Отчет по аудиту безопасности: Анализ инфраструктуры example.com

Специалист по информационной безопасности

2025-12-17

Краткое резюме

Проведен комплексный аудит безопасности веб-ресурса example.com с использованием современных инструментов сканирования (Nmap, SSLScan). Выявлены критические уязвимости конфигурации, требующие немедленного устранения. Общая оценка безопасности: **6/10** - требуется срочное вмешательство.

> ⚠ **Критическое предупреждение**: Обнаружены открытые нестандартные порты (8080, 8443) и потенциальные векторы атак на WordPress административную панель.

Объект тестирования

Параметр	Значение
Домен	example.com
IP-адреса	192.0.2.1
CDN/WAF	Cloudflare
CMS	WordPress 6.9
Дата аудита	17 декабря 2025

Методология тестирования

Аудит проводился в соответствии с методологией NIST Cybersecurity Framework и включал:

- **Сканирование портов** (Nmap 7.94SVN)
- **Анализ SSL/TLS** (SSLScan 2.1.2)
- **Проверка конфигурации веб-сервера**
- **Анализ security headers**
- **Оценка WordPress безопасности**

Архитектура системы

Пользователь → Cloudflare CDN → Origin Server
↓

Порты: 80, 443, 8080, 8443
↓
WordPress 6.9

Ключевые компоненты: - Cloudflare как reverse proxy на всех портах - SSL-сертификат от Google Trust Services (WE1) - Wildcard сертификат (*.example.com) - HTTP/2 и HTTP/3 поддержка

Результаты сканирования

Открытые порты и сервисы

Порт	Протокол	Статус	Сервис	Примечания
80	HTTP	Открыт	Cloudflare proxy	Редирект на HTTPS
443	HTTPS	Открыт	Cloudflare proxy	Основной сайт
8080	HTTP	⚠ Открыт	Cloudflare proxy	Нестандартный порт
8443	HTTPS	× Ошибка 523	Cloudflare proxy	Origin недоступен

SSL/TLS конфигурация

Положительные аспекты: - TLS 1.3 поддерживается (современный протокол) - TLS 1.2 с безопасными шифрами - Отключены устаревшие протоколы (SSL 2.0/3.0, TLS 1.0/1.1) - Perfect Forward Secrecy (ECDHE) - Современные эллиптические кривые (x25519, secp256r1)

Проблемные области: - ⚠ Поддержка CBC-шифров (уязвимы к BEAST, Lucky13) - ⚠ Короткий срок действия сертификата (90 дней) - ⚠ Идентичная конфигурация на всех портах

WordPress анализ

Компонент	Статус	Риск
Версия	WordPress 6.9	Высокий
Админ-панель	/wp-admin/ доступна	Критический
Robots.txt	Раскрывает структуру	🟡 Средний
Генератор	Версия раскрыта	🟡 Средний

Выявленные уязвимости

Критический уровень (CVSS 7.0-10.0)

1. Ошибка конфигурации порта 8443

- **Описание**: Порт 8443 сконфигурирован в Cloudflare, но origin сервер недоступен (HTTP 523)
- **Риск**: Обход защиты Cloudflare, информационная утечка

- **CVSS Score**: 7.5
- **Рекомендация**: Немедленно закрыть порт или исправить конфигурацию

2. Открытый нестандартный порт 8080

- **Описание**: Альтернативная точка входа может использоваться для обхода WAF
- **Риск**: Обход security policies, brute-force атаки
- **CVSS Score**: 7.2
- **Рекомендация**: Закрыть порт или ограничить доступ

🔵 Высокий уровень (CVSS 4.0-6.9)

3. WordPress административная панель

- **Описание**: /wp-admin/ упоминается в robots.txt, версия раскрыта
- **Риск**: Brute-force атаки, эксплуатация уязвимостей
- **CVSS Score**: 6.8
- **Рекомендация**: Скрыть версию, защитить админ-панель

4. Отсутствие критических security headers

- **Описание**: Отсутствуют HSTS, X-Frame-Options, CSP
- **Риск**: Clickjacking, downgrade атаки, XSS
- **CVSS Score**: 5.5
- **Рекомендация**: Добавить недостающие заголовки

🟡 Средний уровень (CVSS 2.0-3.9)

