3 ЛЕКЦИЯ

ЛЕКТОР 2021+

РАХИМОВА Д.Р.

ВЕБ-БЕЗОПАСНОСТЬ

РАСКРЫТИЕ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

03

Казахский Национальный Университет им. Аль-Фараби, Факультет Информационных технологий

Цель лекции и задачи данного урока:

- **Познакомить студентов с определением «кибербезопасность»**
  - дать подробную информацию, определить основные уязвимости и способы их выявление, исправление;
- **Ответить на вопрос: «Что такое раскрытие конфиденциальных данных?»**
  - рассмотреть примеры возникновение угроз, дальнейшие последствия и способы предотвращение угроз;
- **Проверить освоенность темы студентами с помощью теста.**

3 ЛЕКЦИЯ

О ВЕБ-БЕЗОПАСНОСТИ

ТАКЖЕ ИЗВЕСТНА КАК КИБЕРБЕЗОПАСНОСТЬ

В основном это означает защиту веб-сайта или веб-приложения путем обнаружения, предотвращения и реагирования на киберугрозы.

Веб-безопасность - это система мер, политики и протоколов, которые могут защитить веб-сайт или веб-приложение от взлома или проникновения неавторизованного персонала.

Это неотъемлемое [illegible] безопасности жизне[illegible] веб-приложений и веб-сервисов. Все, что применяется в Интернете, должно иметь какую-либо форму веб-безопасности для защиты.

?

Что такое веб-безопасность

3 ЛЕКЦИЯ

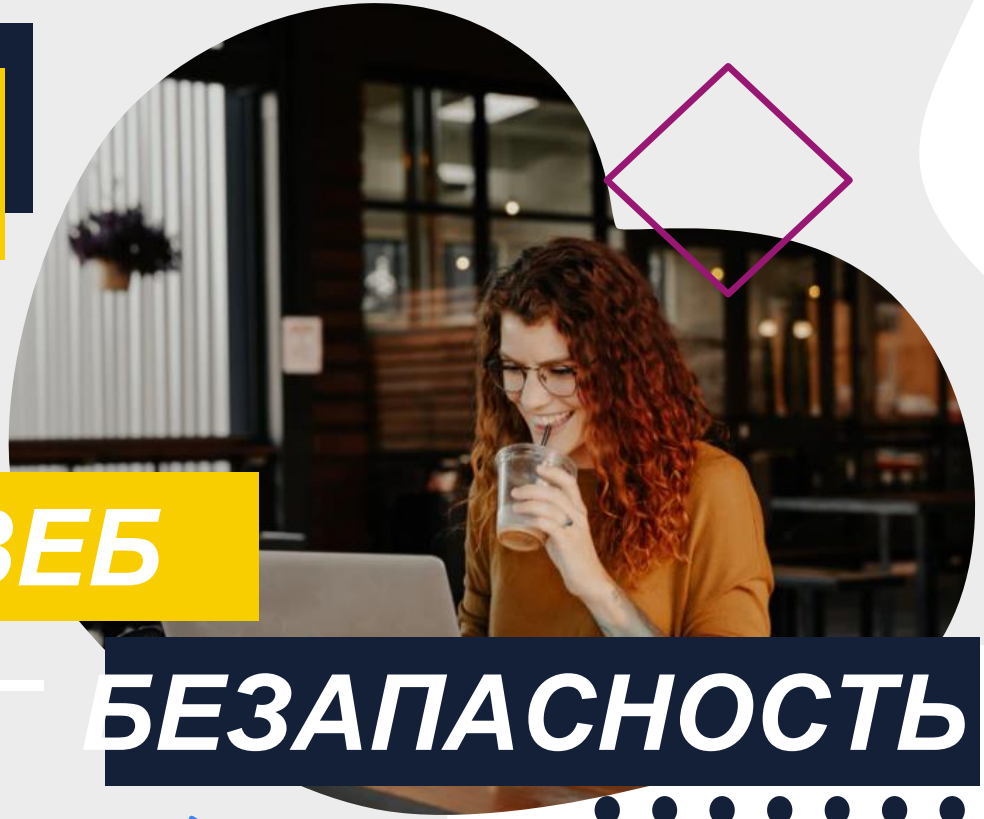
О ВЕБ-БЕЗОПАСНОСТИ

ТАКЖЕ ИЗВЕСТНА КАК КИБЕРБЕЗОПАСНОСТЬ

В основном это означает защиту веб-сайта или веб-приложения путем обнаружения, предотвращения и реагирования на киберугрозы.

Веб-безопасность - это система мер защиты и протоколов, которые могут защитить ваш веб-сайт или веб-приложение от взлома или проникновения неавторизованного персонала.

Это неотъемлемое подразделение информационной безопасности жизненно важно для защиты веб-сайтов, веб-приложений и веб-сервисов. Все, что применяется в Интернете, должно иметь какую-либо форму веб-безопасности для защиты.

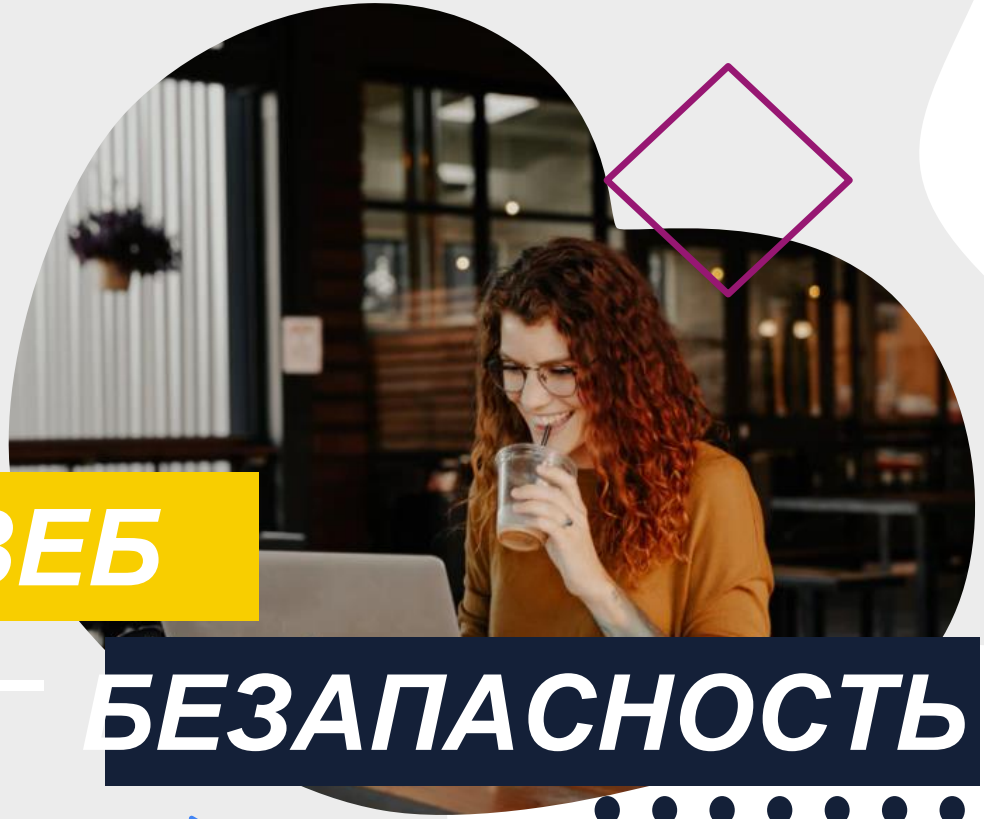


ВЕБ БЕЗАПАСНОСТЬ

Специалисты по кибербезопасности постоянно защищают компьютерные системы от различных типов киберугроз. Кибератаки ежедневно поражают предприятия и частные системы, и количество атак быстро увеличивается. По словам бывшего генерального директора Cisco Джона Чемберса, «есть два типа компаний: те, которые были взломаны, и те, кто еще не знает, что они были взломаны».

Мотивы кибератак многочисленны. Один - деньги. Кибер-злоумышленники могут отключить систему и потребовать плату за восстановление ее работоспособности. Программа-вымогатель - атака, требующая оплаты для восстановления услуг, - сейчас более сложна, чем когда-либо.

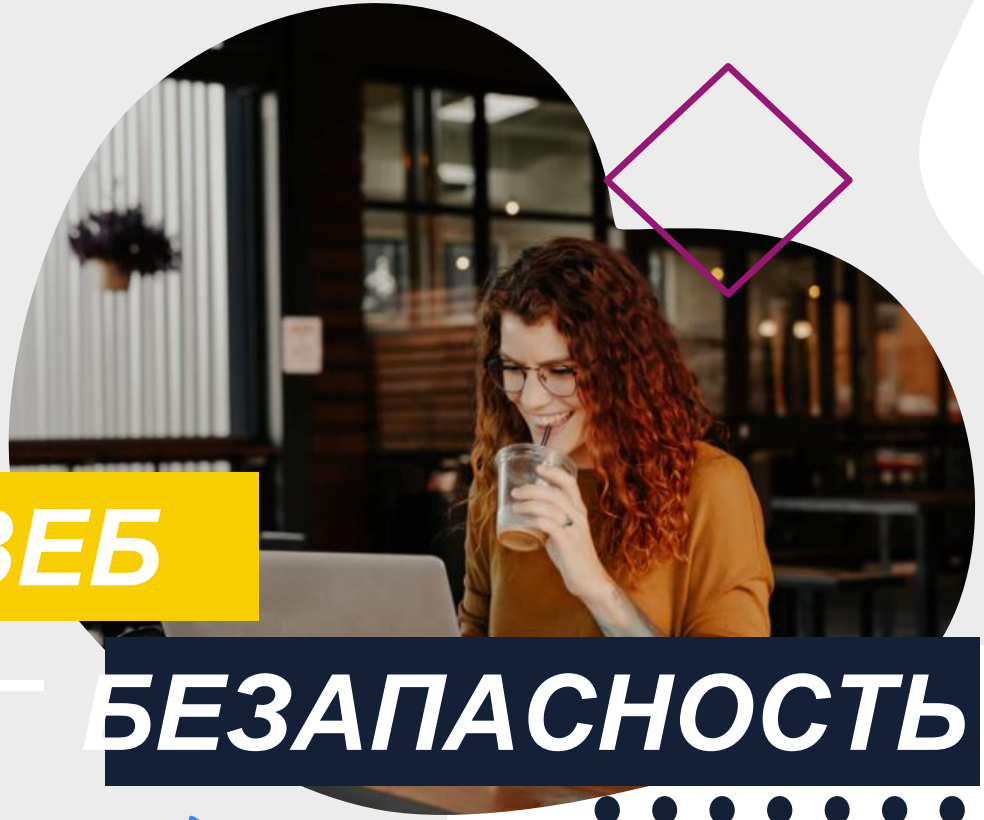
Корпорации уязвимы для кибератак, но и отдельные лица также становятся жертвами, часто потому, что они хранят личную информацию на своих мобильных телефонах и используют небезопасные общедоступные сети. К сожалению, киберпреступность случается каждый день, и для защиты веб-сайтов и веб-приложений от взлома необходимы серьезные меры безопасности.



