УДК 004.056.53

НЕДОСТАТОК КОНТРОЛЯ ДОСТУПА КАК ОДНА ИЗ АКТУАЛЬНЫХ УЯЗВИМОСТЕЙ WEB-ПРИЛОЖЕНИЙ

К.Д. Янович, Д.С. Лапчук

Гомельский государственный университет имени Франциска Скорины, Гомель, Беларусь

Аннотация. В данной работе рассматривается одна из актуальных и наиболее распространенных тенденций в области эксплуатации уязвимостей веб-приложений, которая входит в список OWASP Top Ten и находится на первом месте (A01). Исследование фокусируется на недостатках контроля доступа, которые позволяют неавторизованным пользователям получать доступ к конфиденциальной информации. Анализируются основные причины возникновения таких уязвимостей, включая неправильную настройку списков контроля доступа и отсутствие многофакторной аутентификации. Предлагаются методы защиты, такие как регулярный аудит и использование специализированных инструментов для тестирования безопасности [1].

Ключевые слова: веб-приложения; информационная безопасность; контроль доступа; уязвимости; аутентификация; авторизация; многофакторная аутентификация (MFA); шифрование; Netsparker; Burp Suite.

LACK OF ACCESS CONTROL AS ONE OF THE CURRENT VULNERABILITIES OF WEB APPLICATIONS

K.D. Yanovich, D.S. Lapchuk
Francisk Scorina Gomel State University, Gomel, Belarus

Abstract. This work examines one of the current and most prevalent trends in web application vulnerability exploitation, which is on the OWASP Top Ten list and is ranked number one (A01). The study focuses on access control flaws that allow unauthorized users to access sensitive information. The main causes of such vulnerabilities are analyzed, including improper configuration of access control lists and lack of multi-factor authentication. Protection methods, such as regular auditing and the use of specialized security testing tools, are proposed.
Keywords: web applications; information security; access control; vulnerabilities; authentication; authorization; multi-factor authentication (MFA); encryption; Netsparker; Burp suite

Введение

Веб-приложения предоставляют пользователям возможность интерактивного взаимодействия с контентом в интернете, что делает их важным элементом современной цифровой инфраструктуры. Однако, в силу своей открытости и доступности, веб-приложения становятся объектом различных кибератак, что может привести к утечке конфиденциальной информации и персональных данных. Недостаточная реализация решений по информационной безопасности может сделать веб-приложения уязвимыми для атак со стороны злоумышленников. Существует множество уязвимостей, которые могут быть использованы для компрометации веб-приложений. Одной из наиболее распространенных уязвимостей является недостаток контроля доступа.

Основная часть

Недостатки контроля доступа – уязвимости, связанные с управлением доступа и возникающие, когда приложение неправильно ограничивает доступ к данным или функциям. Недостатки контроля доступа возникают, когда приложение не обеспечивает надлежащую проверку прав доступа пользователей к ресурсам и функционалу. Это может позволить неавторизованным пользователям получить доступ к защищенным данным или выполнять действия, которые должны быть доступны только определенным категориям пользователей.

Например, если пользователь с низким уровнем доступа может получить доступ к административным функциям. Данные уязвимости могут принимать различные формы.

1. Применение небезопасных или предсказуемых паролей. Использование небезопасных или предсказуемых паролей создает значительные риски для безопасности системы. Злоумышленники могут легко подобрать такие пароли с помощью различных методов, что позволяет им получить несанкционированный доступ к конфиденциальной информации и данным пользователей.

2. Неправильно настроенные списки контроля доступа. Неправильная настройка списков контроля доступа может привести к серьезным уязвимостям в системе безопасности. Это происходит, когда права доступа пользователей не соответствуют их ролям и обязанностям, что позволяет неавторизованным пользователям получать доступ к конфиденциальной информации или выполнять действия, которые должны быть ограничены. Такие ошибки в конфигурации могут быть использованы злоумышленниками для получения несанкционированного доступа к ресурсам системы, что ставит под угрозу безопасность данных и целостность информации.

