УДК 004

# Обеспечение безопасности во фреймворке Laravel на примере веб-игры "Сходимость числовых рядов"

*Стрельцова Марина Николаевна*
*Приамурский государственный университет им. Шолом-Алейхема*
*Студент*

*Научный руководитель:*
*Глаголев Владимир Александрович*
*Приамурский государственный университет имени Шолом-Алейхема*
*к.г.н., доцент кафедры информационных систем, математики и правовой информатики*

**Аннотация**
Безопасность личных данных в настоящее время становится одной из самых важных вещей в интернет пространстве. Злоумышленники каждый день придумывают сотни способов украсть важную для пользователя информацию: данные банковских карт, переписки, персональные данные. Для того, чтобы противостоять подобным методам программисты также совершенствуют способы защиты от кражи информации. Современные приложения стараются обеспечить максимальную безопасность, чтобы пользователь мог спокойно работать и не беспокоиться об утечки данных. В данной статье рассмотрены способы обеспечения безопасности во фреймворке Laravel на примере веб-игры «Сходимость числовых рядов».
**Ключевые слова:** безопасность, Laravel, хэширование, аутентификация, CSRF, SQL-инъекции

# Ensuring security in the Laravel framework using the example of the web game "Convergence of Number Series"

*Streltsova Marina Nikolaevna*
*Sholom-Aleichem Priamursky State University*
*Student*

*Scientific adviser:*
*Glagolev Vladimir Alexandrovich*
*Sholom Aleichem Priamursky State University*
*Candidate of Geographical Sciences, Associate Professor of the Department of Information Systems, Mathematics and Legal Informatics*

**Abstract**
Personal data security is now becoming one of the most important things in online advertising. Every day, scammers come up with ways to steal information for the

user: bank card data, correspondence, personal data. In order to resist such methods, programmers are also improving methods of protection against information theft. Modern applications try to provide maximum security so that the user can work calmly and not worry about data leakage. This article discusses ways to ensure security in the Laravel framework using the example of the web game "Convergence of Number Series ".
**Keywords:** security, Laravel, hashing, authentication, CSRF, SQL injection

Безопасность личных данных в настоящее время становится одной из самых важных вещей в интернет пространстве. Злоумышленники каждый день придумывают сотни способов украсть важную для пользователя информацию: данные банковских карт, переписки, персональные данные. Для того, чтобы противостоять подобным методам программисты также совершенствуют способы защиты от кражи информации. Современные приложения стараются обеспечить максимальную безопасность, чтобы пользователь мог спокойно работать и не беспокоиться об утечки данных.

В статье С.В.Ходырева рассматриваются некоторые вопросы обеспечения безопасности персональных данных, упорядочивание и систематизация этого процесса при помощи системы управления информационной безопасностью и методологии GRC [1]. В.О.Бажин и Т.В.Минкина в своей научной работе рассматривают классификацию информационных ресурсов и ее применение для данных, обрабатываемых в информационной системе типового предприятия, а также описывают методологию оценки и управления информационными ресурсами [2]. Научная статья М.Ф.Алиевой посвящена определению влияния информационной безопасности на информационную культуру и развитие современного общества [3]. В статье К.А.Ковалева и Р.В.Глущенко рассмотрены вопросы построения системы информационной безопасности в соответствии со стандартами, предъявляемыми регуляторами по вопросам информационной безопасности в Российской Федерации (ФСБ, ФСТЭК, Роскомнадзор) [4]. Об основных угрозах безопасности информации в виртуальных средах и облачных платформах рассказывают в своем исследовании И.В.Зубарев и П.К.Радин, так же они рассматривают проблемные вопросы защиты гипервизора, сервера управления, виртуальной машины и приложений, и предлагают решения по организации защиты информации в виртуальных средах [5]. В научной работе Y.Ding и др. исследуют конфигурацию, управление состоянием и уязвимости безопасности основного уровня безопасности для разработки плана исследований безопасности бизнес-систем [6]. M.Soni и D.K.Singh рассматривают влияние блокчейна на здравоохранение и биомедицинскую индустрию с целью обеспечения безопасности и конфиденциальности [7].

Целью данного исследования является изучение способов обеспечения безопасности хранения и передачи данных с помощью фреймворка Laravel на примере веб-игры «Сходимость числовых рядов».

Laravel – это PHP фреймворк для разработки web-приложений с выразительным и элегантным синтаксисом. Он позволит упростить решение основных наболевших задач, таких как аутентификация, маршрутизация, сессии и кэширование [8].

Многие веб-приложения предоставляют своим пользователям возможность аутентифицироваться в приложении и «войти в систему». Реализация этого функционала в веб-приложениях может быть сложной и потенциально рискованной задачей. По этой причине Laravel стремится предоставить инструменты, необходимые для быстрой, безопасной и простой реализации аутентификации.

В Laravel существуют готовые стартовые наборы, которые содержат в себе уже описанные правила аутентификации пользователей. В веб-игре был использован популярный набор аутентификации Laravel Breeze.