ВЕБ — БЕЗАПАСНОСТЬ

Существует множество стандартов безопасности, которые необходимо соблюдать постоянно, и эти стандарты реализованы и выделены OWASP.

Самые опытные веб-разработчики из ведущих компаний, занимающихся кибербезопасностью, будут следовать стандартам OWASP, а также внимательно следить за базой данных инцидентов веб-взлома, чтобы узнать, когда, как и почему разные люди взламывают разные веб-сайты и службы.



ВЕБ — БЕЗАПАСНОСТЬ

СПОСОБЫ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ ОТ АТАК

Реальность такова, что умные злоумышленники могут быть достаточно компетентными, чтобы находить недостатки даже в достаточно надежной защищенной среде, поэтому рекомендуется использовать целостную стратегию безопасности.

ШАГИ ПО ЗАЩИТЕ

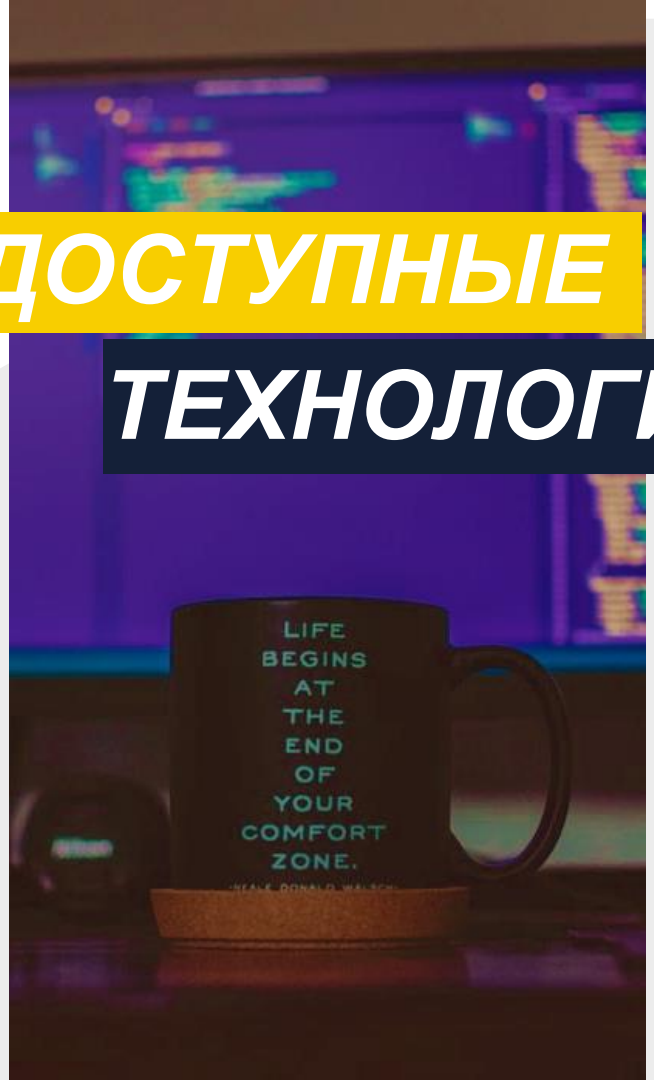
ШИФРОВАНИЕ
Применение современного шифрования.

ИСПРАВЛЕНИЕ
Постоянное исправление обнаруженных уязвимостей.

АУТЕНТИФИКАЦИЯ
Вам точно может помочь настройку правильной аутентификации.

ПРЕДОТВРАЩЕНИЕ КРАЖИ
Предотвращение кражи данных за счет использования безопасных методов разработки программного обеспечения.

