

Сканеры уязвимостей устарели

Почему будущее — за AI-пентестом



1

У кого в компании
есть сканер
уязвимостей?



2

У кого был «зелёный»
отчёт
и всё равно случился
инцидент?



Сканер сверяет вас с чужими поломками



Сканер ищет то, что **уже известно**

Что сканер видит — и что **нет**

Видит



Известные CVE



Устаревшие версии



Типовые паттерны атак

Не видит



Неизвестные уязвимости



Ошибки логики в вашем API



Цепочки мелких находок

Обычный запрос регистрации. Что тут не так?

POST /register/

name=Ivan

email=ivan@example.com

password=*****

group_id=5

← группа «обычный пользователь»

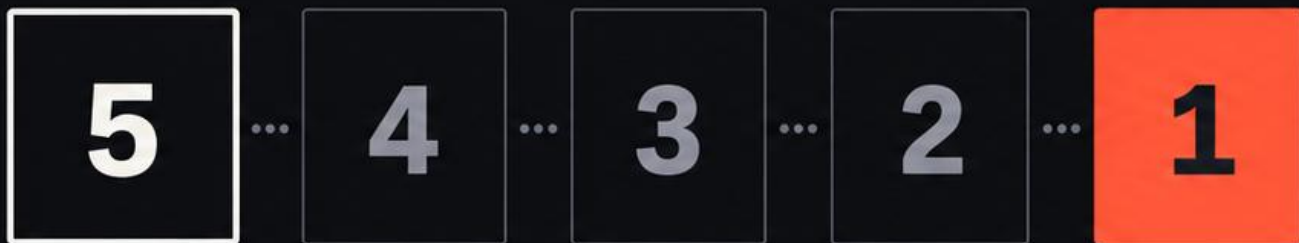
200 OK



Сканер:
нарушений нет

Ни одной сигнатуры атаки,
запрос легитимный.

Человек и агент смотрят на тот же запрос **иначе**



group_id: перебор соседних значений

Для каждого значения регистрирует отдельный аккаунт и сравнит видимую разницу.

	=5	=1
☰ Меню	обычное	админское
</> API	403	200
🛡️ Админка	нет	полный доступ



Одна цифра — и вы администратор. Без паролей и CVE.

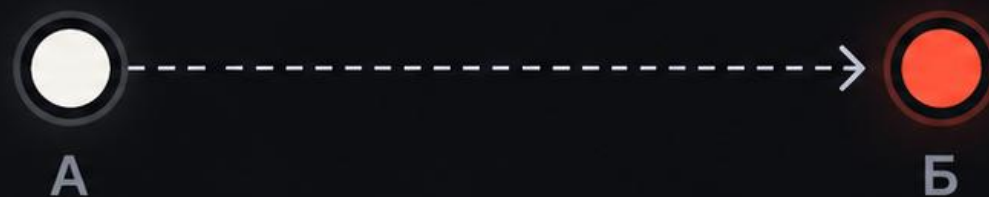
Сканер

Есть ли
совпадение
с базой?

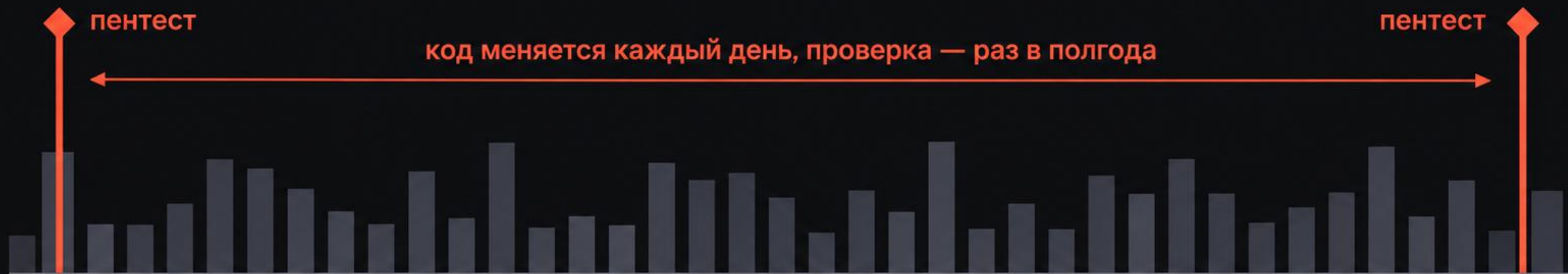


Атакующий

Как попасть
из А в Б?



