Website Security Discussion

Discussion:  (In the news)

Find an example of a recent eCommerce website security incident. Provide a link to the article you chose. Write a short summary of the incident, and include in your summary if it is known how the incident occurred. (Example, was it in injection, social engineering, or another form of attack).  Is the incident tied to a particular CMS or infrastructure?

Please be sure to adhere to the posted guidelines on responses, for example be sure to include the number of the question you are responding to.

Please follow the outlined guidelines of this discussion:

* You should respond to what someone else has posted.  (**Reply to at least 1 other student in your class**). This includes clarifying other peoples comments or providing additional information.
* Keep it professional:
  + This means watch your language and treat each other with respect.
* Assume best intentions:
  + If someone is adding additional information to your comment or answering your question, assume that they are doing just that and that it is not a personal attack against you.  The purpose of this is so that you can all help each other.
* State the question number you are responding to:
  + This will help keep things organized and people will be able to see who is responding to specific questions.
  + This applies also for when you are adding a comment.
    - (EX.) Response for Q1:
    - (EX.) Clarification on Response for Q1:

I will continue to periodically monitor the discussion as well.

<https://www.techradar.com/news/wordpress-force-updates-thousands-of-websites-following-woocommerce-security-breach>

I chose to write about a recent WooCommerce security incident because I just recently finished my quarterly project and used both WordPress and WooCommerce.

The incident covered in the linked article above is described as a “security breach” in the website title, but in reality it does not appear to have been exploited in the wild because the security testing program at WooCommerce was able to identify and patch it quickly.

While this is true, it sounds like the vulnerability was a pretty serious one affecting WooCommerce versions 4.8.0 – 5.6.2 and it allowed anyone to “…impersonate an administrator and completely take over a website without any user interaction or social engineering required.”1

Being a rather new vulnerability with no known examples of use, there is little information about how the vulnerability works at this point, but one researcher at Sucuri noted that it appears to reside inside of the file class-platform-checkout-session.php as this file was completely removed with the recent security patch deployed by WordPress.2

1 *Fadilpašić, S. (2023, March 24). WordPress force updates thousands of websites following Woocommerce Security Breach. TechRadar. https://www.techradar.com/news/wordpress-force-updates-thousands-of-websites-following-woocommerce-security-breach*

2 *Martin, B. (2023, March 31). Critical vulnerability discovered in woocommerce payments. Website Security News. https://blog.sucuri.net/2023/03/critical-vulnerability-discovered-in-woocommerce-payments.html*