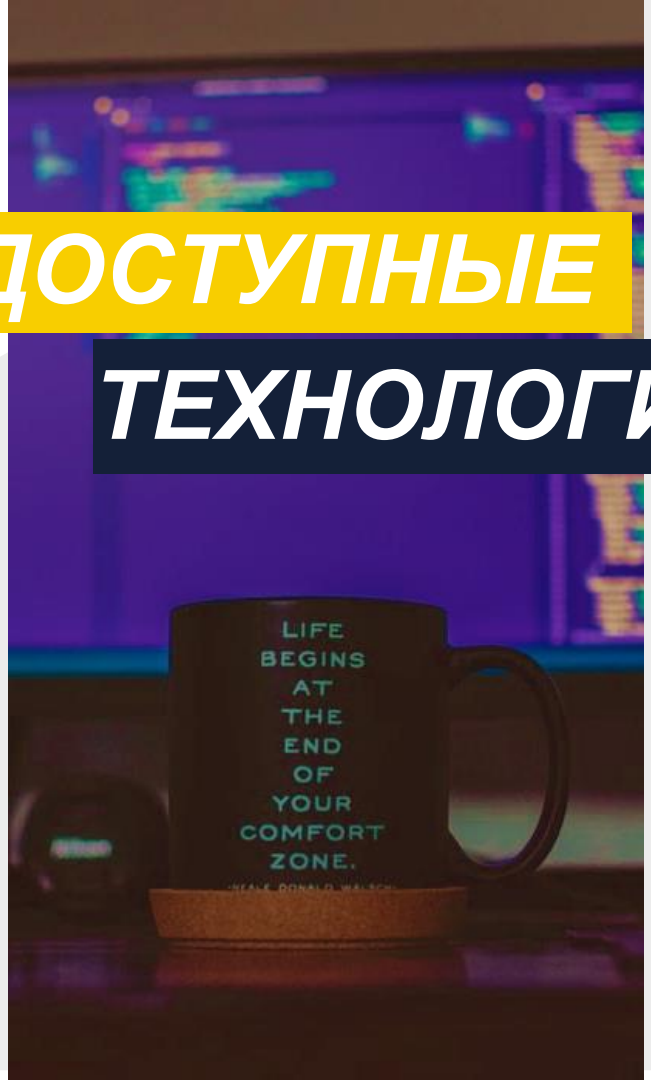
ДОСТУПНЫЕ ТЕХНОЛОГИЙ



ЧЕРНЫЙ ЯЩИК

Инструменты тестирования черного ящика

ДОСТУПНЫЕ ТЕХНОЛОГИЙ

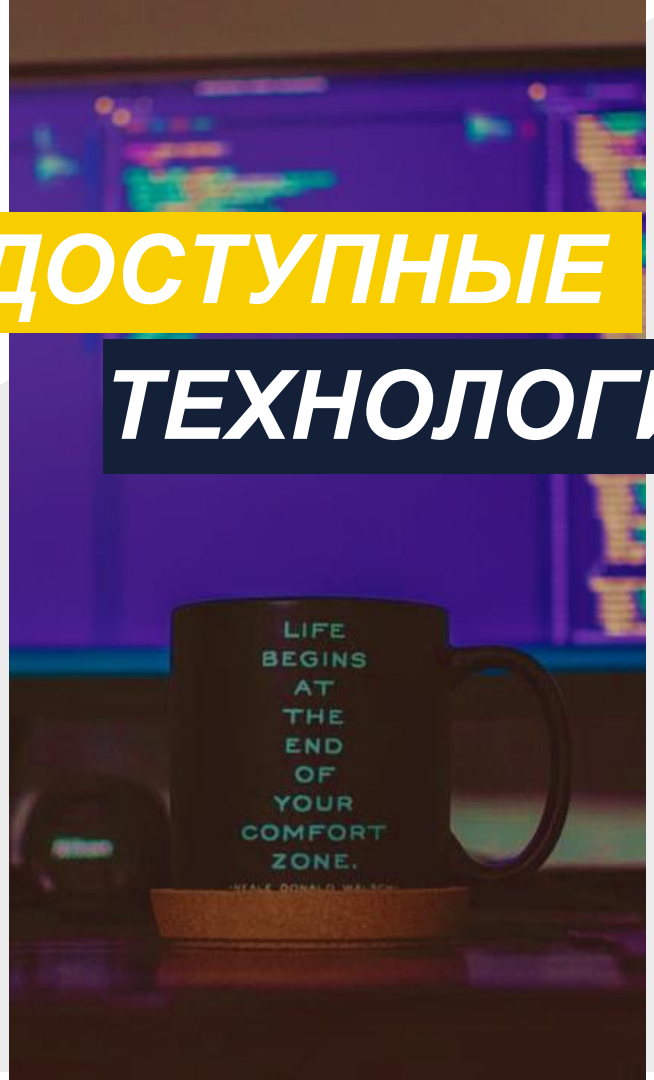


ЧЕРНЫЙ ЯЩИК

Инструменты тестирования черного ящика

ФАЗЗИНГ

Инструменты для фаззинга

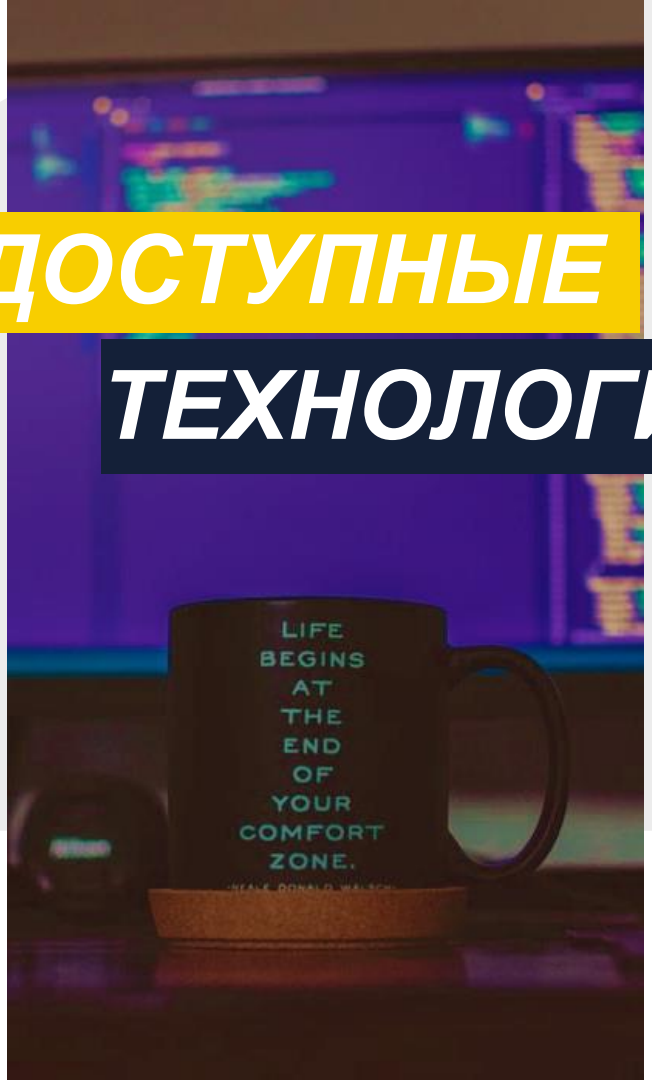


ДОСТУПНЫЕ ТЕХНОЛОГИЙ

ЧЕРНЫЙ ЯЩИК
Инструменты тестирования черного ящика

ФАЗЗИНГ
Инструменты для фаззинга

БЕЛЫЙ ЯЩИК
Инструменты тестирования белого ящика



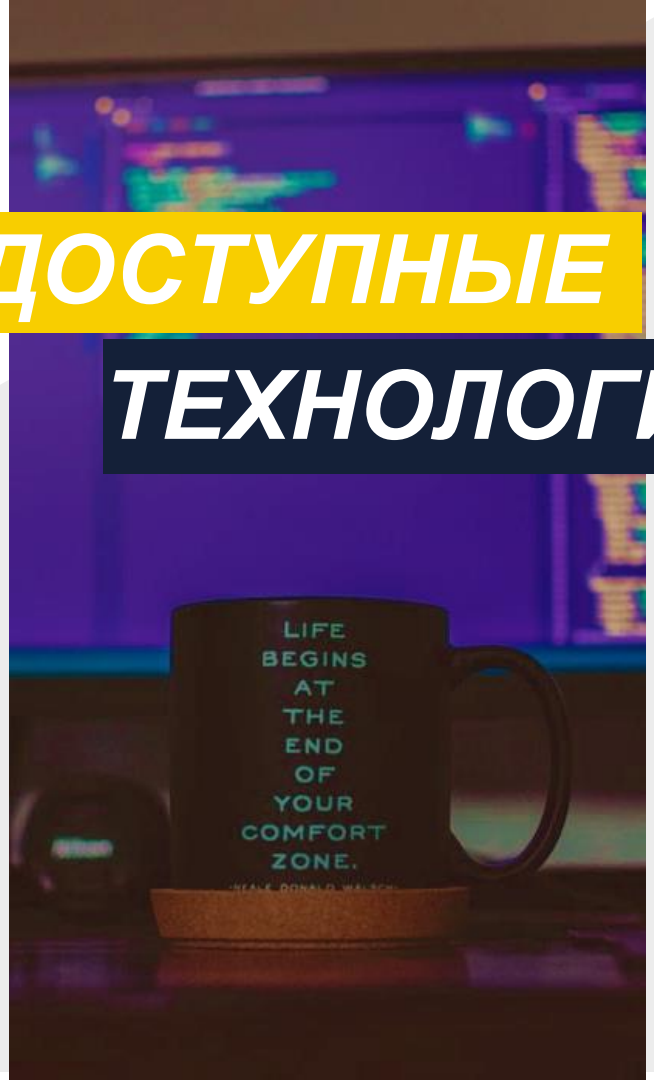
ДОСТУПНЫЕ ТЕХНОЛОГИЙ

ЧЕРНЫЙ ЯЩИК
Инструменты тестирования черного ящика

ФАЗЗИНГ
Инструменты для фаззинга

БЕЛЫЙ ЯЩИК
Инструменты тестирования белого ящика

WAF
Брандмауэры веб-приложений



ДОСТУПНЫЕ ТЕХНОЛОГИЙ

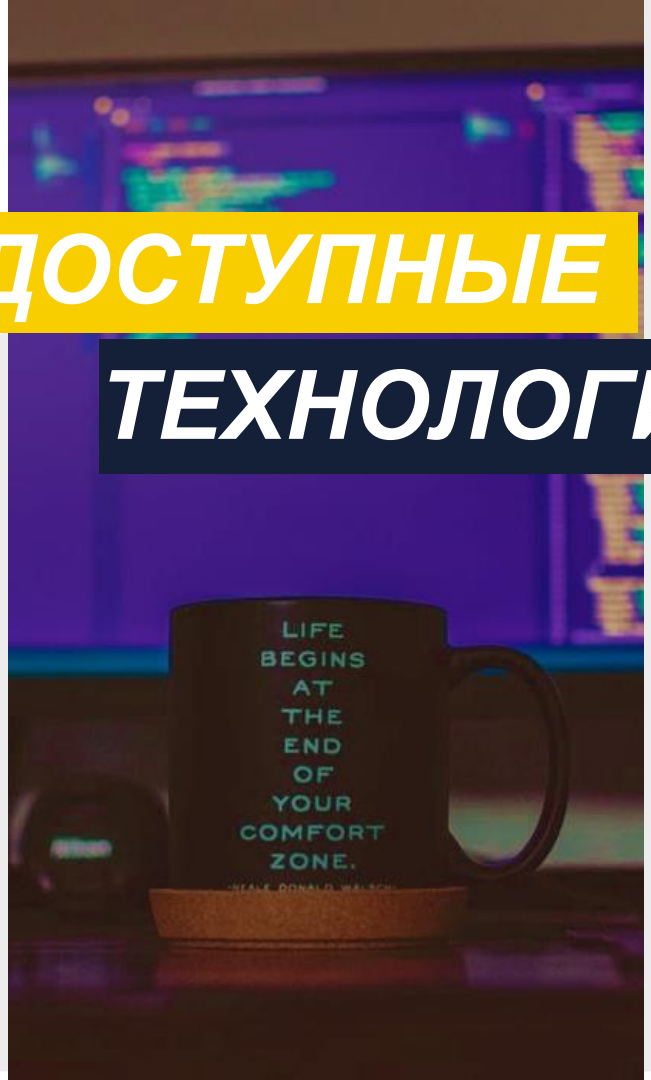
ЧЕРНЫЙ ЯЩИК
Инструменты тестирования черного ящика

ФАЗЗИНГ
Инструменты для фаззинга

БЕЛЫЙ ЯЩИК
Инструменты тестирования белого ящика

WAF
Брандмауэры веб-приложений

СКАНЕРЫ
Сканеры безопасности или уязвимостей



ДОСТУПНЫЕ ТЕХНОЛОГИЙ

ЧЕРНЫЙ ЯЩИК
Инструменты тестирования черного ящика

ФАЗЗИНГ
Инструменты для фаззинга

БЕЛЫЙ ЯЩИК
Инструменты тестирования белого ящика

WAF
Брандмауэры веб-приложений

СКАНЕРЫ
Сканеры безопасности или уязвимостей

ВЗЛОМ
Инструменты для взлома паролей

ОСНОВНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ

Безопасность вашего веб-сайта или веб-приложения зависит от уровня средств защиты, которые были на нем установлены и протестированы.

Существует несколько основных угроз безопасности, которые являются наиболее распространенными способами взлома веб-сайта или веб-приложения

3 ЛЕКЦИЯ

ОСНОВНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ

Безопасность вашего веб-сайта или веб-приложения зависит от уровня средств защиты, которые были на нем установлены и протестированы.

Существует несколько основных угроз безопасности, которые являются наиболее распространенными способами взлома веб-сайта или веб-приложения

1. SQL-инъекция
2. Нарушение пароля
3. Межсайтовый скриптинг
4. Данные нарушения
5. Удаленное включение файлов
6. Внедрение кода

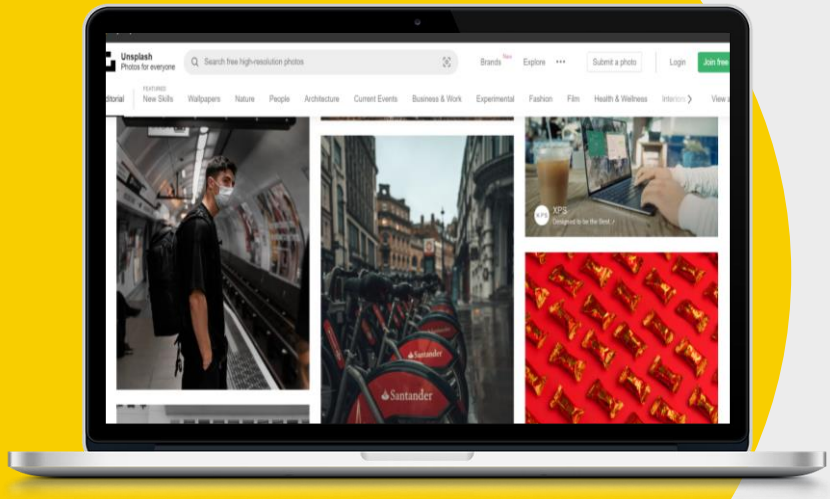
Что такое управление уязвимостями?