Ручной пентест: **сильный, но редкий**



Редко

Релиз во вторник, пентест в декабре



Дорого

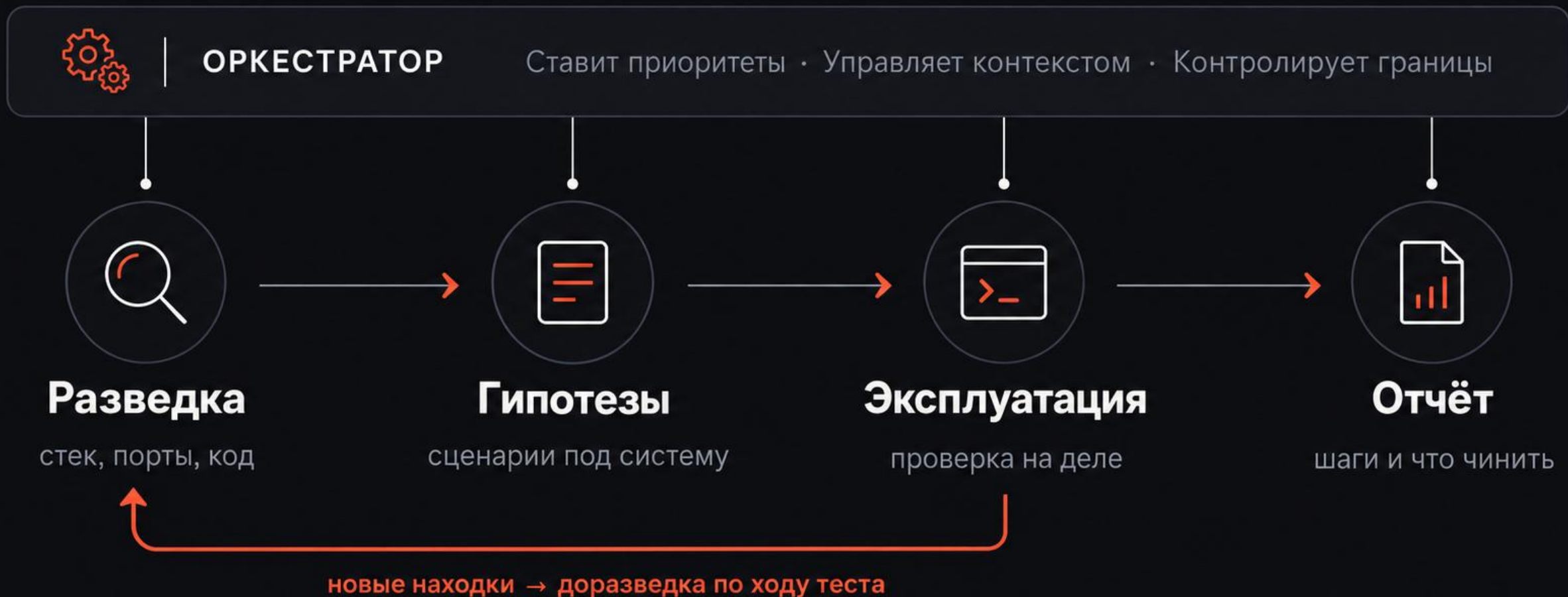
Хороших пентестеров не так много



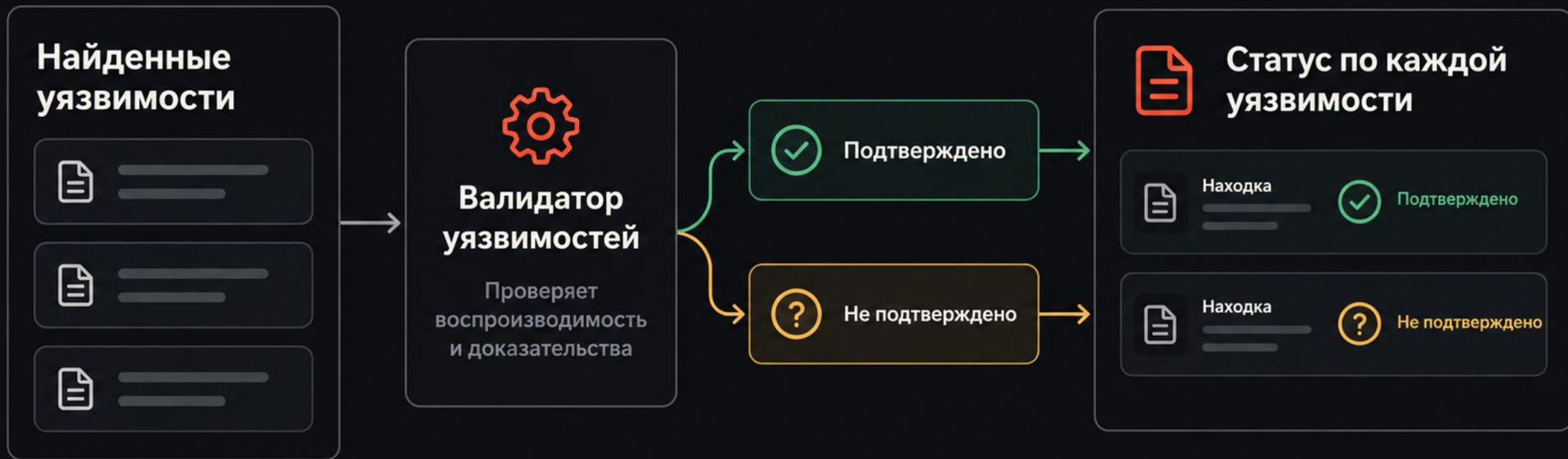
Выборочно

В пентест вложен опыт конкретного человека/команды

Команда агентов, как у живых пентестеров



Каждая находка проходит **верификацию**



Все находки сохраняются с результатом проверки

Где место **AI-пентеста**


Сканер


Ручной


AI-пентест

Мыслит сценариями



Находит неизвестное



Работает постоянно

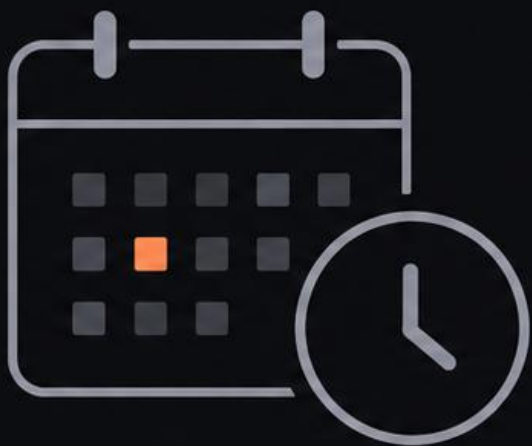


Масштабируется



Для регулятора





Ручной пентест
Раз в год



AI-пентест
В любое время

На наших глазах формируется новый принцип **CART:**
Continuous **A**utomated **R**ed **T**eaming

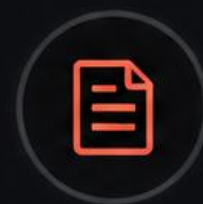
•• TRIADIX: оркестратор ИИ-агентов



Цель: домен,
приложение, API



Команда агентов-
специалистов



Отчёт с
доказательствами

Границы скоупа
задаются при запуске



≈ 50

Пилотных пентестов



0

Сломанных продов

Чем отличается от DAST и BAS



DAST

