



Отчет о пентесте:

<https://seller.tcell.tj/>

AI Penetration Testing Platform | Pentest.red



Общая информация

Параметр	Значение
Цель тестирования	https://seller.tcell.tj/
Название пентеста	Тест 5
Статус	<input checked="" type="checkbox"/> Завершен
Дата создания	17.01.2026, 17:43:59
Дата начала	17.01.2026, 17:44:34
Дата завершения	17.01.2026, 18:56:20
ID пентеста	4711c798-9962-4c22-a3f1-9bfd23a65be5



Цепочка взлома

Обнаружено уязвимостей: 10

Шаг 1: XSS Vulnerability Locations

Тип уязвимости: Cross-Site Scripting

Критичность: MEDIUM

Расположение: Не указано

Описание:

Шаг 2: SSRF Vulnerability Locations

Тип уязвимости: Server-Side Request Forgery

Критичность: MEDIUM

Расположение: Не указано

Описание:

Шаг 3: XSS SINK #1: dangerouslySetInnerHTML in React Component

Тип уязвимости: Cross-Site Scripting

Критичность: MEDIUM

Расположение: Не указано

Описание:

Шаг 4: SSRF SINK #1: node-fetch with User-Controlled URL

Тип уязвимости: Server-Side Request Forgery

Критичность: MEDIUM

Расположение: Не указано

Описание:

Шаг 5: INJECTION_ANALYSIS.md

Тип уязвимости: Unknown

Критичность: MEDIUM

Расположение: Не указано

Описание:

Proof of Concept:

```
```http
POST /auction/api/Reserve/search_reserve_number HTTP/1.1
Host: api-my.tcell.tj
Content-Type: application/json
```

---

## Шаг 6: XSS Vulnerability Locations

**Тип уязвимости:** Cross-Site Scripting

**Критичность:** MEDIUM

**Расположение:** Не указано

**Описание:**

---

## Шаг 7: SSRF Vulnerability Locations

**Тип уязвимости:** Server-Side Request Forgery

**Критичность:** MEDIUM

**Расположение:** Не указано

**Описание:**

---

## Шаг 8: XSS SINK #1: dangerouslySetInnerHTML in React Component

**Тип уязвимости:** Cross-Site Scripting

**Критичность:** MEDIUM

**Расположение:** Не указано

**Описание:**

---

## **Шаг 9: SSRF SINK #1: node-fetch with User-Controlled URL**

**Тип уязвимости:** Server-Side Request Forgery

**Критичность:** MEDIUM

**Расположение:** Не указано

**Описание:**

---

## **Шаг 10: SQL Injection Sources (CRITICAL - 8 Affected Endpoints)**

**Тип уязвимости:** SQL Injection

**Критичность:** CRITICAL

**Расположение:** Не указано

**Описание:**

---

---

**Обнаружено уязвимостей: 10**

### **Шаг 1: XSS Vulnerability Locations**

**Тип уязвимости:** Cross-Site Scripting

**Критичность:** MEDIUM

**Расположение:** Не указано

**Описание:**

---

### **Шаг 2: SSRF Vulnerability Locations**

**Тип уязвимости:** Server-Side Request Forgery

**Критичность:** MEDIUM

**Расположение:** Не указано

**Описание:**

---

## **Шаг 3: XSS SINK #1: dangerouslySetInnerHTML in React Component**

**Тип уязвимости:** Cross-Site Scripting

**Критичность:** MEDIUM

**Расположение:** Не указано

**Описание:**

---

## **Шаг 4: SSRF SINK #1: node-fetch with User-Controlled URL**

**Тип уязвимости:** Server-Side Request Forgery

**Критичность:** MEDIUM

**Расположение:** Не указано

**Описание:**

---

## **Шаг 5: INJECTION\_ANALYSIS.md**

**Тип уязвимости:** Unknown

**Критичность:** MEDIUM

**Расположение:** Не указано

**Описание:**

**Proof of Concept:**

```
```http
POST /auction/api/Reserve/search_reserve_number HTTP/1.1
Host: api-my.tcell.tj
Content-Type: application/json
```

Шаг 6: XSS Vulnerability Locations

Тип уязвимости: Cross-Site Scripting

Критичность: MEDIUM

Расположение: Не указано

Описание:

Шаг 7: SSRF Vulnerability Locations

Тип уязвимости: Server-Side Request Forgery

Критичность: MEDIUM

Расположение: Не указано

Описание:

Шаг 8: XSS SINK #1: dangerouslySetInnerHTML in React Component

Тип уязвимости: Cross-Site Scripting

Критичность: MEDIUM

Расположение: Не указано

Описание:

Шаг 9: SSRF SINK #1: node-fetch with User-Controlled URL

Тип уязвимости: Server-Side Request Forgery

Критичность: MEDIUM

Расположение: Не указано

Описание:

Шаг 10: SQL Injection Sources (CRITICAL - 8 Affected Endpoints)

Тип уязвимости: SQL Injection

Критичность: CRITICAL

Расположение: Не указано

Описание:

Отчет сгенерирован с использованием Claude AI на основе анализа всех файлов результатов пентеста.



Детальные результаты анализа

Детальный анализ недоступен из-за ошибки генерации.



Правовая информация

Данный отчет создан в рамках авторизованного тестирования на проникновение. Все найденные уязвимости должны быть использованы исключительно для улучшения безопасности системы.

© 2026 Pentest.red | Enterprise Security Platform

Дата создания отчета: 19.01.2026, 12:36:04

Отчет сгенерирован автоматически AI Penetration Testing Platform

© 2026 Pentest.red | Enterprise Security Platform

Отчет сгенерирован автоматически AI Penetration Testing Platform