Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный университет геодезии и картографии»
(МИИГАиК)»

Факультет геоинформатики и информационной безопасности

Кафедра геоинформационных систем и технологий

ОТЧЕТ по OWASP

НА ТЕМУ:

«Уязвимость из овасп»

Студент _____ Ахмад Хесров Каримзай

(Подпись, дата)

Преподаватель _____

(Подпись, дата)

2024 г.

СОДЕРЖАНИЕ

Введение

Уязвимость в веб приложении представляет собой слабое место или ошибку в его структуре, коде, конфигурации или бизнес логике, которая может быть использована злоумышленником для неправомерного доступа, модификации данных, отказа в обслуживании (DoS), или других видов атак. Уязвимости могут возникнуть из за неправильного проектирования, программирования, конфигурации или недостаточной защиты.

Исследование и устранение уязвимостей являются важной частью процесса обеспечения безопасности веб приложений. Разработчики, тестировщики безопасности и администраторы должны активно мониторить, анализировать и устранять потенциальные угрозы.

1 Нарушенный контроль доступа

относится к уязвимости в системе безопасности, которая возникает, когда механизмы контроля доступа системы не реализованы или не применены должным образом. Механизмы контроля доступа создаются для обеспечения того, чтобы только авторизованные пользователи или организации могли получать доступ к определенным ресурсам или выполнять определенные действия в системе. Когда контроль доступа нарушен, это означает, что злоумышленник может получить несанкционированный доступ к ресурсам или выполнить действия, которые он не должен иметь возможности.

Эта уязвимость может проявляться различными способами, такими как неадекватные механизмы аутентификации, отсутствие надлежащих проверок авторизации и ненадежный контроль доступа к конфиденциальным данным. Нарушение контроля доступа может иметь серьезные последствия, такие как утечка данных, кража конфиденциальной информации и несанкционированные изменения конфигурации системы. Это представляет собой серьезную угрозу безопасности, и ее следует устранить как можно скорее, чтобы предотвратить потенциальные атаки.

На рисунке (1.1) представлено, сделаны работы на OWASP:

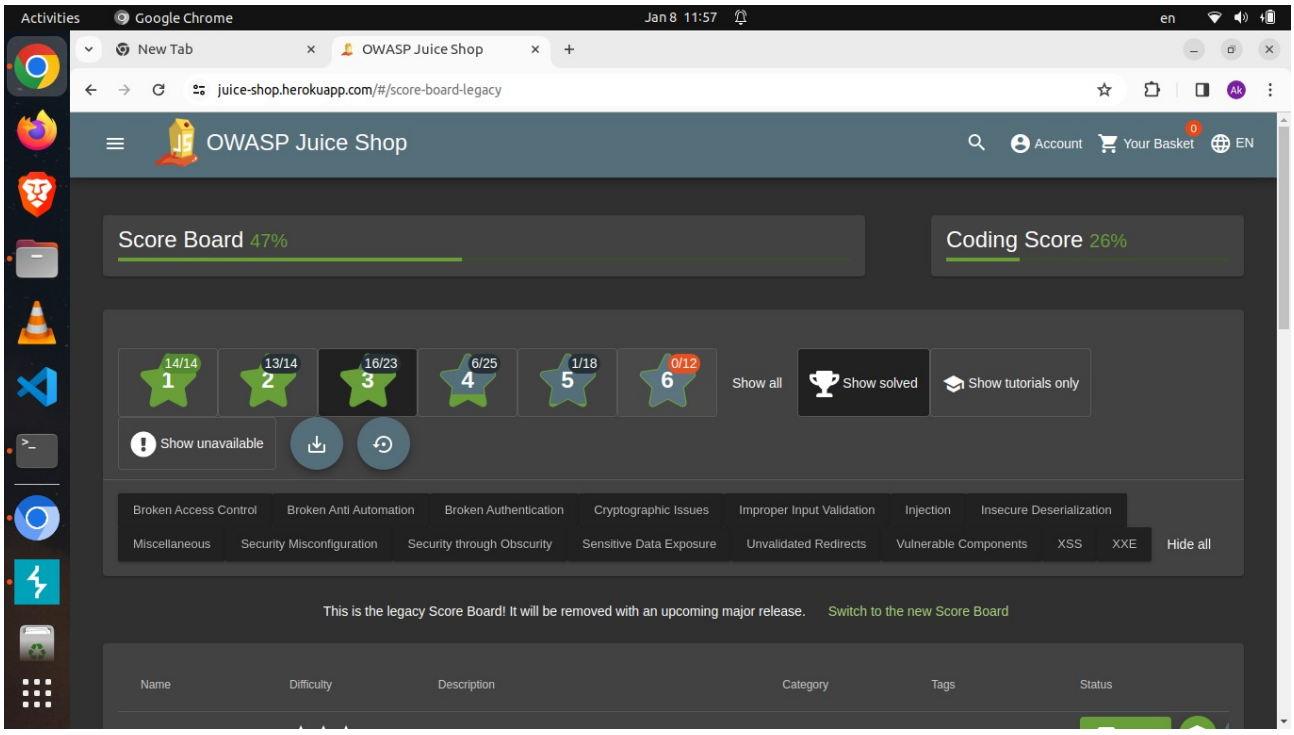

Рис. 1.1. сделаны работы на OWASP

2 Криптографические сбои

Первое, что нужно сделать, это определить потребности в защите данных при передаче и в состоянии покоя. Например, пароли, номера кредитных карт, медицинские записи, личная информация и коммерческая тайна требуют дополнительной защиты. Главным образом, если эти данные подпадают под действие законов о конфиденциальности, например, Общего регламента ЕС по защите данных (GDPR), или правил, например, защиты финансовых данных, таких как Стандарт безопасности данных индустрии платежных карт (PCI DSS).

