WooCommerce Object Injection Vulnerability

WordPress has been vulnerable to some serious vulnerability recently. Last month we did a blog "Security Vulnerability :: Widespread XSS Vulnerability in WordPress Plugins and Themes" which shared the high risk vulnerability that WordPress and its associated plugin have.

Sucuri, the well know company for Security analysis and fix, has yet again raised alarm for another Object Injection Vulnerability. This time it is WooCommerce's security vulnerability which can be used by a hacker to get server access and download any file on the infected server. The hacking is easy in this case and the hacker can remotely trigger it. WooCommerce is the premium plugin that converts your WordPress into an ecommerce platform and to have such vulnerability in it puts your ecommerce portal at high risk.

It is not just the latest version of WooCommerce that is infected but the vulnerability is traced back to version 2.0.20, so all the version after that are at risk. The silver lining here is that the vulnerability is only observed when WooCommerce's "PayPal Identity Token" option is set as yes (which is in most of the store that use Paypal as a payment method).

We know that WooCommerce is a very important plugin for WordPress based Store owners. As a team dedicated to WooCommerce we share this blog and hope it reaches maximum people so that you can update your WooCommerce Store ASAP. We are available for any help and support in case if you need us to do it for you.

Contact us with your store details and we will certainly assist you to secure your WooCommerce Store.