



## Инструкция пользователя «True Tutor»

### Быстрый старт

#### Что вам понадобится

- Документ для обработки (PDF, DOC, DOCX, HTML и др.)
- Доступ к системе «True Tutor»
- 15-30 минут для настройки первого курса

#### Основные этапы работы

1. Загрузка документа → 2. Подготовка документа → 3. Создание глав → 4. Выбор языка и стиля для генерации текста → 5. Генерация вопросов к главам → 6. Генерация общих вопросов ко всему уроку -> 7. Создание иллюстраций -> 8. Экспорт учебного материала.
2. Следуйте подсказкам на каждом этапе

### Этап 1: Загрузка документа

#### Как загрузить документ

1. Нажмите кнопку "Загрузить документ" на главной странице;
2. Выберите файл с вашего компьютера или перетащите в окно;

### Этап 2. Подготовка документа

1. Из предустановленных настроек, выберите формат обучения, который вам подходит;
2. Задайте категорию обучающихся (роль);
3. Проверьте правильность преобразования таблиц и картинок;
4. При необходимости, отредактируйте название курса;
5. Нажмите кнопку «Далее».

◀ Назад

Основные уязвимости WEB приложений.docx ...Не проверен

Дата последнего изменения: 12.8.2025, 05:51

1. Подготовка документа 2. Главы урока 3. Генерированные главы 4. Вопросы к главам 5. Общие вопросы 6. Иллюстрации 7. Публикация Далее >

**Загруженный документ**

Основные уязвимости WEB приложений.docx



**Учебный материал**

Скачать распознанный документ Загрузить отредактированный документ

Выбор пресета для формирования учебного материала  
Для оффлайн обучения (большой объем уроков)

Выбор роли для обучения  
Необходимо для корректного формирования содержимого уроков и вопросов.  
web разработчик

Название урока  
Будет использоваться как название учебного материала при публикации.  
Основные уязвимости WEB приложений.docx

Проверьте правильность преобразования картинок и таблиц

## Этап 3. Создание глав

1. При необходимости скорректируйте желаемый объем глав для разделения текста (по умолчанию он заполнен по выбранному формату обучения);
2. Нажмите кнопку «Разбить на главы»;
3. Проверьте корректность разбиения, при необходимости скорректируйте главы, добавив или удалив;
4. Нажмите «Далее».

◀ Назад

Основные уязвимости WEB приложений.docx ...Не проверен

Дата последнего изменения: 12.8.2025, 07:01

1. Подготовка документа **2. Главы урока** 3. Генерированные главы 4. Вопросы к главам 5. Общие вопросы 6. Иллюстрации 7. Публикация Далее >

✓ Система обработала текст и выделила главы. Проверьте их на полноту информации

**Обработанный документ**

1. SQL Injection (SQLi)

Что это: Внедрение вредоносного SQL-кода через пользовательский ввод, позволяющее атакующему выполнять произвольные запросы к базе данных.

Пример уязвимого кода:

```
python
```

Уязвимо

```
query = f"SELECT * FROM users WHERE name = '{username}' AND password = '{password}'"
```

Как защититься:

- Используйте параметризованные запросы/prepared statements

**Сформированные главы урока**

Задайте желаемый объем глав для генерации текста на следующем шаге.  
ⓘ Это необходимо для разметки текста документа на главы соответствующего объема

Количество слов в главах  
1000 Разбить на главы >

**Глава 1**

Название главы  
1. SQL Injection (SQLi)

Содержание главы

Что это: Внедрение вредоносного SQL-кода через пользовательский ввод, позволяющее атакующему выполнять произвольные запросы к базе данных.

Пример уязвимого кода.

## Этап 4. Выбор языка и стиля для учебного материала

1. Выберите язык и стиль для генерации учебного материала;
2. Нажмите «Сгенерировать текст»;

3. Проверьте текст, скорректируйте при необходимости и нажмите «Далее».

