УГРОЗЫ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ И ИХ КЛАССИФИКАЦИЯ

Каримов И.С.
Магистрант, Бухарский государственный университет
Касимов Ф.Ф.
Научный руководитель:
к.ф.-м.н. доцент. Бухарский государственный университет

Аннотация. *В статье рассматриваются основные угрозы безопасности веб-приложений и их классификация. Описываются наиболее распространенные типы атак, такие как SQL-инъекции, XSS (межсайтовые скриптовые атаки), CSRF (атаки подделки межсайтовых запросов) и другие, а также методы защиты от них. В статье также обсуждаются ключевые аспекты обеспечения безопасности веб-приложений, включая шифрование данных, аутентификацию и авторизацию пользователей, а также управление уязвимостями. Знание и понимание угроз безопасности позволяют разработчикам и организациям эффективно защищать свои веб-приложения от внешних и внутренних рисков, минимизируя возможности для атак и утечек данных.*

Ключевые слова: *угрозы безопасности, веб-приложения, защита данных, шифрование, аутентификация, авторизация, уязвимости, межсайтовые атаки, защита веб-приложений.*

Abstract. *The article discusses the main security threats to web applications and their classification. It describes the most common types of attacks, such as SQL injection, XSS (cross-site scripting), CSRF (cross-site request forgery), and others, as well as methods of protection against them. The article also addresses key aspects of web application security, including data encryption, user authentication and authorization, and vulnerability management. Understanding security threats enables developers and organizations to effectively protect their web applications from external and internal risks, minimizing the potential for attacks and data leaks.*

Keywords: *security threats, web applications, data protection, encryption, authentication, authorization, vulnerabilities, cross-site attacks, web application protection.*

Annotatsiya. *Maqolada veb-ilovalar xavfsizligi uchun asosiy tahdidlar va ularning tasnifi ko'rib chiqiladi. SQL in'ektsiyalari, XSS (xavfsiz bo'lmagan*

skriptlar), CSRF (kross-sayt so'rovlarini soxtalashtirish hujumlari) kabi eng keng tarqalgan hujum turlari va ularni himoya qilish usullari tasvirlanadi. Shuningdek, maqolada veb-ilovalar xavfsizligini ta'minlashning asosiy jihatlari, jumladan, ma'lumotlarni shifrlash, foydalanuvchilarni autentifikatsiya qilish va avtorizatsiya qilish, shuningdek, zaifliklarni boshqarish ko'rib chiqiladi. Xavfsizlik tahdidlarini bilish va tushunish, dasturchilarga va tashkilotlarga o'z veb-ilovalarini tashqi va ichki xavflardan samarali himoya qilish, hujumlar va ma'lumotlar oqibati xavfini minimallashtirish imkonini beradi.

Kalit so'zlar: *xavfsizlik tahdidlari, veb-ilovalar, ma'lumotlarni himoya qilish, shifrlash, autentifikatsiya, avtorizatsiya, zaifliklar, kross-sayt hujumlari, veb-ilovalar himoyasi.*

Введение. С каждым годом веб-приложения становятся неотъемлемой частью нашей жизни и важной составляющей бизнеса. Они обеспечивают доступ к онлайн-услугам, хранят персональные данные пользователей, обрабатывают транзакции и предоставляют бизнесу конкурентные преимущества. Однако с развитием технологий возникает множество угроз безопасности, которые могут привести к утечке данных, потере доверия со стороны пользователей или даже финансовым убыткам. В этой статье мы рассмотрим основные угрозы безопасности веб-приложений, их классификацию и методы защиты от них [1].