3 SQL инъекции

это один из очень распространённых способов взлома сайтов и веб□приложений, работающих с реляционными базами данных.

Этот способ основан на внедрении в выполняемый приложением запрос к базе данных произвольного SQL□кода, переданного злоумышленником. SQL□инъекции являются одной из разновидностей атак типа «инъекция кода».

SQL□инъекции, в зависимости от типа уязвимости, может дать возможность атакующему выполнить произвольный запрос к базе данных. То есть атакующий сможет прочитать содержимое любых таблиц, удалить, изменить или добавить данные, а также есть вероятность получения возможности работы с локальными файлами и выполнения произвольных команд на атакуемом сервере.

Последствия SQL□инъекций:

1. Кража данных;
2. Модификация данных;
3. Удаление данных;
4. Полный взлом системы.

4 Небезопасный дизайн

Небезопасный дизайн в веб приложении относится к ситуациям, когда архитектурные или дизайнерские решения приводят к потенциальным уязвимостям, которые могут быть использованы злоумышленниками для

проведения атак. Эти недостатки могут оставить приложение открытым для различных угроз, таких как несанкционированный доступ, утечки данных, атаки на безопасность и другие виды атак.

1. Недостаточная обработка аутентификации и авторизации;
2. Недостаточная защита сессий;
3. Недостаточная защита от межсайтовой подделки запроса (CSRF);
4. Недостаточная защита от кросс сайтового скриптинга (XSS).

5 Уязвимые и устаревшие компоненты

Уязвимые и устаревшие компоненты в веб приложении представляют собой наиболее распространенную категорию угроз. Эти компоненты могут быть подвержены различным уязвимостям, которые могут быть использованы злоумышленниками для получения несанкционированного доступа, кражи данных или повреждения системы.

Для снижения рисков, связанных с использованием уязвимых и устаревших компонентов, необходимо регулярно проводить оценку безопасности веб приложения и своевременно обновлять компоненты до последних версий.

6 Неправильная конфигурация безопасности

Неправильная конфигурация безопасности может привести к снижению эффективности защитных механизмов веб приложения, что может сделать его уязвимым для атак.

Для снижения рисков, связанных с неправильной конфигурацией безопасности, необходимо использовать стандартные конфигурации безопасности, а также регулярно проводить аудит безопасности веб приложения.

Сбои идентификации и аутентификации в веб приложении

Сбои идентификации и аутентификации могут привести к несанкционированному доступу к веб приложению.

Для снижения рисков, связанных со сбоями идентификации и аутентификации, необходимо использовать надежные механизмы аутентификации, а также регулярно обновлять пароли пользователей.

7 Нарушения целостности программного обеспечения и данных

Нарушения целостности программного обеспечения и данных могут привести к краже данных или повреждению системы.

Для снижения рисков, связанных с нарушениями целостности программного обеспечения и данных, необходимо использовать надежные механизмы защиты от несанкционированного доступа, а также регулярно проводить резервное копирование данных.

8 Сбои ведения журнала безопасности и мониторинга

Сбои ведения журнала безопасности и мониторинга могут затруднить обнаружение и расследование инцидентов безопасности.

Для снижения рисков, связанных со сбоями ведения журнала безопасности и мониторинга, необходимо использовать надежные системы ведения журнала безопасности и мониторинга, а также регулярно проверять их работоспособность.

9 Подделка запроса на стороне сервера

Подделка запроса на стороне сервера (SSRF) — это уязвимость, которая позволяет злоумышленнику заставить веб приложение выполнить произвольный запрос к другому серверу.

Для снижения рисков, связанных с SSRF, необходимо использовать безопасные методы обработки запросов от пользователей, а также ограничивать доступ пользователей к ресурсам, которые не должны быть доступны извне.

Заключение

Рекомендации по снижению рисков, связанных с уязвимостями веб приложений

Для снижения рисков, связанных с уязвимостями веб приложений, необходимо предпринять следующие меры:

- Регулярно проводить оценку безопасности веб приложения. Оценка безопасности должна включать в себя анализ уязвимостей веб приложения, а также оценку эффективности защитных механизмов.
- Своевременно обновлять компоненты веб приложения. Обновления компонентов часто содержат исправления уязвимостей безопасности.

– Использовать стандартные конфигурации безопасности. Стандартные конфигурации безопасности обеспечивают базовый уровень защиты веб приложения.

– Регулярно проводить аудит безопасности веб приложения. Аудит безопасности позволяет выявить и устранить уязвимости, которые могут быть не обнаружены при оценке безопасности.

– Использовать надежные механизмы аутентификации. Надежные механизмы аутентификации позволяют предотвратить несанкционированный доступ к веб приложению.

– Регулярно обновлять пароли пользователей. Актуальные пароли помогают защитить веб приложение от атак, основанных на подборе паролей.

– Использовать надежные механизмы защиты от несанкционированного доступа. Надежные механизмы защиты от несанкционированного доступа помогают предотвратить кражу данных или повреждение системы.

– Регулярно проводить резервное копирование данных. Резервное копирование данных позволяет восстановить данные в случае их повреждения или кражи.

– Использовать надежные системы ведения журнала безопасности и мониторинга. Надежные системы ведения журнала безопасности и мониторинга помогают обнаружить и расследовать инциденты безопасности.

– Использовать безопасные методы обработки запросов от пользователей. Безопасные методы обработки запросов от пользователей помогают предотвратить SSRF и другие атаки, основанные на манипуляциях с запросами от пользователей.

Реализация этих рекомендаций поможет снизить риски, связанные с уязвимостями веб приложений, и обеспечить их безопасность.