- Engage your systems integrator and/or appropriate security personnel to conduct your investigation and remediation efforts

- Determine the scope of the attack:
  - Was credit card information accessed?
  - What information was stolen?
  - How much time has elapsed since the compromise?
  - Was the information encrypted?
- Try to find the attack vector to determine when and how the site was compromised, by reviewing server log files and file changes.
- In certain circumstances, it may be advisable to wipe and reinstall everything or, in the case of virtual hosting, create a new instance. Malware could be hidden in an unsuspected location just waiting to restore itself.
- Remove all unnecessary files. Then reinstall all required files from a known, clean source, such as files from your own version control system or the original distribution files from Adobe.
- Reset all credentials, including the database, file access, payment and shipping integrations, web services, and Admin login. Also reset all integration and API keys as well as accounts that might be used to attack the system.

Using the Magento Commerce Security Scan Service

Magento Security Scan is a service offered by Adobe that allows you to monitor each of your Magento sites for known security risks, and to receive patch updates and security notifications. Including the Magento Security Scan service as a part of your overall security monitoring efforts can help you to:

- Gain insight into the real-time security status of your store.
- Schedule security scan to run weekly, daily, or on demand.
- Receive reports with the results of over thirty security tests and the recommended corrective actions for each failed test.
- Maintain a history of security reports in your Magento account.

The Security Scan service is available for free from the dashboard of your Magento Commerce account. For technical information, see the developer documentation.

Detailed Security Checklist

This section lists some recommended best practices for keeping the customer's Adobe® Magento Commerce installation secure. Many of the checklist items are applicable to securing the computer infrastructure in general, so some of the recommendations may already be implemented.

Use HTTPS

If the Magento Commerce site is newly implemented, strongly consider launching the entire site using HTTPS. Not only does Google use HTTPS as a ranking factor, but also many users will not even consider purchasing from a site that is not secured with HTTPS.

For an existing installation, configure the application to use a securely encrypted HTTPS channel. Although the customer will need to create redirects from HTTP to HTTPS, the effort will future-proof the site. Adobe recommends that all Magento Commerce clients impement this change as soon as possible.

Export Configuration

Adobe highly recommends that customers export and backup their configuration to ease redeployment in the event redeployment may be needed for business continuity purposes. The primary reason to export the configuration to the file system is that the configuration takes precedence over the database configuration. In a read-only file system, this forces a redeploy to change sensitive configuration fields, providing an extra layer of protection.

- For more information on exporting the Magento Commerce configuration: https://devdocs.magento.com/guides/v2.3/config-guide/cli/config-cli-subcommands-config-mgmt-export.html
- For more information on importing the Magento Commerce configuration: https://devdocs.magento.com/guides/v2.3/config-guide/cli/config-cli-subcommands-config-mgmt-import.html

Protect Against Malware

Malware attacks targeting ecommerce sites are all too common, and threat actors continually develop new ways to harvest credit card and personal information from transactions. However, Adobe has found that most site compromises are not due to an innovative hacker; rather, threat actors often take advantage of existing, unpatched vulnerabilities, poor passwords, and/or weak ownership and permission settings in the file system.

In the most commonly experienced form of attack, malicious code is injected into the absolute header or absolute footer of a customer's store. There, the code collects (i.e., skims) form data entered by the end user into the front end of the store, including customer login credentials and checkout form data, and sends it to another location for malicious purposes rather than to the Magento Commerce backend. Additionally, depending on the method used to inject the malware into the Magento Commerce site, the admin panel may be compromised as well, allowing the malware to replace the original payment form with an identical-looking fake form to override any protections set by the payment provider.

Client-side credit card skimmers are a type of malware that is embedded into a merchant's website content and can execute in a user's browser. Once certain actions occur, such as the user submits a form or a text box changes, the skimmer serializes the data and sends it to a third-party endpoint, which are typically other compromised websites that act as a relay to send the data to its final destination.