Управление уязвимостями - это циклическая практика выявления, классификации, устранения и смягчения уязвимостей безопасности. Существенные элементы управления уязвимостями включают обнаружение уязвимостей, оценку уязвимостей и исправление.

Методы обнаружения уязвимостей включают:

- Сканирование уязвимостей
- Тестирование на проникновение
- Взлом Google

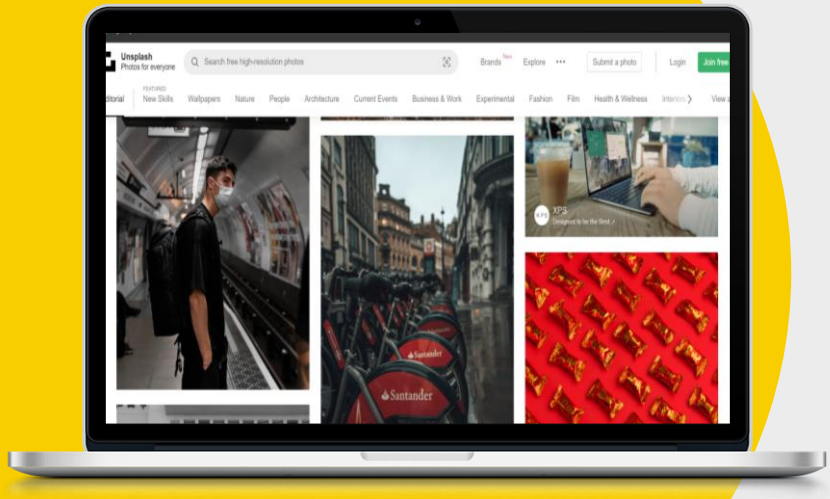
3 ЛЕКЦИЯ



ВИДЫ ВЕБ-БЕЗОПАСНОСТИ

Есть две большие стратегии защиты, которые разработчик может использовать для защиты своего веб-сайта или веб-приложения.

3 ЛЕКЦИЯ

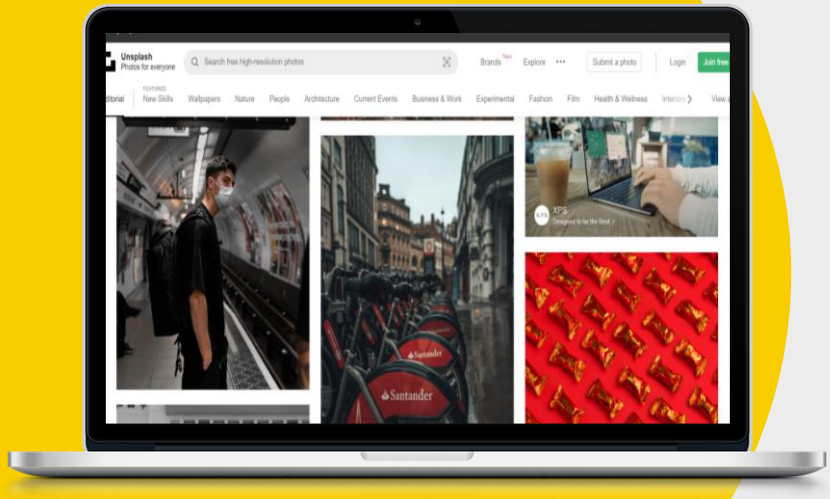


ВИДЫ ВЕБ-БЕЗОПАСНОСТИ

Есть две большие стратегии защиты, которые разработчик может использовать для защиты своего веб-сайта или веб-приложения.

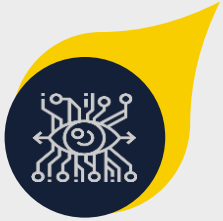
НАЗНАЧЕНИЕ РЕСУРСОВ

3 ЛЕКЦИЯ



ВИДЫ ВЕБ-БЕЗОПАСНОСТИ

Есть две большие стратегии защиты, которые разработчик может использовать для защиты своего веб-сайта или веб-приложения.



