БЕЗОПАСНОСТЬ В RUBY ON RAILS

И.А. Клапаток, И.В. Чибисов, А.А. Виноградов, М.А. Климович

Ruby on Rails (RoR) – это популярная среда для веб-разработки, которая считается довольно легкой в освоении. Но, как и в любых средах разработки, в этой среде также нужно защищаться от разного рода атак.

Ниже представлены распространенные атаки в RoR.

1. XSS/Межсайтовый скриптинг: XSS-атака, наиболее распространенное нарушение безопасности в проектах Ruby on Rails, она может полностью разрушить веб-приложение. Она выбирает из множества точек входа для внедрения вредоносного кода в проект. XSS-атака может быть запущена со страниц результатов поиска, сообщений, комментариев, обзоров и т. д. Здесь вредоносный код остается интегрированным в продукт приложения и доступен для пользователя.

2. CSRF: сокращение от cross-site request forgery (подделка межсайтовых запросов). Использование метода match в файле rout.rb описывает систему обработки пути на сайте. Он помогает сопоставить конкретное действие всем возможным методам HTTP-запроса: GET, POST, PATCH, DELETE и т. д. Сканер безопасности Rails всегда предлагает передавать параметры через альтернативные методы HTTP и отслеживать ответы сервера.

Разработчики RoR создали механизм защиты от таких атак, который называется аутентификация токенов.

3. SQL Инъекции: часто используются злоумышленниками для поиска способа передачи непроверенных данных. Инъекция SQL не только открывает доступ к базе данных, но также предоставляет возможность доступа к конфиденциальным данным. Хакеры часто используют SQL-инъекцию для поиска определенной информации, поскольку она позволяет быстро искать нужные записи. Также хакеры используют возможность вводить вредоносный код в SQL записи.

4. Clickjacking (англ. «захват клика»): Сетевая атака, которая автоматически перенаправляет пользователя на другую страницу без ущерба вашему сайту. Clickjacking – это меньшее из зол. Хакеры часто использую такие атаки, чтобы увеличить количество посетителей стороннего ресурса. В среде разработки RoR появился механизм, который может предотвращать такие перенаправления. Это можно сделать, добавив HTTP-заголовок «X-Frame-Options: SAMEORIGIN» на созданные страницы.

В Ruby on Rails разработаны необходимые механизмы и методы защиты, чтобы обеспечить высокий уровень безопасности. Следуя нескольким кратким руководствам по предотвращению потенциальных проблем безопасности, вы можете легко рассчитывать на преимущества, которые инфраструктура Ruby on Rails предлагает для веб-разработки [1].

Литература

1. Ruby on Rails: Guides [Электронный ресурс]. – Режим доступа: https://rubyonrails.org. – Дата доступа: 10.05.2020.