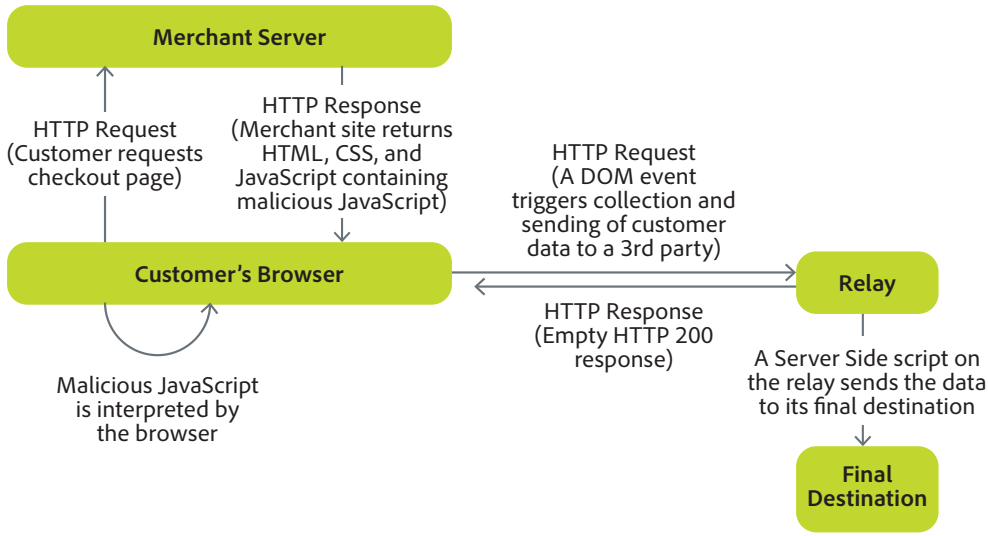

Figure 2: Malware attacks targeting ecommerce sites

If the Magento Commerce site has been attacked by malware, consider following these steps:

General recommendations

- Engage your systems integrator and/or appropriate security personnel to direct your investigation and remediation efforts
- Inform Adobe of your ongoing investigation and remediation efforts
- Create an archive of your current environment and store it in a secure location
- Create a database dump
- Create a backup of the entire web root including media, and admin action log archives
- Remove all data skimmer code from the Absolute Header or Absolute Footer of the site
  - The absolute header can be found by navigating to Content > Design > Configuration > HTML Head > Scripts And Stylesheets
  - The absolute footer can be found by navigating to Content > Design > Configuration > Footer > Miscellaneous HTML
- Check all scopes in the system, e.g., website, store, store view
- Scan the site using publicly available tools to identify any missing security patches and determine if the site has been infected with known malware strains.
- Install the latest version of extensions from the Magento Marketplace and test them in a non-production environment.

Audit Admin user accounts

- Go to the Admin panel of the production site. Remove all unknown Admin accounts from System → Permissions → Users.
- Change passwords on all known Admin accounts and rename overly generic Admin usernames to a unique name (avoid using names like administrator, superuser, or root).
- Remove all unknown and unused accounts, including API accounts. Be sure to keep a record of all removed accounts.
  - Reset all admin user account passwords.
  - Ensure that the accounts of people who are no longer employed are deactivated.
  - Review all SSH and FTP users, remove old or unknown users, and change active users' passwords.

Audit code

- Remove all unknown JavaScript code from Content → Design → Configuration → HTML Head → Miscellaneous Scripts. Check all configuration scope levels, including 'website' and 'store view.' Only keep recognized code, e.g., tracking snippets.