5. CBC-шифры в TLS 1.2

- **Описание**: Поддержка устаревших CBC-шифров
- **Риск**: Атаки типа BEAST, Lucky13
- **CVSS Score**: 3.7
- **Рекомендация**: Отключить CBC-шифры

Рекомендации по устранению

Немедленные действия (24 часа)

1. **Закрыть порт 8443**

```
# Отключить в Cloudflare Dashboard
# Или закрыть на origin сервере
server {
    listen 8443;
    return 444;  # Закрыть соединение
}
```

2. **Ограничить доступ к порту 8080**

```
server {
    listen 8080;
    # Только внутренняя сеть
    allow 192.168.0.0/16;
    deny all;
}
```

3. **Защитить WordPress admin-панель**

```
# .htaccess в /wp-admin/
AuthType Basic
AuthName "Admin Area"
AuthUserFile /path/to/.htpasswd
Require valid-user
```

Краткосрочные улучшения (7 дней)

4. **Добавить security headers**

```
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains; preload";
add_header X-Frame-Options "DENY";
add_header Content-Security-Policy "default-src 'self'";
add_header X-Content-Type-Options "nosniff";
```

5. **Оптимизировать SSL/TLS**

```
# Отключить CBC-шифры
ssl_ciphers "ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384";
ssl_protocols TLSv1.2 TLSv1.3;
```

6. **Настроить Cloudflare WAF**
   - Блокировать доступ к /wp-admin/ для неавторизованных IP
   - Настроить rate limiting для /wp-login.php
   - Включить Bot Fight Mode

Долгосрочные меры (30 дней)

7. **Мониторинг и автоматизация**
   - Автоматическое обновление SSL-сертификатов
   - Мониторинг попыток доступа к защищенным ресурсам
   - Регулярное сканирование на уязвимости
8. **WordPress hardening**
   - Установка security плагинов (Wordfence, iThemes Security)
   - Двухфакторная аутентификация
   - Скрытие версии WordPress
   - Регулярные обновления

Матрица рисков

Уязвимость	Вероятность	Воздействие	Общий риск	Приоритет
Порт 8443 ошибка	Высокая	Высокое	Критический	P0
Порт 8080 открыт	Средняя	Высокое	🟠 Высокий	P1
WordPress админ	Высокая	Среднее	🟠 Высокий	P1
Security headers	Средняя	Среднее	🟡 Средний	P2
CBC-шифры	Низкая	Низкое	🟢 Низкий	P3

План устранения

Фаза 1: Критические исправления (1-2 дня)

- ☐ Закрыть порт 8443 в Cloudflare
- ☐ Ограничить доступ к порту 8080
- ☐ Защитить WordPress админ-панель
- ☐ Добавить базовые security headers

Фаза 2: Улучшения безопасности (1 неделя)

- ☐ Оптимизировать SSL/TLS конфигурацию
- ☐ Настроить Cloudflare WAF правила
- ☐ Установить WordPress security плагины
- ☐ Настроить мониторинг

Фаза 3: Долгосрочные меры (1 месяц)

- ☐ Автоматизация обновлений
- ☐ Регулярные security аудиты
- ☐ Обучение персонала
- ☐ Документирование процедур

Соответствие стандартам

Стандарт	Текущий статус	Требуемые действия
NIST CSF	Частично	Улучшить Protect, Detect функции
ISO 27001	Не соответствует	Внедрить ISMS процессы
PCI DSS	Требует проверки	Усилить защиту данных
GDPR	Базовый уровень	Добавить privacy headers

Заключение

Аудит выявил серьезные проблемы безопасности, требующие немедленного внимания. Основные риски связаны с неправильной конфигурацией портов и недостаточной защитой WordPress административной панели.

Ключевые выводы: - **Критические уязвимости**: 2 (требуют немедленного устранения) - 🔴 **Высокие риски**: 2 (устранить в течение недели) - 🟡 **Средние риски**: 1 (планировать устранение)

Рекомендуемые следующие шаги: 1. Немедленно закрыть проблемные порты 2. Усилить защиту WordPress 3. Добавить недостающие security headers 4. Внедрить регулярный мониторинг безопасности

При правильном выполнении рекомендаций общая оценка безопасности может быть повышена до **8-9/10** в течение 30 дней.

.

Отчет подготовлен в соответствии с лучшими практиками индустрии и стандартами Microsoft Security Development Lifecycle (SDL).