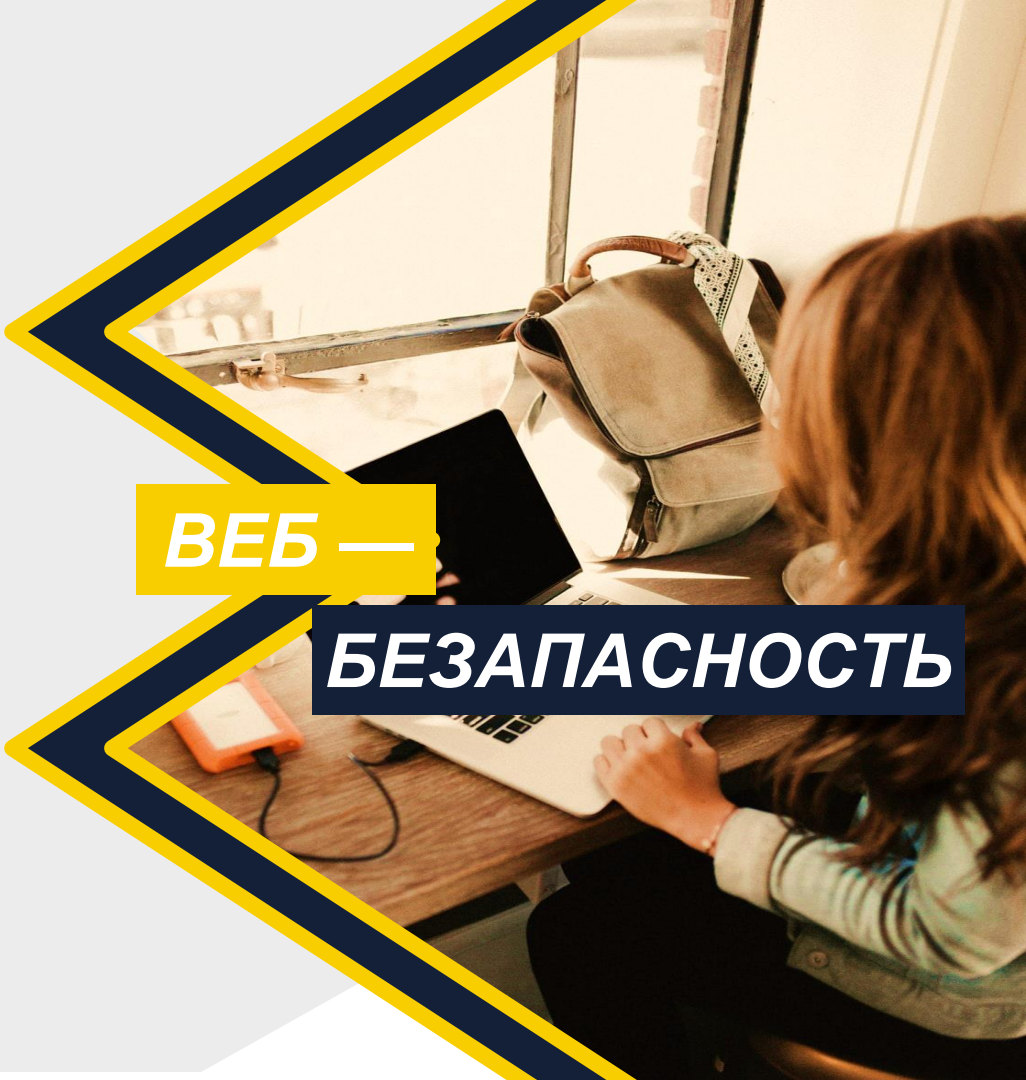
НАЗНАЧЕНИЕ РЕСУРСОВ

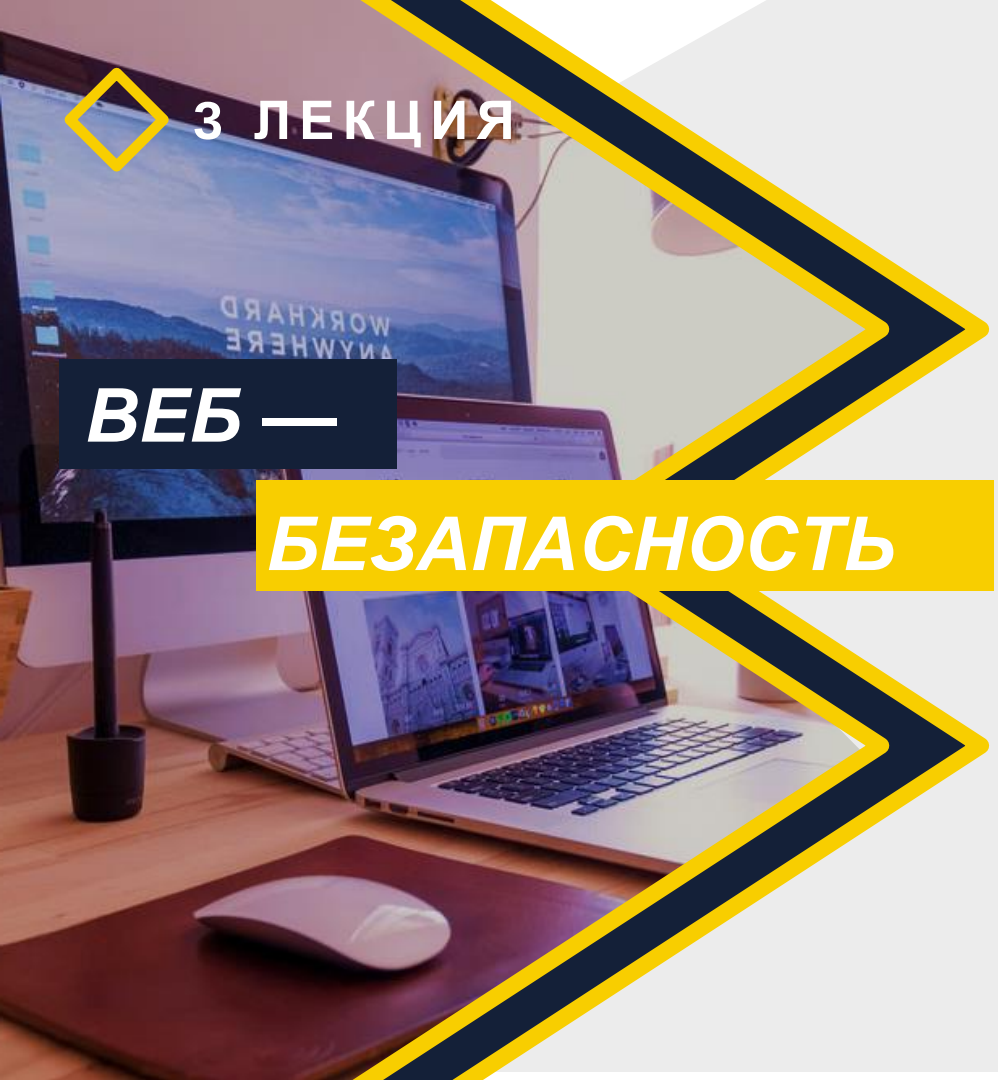
ВЕБ-СКАНИРОВАНИЕ

3 ЛЕКЦИЯ

НАЗНАЧЕНИЕ РЕСУРСОВ

Назначая все необходимые ресурсы причинам, которые предназначены для предупреждения разработчика о новых проблемах и угрозах веб-безопасности, разработчик может получать постоянную и обновленную систему предупреждений, которая поможет им обнаруживать и устранять любые угрозы до того, как безопасность будет официально нарушена.





3 ЛЕКЦИЯ

ВЕБ — БЕЗАПАСНОСТЬ

ВЕБ-СКАНИРОВАНИЕ

Уже существует несколько решений для веб-сканирования, которые можно купить или загрузить. Однако эти решения подходят только для известных угроз уязвимостей - поиск неизвестных угроз может быть намного сложнее. Этот метод может защитить от многих нарушений и, как доказано, обеспечивает безопасность веб-сайтов в долгосрочной перспективе.

Веб-безопасность также защищает посетителей от нижеперечисленных моментов

3 ЛЕКЦИЯ

Веб-безопасность также защищает посетителей от нижеперечисленных моментов

ПОХИЩЕННЫЕ ДАННЫЕ

Киберпреступники часто взламывают данные посетителей, которые хранятся на веб-сайте, такие как адреса электронной почты, платежная информация и некоторые другие детали

3 ЛЕКЦИЯ

Веб-безопасность также защищает посетителей от нижеперечисленных моментов

ПОХИЩЕННЫЕ ДАННЫЕ

Киберпреступники часто взламывают данные посетителей, которые хранятся на веб-сайте, такие как адреса электронной почты, платежная информация и некоторые другие детали

СХЕМЫ ФИШИНГА

это связано не только с электронной почтой, но и с помощью фишинга, хакеры создают макет, который выглядит точно так же, как веб-сайт, чтобы обмануть пользователя, вынуждая его предоставить свои конфиденциальные данные

3 ЛЕКЦИЯ

Веб-безопасность также защищает посетителей от нижеперечисленных моментов

ПОХИЩЕННЫЕ ДАННЫЕ

Киберпреступники часто взламывают данные посетителей, которые хранятся на веб-сайте, такие как адреса электронной почты, платежная информация и некоторые другие детали

СХЕМЫ ФИШИНГА

это связано не только с электронной почтой, но и с помощью фишинга, хакеры создают макет, который выглядит точно так же, как веб-сайт, чтобы обмануть пользователя, вынуждая его предоставить свои конфиденциальные данные

SEO-спам

Необычные ссылки, страницы и комментарии могут отображаться на сайте хакерами, чтобы отвлекать посетителей и направлять трафик на вредоносные веб-сайты

3 ЛЕКЦИЯ

Веб-безопасность также защищает посетителей от нижеперечисленных моментов

ПОХИЩЕННЫЕ ДАННЫЕ

Киберпреступники часто взламывают данные посетителей, которые хранятся на веб-сайте, такие как адреса электронной почты, платежная информация и некоторые другие детали

СХЕМЫ ФИШИНГА

это связано не только с электронной почтой, но и с помощью фишинга, хакеры создают макет, который выглядит точно так же, как веб-сайт, чтобы обмануть пользователя, вынуждая его предоставить свои конфиденциальные данные

SEO-спам

Необычные ссылки, страницы и комментарии могут отображаться на сайте хакерами, чтобы отвлекать посетителей и направлять трафик на вредоносные веб-сайты

Захват сеанса

Некоторые кибер-злоумышленники могут захватить сеанс пользователя и заставить его совершить нежелательные действия на сайте

Веб-безопасность также защищает посетителей от нижеперечисленных моментов

ПОХИЩЕННЫЕ ДАННЫЕ

Киберпреступники часто взламывают данные посетителей, которые хранятся на веб-сайте, такие как адреса электронной почты, платежная информация и некоторые другие детали

СХЕМЫ ФИШИНГА

это связано не только с электронной почтой, но и с помощью фишинга, хакеры создают макет, который выглядит точно так же, как веб-сайт, чтобы обмануть пользователя, вынуждая его предоставить свои конфиденциальные данные

SEO-спам

Необычные ссылки, страницы и комментарии могут отображаться на сайте хакерами, чтобы отвлекать посетителей и направлять трафик на вредоносные веб-сайты

Захват сеанса

Некоторые кибер-злоумышленники могут захватить сеанс пользователя и заставить его совершить нежелательные действия на сайте

Вредоносные перенаправления

Иногда атаки могут перенаправлять посетителей с сайта, который они посетили, на вредоносный сайт

РАСКРЫТИЕ ИНФОРМАЦИИ

Также известное как утечка информации - это когда веб-сайт непреднамеренно раскрывает конфиденциальную информацию о себе пользователям. В зависимости от контекста, веб-сайты могут передавать потенциальному злоумышленнику любую информацию:

- Данные о других пользователях, такие как имена пользователей или финансовая информация
- Технические подробности о веб-сайте и его инфраструктуре
- Конфиденциальные коммерческие или бизнес-данные

?

Что такое раскрытие информации

(конфиденциальных данных)

3 ЛЕКЦИЯ

РАСКРЫТИЕ ИНФОРМАЦИИ

Также известное как утечка информации - это когда веб-сайт непреднамеренно раскрывает конфиденциальную информацию своим пользователям. В зависимости от контекста, веб-сайты могут передавать потенциальному злоумышленнику любую информацию

РАСКРЫТИЕ ИНФОРМАЦИИ

Также известное как утечка информации - это когда веб-сайт непреднамеренно раскрывает конфиденциальную информацию своим пользователям. В зависимости от контекста, веб-сайты могут передавать потенциальному злоумышленнику любую информацию

Данные о других пользователях, такие как имена пользователей или финансовая информация

РАСКРЫТИЕ ИНФОРМАЦИИ

Также известное как утечка информации - это когда веб-сайт непреднамеренно раскрывает конфиденциальную информацию своим пользователям. В зависимости от контекста, веб-сайты могут передавать потенциальному злоумышленнику любую информацию

- Данные о других пользователях, такие как имена пользователей или финансовая информация
- Технические подробности о веб-сайте и его инфраструктуре

РАСКРЫТИЕ ИНФОРМАЦИИ

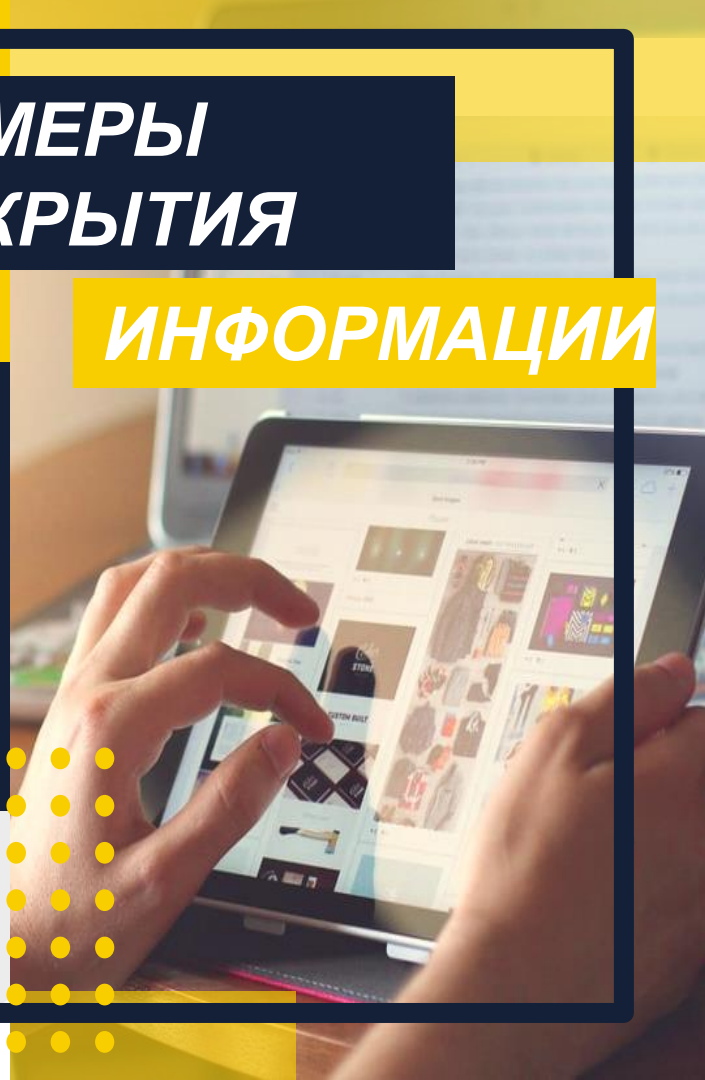
Также известное как утечка информации - это когда веб-сайт непреднамеренно раскрывает конфиденциальную информацию своим пользователям. В зависимости от контекста, веб-сайты могут передавать потенциальному злоумышленнику любую информацию