Laravel Breeze – это простая, минимальная реализация всех возможностей аутентификации Laravel, включая вход в систему, регистрацию, сброс пароля, подтверждение электронной почты и подтверждение пароля. Слой представления Laravel Breeze состоит из простых шаблонов Blade, стилизованных с помощью Tailwind CSS (Рис. 1-2).

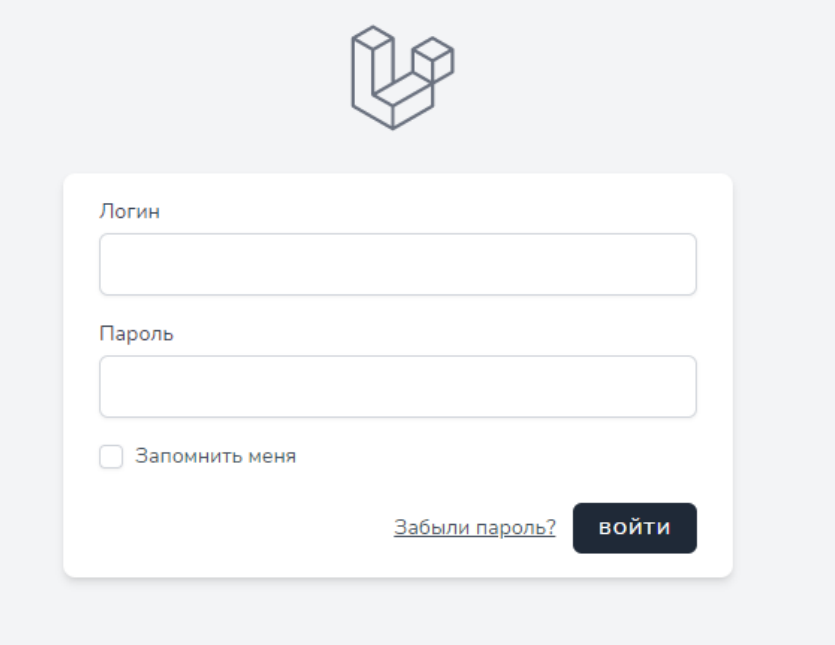


Рисунок 1. Страница аутентификации

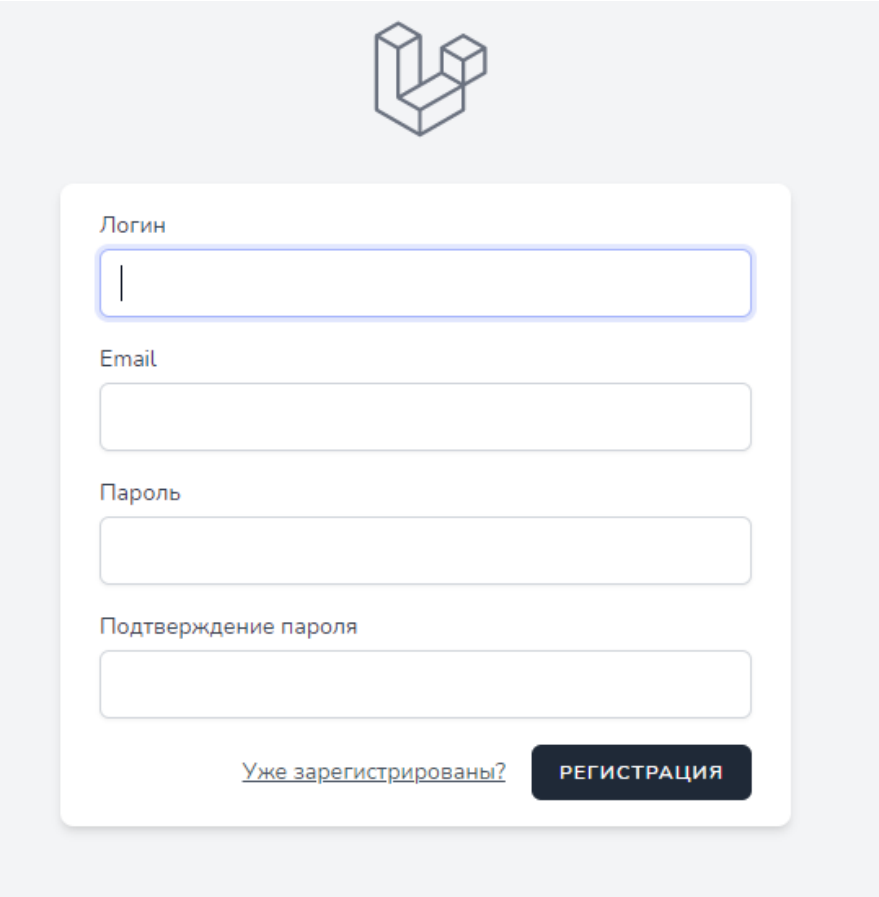


Рисунок 2. Страница регистрации

Пароли зарегистрированных пользователей хранятся в базе данных в зашифрованном виде с помощью фасада Hash, который обеспечивает надёжное Bcrypt-хеширование.

