Отчет о соответствии стандартам безопасности: Анализ веб-сайта example.com

Специалист по информационной безопасности

2025-12-31

Краткое резюме

Данный отчет представляет комплексный анализ соответствия веб-сайта https://example.com международным стандартам безопасности OWASP Top 10 2021, NIST Cybersecurity Framework 2.0 и рекомендациям Microsoft Security Baseline. Анализ основан на результатах автоматизированного сканирования безопасности, выполненного 30 декабря 2025 года с помощью OWASP ZAP (Zed Attack Proxy) версии 2.17.0 от Checkmarx.

> **КРИТИЧЕСКОЕ ПРЕДУПРЕЖДЕНИЕ**: Обнаружена утечка персональных данных (PII) - требуется немедленное вмешательство!

Ключевые выводы:

- Обнаружено **29 предупреждений безопасности** различного уровня критичности
- Выявлена **критическая уязвимость** раскрытия персональных данных (PII)
- Отсутствуют **базовые механизмы защиты** веб-приложения
- Сайт **не соответствует** основным требованиям международных стандартов безопасности

Содержание

Методология анализа

Параметры сканирования

- **Инструмент**: OWASP ZAP 2.17.0 от Checkmarx [1]
- **Дата и время сканирования**: 30 декабря 2025 года, 19:00:53
- **Целевой ресурс**: https://example.com
- **Общее количество endpoints**: 290
- **Контексты**: Все контексты включены по умолчанию

- **Уровни риска**: Высокий, Средний, Низкий, Информационный
- **Уровни достоверности**: Пользователь подтвержден, Высокий, Средний, Низкий

Статистика результатов сканирования

Уровень риска	Количество	Процент	Достоверность
Высокий	1	3.4%	Высокая
🟠 **Средний**	3	10.3%	Высокая/Средняя
Низкий	4	13.8%	Высокая/Средняя/Низкая
i Информационный	21	72.4%	Средняя/Низкая
Всего	**29**	**100%**	-

Технологический стек

Обнаруженные технологии на сайте:

- **CMS**: WordPress с Block Editor
- **Веб-сервер**: LiteSpeed с LiteSpeed Cache
- **CDN**: Cloudflare с Browser Insights
- **Язык программирования**: PHP
- **Дополнительные компоненты**:
  - Blocksy (тема WordPress)
  - Stackable (плагин WordPress)
  - Gravatar (сервис аватаров)
  - Google Font API
- **Протоколы**: HTTP/3, HSTS, RSS, Priority Hints

Детальный анализ уязвимостей

Критические уязвимости (Высокий риск)

1. Раскрытие персональных данных (PII)

CWE-359 | WASC-13 | Достоверность: Высокая

> **КРИТИЧЕСКОЕ НАРУШЕНИЕ**: Обнаружена утечка персональных данных пользователей

Техническое описание:

- Персональная информация пользователей доступна без авторизации
- Нарушение принципов конфиденциальности данных
- Прямое нарушение требований GDPR

Воздействие на бизнес:

- **Регуляторные риски**: Штрафы по GDPR до 4% от годового оборота компании
- **Репутационные потери**: Серьезный ущерб доверию клиентов
- **Юридические последствия**: Возможные судебные иски от пострадавших
- **Операционные риски**: Необходимость уведомления регуляторов в течение 72 часов

🔵 Уязвимости среднего риска

2. Отсутствие Subresource Integrity (SRI)

CWE-345 | WASC-15 | Количество: 5 экземпляров | Достоверность: Высокая

Описание: Внешние ресурсы загружаются без проверки целостности, что создает риск атак на цепочку поставок.

Затронутые ресурсы:

- Google Font API
- Cloudflare CDN ресурсы
- Внешние JavaScript библиотеки

3. Отсутствие Content Security Policy (CSP)

CWE-693 | WASC-15 | Количество: 5 экземпляров | Достоверность: Высокая

Описание: Отсутствует политика безопасности контента, что делает сайт уязвимым для XSS-атак и других инъекций.