- Данные о других пользователях, такие как имена пользователей или финансовая информация
- Технические подробности о веб-сайте и его инфраструктуре
- Конфиденциальные коммерческие или бизнес-данные

3 ЛЕКЦИЯ

ПРИМЕРЫ РАСКРЫТИЯ ИНФОРМАЦИИ

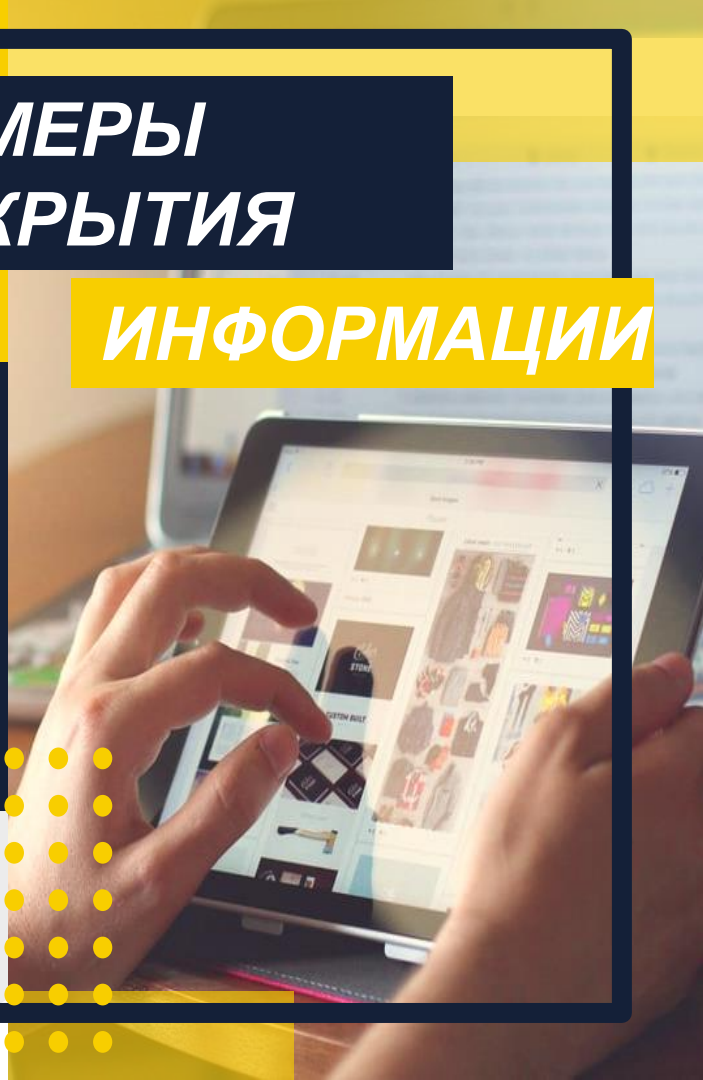
Выявление имен скрытых каталогов, их структуры и содержимого с помощью robots.txt списка файлов или каталогов



3 ЛЕКЦИЯ

ПРИМЕРЫ РАСКРЫТИЯ ИНФОРМАЦИИ

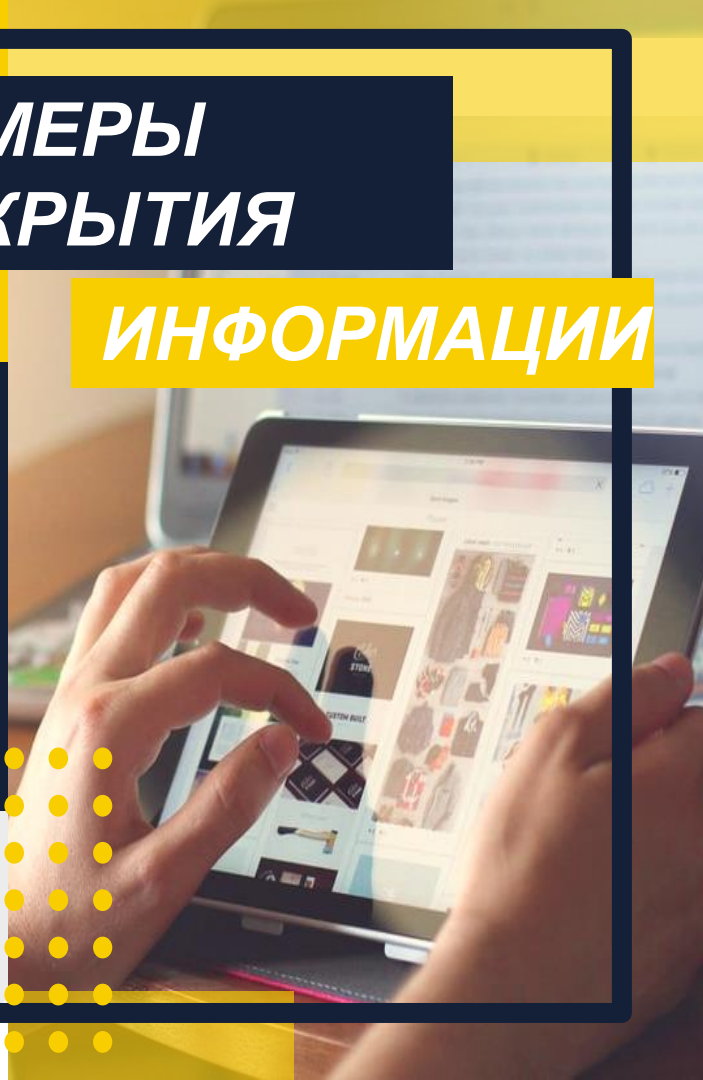
- Выявление имен скрытых каталогов, их структуры и содержимого с помощью robots.txt списка файлов или каталогов
- Предоставление доступа к файлам исходного кода через временные резервные копии



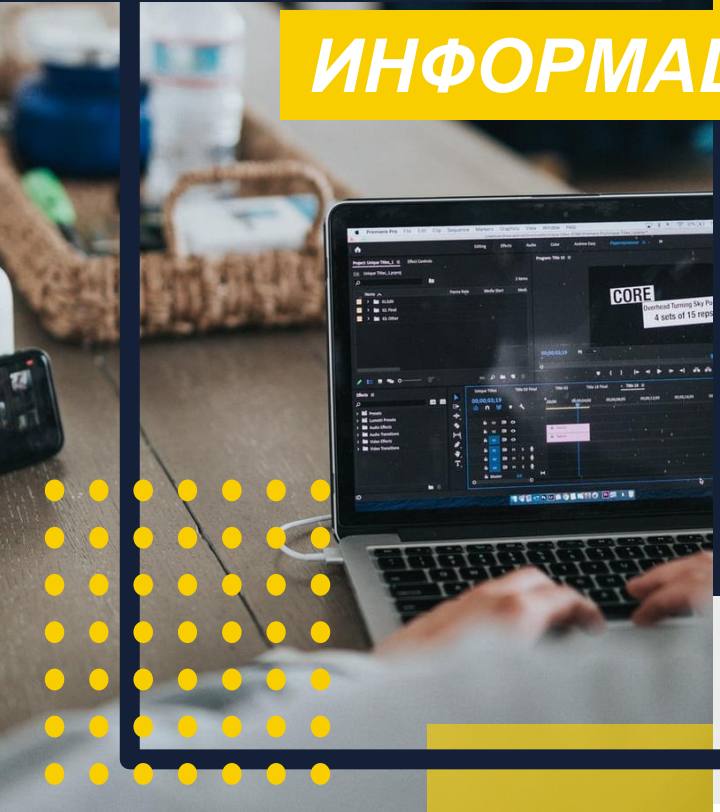
3 ЛЕКЦИЯ

ПРИМЕРЫ РАСКРЫТИЯ ИНФОРМАЦИИ

- Выявление имен скрытых каталогов, их структуры и содержимого с помощью robots.txt списка файлов или каталогов
- Предоставление доступа к файлам исходного кода через временные резервные копии
- Явное упоминание имен таблиц или столбцов базы данных в сообщениях об ошибках

