Отчёт о тестировании на проникновение

Terrania

deuscode.tech

Цель: [redacted] · Дата: 06.08.2026

Резюме для руководства

Проведено неразрушающее тестирование безопасности веб-приложения [redacted] Всего выявлено находок: **7**. Общий уровень риска: **КРИТИЧЕСКИЙ**. Обнаружены уязвимости высокой критичности, требующие немедленного устранения.

1	1	1	2	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

Находки

#	КРИТИЧ.	УЯЗВИМОСТЬ	ГДЕ	ОПИСАНИЕ	РЕКОМЕНДАЦИ
1	CRITICAL	Вход в привилегированную панель одним кликом без пароля	[redacted]	Кнопка «Войти как администратор Панель платформ» ведёт в панель с чувствительными данными без ввода пароля. Видно: [redacted] Панель администратора Дашборд Аккаунты Тарифы Платежи На сайт Выйти Панель администратора Состояние платформы [redacted]	Убрать вход без учётных данных ввести серверну аутентификацию авторизацию по ролям. OWASP A01:2021 Подтверждено: кл по кнопке в реаль браузере -> приватная панель

#	КРИТИЧ.	УЯЗВИМОСТЬ	ГДЕ	ОПИСАНИЕ	РЕКОМЕНДАЦИ
				Демо-данные RU $1 546 MRR $18 552 ARR 20 Акк...»	
2	HIGH	Фиктивная аутентификация (вход без пароля)	[redacted]	Страница входа прямо заявляет вход без пароля/ регистрации («демо-вход»).	Настоящая аутентификация пароль/OTP/OA + серверная проверка сесси «Демо без пароля» держат только на отдельном изолированном стенде без реальных данны OWASP A07:2021 Identification and Authentication Failu Подтверждено: те страницы входа
3	MEDIUM	Нет заголовка content-security-policy	[redacted]	Нет заголовка content-security-policy	CSP — главная защита от XSS и внедрения скриптов. Доба Content-Security Policy OWASP Secure Headers
4	LOW	Нет заголовка x-frame-options	[redacted]	Нет заголовка x-frame-options	Защита от кликджекинга. Добавь X-Frame Options: DENY и CSP frame-ancestors OWASP Secure Headers
5	LOW	Нет заголовка x-content-type-options	[redacted]	Нет заголовка x-content-type-options	Добавь X-Conte Type-Options: nosniff OWASP Secure Headers
6	INFO	Обнаружено 54 URL при глубоком	[redacted]	Полная карта поверхности	Проверь, что вс эндпоинты

#	КРИТИЧ.	УЯЗВИМОСТЬ	ГДЕ	ОПИСАНИЕ	РЕКОМЕНДАЦИ
		обходе		приложения (глубокий обход)	защищены Подтверждено: автоматический обход поверхност
7	INFO	Данные помечены как демонстрационные	[redacted]	На панели есть пометка «демо-данные». Метрики (выручка, аккаунты) могут быть заглушками, а не реальными показателями.	Чётко разделять демо-стенд и прод. Не выдав заглушки за реальные метрики. Демо на отдельном домене без доступа к боевы данным. Подтверждено: бейдж «демо-данные» на приватной панели

Детальный разбор серьёзных находок

CRITICAL **Вход в привилегированную панель одним кликом без пароля**

ГДЕ	[redacted]
ОПИСАНИЕ	Кнопка «Войти как администратор Панель платформ» ведёт в панель с чувствительными данными без ввода пароля. Видно: [redacted] Панель администратора Дашборд Аккаунты Тарифы Платежи На сайт Выйти Панель администратора Состояние платформы [redacted] Демо-данные RU $1 546 MRR $18 552 ARR 20 Акк…»
К ЧЕМУ ПРИВЕДЁТ	Один клик из формы входа даёт полный доступ к панели и данным. В проде это означает компрометацию всех бизнес-данных и данных клиентов без каких-либо усилий со стороны атакующего.
КАК УСТРАНИТЬ	Убрать вход без учётных данных; ввести серверную аутентификацию и авторизацию по ролям.
КЛАССИФИКАЦИЯ	OWASP A01:2021
ПОДТВЕРЖДЕНИЕ	клик по кнопке в реальном браузере -> приватная панель

HIGH **Фиктивная аутентификация (вход без пароля)**

ГДЕ	[redacted]
ОПИСАНИЕ	Страница входа прямо заявляет вход без пароля/регистрации («демо-вход»).
К ЧЕМУ ПРИВЕДЁТ	Отсутствие реальной проверки личности означает, что аккаунты и данные не защищены. Если это не изолированное демо, а прод — доступ к любым данным получает кто угодно.
КАК УСТРАНИТЬ	Настоящая аутентификация: пароль/OTP/OAuth + серверная проверка сессии. «Демо без пароля» держать только на отдельном изолированном стенде без реальных данных.
КЛАССИФИКАЦИЯ	OWASP A07:2021 Identification and Authentication Failures
ПОДТВЕРЖДЕНИЕ	текст страницы входа

Заключение

На ресурсе [redacted] выявлены уязвимости высокой критичности (CRITICAL: 1, HIGH: 1), которые могут привести к компрометации данных или системы. Требуется **немедленное устранение** и последующий ретест.

Объём тестирования: автоматизированная оценка защищённости — разведка, анализ конфигурации, активные проверки OWASP по доступной поверхности. Тестирование неразрушающее, без эксплуатации найденных уязвимостей и без нарушения работы сервиса.

Ограничения: данный отчёт отражает автоматизированную проверку. Он не включает ручной анализ бизнес-логики, тестирование под авторизованными учётными записями и социальную инженерию. Для критичных систем рекомендуется дополнительный ручной пентест.

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 велось комбинацией автоматизированных и ручных методов по методологии OWASP WSTG.

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.
