# Отчет по результатам сканирования безопасности: веб-сайт example.com

Специалист по информационной безопасности

2026-01-17

## Краткое резюме

Данный отчет представляет результаты комплексного сканирования безопасности веб-сайта **example.com** (IP: 188.114.96.12), проведенного 13 января 2026 года с использованием инструмента Nikto 2.1.5. Сканирование выявило **3 потенциальные проблемы безопасности**, требующие внимания администраторов.

> **Общая оценка безопасности**: СРЕДНИЙ УРОВЕНЬ РИСКА
>
> Выявленные проблемы не представляют критической угрозы, но требуют устранения для повышения общего уровня безопасности.

.

## Детали сканирования

### Технические параметры

| Параметр | Значение |
|---|---|
| **Целевой хост** | example.com |
| **IP-адрес** | 188.114.96.12 |
| **Порт** | 443 (HTTPS) |
| **HTTP-сервер** | Cloudflare |
| **Инструмент сканирования** | Nikto 2.1.5 |
| **Дата проведения** | 13 января 2026 г. |
| **Время начала** | 05:24:40 |
| **Время завершения** | 05:31:11 |
| **Общее время** | 6 минут 31 секунда (391 сек) |

### Статистика сканирования

- **Проверено элементов**: 6,544
- **Обнаружено ошибок**: 0
- **Выявлено проблем**: 3

### Параметры командной строки

```
nikto -h https://example.com -ssl -o https_scan.html -F html
```

.

## Выявленные уязвимости и проблемы

### 1. Отсутствие заголовка X-Frame-Options

**Уровень риска**: 🟡 Средний

**Описание проблемы**: Отсутствует заголовок безопасности X-Frame-Options, который защищает от атак типа clickjacking.

**Техническая информация**:

- **URI**: /
- **HTTP-метод**: GET
- **OSVDB ID**: OSVDB-0
- **Тестовые ссылки**: https://example.com:443/

**Потенциальные последствия**:

- Возможность проведения атак clickjacking
- Встраивание сайта в iframe на вредоносных ресурсах
- Обман пользователей через скрытые элементы интерфейса

### 2. Нестандартный заголовок cf-ray

**Уровень риска**: 🟢 Низкий (информационный)

**Описание проблемы**: Обнаружен нестандартный заголовок 'cf-ray' с содержимым: 9bd22015ba62bc6c-ZRH

**Техническая информация**:

- **URI**: /
- **HTTP-метод**: GET
- **Значение заголовка**: 9bd22023ba62bc6c-ZRH
- **OSVDB ID**: OSVDB-0
- **Тестовые ссылки**: https://example.com:443/

**Комментарий**: Данный заголовок является стандартным для сервисов Cloudflare и используется для трассировки запросов. Не представляет угрозы безопасности.

### 3. Несоответствие SSL-сертификата

**Уровень риска**: 🟡 Средний

**Описание проблемы**: Имя хоста 'example.com' не соответствует Common Name (CN) SSL-сертификата 'cdnjs.cloudflare.com'

**Техническая информация**:

- **URI**: /
- **HTTP-метод**: GET
- **Ожидаемое CN**: example.com
- **Фактическое CN**: cdnjs.cloudflare.com

- **OSVDB ID**: OSVDB-0
- **Тестовые ссылки**: https://example.com:443/

**Потенциальные последствия**:

- Предупреждения браузера о небезопасном соединении
- Снижение доверия пользователей
- Возможные проблемы с SEO и индексацией

.

## Рекомендации по устранению

### Приоритетные действия

1. **Настройка заголовка X-Frame-Options**
   - Добавить заголовок X-Frame-Options: DENY или X-Frame-Options: SAMEORIGIN
   - Альтернативно: использовать CSP-заголовок с директивой frame-ancestors
2. **Исправление SSL-сертификата**
   - Получить корректный SSL-сертификат для домена example.com
   - Обновить конфигурацию Cloudflare для использования правильного сертификата
   - Проверить настройки DNS и проксирования

### Дополнительные меры безопасности

- **Внедрение Content Security Policy (CSP)**
  - Настройка комплексной политики безопасности контента
  - Защита от XSS-атак и других векторов
- **Добавление дополнительных заголовков безопасности**:
  - X-Content-Type-Options: nosniff
  - X-XSS-Protection: 1; mode=block
  - Strict-Transport-Security: max-age=31536000
- **Регулярное сканирование безопасности**
  - Проведение ежемесячных проверок
  - Мониторинг новых уязвимостей

.

## План действий

### Немедленные действия (1-3 дня)

- ☐ Настроить заголовок X-Frame-Options в конфигурации веб-сервера
- ☐ Связаться с технической поддержкой Cloudflare по вопросу SSL-сертификата

### Краткосрочные действия (1-2 недели)

- ☐ Получить и установить корректный SSL-сертификат

- ☐ Внедрить дополнительные заголовки безопасности
- ☐ Провести повторное сканирование для проверки исправлений

### Долгосрочные действия (1 месяц)

- ☐ Разработать политику регулярного сканирования безопасности
- ☐ Внедрить систему мониторинга безопасности
- ☐ Обучение команды лучшим практикам веб-безопасности

.

## Заключение

Проведенное сканирование безопасности веб-сайта example.com выявило **3 проблемы средней и низкой критичности**. Несмотря на отсутствие критических уязвимостей, рекомендуется устранить выявленные проблемы для повышения общего уровня безопасности.

Особое внимание следует уделить настройке корректного SSL-сертификата и внедрению заголовков безопасности. Эти меры значительно повысят защищенность сайта и доверие пользователей.

**Следующее сканирование рекомендуется провести через 2 недели** после внедрения исправлений для подтверждения их эффективности.

.

## Приложение: Техническая информация

### Детали сканирования Nikto

**Программное обеспечение**: Nikto 2.1.5
**Количество протестированных хостов**: 1
**Общее время выполнения**: 391 секунда

### Статистика по категориям

| Категория | Количество |
|---|---|
| Проверенные элементы | 6,544 |
| Ошибки сканирования | 0 |
| Выявленные проблемы | 3 |
| Критические уязвимости | 0 |
| Средний риск | 2 |
| Низкий риск | 1 |