УДК 004.056

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ WEB-СЕРВИСОВ

Ишутина Е. (Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный морской технический университет»)

Научный руководитель – к.т.н., доцент Чернов А.И.

(Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный морской технический университет»)

Введение. В последние годы проблемы с безопасностью данных в Интернет-сети становится наиболее актуальны. Согласно статистике аналитиков Group-IB за 2022 году был получен несанкционированный доступ к 311 базам данных российских компаний, а общее количество строк данных пользователей превысило более 1,4 млрд. Персональные данные входят в число важнейших информационных активов компаний, хотя и не являются коммерческой тайной. Их утечка становится угрозой как для владельцев, так и для тех, кто ее допустил. Новым и нынешним пользователям интернета необходимо знать о вероятности инцидентов, связанных с безопасностью, и о шагах, что должны быть предприняты для защиты. В настоящей работе раскрываются возможные угрозы утечки баз данных и возможности их устранения.

Основная часть. В ходе исследования выявлено, что проблема безопасного хранения данных пользователей и компаний актуальна как никогда. Путём поиска веб-ресурсов по шаблону выяснилось, что невероятная часть проектов потенциально подвержена самым простым методам атаки на базы данных. В них может содержаться не только авторизационная информация, но и персональные и платежные данные, которые в перспективе могут быть использованы для фишинга, шантажа или повлечь финансовые потери пользователя. Также отметим, что одни и те же авторизационные данные могут использоваться пользователями на разных ресурсах, что увеличивает риск ещё большей утечки и ещё больших финансовых или репутационных потерь.

Один из способов незаконного доступа к базам данных является SQL-инъекция. Суть таких инъекций – внедрение в данные (передаваемые через GET, POST запросы или значения Cookie) произвольного SQL кода. Если сайт уязвим и выполняет такие инъекции, то в результате формируется запрос, выполняющий действия, определенные злоумышленником. При этом запрос будет являться корректным с точки зрения синтаксиса SQL. Уязвимости данного типа представляют серьезную угрозу. По версии OWASP Top Ten 2021 их можно отнести к категории A01:(Injection).

Метод защиты от данного способа проникновения заключается в предотвращении внедрения SQL-инъекции. В первую очередь необходимо обратить внимание на двойные кавычки, одинарные кавычки и символы обратной косой черты. Без кодирования двойные и одинарные кавычки будут интерпретироваться как разделители строк, а обратные слеши могут использоваться для подрыва любой кодировки, которая выходит за пределы только разделителей строк. Возможность вставлять разделители строк в оператор SQL является одним из основных способов выполнения атаки SQL инъекцией.

Выводы. Несмотря на существующие защиты хранилищ данных, остро стоит проблема утечек персональной информации пользователей веб-ресурсов. Данные являются одним из важнейших ресурсов любой организации. В данной работе проведен анализ актуальности проблемы безопасности персональных данных пользователей, находящихся в базах данных веб-ресурсов. Описан способ атаки на базу данных – SQL-инъекция. А также, рассмотрен метод защиты от данного способа. В целом защитой от данного рода проникновения является

грамотная настройка ПО для работы с базами данных и своевременное его обновление для устранения ошибок безопасности.

Список использованных источников:

1. Статистика Group-IB [Электронный ресурс] URL: https://www.group-ib.ru/media-center/press-releases/database-leaks-record/
2. Методы защиты от sql-инъекций [Электронный ресурс] URL: https://htmlacademy.ru/blog/php/sql-injections
3. OWASP Top Ten [Электронный ресурс] URL: https://owasp.org/www-project-top-ten/

Ишутина И. (автор) Подпись

Чернов А.И. (научный руководитель) Подпись