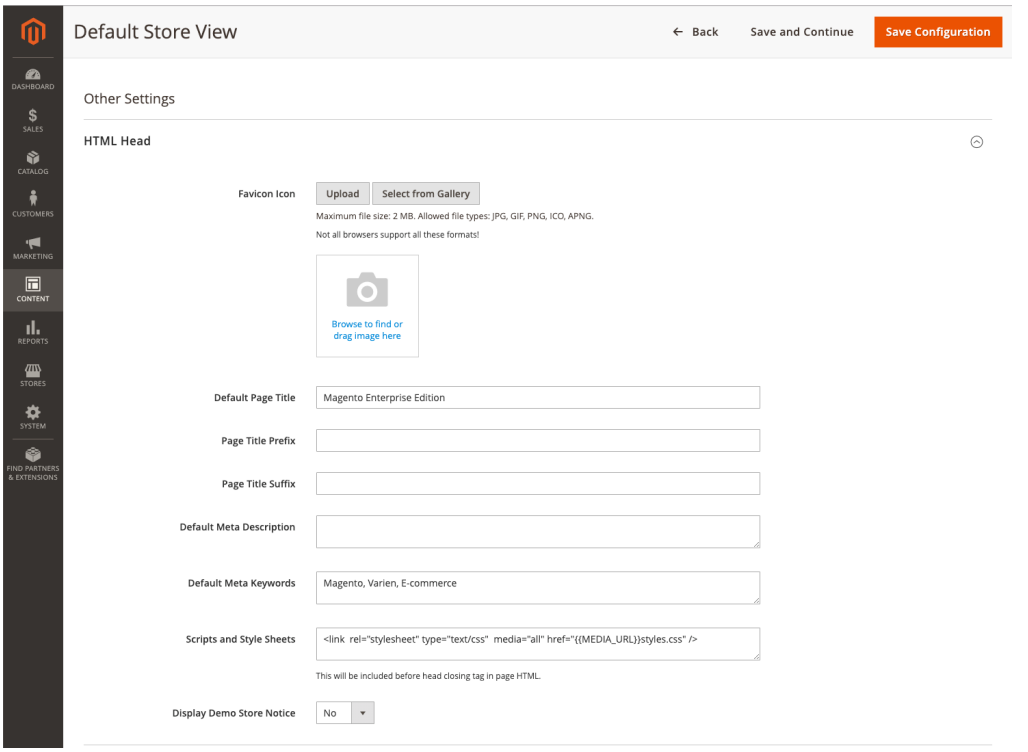

Figure 3: Magento Commerce 2.3.x HTML Header

- Remove all JavaScript code from Content → Design → Configuration → Footer → Miscellaneous HTML. Only replace recognized code, e.g., tracking snippets.

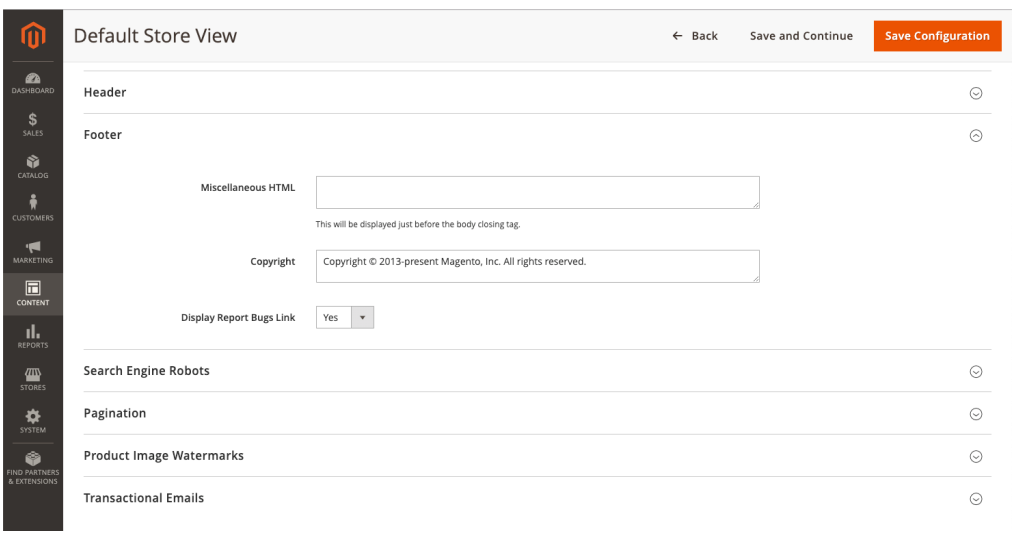

Figure 4: Magento Commerce 2.3.x Footer

- Compare the current production code base to the code base stored in the Version Control System (VCS).
- Quarantine any suspicious code.
- Redeploy the codebase to the production environment to ensure nothing is left behind.

Audit database

- Review any stored procedures for modifications.

- Verify that the database is only accessible by the Magento Commerce instance.
- Verify the malware is no longer present by scanning the site with publicly available malware scanning tools.
- Secure the Admin panel by changing its name and verifying that the site's 'app/etc/local.xml' and 'var' URLs are not publicly accessible.
- Continue to closely monitor the site after the incident as many sites get compromised again within hours. Ensure ongoing log review and file integrity monitoring to quickly detect any signs of new compromise.

Remove Google warnings

- If the site has been flagged by Google as containing malicious code, request a review once the site has been cleaned. Reviews for sites infected with malware take a few days but once Google determines the site is clean, warnings from search results and browsers should disappear within 72 hours. Information on how to request a review is available at https://developers.google.com/webmasters/hacked/docs/request_review.

Review malware results checklist

If publicly available malware scanning tools confirm the site has been impacted, investigate the incident and work with the solution integrator to clean the site and follow the recommended site remediation steps.

Conduct additional reviews

When dealing with advanced attacks, the best course of action is to work with an experienced developer, third-party expert, or solution integrator to fully repair the site and review security practices. Working with a security professional helps ensure the deeper steps are taken to ensure the safety of your business and its customers.

Protect Against Password Guessing Attacks

Brute force password guessing attacks can be a threat to Magento Commerce installations. In some cases, these attacks result in unauthorized Admin panel access. Therefore, Adobe highly recommends the steps outlined below to protect the store against such attacks.

Identify all access points

The first step includes identifying all possible points at which the Magento Commerce installation could be accessed from the outside world. The Admin panel location (the location is generated automatically during installation) generally requires the most protection.

Whitelist IP addresses

Enabling only users coming from a specified IP address or network to access the Magento Commerce site is one of the most reliable ways to protect access to the Admin location.

