Лучшая защита от фишинга – знания. Злоумышленники, занимающиеся фишингом, стремятся выглядеть как можно более убедительно, но зачастую их можно раскрыть по контрольным признакам. Обязательное регулярное обучение основам информационной безопасности и социальной инженерии – это отличный способ предотвращения, который поможет вашей организации выявлять признаки вредоносных электронных писем:

- не доверяйте;
- узнайте какая информация о вас в сети;
- изучите ссылку;
- не переходите по ссылке;
- грамотно управляйте своими паролями;
- регулярное обновление ПО;
- защищайте данные.

УДК [004.056+003.26](075.8)

Студ. А.А. Иванова, К.А. Крайнов
Науч. рук. проф. Урбанович П.П
(кафедра информационных систем и технологий БГТУ)

АНАЛИЗ ЦЕЛЕСООБРАЗНОСТИ И ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В WEB-ПРИЛОЖЕНИЯХ

Мы считаем, что недостаточно знать теорию для понимания истинного масштаба угрозы для информационных ресурсов – ведь уязвимости любого уровня, зачастую могут нести катастрофические последствия [1, 2]. Классификацией векторов атак и уязвимостей занимается сообщество OWASP. Эта организация создала список из 10-и самых опасных векторов атак на Web-приложения [3, 4]. Эти типы уязвимостей будут рассмотрены далее.

Инъекции. Все данные, хранятся в базах данных, обращения к которым строятся в виде запросов, чаще всего написанных на специальном языке запросов SQL. Злоумышленник может внедрить в форму web-интерфейса приложения специальный код, содержащий кусок SQL-запроса. Это уязвимость позволяет злоумышленнику получить доступ к данным и возможность читать/изменять/удалять информацию, которая для него не предназначена.

Недочеты системы аутентификации и хранения сессий. Для того, чтобы отличать одного пользователя от другого, web-приложение использует так называемые сессионные куки. Если ваш идентификатор украдет злоумышленник, а в системе не были реализованы проверки

IP-адреса сессии или наличия более одного соединения в одной сессии, злоумышленник сможет получить доступ в систему с правами владельца.

Межсайтовый скриптинг – XSS. Это еще одна ошибка валидации пользовательских данных, которая позволяет передать JavaScript код на исполнение в браузер пользователя. Атаки такого рода часто также называют HTML-инъекциями, так как внедряемый код исполняется в браузере пользователя.

Небезопасные прямые ссылки на объекты. Такой вид уязвимости является также следствием недостаточной проверки пользовательских данных. Суть ее заключается в том, что при выводе каких-либо конфиденциальных данных, для доступа к объекту используется идентификатор, который передается в открытом виде в адресной строке браузера. Например, есть страница, которая отображает личное сообщение, и она имеет адрес вида:mysite.ru/read_message.jsp?id=123654. Перебирая число после "id=" можно будет читать чужие личные сообщения.

Небезопасная конфигурация. Безопасность web-приложения требует наличия безопасной конфигурации всех компонентов инфраструктуры. Настройки компонентов сервера по умолчанию зачастую небезопасны и открывают возможности к атакам. Например, кража сессионной cookie через JavaScript при XSS-атаке становится возможна благодаря выключенной по умолчанию настройке cookie_http only. При правильной настройке сервера, получить сессионную cookie через JavaScript невозможно.

Незащищенность критичных данных. Самый простой пример – передача данных по протоколу HTTP. Данные, передаваемые этому по протоколу, не шифруются, а при прохождении данных от компьютера пользователя до web-сервера они пройдут достаточно много различных узлов. На каждом из этих узлов может затаиться программа, которая считывает весь трафик и передает злоумышленнику. Такие данные должны передаваться исключительно по протоколу HTTPS, который требует наличие SSL-сертификата.

Отсутствие функций контроля доступа. Суть уязвимости заключается в отсутствии проверки наличия надлежащего доступа к запрашиваемому объекту. Большинство приложений проверяют права доступа, прежде чем отобразить данные в пользовательском интерфейсе. Есть множество вспомогательных служебных запросов, которые, зачастую отправляются в фоновом режиме асинхронно, при помощи технологии AJAX. Если параметры запроса недостаточно тщательно проверяются, злоумышленники смогут подделать запрос для доступа к данным без надлежащего разрешения.