4. Отсутствие защиты от кликджекинга

CWE-1021 | WASC-15 | Количество: 5 экземпляров | Достоверность: Средняя

Описание: Отсутствуют заголовки X-Frame-Options или CSP frame-ancestors, что позволяет встраивать сайт в iframe для проведения атак кликджекинга.

Уязвимости низкого риска

5. Проблемы с транспортной безопасностью

- **Заголовок Strict-Transport-Security не установлен** (CWE-319, 1 экземпляр)
- **Строгая безопасность транспорта отключена** (CWE-319, 5 экземпляров)

6. Отсутствие X-Content-Type-Options

CWE-693 | WASC-15 | Достоверность: Средняя

Описание: Отсутствует защита от MIME-sniffing атак.

7. Раскрытие Unix timestamp

CWE-497 | WASC-13 | Количество: 4 экземпляра | Достоверность: Низкая

Описание: Обнаружено раскрытие временных меток, что может предоставить информацию о времени создания контента.

ℹ Информационные предупреждения

Обнаружено 21 информационное предупреждение, включая:

- Детекция технологий (WordPress, PHP, Cloudflare и др.)
- Проблемы с кэшированием (5 экземпляров)
- Несоответствие кодировки
- Подозрительные комментарии в коде (58 экземпляров)

Анализ соответствия OWASP Top 10 2021

A01:2021 – Нарушение контроля доступа

Статус: × КРИТИЧЕСКОЕ НЕСООТВЕТСТВИЕ

Обнаруженные проблемы:

- **Раскрытие PII** - прямое нарушение принципов контроля доступа
- Отсутствие механизмов защиты чувствительной информации
- Нарушение принципа "запрет по умолчанию"

Рекомендации OWASP:

- Реализация строгого контроля доступа
- Логирование неудачных попыток доступа
- Ограничение скорости API-запросов
- Регулярный аудит прав доступа

A03:2021 – Инъекции

Статус: **СООТВЕТСТВУЕТ** (по результатам сканирования)

Результат: Не обнаружено уязвимостей типа SQL, NoSQL или OS command injection.

A05:2021 – Неправильная конфигурация безопасности

Статус: × КРИТИЧЕСКОЕ НЕСООТВЕТСТВИЕ

Обнаруженные проблемы:

- Отсутствие CSP (5 экземпляров)
- Отсутствие защиты от кликджекинга (5 экземпляров)
- Неправильная настройка заголовков безопасности
- Отсутствие X-Content-Type-Options
- Проблемы с HSTS конфигурацией

A06:2021 – Уязвимые и устаревшие компоненты

Статус: ⚠ ТРЕБУЕТ ПРОВЕРКИ

Обнаруженные компоненты:

- WordPress (версия не определена)
- PHP (версия не определена)
- LiteSpeed веб-сервер
- Множественные плагины: Blocksy, Stackable, LiteSpeed Cache

Рекомендации: Необходим детальный аудит версий всех компонентов.

A08:2021 – Недостатки целостности программного обеспечения и данных

Статус: × НЕСООТВЕТСТВИЕ

Проблемы:

- Отсутствие Subresource Integrity для внешних ресурсов (5 экземпляров)
- Риск компрометации через CDN и внешние библиотеки
- Отсутствие проверки целостности обновлений

A09:2021 – Недостаточное логирование и мониторинг

Статус: × НЕСООТВЕТСТВИЕ

Проблемы:

- Отсутствие информации о системах логирования
- Неизвестно состояние мониторинга безопасности
- Отсутствие системы обнаружения аномалий