3. Недостаточные или неправильные разрешения. Недостаточные или неправильные разрешения могут существенно ослабить систему контроля доступа, предоставляя пользователям больше прав, чем необходимо для выполнения их задач. Это может привести к ситуациям, когда неавторизованные пользователи получают доступ к конфиденциальной информации или могут выполнять критические операции, что нарушает принцип минимальных привилегий. Такие ошибки в настройке разрешений создают уязвимости, которые могут быть использованы злоумышленниками для компрометации системы и утраты данных.

4. Отсутствие аудита и мониторинга. Отсутствие аудита и мониторинга может значительно ослабить систему безопасности, так как не позволяет своевременно выявлять и реагировать на потенциальные угрозы и инциденты. Без регулярного аудита невозможно проверить соответствие текущих настроек безопасности установленным политикам и стандартам, что может привести к незамеченным уязвимостям. Мониторинг, в свою очередь, необходим для оперативного обнаружения подозрительной активности и предотвращения несанкционированного доступа. Недостаток этих процессов создает благоприятные условия для злоумышленников, позволяя им эксплуатировать уязвимости без обнаружения.

5. Отсутствие многофакторной аутентификации. Отсутствие многофакторной аутентификации (MFA) создает значительные риски для безопасности системы. MFA добавляет дополнительный уровень защиты, требуя от пользователей подтверждения их личности с помощью второго фактора, такого как SMS-код или приложение-аутентификатор. Без MFA система становится уязвимой для атак, направленных на подбор паролей или фишинг, что позволяет злоумышленникам получить несанкционированный доступ к учетным записям и конфиденциальной информации. Внедрение MFA является критически важным для повышения уровня безопасности и защиты данных пользователей.

Рассмотрим примеры уязвимостей в коде (рис. 1, 2). В коде представленном на рис. 1 метод viewUserProfile используется для отображения информации профиля пользователя. Однако проверка контроля доступа отсутствует, чтобы гарантировать, что пользователь, вызывающий этот метод, имеет право на просмотр профиля. Злоумышленник может воспользоваться этой уязвимостью, передав другой идентификатор пользователя и получив доступ к профилю другого пользователя. Код, представленный на рис. 2, считывает содержимое файла с помощью встроенной в Python open функции. Однако проверка контроля доступа отсутствует, чтобы гарантировать, что пользователь, вызывающий эту функцию, имеет право на чтение файла. Злоумышленник может воспользоваться этой уязвимостью, передав другое имя файла и получив доступ к конфиденциальным данным.

```
public void viewUserProfile(String userId) {
    User user = getUserById(userId);
    if (user != null) {
        System.out.println("User Name: " + user.getName());
        System.out.println("Email Address: " + user.getEmail());
    }
}
```

Рис. 1. Пример уязвимого кода на языке программирования Java
Fig. 1. An example of vulnerable code in the Java programming language

```
def read_file(filename):
with open(filename, 'r') as f:
    contents = f.read()
return contents
```

Рис. 2. Пример уязвимого кода на языке программирования Python
Fig. 2. Example of vulnerable Python programming language code

Рассмотрим основные методы защиты от недостатков контроля доступа. Для предотвращения уязвимости необходимо внедрять строгие политики аутентификации и паролей, включая использование многофакторной аутентификации там, где это возможно. Убедиться, что все учетные записи пользователей имеют соответствующие уровни доступа и разрешения, и регулярно просматривать и обновлять эти разрешения по мере необходимости. Использовать шифрование для защиты конфиденциальных данных, как при передаче, так и в состоянии покоя. Необходимо внедрить средства контроля доступа на каждом уровне вашей инфраструктуры, включая веб-приложения, операционные системы и сетевую инфраструктуру, а также регулярно устанавливать обновления программного обеспечения и исправления ко всем системам и приложениям для устранения известных уязвимостей в системе безопасности.

