изменяется так, что кажется, будто он пришел с компьютера в местной сети, хотя на самом деле он пришел из Интернета.

ЛИТЕРАТУРА

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации/ П.П. Урбанович. – Минск : БГТУ, 2016, – 220 с.

2. Урбанович, П. П. Компьютерные сети : учебное пособие для студентов высших учебных заведений по техническим специальностям / П. П. Урбанович, Д. М. Романенко, Е. В. Кабак. - Минск: БГТУ, 2011. - 399с.

3. Интернет-портал [Электронный ресурс]/ IT-безопасность. – Режим доступа: http://elims2.blogspot.com.by/2008/03/sniffer.html. – Дата доступа: 20.03.1017.

4. Интернет-портал [Электронный ресурс]/ Определение направления на спуфер с помощью ГНСС-приемника. – Режим доступа: http:// secure.tradition.ru/2018/02/09/. – Дата доступа: 20.03.1017.

УДК004.056

Студ. В.Н. Долговечный
Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

УЯЗВИМОСТИ И МЕТОДЫ ЗАЩИТЫ БАЗ ДАННЫХ НА МОБИЛЬНОЙ ПЛАТФОРМЕ

В соответствии с последними данными исследовательской компании eMarketer [1], специализирующейся на анализе рынка высоких технологий, смартфонами уже пользуется больше четверти мирового населения. Это около 2,5 млрд. человек. И тенденция роста пользователей мобильных устройств продолжается.

Мобильные телефоны в современном мире являются не просто средством связи, а устройством, которое содержит уязвимые персональные данные: номера кредитных карт, электронную почту, геолокационные сведения, профили в социальных сетях, средства удалённого доступа и управления предприятием, фотографии, видео и т. д. Несанкционированный доступ к таким чувствительным данным может привести к критической ситуации [2]. Между тем, рынок мобильных приложений растёт с большой скоростью, а пользователи особенно не задумываются о том, какие разрешения они предоставляют при-

ложениям, устанавливая их на свой смартфон, а также о последствиях, которые могут наступить.

Существует множество классификаций приложений для мобильных устройств, но в контексте информационной безопасности приложений следует выделить две большие группы:

- web-приложения, представляющие собой специальную версию web-сайта;
- мобильные приложения, разработанные под определённую мобильную операционную систему с использованием специализированного API.

Большинство современных мобильных приложений используют базу данных (БД), как инструмент для хранения информации [3]. При разработке мобильного приложения следует учитывать, что данные, которыми оперирует эта БД, могут представлять определенный интерес для третьих лиц. Разработчикам следует приложить множество усилий для сохранения БД от несанкционированного доступа к ней.

По мнению экспертов компании Application Security [4], существует 9 основных угроз БД, которые наиболее часто игнорируются ИТ-персоналом и самими пользователями:

1. Используемые по умолчанию, пустые или слабые пароли и логины;
2. SQL-инъекции;
3. Расширенные пользовательские и групповые права;
4. Активизация неиспользуемых функций БД;
5. Нарушение в управлении конфигурациями;
6. Переполнение буфера;
7. Несвоевременное обновление ПО;
8. Отказ от шифрования данных на мобильных устройствах.
9. DoS-атаки.

Исходя из выше перечисленных угроз, несложно заметить, что в половине случаев защита критически важных данных пользователя зависит от самого пользователя. Соблюдения простых правил и политики безопасности приложения поможет в несколько раз уменьшить риск потери ценных данных.

Рассмотрим защиту БД со стороны разработчика на примере web-приложения для продажи билетов на киносеансы. Схема БД показана на рисунке.