Соответствие NIST Cybersecurity Framework 2.0

GOVERN (Управление) - 20% соответствие

GV.OC-01: Организационная кибербезопасность

- × Отсутствуют доказательства формализованной политики безопасности

GV.RM-01: Управление рисками

- × Не реализованы процедуры управления рисками кибербезопасности

GV.SC-01: Управление цепочкой поставок

- × Отсутствует контроль целостности внешних ресурсов

IDENTIFY (Идентификация) - 60% соответствие

ID.AM-02: Инвентаризация программного обеспечения

- Частично выполнено - идентифицированы основные компоненты

ID.RA-01: Оценка уязвимостей

- Выполнено - проведено сканирование безопасности

ID.RA-02: Анализ угроз

- × Отсутствует систематический анализ угроз

PROTECT (Защита) - 15% соответствие

PR.AC-01: Управление идентификацией и аутентификацией

- × Недостаточно данных для оценки

PR.DS-01: Защита данных в покое

- × Обнаружено раскрытие PII

PR.DS-02: Защита данных при передаче

- ⚠ Частично реализовано (HTTPS, но проблемы с HSTS)

PR.PT-01: Аудит/логирование

- × Недостаточно информации о системах аудита

DETECT (Обнаружение) - 0% соответствие

DE.CM-01: Мониторинг сети

- × Отсутствуют доказательства мониторинга

DE.AE-01: Обнаружение аномалий

- × Отсутствуют системы обнаружения аномалий

RESPOND (Реагирование) - 0% соответствие

RS.RP-01: План реагирования

- × Отсутствуют доказательства плана реагирования

RS.CO-01: Коммуникации

- × Отсутствуют процедуры уведомления о инцидентах

RECOVER (Восстановление) - 0% соответствие

RC.RP-01: План восстановления

- × Отсутствуют доказательства плана восстановления

RC.CO-01: Коммуникации восстановления

- × Отсутствуют процедуры коммуникации при восстановлении

Соответствие Microsoft Security Baseline

Транспортная безопасность

× КРИТИЧЕСКИЕ НЕДОСТАТКИ:

- Заголовок Strict-Transport-Security не установлен (1 экземпляр)
- Строгая безопасность транспорта отключена (5 экземпляров)
- Отсутствует принудительное использование HTTPS для всех ресурсов

Защита контента

× КРИТИЧЕСКИЕ НЕДОСТАТКИ:

- Заголовок X-Content-Type-Options отсутствует
- Отсутствует Content Security Policy (5 экземпляров)
- Нет защиты от MIME-sniffing атак
- Отсутствует защита от кликджекинга

Целостность ресурсов

× СРЕДНИЙ РИСК:

- Отсутствует атрибут Subresource Integrity для внешних ресурсов (5 экземпляров)
- Риск компрометации внешних библиотек от Google Font API, Cloudflare и других CDN
- Отсутствует проверка целостности при загрузке ресурсов

Управление данными

× КРИТИЧЕСКИЙ РИСК:

- Обнаружена утечка персональных данных
- Отсутствует классификация данных
- Нет контроля доступа к чувствительной информации

План устранения уязвимостей

Фаза 1: Критические исправления (0-7 дней)

ПРИОРИТЕТ 1: Устранение утечки PII (0-3 дня)

- ☐ **День 1**: Немедленная идентификация и блокировка источников утечки PII
- ☐ **День 2**: Реализация маскирования/шифрования чувствительных данных
- ☐ **День 3**: Внедрение строгого контроля доступа к персональным данным
- ☐ **День 3**: Уведомление регуляторов в соответствии с GDPR (72 часа)

ПРИОРИТЕТ 2: Базовые заголовки безопасности (4-7 дней)

- ☐ **День 4-5**: Внедрение Content Security Policy

```
Content-Security-Policy: default-src 'self';
script-src 'self' 'unsafe-inline' https://cdnjs.cloudflare.com https://fonts.googleapis.com;
style-src 'self' 'unsafe-inline' https://fonts.googleapis.com;
img-src 'self' data: https: https://secure.gravatar.com;
frame-ancestors 'none';
base-uri 'self';
```

- ☐ **День 6**: Настройка защиты от кликджекинга

```
X-Frame-Options: DENY
```

- ☐ **День 6**: Настройка HSTS

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

- ☐ **День 7**: Тестирование и валидация изменений

Фаза 2: Средние исправления (8-30 дней)

