С.Сейфуллиннің 125 жылдығына арналған **«Сейфуллин оқулары – 15: Жастар, ғылым, технологиялар: жаңа идеялар мен перспективалар»** атты халықаралық ғылыми-теориялық конференциясының материалдары = Материалы Международной научно-теоретической конференции **«Сейфуллинские чтения – 15: Молодежь, наука, технологии – новые идеи и перспективы»**, приуроченной к 125 - летию С.Сейфуллина. - 2019. - Т.I, Ч.2 - С.136-137

О МОДЕЛИ ЗАЩИТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕБ-САЙТА

Жолай Б.А.

В настоящее время модели защиты веб-приложений разрабатываются на основе анализа данных статистических исследовании безопасности веб-приложений. По результатам анализа выделяют основные уязвимости веб-приложений и учитывают наиболее распространенные атаки злоумышленника веб-приложения. Проблемы безопасности [1] связаны с утечкой информации, финансовыми и репутационными потерями организаций, владеющих этими приложениями. Наиболее распространены SQL-инъекции как уязвимость веб-безопасности, которая позволяет злоумышленнику вмешиваться в запросы в базе данных собственника веб-приложения. В этом случае злоумышленник также может просматривать данные, принадлежащие другим пользователям, или любые другие данные, к которым приложение имеет доступ; может изменить или удалить эти данные. Такое вмешательство приводит к изменениям содержимого или поведения веб-приложения.

Наряду с этим распространенной уязвимостью являются недочеты в системе аутентификации, к которым относят следующие: учетные данные аутентификации пользователя не защищены при хранении; предсказуемые учетные данные для входа; идентификаторы сеанса уязвимы; пароли, идентификаторы сеансов и другие учетные данные отправляются через незашифрованные соединения и многие другие. Методы и этапы защиты веб-приложений являются адекватным ответом на атаки злоумышленника. Чтобы предотвратить нарушение аутентификации и управление сеансами нужно придерживаться правил, в том числе учетные данные аутентификации пользователя должны быть защищены при хранении с использованием хеширования или шифрования. Предъявляются определенные требования к процедурам аутентификации и ее характеристикам. Так минимальная длина пароля должна быть не менее восьми символов, сложность пароля устанавливают правилом: пароли должны состоять из букв, цифр, знаков препинания, математических и других условных символов. Комбинация на основе сочетания длины пароля с его сложностью затрудняет угадывание пароля при использовании атаки методом перебора.

Статистически распространенной уязвимостью является незащищенность конфиденциальных данных. Однако пользователи доверяют

свои данные, считая что сервер защитит эти конфиденциальные данные. С увеличением количества доступных веб-приложений уязвимость пользовательских данных только возросла. К рекомендациям можно отнести следующие правила: важно зашифровать данные, включая архивы. Рекомендуют применять шлюзы безопасной аутентификации, используя стандартные технологии безопасностиSSL или TSL, чтобы обеспечить шифрование всех данных, передаваемых между браузером и веб-сервером. Мерами предотвращения атак является применение паролей, проведение регулярной оценки риска, выполнение безопасного резервного копирования по определенному плану. Эти меры позволяют уменьшить потери, увеличивают безопасность пользователя и собственника веб-приложений.

Список литературы

1 Viktorova V.S., Lubkov N.V., Stepanyants A.S.RELIABILITY MODELS AND ANALYSIS OF SYSTEMS WITH PROTECTION // Automation and Remote Control. 2018. Т. 79. № 7. С. 1270-1286.

Научный руководитель.к.п.н., ст. преп. каф. ИС Абдыгаликова Г.А