Отчёт о тестировании на проникновение

Terrania
deuscode.tech

Цель: [redacted] · Дата: 08.08.2026

Резюме для руководства

Проведено неразрушающее тестирование безопасности веб-приложения [redacted] Всего выявлено находок: **9**. Общий уровень риска: **СРЕДНИЙ**. Критических уязвимостей не выявлено; рекомендуется устранить недостатки конфигурации.

0	0	2	5	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

Находки

#	КРИТИЧ.	УЯЗВИМОСТЬ	ГДЕ	ОПИСАНИЕ	РЕКОМЕНДАЦИЯ
1	MEDIUM	Нет заголовка content-security-policy	[redacted]	Нет заголовка content-security-policy	CSP — главная защита от XSS и внедрения скриптов. Добавь Content-Security-Policy OWASP Secure Headers
2	MEDIUM	Нет заголовка strict-transport-security	[redacted]	Нет заголовка strict-transport-security	HSTS. Добавь Strict-Transport-Security: max-age=31536000; includeSubDomains OWASP Secure Headers
3	LOW	Заголовок X-Powered-By раскрывает стек	[redacted]	X-Powered-By: Next.js — облегчает атакующему подбор эксплойтов под конкретную версию	Убрать заголовок X-Powered-By OWASP A05
4	LOW	Нет заголовка x-frame-options	[redacted]	Нет заголовка x-frame-options	Защита от кликджекинга. Добавь X-Frame-Options: DENY или CSP frame-ancestors OWASP Secure Headers

#	КРИТИЧ.	УЯЗВИМОСТЬ	ГДЕ	ОПИСАНИЕ	РЕКОМЕНДАЦИЯ
5	LOW	Нет заголовка x-content-type-options	[redacted]	Нет заголовка x-content-type-options	Добавь X-Content-Type-Options: nosniff OWASP Secure Headers
6	LOW	Cookie без [redacted]	[redacted]	Cookie доступна из JS — усиливает ущерб от XSS	Добавь флаг [redacted]
7	LOW	Cookie без Secure	[redacted]	Cookie уходит по [redacted]	Добавь флаг Secure
8	INFO	Определён технологический стек	[redacted]	Технологии: Next.js (React), Next.js SSR/ISR, X-Powered-By: Next.js	Поддерживать компоненты в актуальном состоянии; минимизировать раскрытие версий (заголовки, бандлы). Подтверждено: анализ технологий приложения
9	INFO	Обнаружено 165 URL при глубоком обходе	[redacted]	Полная карта поверхности приложения (глубокий обход)	Проверь, что все эндпоинты защищены Подтверждено: автоматический обход поверхности

Детальный разбор серьёзных находок

Уязвимостей высокой критичности не выявлено. Ниже — общие рекомендации по устранению замечаний конфигурации.

Заключение

Критических уязвимостей на [redacted] не выявлено. Обнаружены недостатки конфигурации безопасности (MEDIUM: 2), которые снижают защищённость и должны быть устранены в плановом порядке.

Объём работ: комплексная оценка защищённости веб-приложения и его сетевой поверхности по методологии OWASP: разведка, анализ конфигурации, контроль доступа, инъекции, известные уязвимости. Тестирование неразрушающее, без эксплуатации найденных уязвимостей и без нарушения работы сервиса.

Область и рекомендации: работы охватывали веб-приложение и его доступную поверхность. Углублённый анализ бизнес-логики, криптографии и тестирование под привилегированными

учётными записями проводятся в рамках расширенного пентеста по отдельному запросу. Рекомендуется периодический повторный аудит.

Методология и покрытие

Проведено: разведка инфраструктуры и поддоменов, картирование поверхности приложения и API, анализ заголовков безопасности и TLS, тестирование на инъекции (SQL, XSS), нарушения контроля доступа, некорректную конфигурацию, известные уязвимости (CVE) и раскрытие чувствительных данных. Тестирование проводилось по методологии OWASP WSTG (Web Security Testing Guide).

Шкала критичности соответствует диапазонам CVSS: CRITICAL 9.0–10.0, HIGH 7.0–8.9, MEDIUM 4.0–6.9, LOW 0.1–3.9.

> Тестирование проводилось с авторизации владельца ресурса, неразрушающими методами. Отчёт носит рекомендательный характер. Отсутствие находки не гарантирует отсутствия уязвимости — рекомендуется периодический ретест.
