МОДЕЛЬ ОЦЕНКИ КАЧЕСТВА WEB-ПРИЛОЖЕНИЙ, ОСНОВАННАЯ НА ОБНАРУЖЕНИИ УЯЗВИМОСТЕЙ К SQL-ИНЪЕКЦИЯМ

Оношко Д.Е., Бахтизин В.В.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Беларусь, onoshko@bsuir.by, bww@bsuir.by

Abstract. Factors affecting the quality of web-applications in the context of distance learning are presented. A brief description of an SQL-injection vulnerability detection method is given. A quality model based on the results of vulnerability detection process is proposed.

Важной задачей при организации дистанционного обучения является обеспечение эффективного взаимодействия участников учебного процесса. В настоящее время наиболее широкое распространение в этой области получили web-приложения. Вместе с тем, значительное количество пользователей по сравнению с другими видами приложений обусловливает повышенные требования к качеству web-приложений. Кроме того, поскольку возможность несанкционированного доступа и модификации информации, находящейся под управлением web-приложения для дистанционного обучения может представлять интерес для студентов, а доступ к web-приложению могут иметь не только участники учебного процесса, особые требования предъявляются к свойствам web-приложений, лежащим в области информационной безопасности.

Наиболее распространённым и серьёзным видом дефектов web-приложений по состоянию на 2017 год по данным OWASP остаются уязвимости к инъекциям, среди которых значительную долю составляют SQL-инъекции [1]. Сущность этого дефекта заключается в наличии в коде web-приложения логических ошибок, из-за которых данные, поступающие извне, поступают в текст запроса к системе управления базами данных (СУБД) без предварительной обработки.

Несмотря на то, что подобные ошибки являются логическими, они имеют ряд свойств, позволяющих дать их формализованное описание, что, в свою очередь, позволяет разработать модель [2] и метод [3] обнаружения уязвимостей к SQL-инъекциям в web-приложениях, основанные на статическом анализе исходных кодов с элементами абстрактной интерпретации.

Основой для метода обнаружения уязвимостей является разбиение web-приложения на множество составляющих его процедур $P = \{p_1, \ldots, p_N\}$, $N > 0$, каждая из которых характеризуется некоторым набором параметров. В ходе анализа параметры получают оценки, характеризующие способность соответствующих процедур противостоять SQL-инъекции при получении данных через эти параметры. В общем случае система оценок является бинарной, однако может быть расширена для адаптации метода к требованиям конкретного проекта, а также с целью минимизации ложноположительных результатов.

Оценки для стандартных процедур известны заранее. Для определения порядка, в котором следует производить оценку процедур, строится граф зависимостей (ориентированный), вершины которого соответствуют процедурам web-приложения, а дуги – вызовам процедур в направлении от вызывающей к вызываемой. Пример такого графа приведён на рисунке 1.

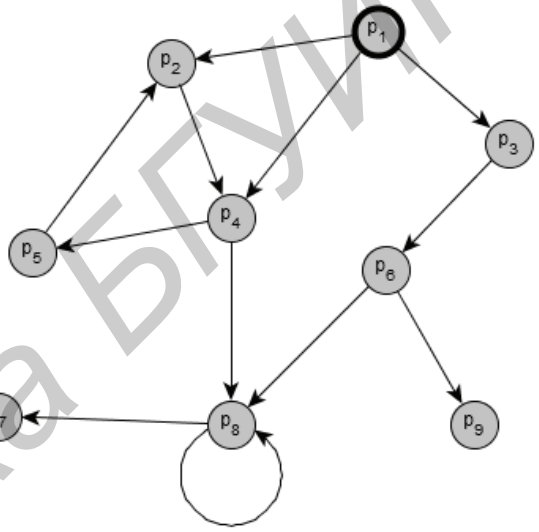

Рисунок 1 – Пример графа зависимостей web-приложения

Граф зависимостей позволяет также обнаруживать рекурсивные вызовы, которые являются потенциально проблемными для анализа участками web-приложения.

Поскольку графы зависимостей реальных web-приложений характеризуются значительными размерами, обнаружение уязвимостей целесообразно проводить в автоматизированном режиме с использованием программного средства (ПС) обнаружения уязвимостей. Важным преимуществом такого подхода является возможность сбора дополнительной информации о web-приложении, которая в дальнейшем может быть использована для оценки его качества.

Актуальным международным стандартом, регламентирующим вопросы оценки качества программных средств, в настоящее время является ISO/IEC 25010:2011 [4]. Модель качества продукта, приводимая в этом стандарте, является трёхуровневой и состоит из характеристик и подхарактеристик и мер, причём только набор мер может подвергаться изменениям, тогда как характеристики и подхарактеристики определяют структуру модели качества.