TrueTutor

◀ Назад

Основные уязвимости WEB приложений.docx

Дата последнего изменения: 12.8.2025, 07:01

На проверке

1. Подготовка документа 2. Главы урока 3. Сгенерированные главы 4. Вопросы к главам 5. Общие вопросы 6. Иллюстрации 7. Публикация

Далее >

Выберите язык и стиль написания для начала генерации текста

Язык: Русский  
Стиль написания: Для инженеров

Количество слов в абзацах: 300

Стиль написания: Для инженеров

Для студентов  
Для поколения Z  
Для рабочих специальностей

Глава 1: 1. SQL Injection (SQLi)

Что это: Внедрение вредоносного SQL-кода через пользовательский ввод, позволяющее атакующему выполнять произвольные запросы к базе данных.  
Пример уязвимого кода:  
python  
Уязвимо

## Этап 5. Вопросы к главам

1. Задайте количество основных и ситуативных вопросов к каждой главе
2. Сгенерируйте вопросы
3. Проверьте корректность сгенерированных вопросов, при необходимости скорректируйте
4. Проверьте текст вариантов ответа и определение правильно, при необходимости скорректируйте
5. Если необходимо добавьте вопросы вручную

TrueTutor

◀ Назад

Основные уязвимости WEB приложений.docx

Дата последнего изменения: 12.8.2025, 07:01

На проверке

1. Подготовка документа 2. Главы урока 3. Сгенерированные главы 4. Вопросы к главам 5. Общие вопросы 6. Иллюстрации 7. Публикация

Далее >

Система сформировала вопросы к главам. Проверьте их корректность.

Вопросы к тексту: 4  
Ситуативные вопросы: 0  
Сгенерировать вопросы >

Глава 1: 1. SQL Injection (SQLi)

### Уязвимость SQL-инъекции

\*\*Что такое SQL-инъекция\*\*  
SQL-инъекция – это тип атаки, при котором злоумышленник внедряет вредоносный SQL-код через пользовательский ввод. Это позволяет атакующему выполнять произвольные запросы к базе данных, что может привести к утечке, изменению или удалению данных. Уязвимость возникает, когда входные данные пользователя не проверяются и напрямую вставляются в SQL-запросы.

\*\*Как работает атака\*\*  
Если приложение формирует SQL-запрос, используя строку,

Вопросы к главе 1

Вопрос 1

Что происходит при SQL-инъекции, если пользовательский ввод не проверяется перед вставкой в SQL-запрос?

Варианты ответов

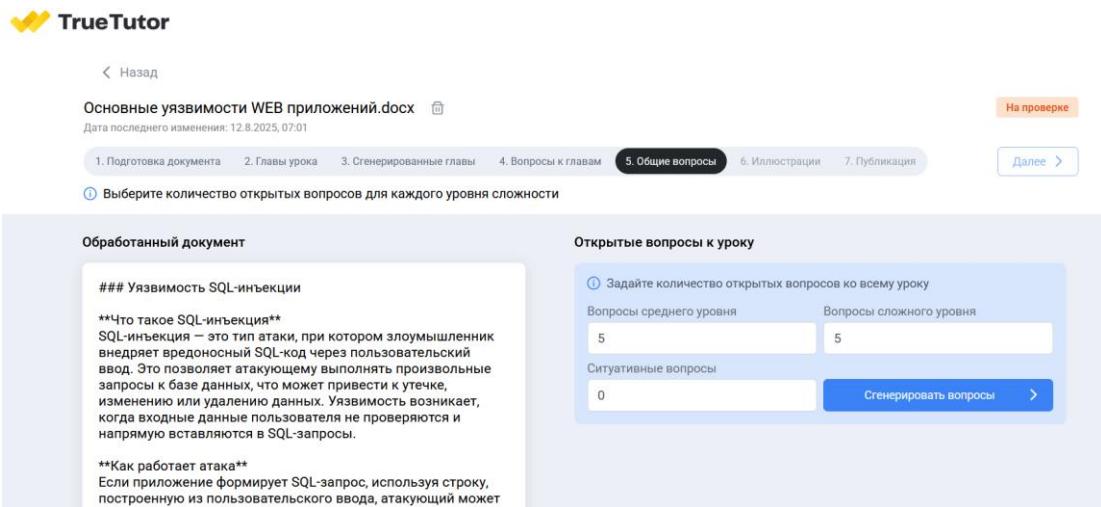
Злоумышленник может выполнить произвольные запросы к базе данных, включая чтение, изменение или удаление данных

