ТЕХНИЧЕСКИЕ НАУКИ

ЗАЩИТА САЙТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Ермураков С.С.[1], Трубачева С.И.[2]

[1]Ермураков Сергей Сергеевич - студент,
кафедра информатики и систем управления, факультет информатики и телекоммуникаций;
[2]Трубачева Светлана Ивановна - кандидат технических наук, доцент, профессор,
кафедра информатики и систем управления,
Образовательная автономная некоммерческая организация
высшего профессионального образования
Волжский университет им. В.Н. Татищева,
г. Тольятти

Аннотация: *в статье анализируются наиболее распространенные уязвимости, которые активно используют злоумышленники при атаках на веб-приложения.*
Ключевые слова: *веб, сайты, защита, кибер-атака.*

Современные реалии показывают постоянно растущие атаки на веб-приложения — до 80% случаев компрометации систем начинаются с веб-приложения. В статье будут рассмотрены наиболее распространенные уязвимости, которые активно используют злоумышленники, а также эффективные методы противодействия им с использованием Web Application Firewall.

При увеличении количества инструментов и техник атак все сложнее становится обеспечить доступность сайта, защитить веб-приложение или его компоненты от взлома и подмены контента. Несмотря на усилия технических специалистов и разработчиков обороняющаяся сторона традиционно занимает догоняющую позицию, реализовывая защитные меры уже после того, как веб-приложение было скомпрометировано. Веб-сайты подвергаются атакам из-за публичной доступности, не всегда качественно написанному коду, наличию ошибок в настройке серверной части, а также отсутствующему контролю со стороны службы ИБ, тем самым обеспечивая злоумышленникам доступ к критичным данным [3].

В связи с этим возникает необходимость использовать защитные средства, учитывающие архитектуру веб-приложения, и не приводящие к задержкам в работе сайта.

Статистика показывает, что многие веб-приложения компрометируются также, как и годами ранее — это разного рода инъекции, инклуды, клиент-сайд атаки, поэтому защитное средство должно уметь выявлять и блокировать атаки, направленные на эксплуатацию следующих уязвимостей:

SQL Injection — sql инъекции;
Remote Code Execution (RCE) — удаленное выполнение кода;
Cross Site Scripting (XSS) — межсайтовый скриптинг;
Cross Site Request Forgery (CSRF) — межстайтовая подделка запросов;
Remote File Inclusion (RFI) — удалённый инклуд [1];
Local File Inclusion (LFI) — локальный инклуд;
Auth Bypass — обход авторизации [1];
Insecure Direct Object Reference — небезопасные прямые ссылки на объекты;
Bruteforce — подбор паролей.

Защита на прикладном уровне

Протокол прикладного уровня — протокол верхнего (7-го) уровня сетевой модели OSI, обеспечивает взаимодействие сети и пользователя. Уровень разрешает приложениям пользователя иметь доступ к сетевым службам, таким, как обработчик запросов к базам данных, доступ к файлам, пересылке электронной почты. Защита на прикладном уровне является наиболее надежной. Уязвимости, эксплуатируемые злоумышленниками, зачастую полагаются на сложные сценарии ввода данных

пользователем, что делает их трудноопределимыми с помощью классических систем обнаружения вторжений [4].

Одним из источников, позволяющих выявлять новые сценарии и реализацию атак на веб-приложения, являются «Лаборатории тестирования на проникновение», имитирующие реальную инфраструктуру современных компаний. В лабораториях принимают участие около 9000 специалистов по информационной безопасности со всего мира, с разным уровнем подготовки, навыков и инструментария. Анализ атак, направленных на объекты лаборатории, позволяют составить модели нарушителя и реализации векторов атаки.

Список литературы

1. *Касперски Крис.* Искусство дизассемблирования / Крис Касперски, Ева Рокко. М.: БХВ-Петербург, 2009. 896 с.
2. *Колисниченко Д.Н.* Анонимность и безопасность в Интернете. От «чайника» к пользователю / Д.Н. Колисниченко. М.: БХВ-Петербург, 2012. 240 с.
3. Руководство для программиста на Java. 75 рекомендаций по написанию надежных и защищенных программ. М.: Вильямс, 2014. 256 с.
4. *Соколов А.В.* Защита от компьютерного терроризма. Справочное пособие / А.В. Соколов, О.М. Степанюк. Москва: СИНТЕГ, 2002. 496 с.
5. *Эриксон Джон.* Хакинг. Искусство эксплойта / Джон Эриксон. М.: Символ-плюс, 2010. 512 с.

НОВЫЕ ТЕХНОЛОГИИ СТРОИТЕЛЬСТВА МНОГОЗАБОЙНЫХ СКВАЖИН

Игнатьев М.А.[1], Игнатьева А.О.[2], Ямалетдинов А.А.[3], Мухамадиев И.С.[4]

[1]Игнатьев Максим Александрович – студент;
[2]Игнатьева Анастасия Олеговна – студент;
[3]Ямалетдинов Айдар Анисович - студент;
[4]Мухамадиев Ильдар Салимянович - студент,
кафедра бурения нефтяных и газовых скважин,
Уфимский государственный нефтяной технический университет,
г. Уфа

Основная форма многозабойных скважин была предложена в 50-х годах прошлого столетия, но существующие в то время методики углубления скважин и оборудование для закачивания скважин не позволяли осуществлять их массовое строительство.

Схемы расположения многоствольных горизонтальных скважин (МСГС) в пласте представляют собой одиночную скважину, либо несколько боковых ответвлений, которые образуют, веер в горизонтальной плоскости или располагаются по вертикали друг над другом. На рисунке 1 представлены схемы ответвлений и инструмента, с помощью которого проводится отклонение строящегося ствола скважины.