Межсайтовая подделка запроса (CSRF/XSRF). Атаки позволяют злоумышленнику выполнять от имени жертвы действия на сервере. Например, в некоторой платежной системе для перевода средств на другой аккаунт, есть страница вида: bank.com/money.jsp?amount=10&account=123. Где amount – сумма для перевода и account – номер аккаунта, куда должны быть переведены средства. Если жертва заходит на сайт, созданный злоумышленником, от её лица тайно отправляется запрос на вышеуказанную страницу платежной системы. В итоге деньги уйдут на счет злоумышленника. Предполагается, что жертва должна была предварительно пройти аутентификацию в платежной системе.

Использование компонентов с известными уязвимостями. Зачастую web-приложения написаны с использованием специальных библиотек или «фреймворков», которые поставляются сторонними компаниями. В большинстве случаев эти компоненты имеют открытый исходный код, а это означает, что они есть не только у вас. Также уязвимости ищут (и находят) в более низкоуровневых компонентах системы, таких как сервер базы данных, web-сервер, и наконец, компоненты операционной системы вплоть до ее ядра. Очень важно использовать последние версии компонентов и следить за появляющимися известными уязвимостями на сайтах типа securityfocus.com.

Непроверенные переадресации и пересылки. Web-приложения зачастую переадресуют пользователя с одной страницы на другую. Атакующий может использовать такие страницы для переадресации жертвы на подложный сайт, который может иметь очень схожий или неотличимый интерфейс, это может привести к краже конфиденциальных данных.

Мы рассмотрели основные виды уязвимостей, постарались рассказать о них максимально простым языком, а также показать на простых практических примерах, какие риски несут для бизнеса те или иные атаки. В ходе исследования мы выяснили, что web-приложение может быть атаковано с любой стороны, что, в свою очередь, показывает, что даже самое простое web-приложение необходимо защищать хотя бы самыми базовыми способами. Это может минимизировать количество взломов и утечек данных из приложения.

ЛИТЕРАТУРА

1. Урбанович, П. П. Киберпространство: тренды, угрозы и безопасность / П. П. Урбанович // Интеграция и развитие научно-технич. и образовательного сотрудничества – взгляд в будущее: сборник статей II Междунар. научно-техн. конф. "Минские научные чтения – 2019", Минск, 11-12 декабря 2019 г.: в 3 т. Т. 3. – Минск: БГТУ, 2020. – С. 180–185.

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

2. Хоффман, Э. Безопасность веб-приложений/ Э. Хоффман. – М.: Прогресс-книга, 2021. – 330 с.

3. Тронкон, П. Bash и кибербезопасность: атака, защита и анализ из командной строки Linux/ П.Тронкон, К.Олбинг. – СПб.: Питер, 2020. – 288 с.

УДК 004.93

Маг. В.Д. Колодкин
Науч. рук. доц. Н.А. Жиляк
(кафедра информационных систем и технологий, БГТУ)

МЕТОД ОПТИМИЗАЦИИ ИНФОРМАЦИОННОГО МОДЕЛИРОВАНИЯ СИСТЕМ БЕЗОПАСНОСТИ

Методы проектирования с каждым годом становятся все прогрессивнее, применяется современное программное обеспечение, в результате чего возрастает эффективность труда и уменьшается время на разработку конкретного проекта. Процесс перехода от традиционных методов проектирования к BIM технологиям в первую очередь обусловлен быстрым развитием информационных технологий и появлением на рынке специализированного программного обеспечения, при использовании которого появляется возможность создания цифровой информационной модели объекта строительства. Существование данной модели позволяет использовать огромное количество средств автоматизированного управления, анализа и проверок; выпуска рабочей и проектной документации; совершенствования процесса строительства и визуального управления, оценки и анализа сметной стоимости и. т.д., но также позволит всем задействованным участникам проекта получать доступ к информации об объекте. Несомненным плюсом BIM-моделей является их взаимозаменяемость, т. е. при замене или изменении отдельных частей, компонентов информационной модели произойдет автоматическое обновление ее конфигурации, а также параметров связанных документов.

Логика BIM-моделирования часто бывает слишком тяжеловесной для решения простых задач. Чтобы обойти ограничения стандартных инструментов, оптимизировать работу вBIM-программе или расширить её возможности, можно использовать плагины. Плагины – это программные модули или файлы, которые добавляют дополнительные