Система автоматически блокирует подозрительные запросы и предупреждает администратора

## Этап 6. Общие вопросы

1. На этом этапе вы можете задать количество вопросов ко всему уроку разного уровня сложности;
2. Проверьте корректность сгенерированных вопросов, при необходимости, отредактируйте;

3. Проверьте корректность правильного ответа, сгенерированного системой – с ним система будет сравнивать ответ ученика.



The screenshot shows the 'TrueTutor' software interface. At the top, there is a navigation bar with tabs: '1. Подготовка документа', '2. Главы урока', '3. Сгенерированные главы', '4. Вопросы к главам', '5. Общие вопросы' (which is selected and highlighted in dark blue), '6. Иллюстрации', and '7. Публикация'. There is also a 'На проверке' (On review) button and a 'Далее >' (Next) button. The main area is divided into two sections: 'Обработанный документ' (Processed document) on the left and 'Открытые вопросы к уроку' (Open questions for the lesson) on the right. The 'Обработанный документ' section contains a text box with the following content:

```
### Уязвимость SQL-инъекции
**Что такое SQL-инъекция?**
SQL-инъекция – это тип атаки, при котором злоумышленник внедряет вредоносный SQL-код через пользовательский ввод. Это позволяет атакующему выполнять произвольные запросы к базе данных, что может привести к утечке, изменению или удалению данных. Уязвимость возникает, когда входные данные пользователя не проверяются и напрямую вставляются в SQL-запросы.

**Как работает атака?**
Если приложение формирует SQL-запрос, используя строку, построенную из пользовательского ввода, атакующий может
```

The 'Открытые вопросы к уроку' section contains a form for setting question counts:

Задайте количество открытых вопросов ко всему уроку

Вопросы среднего уровня	Вопросы сложного уровня
5	5

Ситуативные вопросы: 0

**Сгенерировать вопросы >**

## Этап 6. Иллюстрации

1. Задайте параметры иллюстраций к вашему уроку - ключевые слова направления деятельности, стиль и цвет;
2. Нажмите «Сгенерировать иллюстрации»;  
Если вас не устроили изображения, измените параметры и попробуйте снова;
3. Для перегенерации одного конкретного изображения при наведении нажмите «Еще вариант»;
4. Для замены сгенерированного изображения своим при наведении на картинку нажмите «Загрузить свою» и выберите файл изображения.

Иллюстрации к главам и фактам

Если не задать промт, система сгенерирует изображения на основе текста урока

Направление деятельности Стиль изображения

разработка web приложений минимализм

Акцентный цвет

#3e3391

Сгенерировать иллюстрации >

Иллюстрация к главе



Ещё вариант Загрузить свою

## Этап 7. Публикация урока

На данном этапе вы можете:

1. Просмотреть все полученные материалы по разделам;
2. Скачать файл урока в формате .docx;
3. Сгенерировать курс в формате для загрузки в корпоративную LMS (формат SCORM 1.2 и для iSpring).



◀ Назад

Основные уязвимости WEB приложений.docx

Дата последнего изменения: 12.8.2025, 07:01

На проверке

1. Подготовка документа 2. Главы урока 3. Сгенерированные главы 4. Вопросы к главам 5. Общие вопросы 6. Иллюстрации 7. Публикация

Содержание Учебный материал

Глава 1 1. SQL Injection (SQLi)

Глава 2 2. Cross-Site Scripting (XSS)

Глава 3 3. Cross-Site Request Forgery (CSRF)

Скачать в формате DOCX Экспортировать... Опубликовать

Выберите элемент для просмотра

SCORM 1.2 iSpring-suite

**ГОТОВО, МОЖНО ПРИСТУПАТЬ К ОБУЧЕНИЮ!**