Заранее заложенные
шаблоны атак



BAS

Известные тактики
MITRE ATT&CK



TRIADIX

Сценарий строится
на лету



Oday

в российских продуктах с лицензиями ФСТЭК

От месяцев **к часам**

Классический пентест



Подрядчик



Скоуп



Ожидание
слота



Тест и отчёт

1–2 месяца



Оркестратор ИИ-агентов

Первые находки в течение нескольких часов



Параллельно

На нескольких
целях сразу



По запросу

Платите за вычислительные
мощности, не за человеко-часы

Какие направления уже проверены

УспешноРасширеннаяОтчёт готов

Широкое покрытие · #a945c57d · 08 окт. 2026 г., 23:02

2h 43m Прошло62 Находки

ПодготовкаРазведкаСогласование контураПроверкиОтчёт

ОбзорОхват 15Вспомогательные модули 18Находки 62Секреты 29Ма

Охват

Текущие приоритеты, решения и назначенная работа.

ПРИОРИТЕТНЫЕ ВЕТВИ14

external-perimeter-networkНаивысшийИсследованоЗавершить

172.23.10.19/32

ВажностьSole authorized external endpoint; prerequisite to every downstream foothold and pivot.

Текущее решениеrecon-ext-perimeter succeeded: full-range TCP scan found only 8081 and 8082 listening.

