POSITIVE TECHNOLOGIES

ЗАО / ПОЗИТИВ ТЕКНОЛОДЖИЗ
107241 / МОСКВА / ЩЕЛКОВСКОЕ ШОССЕ / Д.23А
ТЕЛ.: +7 (495) 744 01 44 / ФАКС: +7 (495) 744 01 87 / PT@PTSECURITY.RU
WWW.PTSECURITY.RU / WWW.MAXPATROL.RU / WWW.SECURITYLAB.RU

АНАЛИЗ И ОЦЕНКА БЕЗОПАСНОСТИ WEB-ПРИЛОЖЕНИЙ

Сергей Гордейчик, системный архитектор компании Positive Technologies

Безопасность Web-приложений уже не первый год является важным элементом защиты информационных систем. Учитывая тенденцию к переносу стандартных клиент-сервеных приложений в Web-среду, растущую популярность технологий AJAX и других элементов Web 2.0 можно констатировать, что с течением времени актуальность защиты онлайн-приложений только возрастет.

Не смотря на это, индустрия пока не сумела сформировать адекватный ответ на угрозы, возникающие при использовании Web-систем. Как показывает опыт по проведению тестов на проникновение и аудитов информационной безопасности - уязвимости в Web-приложениях являются одними из наиболее распространенных недостатков защиты сетевой безопасности. Общемировая [1] и российская статистика [2] показывает, что в более чем шестидесяти процентов сайтов обнаруживаются критичные уязвимости, а в девяносто трех случаев из ста в программном обеспечении Web-приложения содержатся уязвимости средней степени риска. Причем наиболее распространенными уязвимостями являются "Межсайтовое выполнение сценариев", "Внедрение операторов SQL" и различные варианты утечки информации, которые широко описаны в "научно-популярной" и специализированной литературе, а также с высокой степенью достоверности могут быть обнаружены с помощью автоматизированных средств, таких как сканеры уязвимостей.

В качестве основных подходов, используемых для защиты Web-приложений можно выделить:

- использование Web Application Firewall;

- тесты на проникновение и полный анализ защищенности, включая анализ исходного кода;

- безопасность как элемент SDLC.

Каждый из типов работ имеет свои достоинства и недостатки, степень охвата функций приложения.

Системы Web Application Firewall (WAF) несколько лет назад были на взлете. Было реализовано множество проектов в этом направлении и в большинстве своем они интегрированы в другие средства защиты (системы предотвращения атак, межсетевые экраны). Силами сообщества были выработаны критерии для оценки подобных систем [3]. Однако сейчас функции WAF в полном объеме используются крайне редко. Это связанно, прежде всего, с тем, что такие системы не работают «из коробки» и требуют серьезной настройки для эффективной работы с одной стороны и минимизации ложных срабатываний с другой.

Тесты на проникновение и полный анализ защищенности, являются наиболее распространенным подходом к повышению защищенности Web-приложений. В зависимости от используемых методик степень покрытия API приложения [4] составляет от 23 до 96%. В качестве критериев оценки обычно используется комбинация «белого списка» необходимых функций безопасности и «черного списка» известных уязвимостей. Для формирования «белого списка» хорошо подходит раздел требований к функциям безопасности (security functional

requirements) ISO 15408 «Общие критерии оценки безопасности информационных технологий». Черный список, как правило, формируется на основе Open Web Application Security Project Top Ten [5] и Web Security Threat Classification [6].

Анализ защищенности не лишен недостатков. Зачастую работы проводятся в конце цикла разработки приложения, что увеличивает затраты на внесение изменений и вызывает серьезное противодействие со стороны разработчиков. Качество работ очень сильно зависит от используемых методик и уровня аудиторов.

Учет аспектов безопасности в рамках цикла разработки программного обеспечения является эффективным, но и наиболее редко используемым подходом. При ранних инвестициях в безопасность требования по защите учитываются на уровне дизайна и разработки, что снижает количество возможных проблем и упрощает дальнейшее поддержание системы в защищенном состоянии.

[1] Web Application Security Consortium, «Web Application Security Statistics»

http://webappsec.org/projects/statistics/

[2] Positive Technologies, «Статистика уязвимости Web-приложений за 2007 год»

http://www.ptsecurity.ru/stat2007.asp

[3] Web Application Security Consortium, «Web Application Firewall Evaluation Criteria»

http://webappsec.org/projects/wafec/

[4] A Fortify Research Report, "Taking the blinders off black box security testing" http://www.bitpipe.com/detail/RES/1164731890_782.html?src=econsult

[5] Open Web Application Security Project, «OWASP Top Ten»,

http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[6] Web Application Security Consortium, «Web Security Threat Classification»

http://webappsec.org/projects/threat/