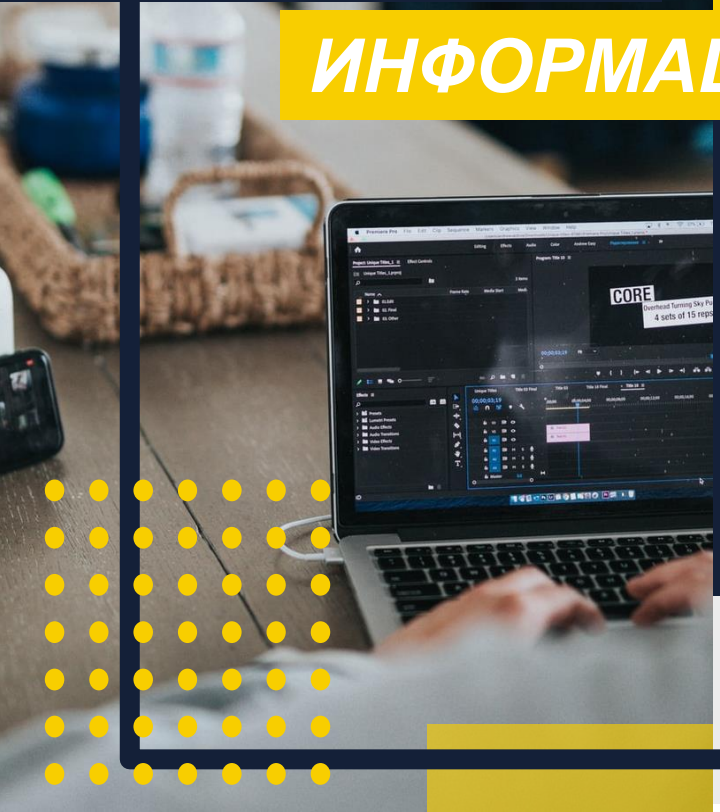


ПРИМЕРЫ РАСКРЫТИЯ ИНФОРМАЦИИ



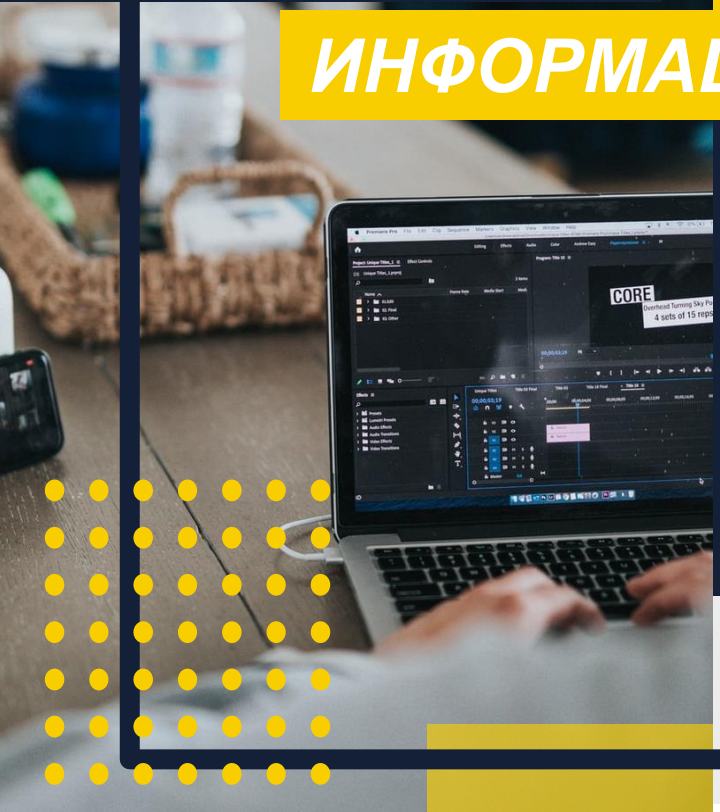
Неоправданное раскрытие конфиденциальной информации, такой как данные кредитной карты

ПРИМЕРЫ РАСКРЫТИЯ ИНФОРМАЦИИ



- Неоправданное раскрытие конфиденциальной информации, такой как данные кредитной карты
- Жесткое кодирование ключей API, IP-адресов, учетных данных базы данных и т.д. в исходном коде

ПРИМЕРЫ РАСКРЫТИЯ ИНФОРМАЦИИ



- Неоправданное раскрытие конфиденциальной информации, такой как данные кредитной карты
- Жесткое кодирование ключей API, IP-адресов, учетных данных базы данных и т.д. в исходном коде
- Намек на наличие или отсутствие ресурсов, имен пользователей и т. д. посредством тонких различий в поведении приложений

УЯЗВИМОСТИ

Уязвимости, связанные с раскрытием информации, могут возникать бесчисленным множеством различных способов, но в целом их можно разделить на следующие категории:

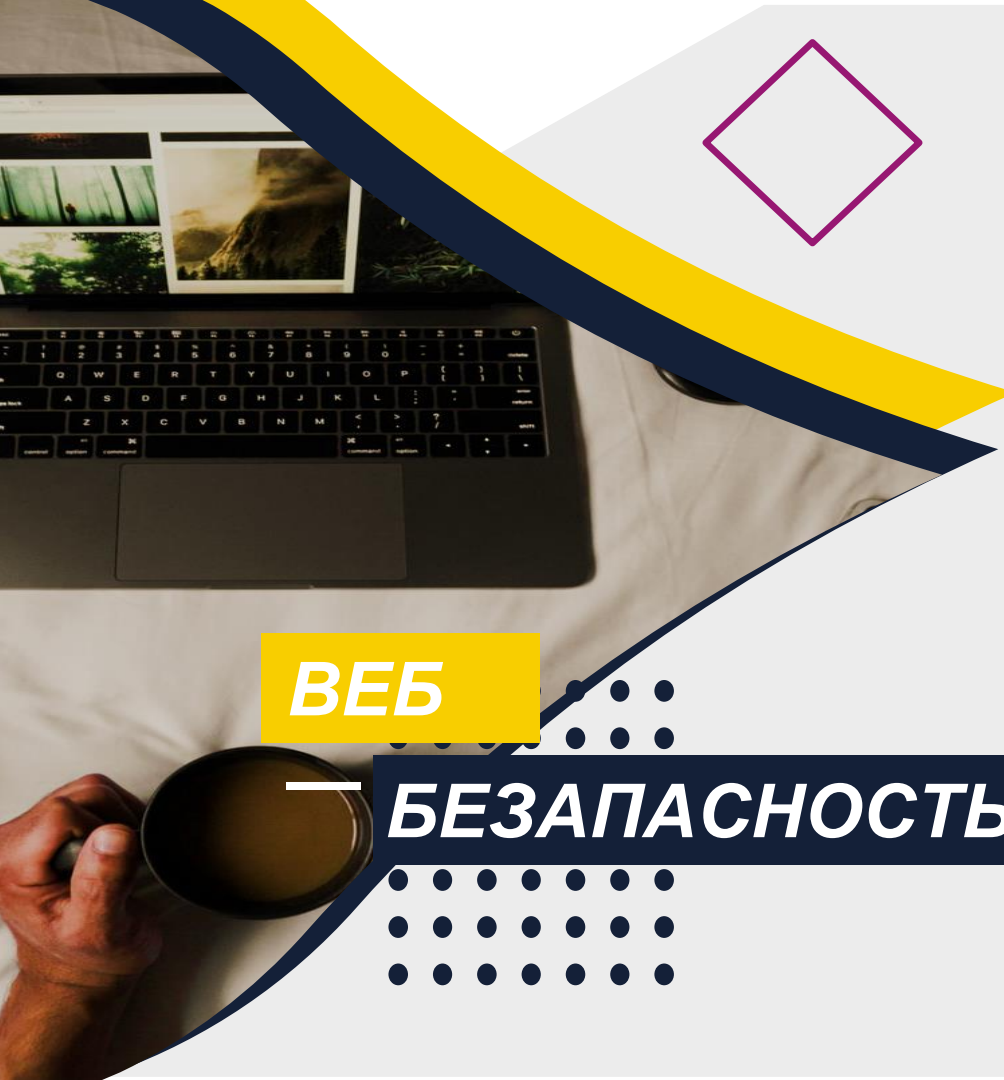
3 ЛЕКЦИЯ

УЯЗВИМОСТИ

Уязвимости, связанные с раскрытием информации, могут возникать бесчисленным множеством различных способов, но в целом их можно разделить на следующие категории:

НЕСПОСОБНОСТЬ УДАЛИТЬ

Неспособность удалить внутренний контент из общедоступного контента . Например, комментарии разработчиков в разметке иногда видны пользователям в производственной среде.



ВЕБ — БЕЗАПАСНОСТЬ

УЯЗВИМОСТИ

НЕБЕЗОПАСНАЯ КОНФИГУРАЦИЯ

Небезопасная конфигурация сайта и связанных технологий . Например, если не отключить функции отладки и диагностики, злоумышленники могут получить полезные инструменты, которые помогут им получить конфиденциальную информацию. Конфигурации по умолчанию также могут сделать веб-сайты уязвимыми, например, отображая слишком подробные сообщения об ошибках.

Некорректный дизайн & поведение

Некорректный дизайн и поведение приложения . Например, если веб-сайт возвращает отдельные ответы при возникновении различных состояний ошибки, это также может позволить злоумышленникам перечислить конфиденциальные данные , такие как действительные учетные данные пользователя.

3 ЛЕКЦИЯ

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ УЯЗВИМОСТЬ

Полностью предотвратить раскрытие информации сложно из-за огромного количества способов, которыми это может произойти. Однако есть несколько общих рекомендаций, которым вы можете следовать, чтобы минимизировать риск проникновения подобных уязвимостей на ваши собственные веб-сайты.

ОСВЕДОМИТЬ О ИНФОРМАЦИИ

Убедитесь, что вы полностью осведомлены о конфиденциальной информации. Иногда, казалось бы, безобидная информация может быть намного полезнее для злоумышленника, чем люди думают. Выявление опасностей может помочь обеспечить более [illegible] обращение с конфиденциальной информацией в вашей организации.

