ПРОГРАММНОЕ СРЕДСТВО ОЦЕНКИ НАДЁЖНОСТИ WEB-ПРИЛОЖЕНИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Оношко Д. Е.

Бахтизин В. В. – к.т.н., доцент

Переход к использованию распределённых систем обработки информации привёл к увеличению доли web-приложений в общей массе разрабатываемых программных средств. Однако в отличие от desktop-приложений web-приложения доступны для непосредственного воздействия любому пользователю сети Internet, поэтому к надёжности таких приложений предъявляются повышенные требования.

Как правило, проблемы безопасности, обнаруживаемые в web-приложениях, возникают из-за некорректной обработки поступающих от пользователя данных, поэтому наиболее уязвимой частью таких ПС остаётся код, отвечающий за обмен данными с пользователем. Наличие в нём ошибок может быть использовано злоумышленником для выполнения произвольных действий на сервере приложений или компьютерах других пользователей ПС.

Единственный способ обнаружения всех подобных ошибок — анализ исходных кодов — является рутинной процедурой, трудоёмкость которой очевидно выше трудоёмкости разработки оцениваемого ПС. Поэтому целесообразно использование автоматизированных средств контроля качества кода, ориентированных на обнаружение типовых уязвимостей. Числовые характеристики, получаемые в результате такого анализа, могут использоваться для оценки общего уровня надёжности анализируемого ПС.

Для формализации получаемых анализатором результатов предлагается ввести понятие «точка входа данных» и определить его как семантически неделимую единицу данных, поступающих в оцениваемое ПС извне. Примерами таких точек входа могут быть поля ввода имени пользователя, пароля, текстов сообщений и т.д. При этом анализатор должен не только обнаруживать уязвимости, но и определить множество точек входа, которые могут быть использованы злоумышленником для их эксплуатации. Тогда в качестве одной из числовых характеристик надёжности ПС может использоваться отношение количества неэксплуатируемых точек входа к их общему количеству.

Необходимость выявлять не только потенциальные проблемы, но и связанные с ними точки входа предопределяет наличие в составе анализатора модулей, выполняющих лексический, синтаксический и семантический анализ исходных кодов оцениваемого ПС. Автоматизированная оценка возможности использования точек входа для осуществления атак может быть реализована за счёт применения структуры данных, описывающей пути прохождения данных в анализируемом веб-приложении и содержащей оценки для отдельных элементов этих путей — переменных, формальных параметров процедур и т.п. Такая структура данных может быть получена в результате семантического анализа и в общем случае представляет собой ориентированный граф.

В простейшем случае оценка элементов путей прохождения данных может носить бинарный характер: «опасные» или «безопасные». При этом следует отметить, что одна и та же оценка будет иметь различный смысл для переменных и формальных параметров процедур. Оценка переменной показывает, прошли ли содержащиеся в переменной данные обработку, которая исключает их использование для выполнения атаки. В то же время оценка формального параметра процедуры определяет, какую оценку должна иметь переменная, передаваемая в качестве фактического параметра, чтобы вызов процедуры не создавал условий для возникновения уязвимости. При этом можно сформулировать следующие правила, соблюдение которых делает вызов процедуры корректным:

1. Если формальный параметр процедуры имеет оценку «безопасные», то фактический параметр должен иметь оценку «безопасные».

2. Если формалный параметр процедуры имеет оценку «опасные», то фактический параметр может иметь любую оценку.

Для практических целей шкала оценок может быть расширена. Так, например, некоторые последовательности преобразований, не известные анализатору заранее, могут делать данные безопасными, но автоматизированное определение того, является ли некоторое преобразование таковым, крайне затруднено, поскольку требует детального анализа семантики кода. Реализация такого функционала может существенно повысить сложность анализатора, почти не повышая его эффективности: может быть достигнуто только снижение количества ложных срабатываний.

По этой причине целесообразно предоставить пользователю ПС анализа исходных кодов возможность явно указать, что та или иная процедура производит преобразование, приводящее данные в безопасный для дальнейшего использования формат. Для данных, безопасность которых обеспечивается таким образом, нежелательно применять оценку «безопасные». Вместо этого имеет смысл применить оценку «условно безопасные», что позволит предоставить пользователю возможность осуществлять выбор между полностью автоматизированным обнаружением уязвимостей и режимом обнаружения, учитывающим рекомендации пользователя. При этом необходимо скорректировать множество применяемых правил соответствия формальных и фактических параметров.

Предложенное ПС для анализа исходных кодов должно позволить автоматизировать процесс оценки надёжности web-приложений и, как следствие, снизить стоимость их разработки.