Универсальный метод защиты веб-приложений

Адамов Андрей Владимирович
ГОУ ВПО "Тюменский государственный университет"(Тюмень), Россия

Бабич Андрей Владимирович
ГОУ ВПО "Тюменский государственный университет"(Тюмень), Россия
e-mail: andrey.post@gmail.com

Работа посвящена анализу универсальных методов обеспечения безопасности веб сайтов. В частности, рассматривается такая технология как Web Application Firewall (WAF).
По данным статистики WASC (Web Application Security Consortium)[1], более 13% сайтов могут быть скомпромитированы полностью автоматически, 80-96% из которых имеют высокую степень уязвимостей, 86% — среднюю степень уязвимостей, 37% — низкую.
WAF — это межсетевой экран, накладывающий определенный набор правил на то, как происходит взаимодействие сервера и клиента, обрабатывая HTTP-пакеты. В основе лежит тот же принцип, что и в обычных фаерволах — контроль и анализ всех пакетов, поступающих от клиента. WAF опирается на набор правил, с помощью которого выявляется факт атаки по сигнатурам — признакам активности пользователя, которые могут означать нападение.
Основной задачей WAF является снижение угроз за счет минимизации влияния человеческого фактора на безопасность сайтов.
Web Application Firewall разделяют на 2 типа: аппаратный и программный.
Обработка правил в WAF может осуществляться по принципу blacklist, whitelist или смешано.
На сегодняшний день, почти все брандмауэры веб приложений призваны защитить от основных типов угроз свойственных веб сайтам:
? SQL инъекция
? Межсайтовый скриптинг (XSS)
? Межсайтовые подделки запросов (CSRF)
? Спам в комментариях
? Распределенный отказ в обслуживании (DDoS-атаки)
? Отсутствие таймаута сессии
? Обратный путь в директориях
Основной проблемой, существующей на данный момент, являются ограниченные возможности текущей технологии WAF в обеспечении защиты от широкого спектра угроз. А также возможность обхода существующих на данный момент брандмауэров [2].
Один из возможных вариантов решения указанной проблемы видится в применении методов поведенческого анализа. Принцип такого подхода в корне отличается от сигнатурного. Здесь за основу берется нормальное поведение, а целью является обнаружение отклонений. К примеру, в скрипте С чтение из таблицы А — нормально, если происходит чтение из таблицы Б, это считается аномальным. Данный подход, в теории, может закрыть недостатки существующих WAF основанных на сигнатурном анализе.

Список литературы

1. Статистика уязвимостей Web-приложений за 2008 год – Режим доступа: http://ru.scribd.com/doc/21324267/WASC-Web-Application-Security-Statistics-2008-Russian
2. Дмитрий Евтеев, Методы обхода Web Application Firewall – Режим доступа: http://www.ptsecurity.ru/download/PT-devteev-CC-WAF.pdf
3. ModSecurity – Режим доступа: http://modsecurity.org,
4. Barracuda Networks, Inc. (US) – Режим доступа: http://barracudanetworks.com,