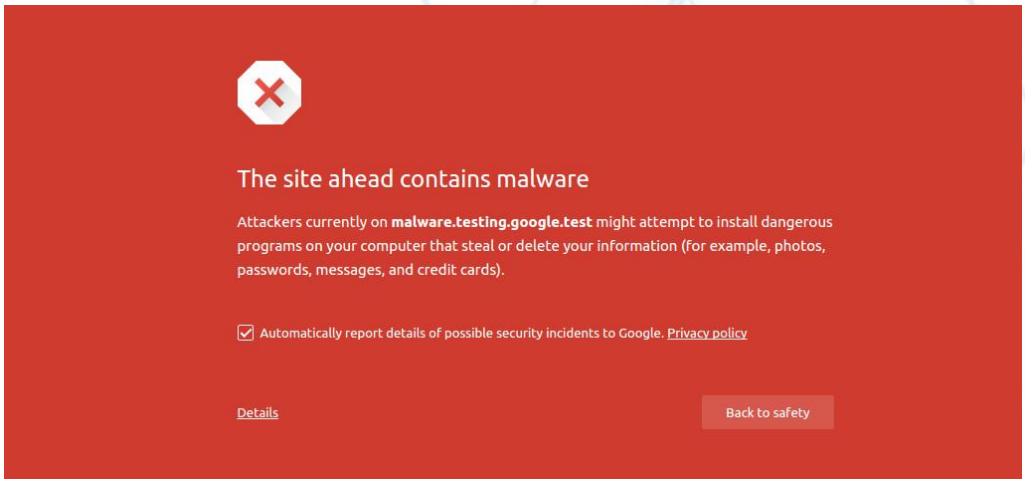
Угроза безопасности веб-приложения — это возможность для злоумышленников использовать уязвимости приложения с целью получения несанкционированного доступа, кражи данных или нарушения его работы. Веб-приложения подвергаются риску из-за множества факторов, таких как недостаточная защита данных, ошибки в кодировании или неправильная конфигурация серверов. Основными угрозами могут быть атаки на серверы, базы данных, а также взлом учетных записей пользователей [2].

Эти угрозы связаны с тем, как приложение обрабатывает данные, получаемые от пользователей. Злоумышленники могут манипулировать вводимыми данными с целью проникновения в систему.

Основные виды атак:

- SQL-инъекции (SQL Injection): Атака, при которой злоумышленник вставляет вредоносный SQL-код в поля ввода данных, такие как формы на сайте. Это может привести к утечке данных, повреждению базы данных или получению несанкционированного доступа.

- Межсайтовые скриптовые атаки (XSS - Cross-Site Scripting): Вредоносный скрипт, внедренный на веб-странице, который может выполняться в браузере жертвы, например, для кражи cookie-файлов или выполнения действий от имени пользователя.
- Подделка межсайтовых запросов (CSRF - Cross-Site Request Forgery): Атака, при которой злоумышленник заставляет пользователя выполнить нежелательное действие на сайте, например, перевести деньги или изменить настройки аккаунта.



Основные типы угроз информационной безопасности веб-приложения: Угрозы конфиденциальности – несанкционированный доступ к данным.

1. Угрозы целостности – несанкционированное искажение или уничтожение данных.

2. Угрозы доступности – ограничение или блокирование доступа к данным.

Основным источником угроз информационной безопасности веб-приложения являются внешние нарушители. Внешний нарушитель – лицо, мотивированное, как правило, коммерческим интересом, имеющее возможность доступа к сайту компании, не обладающий знаниями об исследуемой информационной системе, имеющий высокую квалификацию в вопросах обеспечения сетевой безопасности и большой опыт в реализации сетевых атак на различные типы информационных систем [3].

Говоря простыми словами — основная угроза безопасности сайта — хакерская атака. Она может иметь конечную цель, быть т.н. целевой атакой, либо атака носит бессистемный характер, по принципу — атакую все подряд, что-нибудь да сломается.

В первом случае злоумышленник может выявлять максимально возможное количество векторов атаки для составления и реализации потенциально успешных сценариев взлома, во втором же объекты атакуются массово, обычно использую несколько поверхностных уязвимостей.

Виды угроз

Угрозы безопасности связаны с несколькими факторами: в первую очередь это уязвимости веб-приложений или их компонентов. Во вторую — с используемыми механизмами проверки идентификации. В третью очередь угрозы безопасности относятся к атакам на самих пользователей, клиент-сайд атаки. Четвертый вид угроз — утечка или разглашение критичной информации. Пятый вид угроз — логические атаки.