Неделя 2: Subresource Integrity

- ☐ Внедрение SRI для всех внешних ресурсов

```
<link
href="https://fonts.googleapis.com/css2?family=Roboto:wght@300;400;700&display=swap"
    rel="stylesheet"
    integrity="sha384-hash"
    crossorigin="anonymous">
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.6.0/jquery.min.js"
     integrity="sha384-
vtXRMe3mGCbOeY7l30aIg8H9p3GdeSe4IFlP6G8JMa7o7lXvnz3GFKzPxzJdPfGK"
     crossorigin="anonymous"></script>
```

Неделя 3: Дополнительные заголовки безопасности

- ☐ Внедрение X-Content-Type-Options

```
X-Content-Type-Options: nosniff
```

- ☐ Настройка дополнительных заголовков

```
X-XSS-Protection: 1; mode=block
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(), microphone=(), camera=()
```

Неделя 4: Аудит компонентов

- ☐ Проверка версий WordPress, PHP и всех плагинов
- ☐ Обновление устаревших компонентов
- ☐ Удаление неиспользуемых плагинов и тем
- ☐ Настройка автоматических обновлений безопасности

Фаза 3: Долгосрочные улучшения (31-90 дней)

Месяц 2: Мониторинг и логирование

- ☐ Внедрение системы мониторинга безопасности (SIEM)
- ☐ Настройка централизованного логирования
- ☐ Создание дашбордов безопасности
- ☐ Настройка алертов на подозрительную активность

Месяц 3: Процедуры и политики

- ☐ Разработка политики информационной безопасности
- ☐ Создание процедур реагирования на инциденты
- ☐ Разработка плана восстановления после инцидентов
- ☐ Обучение персонала основам кибербезопасности
- ☐ Регулярные тесты на проникновение

Заключение

Анализ безопасности веб-сайта https://example.com выявил **критические недостатки** в области защиты информации. Сайт **не соответствует** основным требованиям международных стандартов безопасности OWASP Top 10 2021, NIST CSF 2.0 и Microsoft Security Baseline.

Критическая оценка рисков:

- **Текущий уровень риска**: **КРИТИЧЕСКИЙ**
- **Основная угроза**: Утечка персональных данных пользователей
- **Регуляторные риски**: Высокие штрафы по GDPR (до 4% от годового оборота)
- **Репутационные риски**: Серьезная потеря доверия клиентов
- **Операционные риски**: Возможная приостановка деятельности

Соответствие стандартам:

Стандарт	Уровень соответствия	Критические проблемы
OWASP Top 10 2021	20%	A01, A05, A08, A09
NIST CSF 2.0	19%	Все функции кроме частичной идентификации
Microsoft Security Baseline	15%	Транспорт, контент, данные

Ключевые рекомендации:

1. **Немедленное устранение** утечки персональных данных (0-3 дня)
2. **Внедрение базовых механизмов защиты** веб-приложения (4-7 дней)
3. **Регулярное обновление** всех компонентов системы
4. **Создание процедур** мониторинга и реагирования на инциденты
5. **Обучение персонала** основам информационной безопасности

Прогноз улучшения:

- **После Фазы 1**: Снижение риска до 🟡 **СРЕДНЕГО** (устранение критических уязвимостей)
- **После Фазы 2**: Снижение риска до **НИЗКОГО** (базовая защита)
- **После Фазы 3**: Достижение 🟢 **ПРИЕМЛЕМОГО** уровня безопасности (соответствие стандартам)

Следующие шаги: Рекомендуется **немедленно** приступить к реализации Фазы 1 плана устранения уязвимостей, уделив особое внимание устранению утечки персональных данных и уведомлению регуляторов в соответствии с требованиями GDPR.

Ссылки

[1] OWASP Foundation. (2024). *OWASP Zed Attack Proxy (ZAP)*. https://zaproxy.org

[2] OWASP Foundation. (2021). *OWASP Top 10:2021*. https://owasp.org/Top10/2021/

[3] NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20