

# New Features Introduced in Magento 2.0.1

Recently Magento announced new Magento 2.0.1 releases in order to enhance the security and functionality of your Magento based website. The releases come up with several other imperative functional updates. These updates come down to the followings:

1. Magento 2.0.1 incorporates official support for PHP 7.0.2 (Our Previous Blog: <http://envisionecommerce.com///the-rise-of-php-7-most-important-shift-in-lamp-stack/>)
2. This support further encourages dramatic performance improvements
3. Reduces memory consumption significantly.
4. There are multiple security & functional fixes addressed by Magento 2.0.1. These fixes contain:
  - XSS in backend via user name – APPSEC-1263
  - Block cache exploit – APPSEC-1247
  - Stored XSS in Order Comments – APPSEC-1239
  - SQL Injection via layered navigation
  - Guest order view protection code vulnerable to brute-force attack – APPSEC-1270
  - XSS in Product Custom Options – APPSEC-1267
  - Editing or Deleting Reviews with no permission – APPSEC-1268
  - CAPTCHA Bypass – APPSEC-1283
  - Reflected XSS with cookie header – APPSEC-1255
  - CSRF Delete Items from Cart – APPSEC-1212
  - Injected code can be stored in database – APPSEC-1240
  - Incorrect filter – APPSEC-1282

The newer version of Magento 2.0 will help developers in a much better way to be updated with their learning curve. In

some case, if you feel a need for helping hands to apply  
Magento update services, we are happy to help you out.