Уязвимости веб-приложений, как правило, приводят к выполнению кода на удаленном сервере. Все серверы используют данные, переданные пользователем при обработке запросов. Часто эти данные используются при составлении команд, применяемых для генерации динамического содержимого. Если при разработке не учитываются требования безопасности, злоумышленник получает возможность модифицировать исполняемые команды. К такого рода уязвимостям относятся, например, SQL-injection.

Целевые атаки — это атаки, специально нацеленные на один сайт или их группу, объединенную одним признаком (сайты одной компании, либо сайты, относящиеся к определённой сфере деятельности, либо объединенные рядом признаков). Опасность таких атак заключается именно в «заказном» характере. Исполнителями таких атак становятся, как правило, злоумышленники, обладающие высокой квалификацией в области безопасности веб-приложений [4].

Целью таких атак обычно является получение конфиденциальной информации, которая может быть использована недобросовестными

конкурентами или преступниками для получения прибыли.

Нецелевые атаки — это атаки, которые проводится фактически “на удачу”, а ее жертвами становятся случайные веб-сайты независимо от популярности, размера бизнеса, географии или отрасли. Нецелевая атака на сайт – это попытка получения несанкционированного доступа к веб-ресурсу, при которой злоумышленник не ставит целью взломать конкретный сайт, а атакует сразу сотни или тысячи ресурсов, отобранных по какому-то критерию. Например, сайты, работающие на определенной версии системы управления сайтом. Такого рода атаки бьют по «площадям», стараясь охватить максимальное количество сайтов при минимуме затрат.


Продам Shell,ftp,smtp

Продаю: WSO-FTP-SMTP
- шеллы без параметров, оптом
- шеллы с функцией (mail) для рассылки
- бурж шеллы с pr 1-2, оптом
- бурж шеллы с pr от 3 до 9
- снг шеллы с тиц от 10 и до совсем жирных
- шеллы с ру и бурж трафом от 500 уников и до совсем жирных
- ftp с параметрами и без них

Так же в наличии выборки по доменной зоне.

Jabber:

Готов работать через гаранта!

При удачной попытке атаке злоумышленник старается извлечь из этого пользу: закрепиться на сайте, загрузив хакерский скрипт (бэкдор, веб-шелл), добавить еще одного администратора, внедрить вредоносный код или получить необходимую информацию из базы данных [5].

Нецелевые атаки — это атаки, которые проводится фактически “на удачу”, а ее жертвами становятся случайные веб-сайты независимо от популярности, размера бизнеса, географии или отрасли. Нецелевая атака на сайт – это попытка получения несанкционированного доступа к веб-ресурсу, при которой злоумышленник не ставит целью взломать конкретный сайт, а атакует сразу сотни или тысячи ресурсов, отобранных по какому-то критерию. Например, сайты, работающие на определенной версии системы управления сайтом. Такого рода атаки бьют по «площадям», стараясь [6].

В первую очередь это несет угрозу работоспособности сайта. Во вторую, но не менее важную, — сохранность пользовательских данных. Из этих причин вытекает логичное следствие — финансовые и репутационные потери компании. Хакеры используют ваш сайт для атак на другие ресурсы, в качестве опорного плацдарма, для рассылки спама или проведения DoS атак. Ваш сайт блокируют поисковики и браузеры, вы теряете пользователей. Атака на веб-сайт в корпоративной среде может является т.н. точкой входа в корпоративную сеть компании [7]. Атаки на системы электронной коммерции могут быть использованы для совершения мошеннических действий, похищения клиентских баз и т.д. Также, все эти атаки могут быть нацелены на дальнейшее «заражение» пользователей сайта, например с помощью т.н. эксплоит-паков — средств эксплуатации уязвимостей браузеров и их компонентов, в том числе и с применением социотехнических векторов атаки.

