ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

В.С. Ардесов, Д.Р. Салихов, А.Р. Халиков

ИССЛЕДОВАНИЕ ПРОБЛЕМ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ИНТЕРНЕТ-БРАУЗЕРОВ ПОСТРОЕННЫХ НА БАЗЕ WEBKIT

(Уфимский государственный авиационный технический университет)

В современном мире веб-приложения широко распространены. В интернете люди общаются, узнают что-то новое, совершают покупки и выполняют множество других повседневных задач. Для доступа ко всем этим сервисам и веб-приложениям пользователи используют современные интернет-браузеры. Сегодня интернет-браузер это окно в мир информационных технологий. Каждый день мы доверяем веб-сайтам множество персональных данных, данные кредитных карт и другой персональной информации. Но так ли надежно защищены эти данные? Ведь если даже сайт не имеет уязвимостей, то угрозой безопасности может стать использование уязвимого браузера. Именно поэтому было решено проверить современные интернет браузеры на возможность использования некоторых типов уязвимостей в целях доступа к конфиденциальной информации. Целью данной работы является исследование безопасности современных интернет-браузеров.

Для хранения данных об авторизации, настроек, предпочтений пользователя, произведения транзакций и прочего, современные веб-браузеры используют, так называемые, файлы cookie.

Cookie – это фрагмент данных, отправленный веб-сервером для хранения на компьютере пользователя.

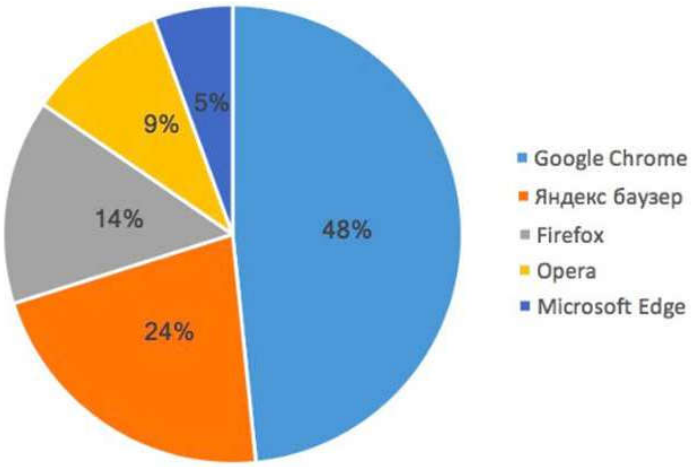

Рисунок 1 – Диаграмма популярности браузеров в России (октябрь 2016)

В мире, существует множество различных браузеров, однако в нашей стране особой популярностью пользуются 5 различных браузера [2]: Google Chrome, Яндекс.Браузер, Opera, Mozilla Firefox, Microsoft Edge (см. рис. 1). Google Chrome, Яндекс.Браузер и Opera, лидеры этой пятерки, построены на базе одного свободного движка для отображения веб страниц WebKit. Это означает, что эти браузеры имеют сходное внутреннее устройство и, как следствие, используют сходные форматы и механизмы для хранения данных. Для хранения cookie, все браузеры на базе WebKit, используют файл базы данных формата sqlite3, со структурой изображенной на рисунке 2, в ОС Windows различаются лишь пути к файлу для cookie:

Google Chrome: %LOCALAPPDATA%\Google\Chrome\User Data\Default\Cookies
Opera: %APPDATA%\Opera Software\Opera Stable\Cookies
Яндекс.Браузер:%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Cookies