Для выявления рассматриваемой уязвимости чаще всего используют сканеры уязвимостей. Это инструменты, которые автоматически анализируют системы и программное обеспечение на наличие потенциальных уязвимостей.

На основе отзывов, Netsparker часто упоминается как один из лучших сканеров уязвимостей. Netsparker отмечен за свою точность в обнаружении потенциальных уязвимостей в веб-приложениях и использование автоматизации машинного обучения, что делает его одним из лучших на рынке. Одним из самых популярных является Burp Suite – мощный инструмент для тестирования безопасности веб-приложений, который включает в себя множество функций для анализа и эксплуатации уязвимостей. Опытные пентестеры используют Metasploit – фреймворк для тестирования на проникновение, который включает в себя множество эксплойтов для различных уязвимостей.

Помимо сканеров уязвимостей, существуют различные плагины для браузеров, которые помогают обнаруживать уязвимости и снизить риски кибератак и утечки данных. Наиболее популярными являются:

LiveHTTPHeaders – надстройка Firefox, которая может использоваться для просмотра и изменения HTTP-заголовков, позволяя тестировщикам проверять уязвимости контроля доступа, связанные с механизмами аутентификации на основе заголовков.

EditThisCookie – расширение Chrome, которое можно использовать для редактирования файлов cookie и манипулирования ими, позволяя тестировщикам проверять уязвимости контроля доступа, связанные с механизмами аутентификации на основе файлов cookie.

ModHeader – расширение Chrome, которое можно использовать для изменения заголовков HTTP, позволяя тестировщикам проверять уязвимости контроля доступа, связанные с механизмами аутентификации на основе заголовков.

Использование предоставленных средств обнаружения веб-уязвимостей позволяет своевременно обнаружить недостаток контроля доступа и предотвратить утечку данных.

Заключение

Недостаток контроля доступа является критической уязвимостью в веб-приложениях, занимая первое место в списке OWASP Top Ten. Эта уязвимость может привести к утечке конфиденциальной информации и подрыву доверия пользователей.

Для защиты веб-приложений необходимо внедрять строгие политики аутентификации и авторизации, регулярно проверять и обновлять разрешения пользователей, а также использовать шифрование для защиты данных. Регулярное обновление программного обеспечения также важно для поддержания безопасности.

Инструменты, такие как Netsparker, Burp Suite и Metasploit, помогают выявлять и устранять уязвимости контроля доступа. Плагины для браузера, такие как LiveHTTPHeaders, EditThisCookie и ModHeader, полезны для ручного тестирования.

Таким образом, комплексный подход и использование специализированных инструментов являются ключевыми для обеспечения безопасности веб-приложений.

Список использованных источников

1. Андреева О. TOP10 уязвимостей в веб-приложениях в 2021–2023 годах. [Электронный ресурс] / О. Андреева, Kaspersky Security Services // Securelist by Kaspersky: Исследование. – 2024. – 12 марта. – URL: https://securelist.ru/top-10-web-app-vulnerabilities/109215/. – Дата доступа: 25.02.2025.

Сведения об авторах

Янович К.Д., студентка 2 курса факультета Физики и информационных технологий, специальности «Кибербезопасность», Гомельский государственный университет имени Франциска Скорины, karifox100@gmail.com.
Лапчук Д.С., студент 2 курса факультета Физики и информационных технологий, специальности «Кибербезопасность», Гомельский государственный университет имени Франциска Скорины, Danik_lapchuk@mail.ru.

Information about the authors

Yanovich K.D., 2nd year student of the Faculty of Physics and Information Technologies, major "Cyber Security", Francisk Scorina Gomel State University, karifox100@gmail.com.
Lapchuk D.S., 2nd year student of the Faculty of Physics and Information Technologies, major "Cyber Security", Francisk Scorina Gomel State University, Danik_lapchuk@mail.ru.