Эти угрозы связаны с тем, как приложение обрабатывает данные, получаемые от пользователей. Злоумышленники могут манипулировать вводимыми данными с целью проникновения в систему.

Распространение атак на веб-приложения связаны с двумя основными факторами: халатное отношение к безопасности сайта и низкий порог входа потенциальных злоумышленников [8]. В большинстве случаев на сайтах не используются специальные средства обнаружения, мониторинга и защиты, а также нет ответственного персонала и осведомленности об угрозах безопасности сайта. Качеству кода и безопасной настройке веб-приложения (и веб-сервера) уделяется мало внимания. Распространение утилит и сканеров безопасности веб-приложений обуславливает низкий порог вхождения потенциальных злоумышленников [9]. А многочисленные коммюнити и «околохакерские» форумы способствуют распространению техник атак среди всех желающих. Также этому способствует широкая и довольно оперативная огласка об обнаружении новых уязвимостей или технических аспектах атак.

Необходимо не забывать о соблюдении базовых мер безопасности при разработке и поддержке работы сайта: обновлять CMS и ее компоненты; регулярно менять пароли; отказаться от использования устаревших протоколов; настроить и использовать HTTPS/HSTS. Используйте WAF для своевременного обнаружения и блокирования различных веб-атак [10]. Это позволит быть спокойным за защищенность веб-приложений от хакерских атак и их последствий.

Заключение. Угрозы безопасности веб-приложений остаются актуальной проблемой для бизнеса и пользователей. Разнообразие атак, включая SQL-инъекции, XSS, CSRF и другие, ставит перед разработчиками задачу создания безопасных приложений. Важно применять комплексный подход к обеспечению безопасности, включая использование современных методов защиты, регулярные обновления и мониторинг безопасности. Защита от угроз требует внимательности и непрерывной работы, но она является необходимым условием для обеспечения надежности и доверия к веб-приложениям.

Список использованной литературы

1) Хайдаров А., Жумаев Ж., Шафиев Т.Р. Основы математического моделирования// Учебник. Бухара. «Дурдона», 2022. 216 с.
2) Жумаев Ж., Мирзаева Ш.У. Совершенствование процесса экстракции лакричного корня в среде CO2// Монография. Изд-ва «Дурдона». 2023. 144 с.
3) Агалаков С.А., Эконометрические модели [Текст] : учебное пособие / С. А. Агалаков ; М-во образования и науки Российской Федерации, Федеральное гос. бюджетное образовательное учреждение высш. проф. образования Омский гос. ун-т им. Ф. М. Достоевского. - Омск : Изд-во Омского гос. ун-та им. Ф. М. Достоевского, 2015. - 140 с.
4) Шоу, Д. «Безопасность веб-приложений. Принципы и практика защиты». — Книга, которая охватывает основные аспекты безопасности веб-приложений, включая защиту от атак и уязвимостей.
5) Шевчук, В., Логвиненко, А. «Практическое руководство по безопасности веб-приложений». — Пособие, предлагающее рекомендации по безопасному проектированию и защите веб-приложений.
6) Решетников, А. «Атаки на веб-приложения и способы защиты». – Статья, в которой рассмотрены современные методы защиты веб-приложений от различных типов атак.
7) Санчес, Х. «Веб-приложения: уязвимости и защита». — Руководство по безопасному проектированию и защите веб-приложений, включая примеры атак и способы защиты.

8) Арсичевский, С. «Практическое руководство по безопасности веб-приложений». - Руководство по разработке безопасных веб-приложений с акцентом на актуальные угрозы и методы защиты.
9) Использование метода композиционного планирования эксперимента для описания технологических процессов: метод. указания / сост. А.Н.Гайдадин, С.А.Ефремова; ВолгГТУ. – Волгоград, 2008. – 16 с.
10) Стивен С. Майерс. – Применение методов защиты от современных угроз безопасности для веб-приложений. Web Application Security: Exploitation and Countermeasures for Modern Web Applications".