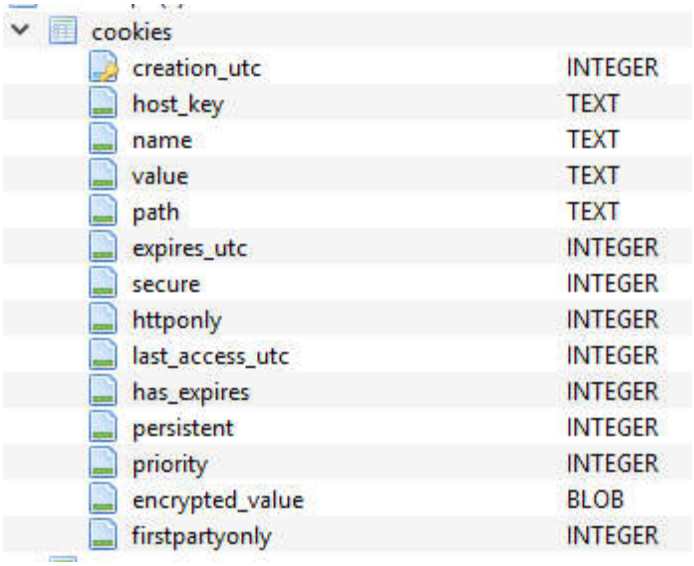

Рисунок 2 – Структура файла базы данных используемого для хранения cookie

Хотя, поле encryped_value таблицы cookies является зашифрованным, это не означает, что пользовательские данные хранятся достаточно надежно. В качестве алгоритма шифрования здесь используется технология □r□□t□r□t□□tD□t□. Это одна из функций интерфейса DPAPI (Data Protection Application Programming Interface) в ОС Windows [1,3]. Все настройки и параметры шифрования хранятся в реестре, для каждого пользователя системы. Это означает, что записи в базе данных не удастся расшифровать на другом компьютере, однако ничего не помешает расшифровать данные на компьютере "жертвы". Именно в этом заключается проблема рассмотренная в данной статье.

В доказательство этого, на языке программирования C#, был написан код представленный в листинге 1. Внедрив этот код в приложение, которое будет

запущено на компьютере жертвы, можно расшифровать все данные содержащимся в файле базы данных, которые без труда можно будет без труда интегрировать в свой браузер (например, с помощью расширения EditMyCookie) и использовать для получения доступа к конфиденциальным данным, например аккаунтам в социальных сетях, онлайн-банкинге и прочих сервисах.

```
            using (var reader = cmd.ExecuteReader())
               {
                   while (reader.Read())
                   {
                       var cookie = new Cookie();
                       cookie.domain = reader.GetString(0);
                       var encryptedData = (byte[])reader[8];
                       var decodedData = Sys-
tem.Security.Cryptography.ProtectedData.Unprotect(encryptedData, null, Sys-
tem.Security.Cryptography.DataProtectionScope.CurrentUser);
                       var plainText = Encoding.ASCII.GetString(decodedData);
                       cookie.value = plainText;

                       yield return cookie;
                   }
               }
```

Листинг 1 – Фрагмент исходного кода алгоритма расшифровки cookie

Вывод: большинство современных браузеров уязвимо к подобному методу атаки, что в свою очередь означает, что данные миллионов пользователей современных веб-приложений потенциально находятся под угрозой неправомерного доступа. Самый действенный способ защиты от подобных атак – проявлять бдительность при работе в интернете, не скачивать и не устанавливать программное обеспечение от неизвестных разработчиков и использовать антивирусное ПО.

Литература

1. Лебеденко А.В., Артеменко М.А., Кушнарев А.А. Исследование уязвимостей в хранении интернет - браузером конфиденциальных данных. / А.В. Лебеденко, М.А. Артеменко, А.А. Кушнарев. // Новая наука: опыт, традиции, инновации, ООО “Агентство международных исследований”, Уфа, 2016. – С. 78-82. ISSN: 2412-9747

2. Хвостенко Т.М., Булучев Валентин, Баранов Алексей. Дискуссия на тему: Браузеры. / Хвостенко Т.М., Булучев Валентин, Баранов Алексей. // Вестник образовательного консорциума среднерусский университет. Информационные технологии, БИУП, Брянск, 2013. – С. 38-41.

3. Гордейчик С.В. Оценка защищенности интернет-пользователей / С.В. Гордейчик // Безопасность информационных технологий, классное снаряжение, москва, 2011, - С. 103-107. ISSN: 2074-7128/EISSN: 2074-712