Проверка авторизации и регистрации

WIN-1-22

Тестрование Авторизции и регистрации

Выполнил:

Бактыбеков Н.Б.

May 12, 2023

Проверка авторизации и регистрации

Введение

Авторизационное и регистрационное тестирование — это тип тестирования программного обеспечения, который гарантирует, что пользователи могут получить доступ только к тем ресурсам и функциям, на доступ к которым им предоставлен доступ. Этот тип тестирования важен для обеспечения безопасности и конфиденциальности данных пользователей.

Цели тестирования

Целями авторизационного и регистрационного тестирования являются:

- Уьбедиться, что пользователи могут получить доступ только к тем ресурсам и функциям, к которым у них есть доступ.
- Уьбедиться, что пользователи не могут получить доступ к ресурсам и функциям, на доступ к которым у них нет прав.
- Уьбедиться, что пользователи не могут обойти процесс авторизации.

Методы тестирования

Существует множество методов, которые можно использовать для проверки авторизации и регистрации. Некоторые из наиболее распространенных методов включают в себя:

- Тестирование «черного ящика»: при тестировании «черного ящика» тестер не имеет никаких знаний о внутренней реализации программного обеспечения. Тестер просто вводит данные в программу и наблюдает за выводом.
- Тестирование белого ящика: при тестировании белого ящика тестер знает внутреннюю реализацию программного обеспечения. Эти знания можно использовать для выявления потенциальных уязвимостей безопасности.
- Тестирование безопасности. Тестирование безопасности — это тип тестирования, направленный на выявление и устранение уязвимостей безопасности. Тестирование безопасности может использоваться для выявления уязвимостей в процессе авторизации и регистрации.

Инструменты тестирования

Существует множество инструментов, которые можно использовать для автоматизации проверки авторизации и регистрации. Некоторые из самых популярных инструментов включают в себя:

- OWASP Zed Attack Proxy (ZAP): ZAP — это бесплатный инструмент тестирования безопасности с открытым исходным кодом, который можно использовать для выявления и устранения уязвимостей безопасности.
- Burp Suite: Burp Suite — это коммерческий инструмент для тестирования безопасности, который предлагает широкий спектр функций для выявления и устранения уязвимостей

безопасности.

- Nessus: Nessus — это коммерческий сканер уязвимостей, который можно использовать для выявления уязвимостей безопасности в различных системах.

Контрольный список тестирования

Ниже приведен контрольный список пунктов, которые следует учитывать при тестировании авторизации и регистрации:

- Уьбедиться, что пользователи могут получить доступ только к тем ресурсам и функциям, на доступ к которым они имеют право.
- Уьбедиться, что пользователи не могут получить доступ к ресурсам и функциям, на доступ к которым у них нет прав.
- Уьбедиться, что пользователи не могут обойти процесс авторизации.
- Уьбедиться, что процесс авторизации безопасен и его нельзя легко обойти.
- Уьбедиться, что процесс авторизации является масштабируемым и может обрабатывать большое количество пользователей.
- Уьбедиться, что процесс авторизации надежен и не дает сбоев под нагрузкой.

Заключение

Тестирование авторизации и регистрации является важной частью тестирования программного обеспечения. Тестируя процесс авторизации и регистрации, тестировщики могут помочь обеспечить безопасность и конфиденциальность данных пользователей.