To find your location's IP address, go to https://www.google.com/search?q=what+is+my+ip. The results should show an address similar in structure to 111.222.333.444 . If the Magento Commerce site uses dynamic IP addresses or accesses the Magento Commerce backend through a mobile device, this Google command will fail.

If you employ a remote workforce, it's important to add the IP addresses of these remote employees to ensure their access to the network.

Securing the Admin Panel

Use Non-Default Adobe Admin URL

A simple Admin URL makes it easier to target attacks on specific locations using automated password guessing. To prevent against this type of attack, Adobe by default creates a random

admin URL when you install the product. Use the following command to display the current admin URL:

bin/Magento info:adminurl

You can change this admin URL in three ways:

- This command:
  bin/Magento setup:config:set --backend-frontname=<value>
- The env.php file
- The Admin panel

Although the use of a non-default admin URL will not secure the site, its use will help prevent large-scale automated attacks. We recommend further securing access using two-factor authentication and CAPTCHA options provided by Adobe.

Update Admin account security

Additionally, Adobe recommends that the Admin panel be configured to limit the number of password reset requests per hour, setting the maximum number of login failures before the account is locked. Also, it's best practice is to set the lockout time to a minimum of 30 minutes. These two settings can also be configured through the Admin panel by navigating to:

Stores > Configuration > Advanced > Admin > Security

Enable ReCAPTCHA

ReCAPTCHA is the code combinations of letters and numbers designed to verify human response. You should protect your Magento Commerce Admin panel against automated brute force attacks by enabling ReCAPTCHA. For more information on how to enable ReCAPTCHA, please go to: https://devdocs.magento.com/guides/v2.3/security/google-recaptcha.html

Two-Factor Authentication

Adobe builds in certain controls to prevent brute force attacks, including two-factor authentication (2FA) for the core Magento Commerce application. 2FA prevents brute force attacks as well as unauthorized access. You can find more information about configuring 2FA for site admin access here: https://devdocs.magento.com/guides/v2.3/security/two-factor-authentication.html.

Additional Recommendations

- Use a VPN tunnel and block any other access to the services (you will need to work with your hosting provider to set up this method).
- Review your server and source code repository for "development leftovers." Make sure there are no accessible log files, publicly visible .git directories, tunnels to execute SQL, database dumps, phpinfo files, or any other unprotected files that are not required, and that might be used in an attack.
- Use a Web Application Firewall to analyze traffic and discover suspicious patterns, such as credit card information being sent to an attacker.
- Set up strong passwords and change them at least every 90 days, as recommended by the PCI Data Security Standard in section 8.2.4. You can check your password lifetime setting in the following locations:
  - Stores > Configuration > Advanced > Admin > Security > Password Lifetime set to 90 days (default setting)
- Each month, review all of your Admin user accounts and remove any that you do not recognize, or are no longer valid or active.
- Make sure to have a process for removing accounts that are no longer needed, like accounts of employees who are no longer part of the company.

- Use the principle of least privilege when assigning permissions to roles and roles to user accounts.

Preventing Clickjacking Exploits

Adobe safeguards your store from clickjacking attacks by using an X-Frame-Options HTTP request header. For more information, see X-Frame-Options header.

Non-secure functions

Using functions that are known to be exploitable or insecure can lead to remote code execution or weak cryptography. As a developer, you should avoid using functions that introduce vulnerabilities in your code.

PHP functions to avoid

The following is a list of PHP functions that are known to be vulnerable and exploitable. Avoid using these functions in your code.

- **eval** — Using eval is considered bad practice because of its ability to execute arbitrary PHP code.
- **serialize/unserialize** — Attackers can create an exploit for these functions by passing a string with a serialized arbitrary object to the unserialize function to run arbitrary code.
- **md5** — The algorithm for this function is known to have cryptographic weaknesses. You should never use this function for hashing passwords or any other sensitive data.
- **srand** — Using a predetermined number to seed the random number generator results in a predictable sequence of numbers.
- **mt_srand** — This function is a pseudo-random number generator (PRNG) and is not cryptographically secure.

Conclusion

Establishing and maintaining a secure environment for Magento Commerce is a responsibility that is shared between you and Adobe, and the intent of this guide is to provide you with the best practices for the customer's side of the equation. While there is no single way to eliminate all security risks, following the steps in this guide will harden your Magento Commerce installation and make it a less attractive target for malicious attacks—helping ensure the security of the solution and your customers' sensitive information.

For more information, please visit: http://www.adobe.com/security.

Adobe

Adobe
345 Park Avenue
San Jose, CA 95110-2704
USA
trust.adobe.com