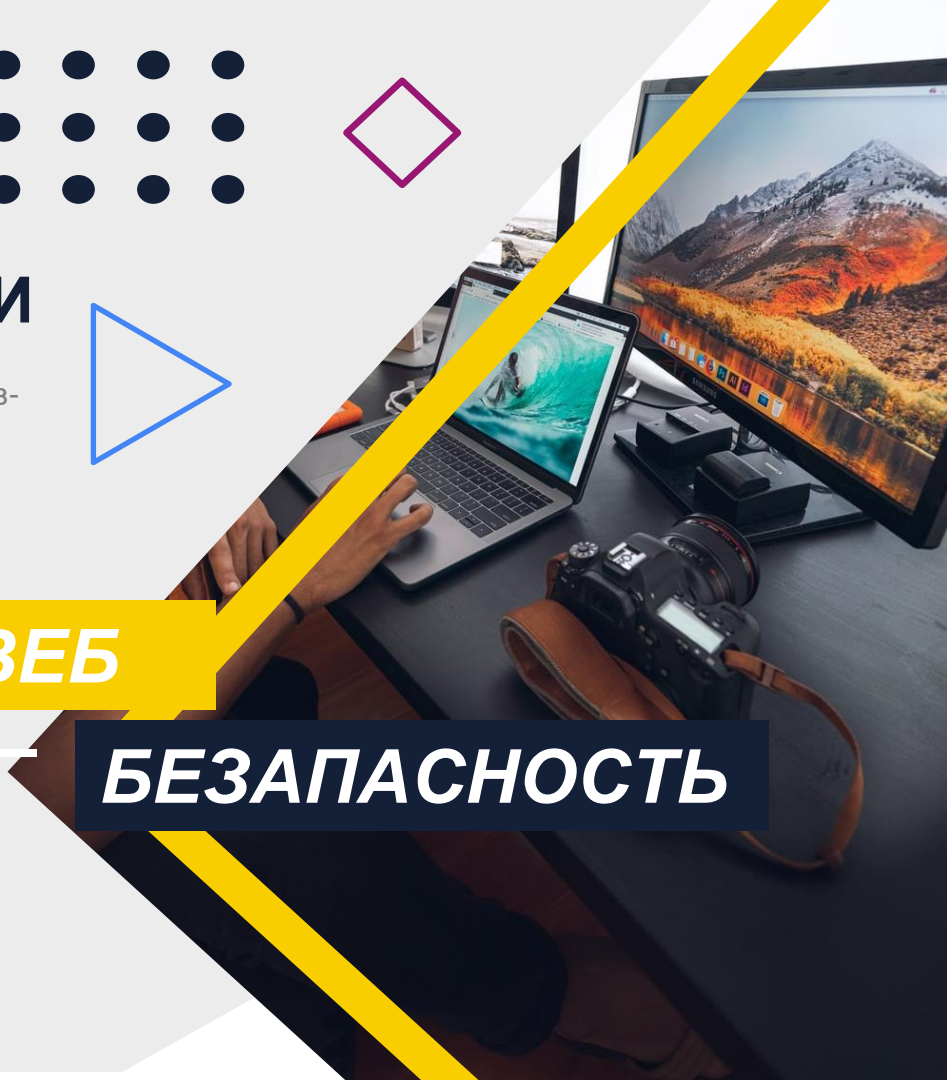
?

Как предотвратить раскрытие информации уязвимости

3 ЛЕКЦИЯ

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ УЯЗВИМОСТИ

Полностью предотвратить раскрытие информации сложно из-за огромного количества способов, которыми это может произойти. Однако есть несколько общих рекомендаций, которым вы можете следовать, чтобы минимизировать риск проникновения подобных уязвимостей на ваши собственные веб-сайты.



ВЕБ — БЕЗАПАСНОСТЬ

3 ЛЕКЦИЯ

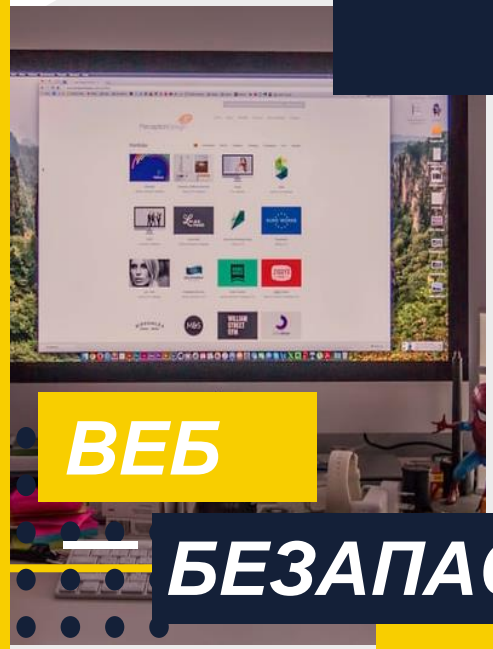
СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ УЯЗВИМОСТИ

Полностью предотвратить раскрытие информации сложно из-за огромного количества способов, которыми это может произойти. Однако есть несколько общих рекомендаций, которым вы можете следовать, чтобы минимизировать риск проникновения подобных уязвимостей на ваши собственные веб-сайты.

ОСВЕДОМИТЬ О ИНФОРМАЦИИ

Убедитесь, что все, кто участвует в создании веб-сайта, полностью осведомлены о том, какая информация считается конфиденциальной. Иногда, казалось бы, безобидная информация может быть намного полезнее для злоумышленника, чем люди думают. Выделение этих опасностей может помочь обеспечить более безопасное обращение с конфиденциальной информацией в вашей организации.

3 ЛЕКЦИЯ



ВЕБ — БЕЗАПАСНОСТЬ

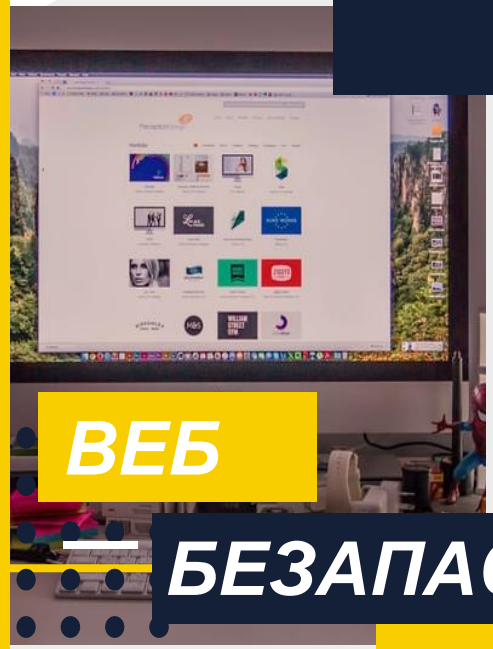
О СПОСОБАХ ЗАЩИТЫ

ЗАЩИТА ИНФОРМАЦИИ УЯЗВИМОСТИ

ПОСТОЯННАЯ ПРОВЕРКА

Проверяйте любой код на предмет потенциального раскрытия информации как часть процессов контроля качества или сборки. Некоторые связанные задачи, например удаление комментариев разработчиков, должно быть относительно легко автоматизировать.

3 ЛЕКЦИЯ



ВЕБ — БЕЗАПАСНОСТЬ

О СПОСОБАХ ЗАЩИТЫ

ЗАЩИТА ИНФОРМАЦИИ УЯЗВИМОСТИ

ПОСТОЯННАЯ ПРОВЕРКА

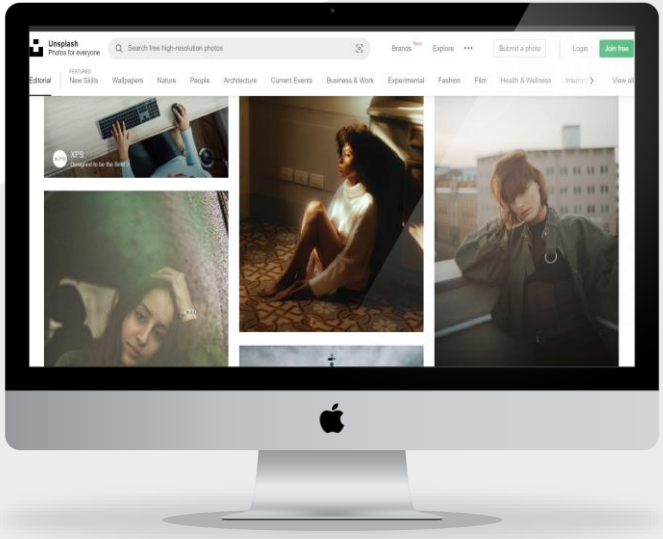
Проверяйте любой код на предмет потенциального раскрытия информации как часть процессов контроля качества или сборки. Некоторые связанные задачи, например удаление комментариев разработчиков, должно быть относительно легко автоматизировать.

ОБЩИЕ СООБЩЕНИЯ ОБ ОШИБКАХ

По возможности используйте общие сообщения об ошибках. Не сообщайте злоумышленникам о поведении приложения без надобности.

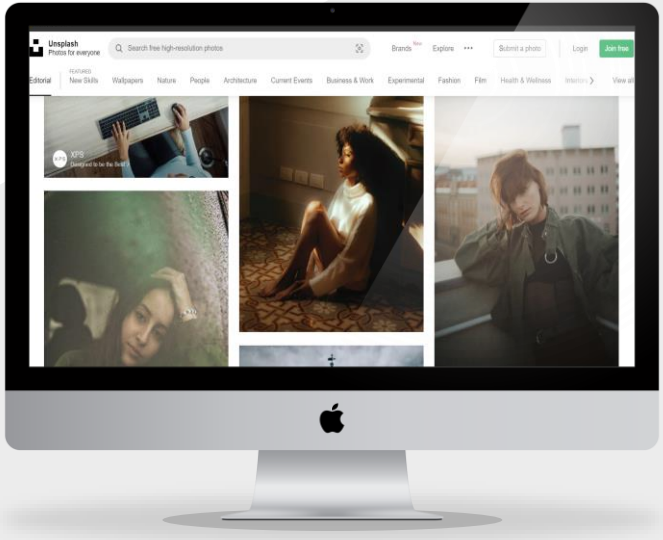
О СПОСОБАХ ЗАЩИТЫ

ЗАЩИТА ИНФОРМАЦИИ УЯЗВИМОСТИ



ДВОЙНАЯ ПРОВЕРКА

Дважды проверьте, что в производственной среде отключены все функции отладки или диагностики.



О СПОСОБАХ ЗАЩИТЫ

ЗАЩИТА ИНФОРМАЦИИ УЯЗВИМОСТИ

ДВОЙНАЯ ПРОВЕРКА

Дважды проверьте, что в производственной среде отключены все функции отладки или диагностики.

ПОНИМАНИЕ КОНФИГУРАЦИИ

Убедитесь, что вы полностью понимаете параметры конфигурации и последствия для безопасности любых сторонних технологий, которые вы внедряете. Найдите время, чтобы изучить и отключить любые функции и настройки, которые вам действительно не нужны.

СПАСИБО ЗА ВНИМАНИЕ!