Также в Laravel присутствует система защиты маршрутов, которая подразумевает создание посредника. Посредник маршрута используется для того, чтобы разрешить только аутентифицированным пользователям доступ к указанному маршруту. Laravel содержит посредник auth, который ссылается на класс Illuminate\Auth\Middleware\Authenticate. Когда посредник auth обнаруживает неавторизованного пользователя, он перенаправляет пользователя на именованный маршрут login, который в свою очередь перенаправляет на страницу аутентификации, как на рисунке 1.

```
Route::get( uri: '/start', [App\Http\Controllers\StartController::class, 'start'])->middleware(['auth'])

Route::post( uri: '/begin', [App\Http\Controllers\StartController::class, 'begin'])->middleware(['auth'])

Route::post( uri: '/continue', [App\Http\Controllers\StartController::class, 'continue'])->middleware(['auth'])

Route::get( uri: '/level/{currentlevel}', [App\Http\Controllers\StartController::class, 'continue'])->middleware(['auth'])
```

Рисунок 3. Защита маршрутов с помощью посредника auth

При использовании Laravel Breeze к попыткам входа в систему будет автоматически применяться ограничение. По умолчанию, если пользователь не сможет предоставить правильные учетные данные после нескольких попыток, то он не сможет войти в систему в течение одной минуты. Частота

попыток уникальна для имени пользователя/адреса электронной почты в совокупности с IP-адресом.

Подделка межсайтовых запросов - это разновидность вредоносного эксплойта, при котором неавторизованные команды выполняются от имени аутентифицированного пользователя. Laravel упрощает защиту приложения от атак с подделкой межсайтовых запросов (CSRF).

Представим, что у приложения есть /user/email маршрут, который принимает POST запрос на изменение адреса электронной почты аутентифицированного пользователя. Скорее всего, этот маршрут ожидает, что email поле ввода будет содержать адрес электронной почты, который пользователь хотел бы начать использовать.

Без защиты CSRF вредоносный веб-сайт может создать HTML-форму, которая указывает на /user/email маршрут вашего приложения и отправляет собственный адрес электронной почты злонамеренного пользователя.

Если вредоносный веб-сайт автоматически отправляет форму при загрузке страницы, злоумышленнику нужно только соблазнить ничего не подозревающего пользователя приложения посетить свой веб-сайт, и его адрес электронной почты будет изменен в приложении.

Чтобы предотвратить эту уязвимость, следует проверять каждый входящий POST, PUT, PATCH или DELETE запрос на наличие CSRF токена, чтобы вредоносные приложения были не в состоянии получить доступ.

Laravel автоматически генерирует «токен» CSRF для каждой активной пользовательской сессии, управляемой приложением. Этот токен используется для проверки того, что аутентифицированный пользователь является лицом, действительно выполняющим запросы к приложению. Поскольку этот токен хранится в сеансе пользователя и изменяется каждый раз при повторном создании сеанса, вредоносное приложение не может получить к нему доступ (Рис. 4).


Рисунок 4. Внедрение CSRF защиты с помощью шаблонизатора Blade

Существует также угроза SQL-инъекций, которая связана с вставкой нефильтрованных произвольных данных пользователя в SQL-запрос. По умолчанию Laravel защищает от такого типа атак, поскольку и конструктор запросов, и Eloquent используют класс объектов данных PHP (PDO). PDO использует подготовленные операторы, которые позволяют безопасно передавать любые параметры без необходимости их удаления и санации.

В рамках данного исследования был проведен анализ существующих способов обеспечения безопасности во фреймворке Laravel на примере веб-

игры «Сходимость числовых рядов». Laravel обеспечивает безопасность приложений, защищая от таких угроз, как SQL-инъекции или межсайтовые подделки запросов (CSRF). Данные методы позволяют защитить пользователей от потери важных данных.

**Библиографический список**


1. Ходырев С. В. Обеспечение безопасности персональных данных при помощи систем система управления информационной безопасностью //Проблемы управления речными бассейнами при освоении Сибири и Арктики в контексте глобального изменения климата планеты в XXI веке. 2017. С. 264-268.
2. Бажин В. О., Минкина Т. В. Основные задачи системы безопасности для управления информационной системой организации //Студенческая наука для развития информационного общества. 2017. С. 275-277.
3. Алиева М. Ф. Информационная безопасность как элемент информационной культуры //Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2012. №. 4.
4. Ковалева К. А., Глущенко Р. В. Построение системы информационной безопасности //Международный студенческий научный вестник. 2014. №. 1. С. 38-38.
5. Зубарев И. В., Радин П. К. Основные угрозы безопасности информации в виртуальных средах и облачных платформах //Вопросы кибербезопасности. 2014. №. 2 (3).
6. Ding Y. et al. Research and application of security baseline in business information system //Procedia Computer Science. 2021. Т. 183. С. 630-635.
7. Soni M., Singh D. K. Blockchain-based security & privacy for biomedical and healthcare information exchange systems //Materials Today: Proceedings. 2021.
8. Laravel URL: https://laravel.com/ (дата обращения: 25.05.2021).