УДК 004.492

АНАЛИЗ МЕТОДОВ ПРЕДОТВРАЩЕНИЯ ОБХОДА МЕЖСЕТЕВОГО ЭКРАНА ВЕБ-ПРИЛОЖЕНИЙ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ОБРАБОТКИ ВРЕДОНОСНЫХ ЗАПРОСОВ

Крылов И.Д. (ИТМО)

Научный руководитель – доктор технических наук, старший научный сотрудник, профессор Швед В.Г. (ИТМО)

Введение. Существующие правила обработки входящих запросов в межсетевых экранах веб-приложений (WAF) подвергаются обходу со стороны злоумышленников, тем самым появляется повышенный риск эксплуатации существующих уязвимостей в веб-приложениях и компрометации защищаемой информации. Проблема некачественной настройки правил фильтрации входящего трафика в WAF является актуальной для пользователей данной технологии по сей день. Есть необходимость проработки методов предотвращения обхода межсетевых экранов веб-приложений [1].

Основная часть. Рассматриваются методы предотвращения обхода межсетевых экранов веб-приложений, охватывающие различные аспекты, такие как обнаружение и блокировка символьных методов обхода, контроль целостности запросов, управление сессиями, валидация заголовков. Данные методы необходимо использовать в системе для повышения уровня защищенности и снижения рисков обхода WAF.

Обнаружение и блокировка символьных методов обхода производится за счет применения регулярных выражений для поиска характерных последовательностей в запросе. Контроль целостности запросов производится посредством высчитывания хэш-функции содержимого запроса, после чего сравнивает полученное значение с исходным. Метод управления сессиями сконцентрирован на аутентификацию пользовательских сессий для предотвращения поддельных запросов и атак с использованием украденных сессий. Метод валидации заголовков представляет собой проверку HTTP-запросов на соответствие ожидаемым стандартам и формам [2].

Выводы. В результате был проведен анализ методов предотвращения обхода WAF, для каждого из методов разработаны примеры эксплуатации, что в дальнейшем будет использовано для разработки методики предотвращения обхода межсетевых экранов веб-приложений.

Список использованных источников

1. Колегов Д. Н., Брославский О. В., Олексов Н. Е. Неинвазивный метод контроля целостности cookie в веб-приложениях //Прикладная дискретная математика. Приложение. – 2015. – №. 8. – С. 85-89.
2. Gupta S., Gupta B. B. JS-SAN: defense mechanism for HTML5-based web applications against javascript code injection vulnerabilities //Security and Communication Networks. – 2016. – Т. 9. – №. 11. – С. 1477-1495.

Автор _____ Крылов И.Д.

Научный руководитель _____ Швед В.Г.