ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНОЙ СТРАНИЦЫ ИНТЕРНЕТ - САЙТА МАГИСТРАТУРЫ ОТ WEB - АТАК

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Кухарчик Е.И., Конопелько И.А.

Казека А.А. – канд. техн. наук, доцент

Интернет сегодня – это то, без чего не может прожить подавляющая часть населения. Сегодня Интернет открывает для людей безграничные возможности. Для кого-то – это просто развлечение, а для других – это работа и учеба. Изначально, интернет – сайты представляли собой совокупность статичных документов, но в настоящее время большинству из них свойственна динамичность и интерактивность. В связи с этим, в интернет-пространстве начало увеличиваться количество персональных страниц пользователей интернет- ресурсов. Для быстрого поиска необходимой информации студентам и магистрантам на интернет-портале университета, предлагается создание такой страницы обучающегося.

Персональная страница обучающегося – это дополнительные возможности интернет-портала, которые позволяют:

1. Получать актуальную информацию.
2. Отправлять сообщения (заявления, предложения и т.д.).
3. Оперативно менять свои контактные данные.
4. Посмотреть расписание занятий.
5. Проверить отметки в электронной зачётке.
6. Посмотреть свой учебный план.
7. Посмотреть информацию об оплате за обучение.

Не смотря на все удобство использования персональной страницы она содержит конфиденциальную информацию обучающегося, которая может попасть в руки злоумышленника. Одни из самых распространенных способов заполучить конфиденциальную информацию [1]:

1. Подбор – подбор имени пользователя и пароля.
2. Небезопасное восстановление паролей (Weak Password Recovery Validation).

Основные методы противодействия злоумышленникам заключаются в уменьшении количества попыток ввода не правильного пароля. При восстановлении пароля использовать электронную почту, или мобильный телефон, указанный при регистрации. Кроме того, следует учитывать о нарушение доступности Web сервера (ddos attack), переполнение базы данных интернет-роботами (Insufficient Anti-automation), рассылка спама, внедрение вредоносного кода.

Чтобы не стать жертвой злоумышленника, нужно тщательно продумывать план защиты интернет-портала или и персональной страницы на стадии разработки. А для дальнейшей поддержки безопасности, требуется проводить аудит информационной безопасности. [2]

Аудит информационной безопасности позволяет получить наиболее полную и объективную оценку защищенности информационной системы, локализовать имеющиеся проблемы и разработать эффективную программу построения системы обеспечения информационной безопасности организации.

Аудит безопасности сайта осуществляется путем тестирования на устойчивость сайта к комбинированным методам и техникам взлома. В случаях использования популярной CMS (Битрикс, NetCat, WordPress, Joomla!, Drupal и т.д.) [3], дополнительно проводится проверка устойчивости системы к известным эксплойтам. По завершению тестирования на проникновения составляется подробный отчет, содержащий обнаруженные уязвимости, способы их эксплуатации, а также рекомендации по их устранению.

Список использованных источников:

1. Жуков Ю. В. – Основы веб-хакинга. Нападение и защита (2-е изд.) – 2012 г.
2. Ярочкин В. И. – Информационная безопасность: учеб. для вузов. (2-е изд.) – 2005 г.
3. Система управления содержимым [Электронный ресурс] https://ru.wikipedia.org/wiki/Content_Management_System
4. Обзор эксплойтов [Электронный ресурс] https://xakep.ru/2011/07/04/57578/