С точки зрения последующего использования оптимальными являются меры, значения которых являются относительными величинами и лежат в диапазоне [0;1]. Для вычисления таких мер оптимальными являются формулы вида:

$$X = \frac{A}{B}; \quad (1)$$

$$X = 1 - \frac{A}{B}, \quad (2)$$

где X – значение меры; A – абсолютная величина, характеризующая то или иное свойство ПС, $A \geq 0$; B – абсолютная величина, характеризующая максимально возможное значение величины A, $B > 0$.

В модель оценки качества web-приложений в контексте обнаружения уязвимостей предлагается включать, среди прочих, меры, приведённые в таблице 1.

Таблица 1 – Меры качества web-приложений в контексте обнаружения уязвимостей

Мера	Формула	Описание
Достаточность обработки данных	2	A – количество точек входа данных, допускающих проведение атак; B – общее количество точек входа данных.
Стабильность при внесении изменений	1	A – количество in-параметров с оценкой U; B – общее количество in-параметров. Учитываются in-параметры всех процедур, кроме стандартных.
Корректность обработки данных	1	A – количество in-параметров, для которых соблюдаются правила передачи данных; B – общее количество in-параметров.
Избыточность обработки данных	1	A – количество in-параметров, при передаче которых оценка данных выше (лучше) оценки формального параметра; B – общее количество вызовов с передачей данных в in-параметры. Учитываются in-параметры всех процедур, кроме стандартных.
Анализируемость обработки данных	2	A – количество in-параметров с оценкой UDS; B – общее количество in-параметров с оценками S или UDS.
Устойчивость к SQL-инъекциям	2	A – количество in-параметров, получающих данные с оценкой ниже (хуже) оценки формального параметра; B – общее количество in-параметров. Учитываются только in-параметры для процедур взаимодействия с СУБД.

Приведённые меры предлагается включать в модель качества в соответствии с диаграммой, приведённой на рисунке 2.

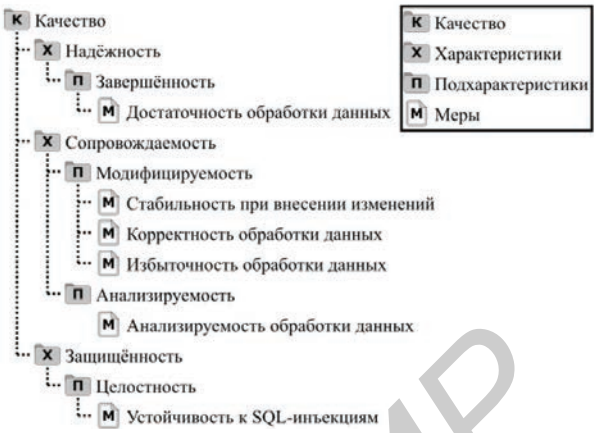

Рисунок 2 – Модель качества web-приложений в контексте обнаружения уязвимостей

Для получения интегральной оценки качества предлагается использовать формулы, аналогичные приведённым в ГОСТ 28195-99 [5]. При этом рекомендуется выбирать весовые коэффициенты так, чтобы выполнялись условия

$$\sum_{k=1}^{m} V_{jk}^{M} = 1; \quad (3)$$

$$\sum_{j=1}^{s} V_{ij}^{S} = 1; \quad (4)$$

$$\sum_{i=1}^{c} V_{i}^{C} = 1, \quad (5)$$

где V_{jk}^{M} – весовой коэффициент k-й меры j-й подхарактеристики, V_{ij}^{S} – весовой коэффициент j-й подхарактеристики i-й характеристики, V_{i}^{C} – весовой коэффициент i-й характеристики качества.

Полученная оценка может использоваться в качестве исходных данных для обеспечения качества web-приложения на всех этапах жизненного цикла с момента появления прототипа.

Литература

1. OWASP Top 10 2017. The Ten Most Critical Web Application Security Risks. Release Candidate 2. [Электронный ресурс.] – Режим доступа: https://www.owasp.org/images/b/b0/OWASP_Top_10_2017_RC2_Final.pdf. – Дата доступа: 12.11.2017.

2. Бахтизин, В. В. Модель обнаружения уязвимостей в web-приложениях. / В. В. Бахтизин, Д. Е. Оношко. – Доклады БГУИР. – 2016. – №1(95). – С.5-11.

3. Оношко, Д. Е. Метод обнаружения уязвимостей к SQL-инъекциям в WEB-приложениях / Д. Е. Оношко, В. В. Бахтизин // Технологии информатизации и управления: сб. научн. ст. Вып 3. В 2 кн. Кн. 1 / под ред. А. М. Кадана, Е. А. Свирского. – Минск: РИВШ, 2017. – С.66-76.

4. ISO/IEC 25010:2011. Системная и программная инженерия. Требования к качеству и оценка программного продукта (SQuaRE). Модели качества систем и программных средств.

5. ГОСТ 28195-99. Оценка качества программных средств. Общие положения.