пользователей [1]. Запретить им никто не может, потому что все находятся в равных условиях, обладают равными правами и могут в равной степени исполнять и даже нарушать свои обязанности. Все пользователи blockchain образуют собой сеть компьютеров, на каждом из которых хранится копия данных blockchain. Обычно это полная копия всех блоков, но, в принципе, можно хранить лишь нужные на конкретном компьютере данные. Благодаря этому выключить или сломать blockchain практически невозможно, поскольку для этого надо выключить или сломать все компьютеры. Пока есть хоть один пользователь, blockchain существует [1]. Каждый новый пользователь расширяет и укрепляет эту сеть. Причем все компьютеры равноправны, там нет организаторов, модераторов, контролеров и менеджеров. Каждый отвечает за себя сам. Криптография – это основа blockchain, которая обеспечивает работу системы. Криптография в blockchain гарантирует безопасность, причем основанную на прозрачности и проверяемости всех операций. Различные криптографические техники гарантируют неизменность журнала транзакций blockchain, решают задачу аутентификации и контролируют доступ к сети и данным в blockchain в целом. Исходя из вышеизложенного, можно сделать вывод о том, что использование описанной технологии позволяет достаточно надежно осуществлять защиту информации. Рассмотренная технология достаточно успешно используется авторами работы.

Литература

1. Antonopoulos, A. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, 2014. 298 p.

МЕТОДЫ ЗАЩИТЫ ОТ SQL-ИНЪЕКЦИЙ

М.П. Хоронеко, М.А. Медунецкий, А.С. Летохо

SQL-инъекции были и остаются наиболее критичными уязвимостями приложений. Обычно атаки типа SQL-инъекций рассматривают относительно web-приложений, однако данной уязвимости подвержены любые клиент-серверные и сервис-ориентированные приложения, работающие с системами управления базами данных. SQL-инъекция – это атака, при которой злоумышленник производит вставку вредоносного кода в строки, передающиеся на сервер СУБД для синтаксического анализа и выполнения. Данная уязвимость состоит в том, что веб-приложение некорректно проверяет данные от пользователя, которые в дальнейшем используются для генерации SQL-запросов к базе данных.

SQL-инъекции можно классифицировать следующим образом:

1) по месту нахождения в запросе (инъекции в строковом параметре и в числовом параметре);

2) по способу внедрения инъекции (обычные и «слепые»).

Для успешного внедрения SQL-инъекций необходимо знать следующие параметры: способ передачи данных в веб-приложении, тип и версию СУБД, имя текущего пользователя, назначенные роли и системные привилегии.

В зависимости от назначенных текущему пользователю ролей и привилегий злоумышленник может попытаться извлечь хэши паролей пользователей СУБД, получить структуру БД и конфиденциальные данные или выполнить команды ОС, а также доступ к функциональным возможностям СУБД, а в некоторых случаях – к операционной системе сервера, на котором функционирует СУБД.

Приведем основные методы защиты веб-приложений:

– максимально возможная фильтрация данных;

– использовать при сравнении кавычки SELECT ...WHERE name='$name';

– фильтрация символов “%” и “_” при использовании SQL-функции LIKE.

– создание белого списка запросов на которые будет отвечать приложение.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ANGULAR ПРИЛОЖЕНИЙ

А.Л. Хотеев, А.С. Дроздов, Н.В. Харитонов, Е.И. Нехведович

Мир программного обеспечения эволюционирует с огромной скоростью. Всего пару лет назад настольные компьютеры и ноутбуки являлись основными устройствами, под которые

ориентировалась веб-разработка. Сегодня распределенные веб-приложения заменяют монолитные десктопные во многих сферах бизнеса. Поэтому крайне важно соблюдать нормы защиты веб-приложений. Фреймворк Angular.js поставляется с предварительно настроенными стратегиями по обеспечению безопасности от JSON уязвимостей и XSRF атак.

JSON уязвимости дают возможность веб-сайту третьих лиц подменить ваш URL для ресурса JSON, на запрос JSONP при определенных условиях. Для защиты от данного вида атаки сервер добавляет префикс ")]}',n" для всех ответов на запросы в формате JSON. Angular.js будет автоматически вырезать префикс перед обработкой ответа в формате JSON.

CSRF – вид атак на посетителей веб-сайтов, использующий недостатки протокола HTTP. Смысл атаки заключается в выполнении нежелательных действий на сайте ом имени аутентифицированного там пользователя. Angular.js предоставляет следующий механизм защиты от CSRF. При выполнении запросов XHR сервис $http считывает токен из файла cookie (по умолчанию XSRF-TOKEN) и задает его в качестве заголовка HTTP (по умолчанию X-XSRF-TOKEN). Поскольку только JavaScript, который работает на вашем домене, может читать cookie, ваш сервер может быть уверен, что XHR пришел из JavaScript, работающего на вашем домене. При первом GET запросе сервер возрващает в файле cookie токен с именем XSRF-TOKEN. Последующие XHR запросы сервер способен проверить, сравнивая значение coockie и присланного HTTP заголовка X-XSRF-TOKEN, чтобы удостовериться, что запрос не подделанный. Токен должен быть уникальным для каждого пользователя.

Литература

1. The Cross-Site Request Forgery (CSRF/XSRF) [Электронный ресурс]. – URL http://www.cgisecurity.com/csrf-faq.html (дата обращения: 16.05.2018).

2. Официальная документация по AngularJS [Электронный ресурс]. – URL: https://docs.angularjs.org/api/ng/service/$http (дата обращения: 16.05.2018).

ЭЛЕКТРОМИГРАЦИОННЫЕ ПРОЦЕССЫ В МЕЖСОЕДИНЕНИЯХ ИНТЕГРАЛЬНЫХ МИКРОСХЕМ

А.Г. Черных, В.В. Шульгов

Информационная безопасность требует совершенствования элементной базы микроэлектронных устройств защиты информации. По мере уменьшения размеров и совершенствования структуры микроэлектронных устройств возрастает роль многоуровневой системы межсоединений интегральных микросхем (ИМС) и основным ограничительным фактором в системе межсоединений является электромиграционная стойкость.

В работе представлены методы, которые позволяют провести оценку электромиграционной стойкости металлических межсоединений ИМС. Основные методы испытаний на стойкость к электромиграции условно можно разделить на испытания структур в составе корпуса (EM PLR) и испытания структур в составе пластины (EM WLR). При EM PLR испытания на электромиграцию проводятся в составе корпуса при постоянном токе и температуре К методам WLR–испытаний на отказ, вызванный электромиграцией, относят: изотермический тест (ISOT) и стандартный тест для ускорения электромиграции в структурах на пластине (SWET). Проведен анализ указанных методов, показано, что выбор метода зависит от задач, поставленных перед исследованиями.

Проведены исследования параметров электромиграции в межсоединениях ИМС на тестовых структурах с алюминиевой пленкой, а также сплавов Al+2%Cu и Al+1%Ho. После окончания электромиграционного теста структуры исследовали на оптическом и сканирующем электронном микроскопе, а микроструктуру пленок исследовали методом, основанном на дифракции обратно рассеянных электронов в электронном микроскопе. Проведенные исследования показали, что при наличии в алюминиевых пленках 2%Cu и 1%Ho приводит к малому порообразованию и следовательно к меньшему сопротивлению, чем в чистой алюминиевой пленке. Представлена корреляция полученных результатов для различных методов испытаний.