# Below information are gathered from various search results from google as part of initial research on project selection

# Magento (<https://magento.com/>)

# Magento is an [open-source](https://en.wikipedia.org/wiki/Open-source_software) [e-commerce platform](https://en.wikipedia.org/wiki/E-commerce) written in [PHP](https://en.wikipedia.org/wiki/PHP). It uses multiple other PHP frameworks such as [Laminas](https://en.wikipedia.org/wiki/Laminas) and [Symfony](https://en.wikipedia.org/wiki/Symfony). Magento [source code](https://en.wikipedia.org/wiki/Source_code) is distributed under [Open Software License (OSL)](https://en.wikipedia.org/wiki/Open_Software_License) v3.0. Magento was acquired by [Adobe Inc](https://en.wikipedia.org/wiki/Adobe_Inc) in May 2018 for $1.68 Billion USD.

# More than 100,000 online stores have been created on this platform. The platform code has been downloaded more than 2.5 million times, and $155 billion worth of goods have been sold through Magento-based systems in 2019. Two years ago, Magento accounted for about 30% of the total market share (from Wiki page).

# GitHub repo:

# <https://github.com/magento/magento2>

# \*open for bugfixes.

# What are the threats perceived by users of the software in its intended operational environment?

* Credit Card Hijack
* Ransomware
* Cacheleak vulnerability
* GuruInc Javascript Hack
* Outdated Magento version
* Unprotected development files

4 Most Vulnerable Security Attacks which may threaten eCommerce

* Server Attacks
* Website Defacement
* Silent Card Capture
* Botnetting

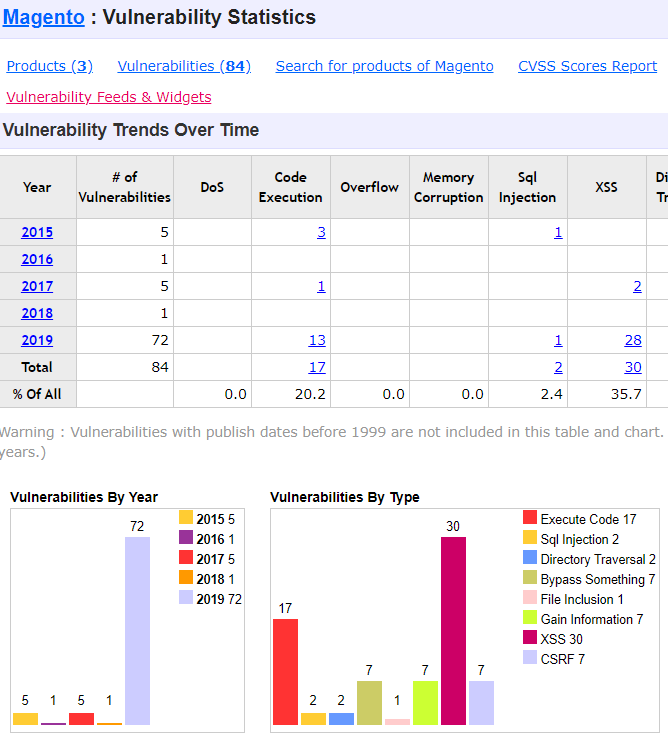
# Develop a list of security features in the software

# Magento-based web stores would be incomplete if we didn’t mention the importance of regular security check-ups. Even with multiple security measures they take, retailers need expert assessment of how effectively their business is protected from cybercriminals. Here are the methods they can use.

* Security audits
* Penetration testing
* Safe environment
* Protected file system
* Protected admin panel
* Reliable extensions

A brief summary of security-related history for the software (E.g., known vulnerabilities, security-related engineering decisions, security feature additions/removal, etc

# From: https://www.cvedetails.com/vendor/15393/Magento.html



Describe a hypothetical operational environment (e.g., home, office, enterprise, bank, government, etc.) where the users will expect security functionality from the software.

# magento 2.3.4 update

Security Tips:

* Two-Factor Authorization
* Update Software in Time
* Backup Regularly
* Use Complex Password