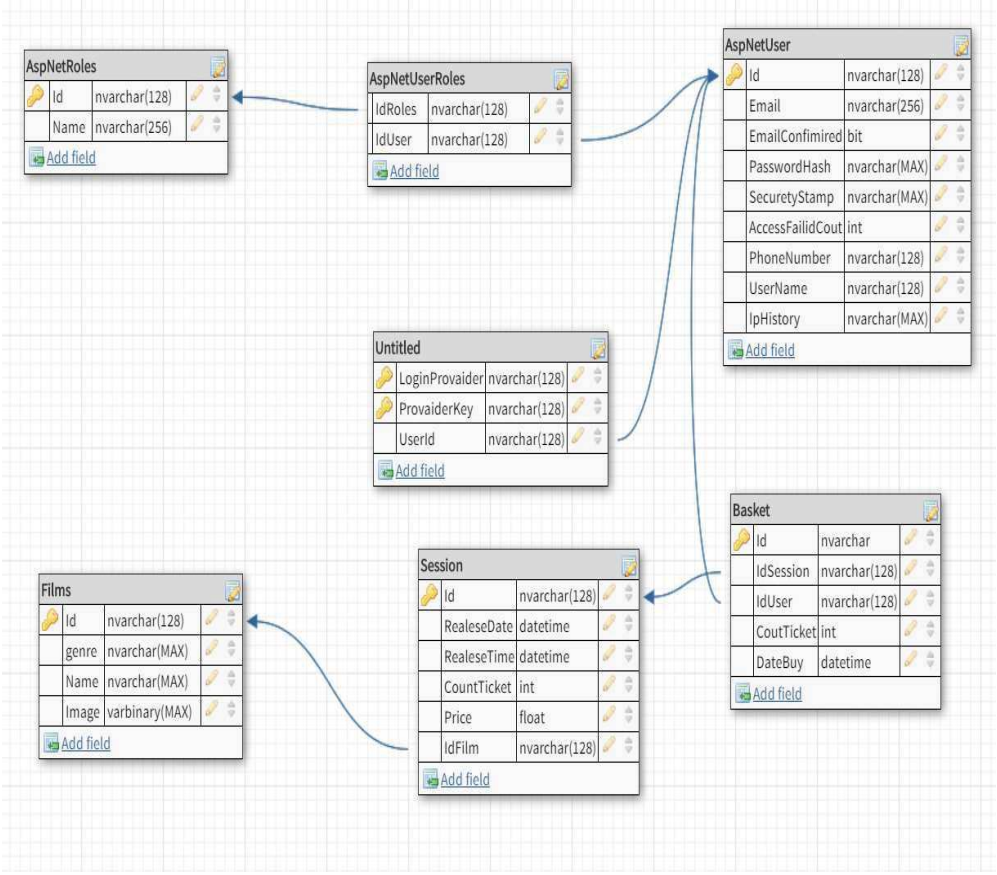

Рисунок – Схема БД

Для защиты БД от атак типа SQL-Injection мы использовали комплексный подход:

1. Проводится “жесткая” валидация данных, полученных от пользователя. Проверка данных идет, как на «клиенте» (HTML, Java-Script) так и на сервере (валидация средствами языка C#).

2. Используется технология программирования Object-Relational Mapping (ORM), которая связывает БД с концепциями объектно-ориентированных языков программирования (пример запроса на рисунке 2). Этот подход демонстрирует хорошую стойкость к атакам типа SQL-Injection за счет способа обращения к БД. Он создает виртуальную хранимую процедуру, по которой и обращается за данными. Так же нам не нужно писать SQL-код для работы с БД, что уменьшает количество ошибок, которыми может воспользоваться хакер.

```
public User FindById(string id)
{
    return _users.AsQueryable().FirstOrDefault(x => x.Id == id);
}
```

Рисунок – Пример использования ORM

Мы заметили, что использование ORM решает ещё ряд проблем: расширенные пользовательских и групповых прав, активизация неиспользуемых функций БД и нарушение в управлении конфигурациями. Мы обращаемся к БД как стандартный пользователь, который имеет ограниченное количество прав для работы с БД (основные – чтение и запись). Даже, если хакер получит возможность управления этими функциями, он не сможет изменять данные или удалить саму БД. Ещё один плюс ORM – он не создаст ненужных функций.

PasswordHash
AJnuMq9q84X7DeY/O2f6ZONd8OqCzCd7KEYPjF7n8ZHXd2i1WVOYCzcH9o5mNQ0eGA==
ADo8uYHPYwdNkPR4TA84RIxgfexg3MPhIqxTwIHrL6iv20znhIEkWNI/aUqLM7K2Eg==
ABQD1GDha7Ih9tcyFrH2bV4RFI24Xcyw5V5CbocKcZp3ky4FHXpPJMZQ/Mve5r5DOA==

Рисунок – Пример хранения данных в шифрованном виде

Самые важные данные в БД лежат в зашифрованном виде. Это сделано для того, чтобы злоумышленник, при их извлечении, не смог ими воспользоваться. Для этого использовался стандартный алгоритм шифрования AES128.

ЛИТЕРАТУРА

1. Интернет-портал [Электронный ресурс]/ Аналитический центр InfoWatch. Глобальное исследование утечек корпоративной информации и конфиденциальных данных, 2017. – Режим доступа: https://www.infowatch.ru/report2017. – Дата доступа: 20.01.2018.

2. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие/ П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

3. Urbanowicz, P. Bazy danych. Teoria i praktyka/ P.Urbanowicz, M. Płonkowski, D.Urbanowicz. – Lublin: Wydawnictwo KUL. – 2010. – 379 p.

4. Интернет-портал [Электронный ресурс]/ Защита и безопасность БД. – Режим доступа: https://www.scienceforum.ru/2015/1121/14145. – Дата доступа: 20.03.2018.

5. Ховард, М. Защищенный код/ М. Ховард, Д. Лебланк, (2-е издание). – М: издательство «Русская Редакция», 2005. — 704 с.