Обновлено09 окт. 2026 г., 01:40

Работаrecon-ext-perimeter

Находки5Критичный

external-web-shop-appНаивысшийИсследованоЗавершить

172.23.10.19:8081

ВажностьRichest attack surface on the endpoint and strongest candidate for initial host foothold.

Текущее решениеpentest-shop-app proved every shop chain and harvested all shop flags; the redundant source-armed sibling pentest-shop-source-rce was cancelled.

Обновлено09 окт. 2026 г., 01:40

Работাপentest-shop-app, pentest-shop-source-rce

Находки2Высокий

internal-network-pivotНаивысшийИсследованоУглубить

discovered-internal-cidrs

ВажностьFinal campaign objective (NET3 vault main flag) lives behind this pivot; it is the critical path now that the DMZ web surface is characterized and

Текущее решениеValidated re-runnable www-data code execution on both 172.23.10.19:8081 and :8082,

Обновлено09 окт. 2026 г., 01:40

Работাপentest-internal-pivot, pentest-net1-ftp-pivot

Находки

ОХВАТ



Приоритеты

Текущие приоритеты, решения и назначенная работа.



Назначенная работа

Кто и что проверяет по каждому направлению.



Результат проверки

Статус решений и найденные результаты.

Что сделали агенты

Успешно

Расширенная

Отчёт готов

Параметры

← К запускам

Сравнить

Повторный запуск

Широкое покрытие · #a945c57d · 08 окт. 2026 г., 23:02

2h 43m Прошло 62 Находки

Подготовка

Разведка

Согласование контура

Проверки

Отчёт

Обзор

Охват 15

Вспомогательные модули 18

Находки 62

Секреты 29

Ма:

Вспомогательные модули

18

Активная работа отдельно от итогов завершённых вспомогательных модулей.

Все 18

Активные 0

Завершённые 18

recon-ext-web

Завершено

100%

▼

recon-ext-perimeter

Завершено

100%

▼

pentest-blog-app

Завершено

100%

▼

pentest-shop-app

Завершено

100%

▼

recon-internal-topology

Завершено

100%

▼

pentest-blog-source-rce

exploitation

25%

▼

pentest-shop-source-rce

Отменен

0%

▼

Отчёт

4

Русский отчет

PDF

1.8 MB · 09 окт. 2026 г., 01:45

↓

Русский отчет

MARKDOWN

146.2 KB · 09 окт. 2026 г., 01:45

↓

Английский отчет

PDF

1.8 MB · 09 окт. 2026 г., 01:40

↓

Английский отчет

MARKDOWN

94.1 KB · 09 окт. 2026 г., 01:40

↓

- МОДУЛИ

✓ —
○ —

Задачи и статусы

Какие модули запускались и в каком состоянии: активные, завершённые или отменённые.
- ⚙

Ход работы

Как агенты выполняли запланированные этапы и с каким прогрессом.
- 📄

Источники находок

Где зафиксированы результаты работы: отчеты и артефакты в разных форматах.

Все находки в одном пространстве

Успешно

Расширенная

Отчёт готов

Широкое покрытие · #a945c57d · 08 окт. 2026 г., 23:02

🕒 2ч 43м Прошло 🛡️ 62 Находки

Подготовка

Разведка

Согласование контура

Проверки

Отчёт

Обзор

Охват 15

Вспомогательные модули 18

Находки 62

Секреты 29

Ма

Находки этого запуска

Находки, включенные в основные итоги отчета и метрики критичности.

Подтвержденные 58

Неподтвержденные 4

От модулей проверки 78

Поиск находок

58 / 58

Свернуть все

Критические 15

Apache 2.4.49 path traversal and RCE (CVE-2021-41773) on the multi-homed internal bridge 172.31.10.2 enables internal pivoting 172.31.10.2:80 (also 172.31.20.10 and 198.18.0.5)

Критическая

Internal Flask portal Jinja2 SSTI yields root RCE (172.31.20.3:8000)

Критическая

Jinja2 server-side template injection in Flask portal /hello (172.31.20.3:8000) yields root RCE 172.31.20.3:8000

Критическая

MySQL UNION SQL injection in product.php plus the FILE-privileged database account enables INTO OUTFILE webshell RCE (172.23.10.19:8081) 172.23.10.19:8081 (shop application, MySQL shopdb account shop)

Критическая

Node/Express API JWT authentication bypass: weak HS256 secret secret and accepted alg=none grant administrative access 172.31.20.5:3000 (and its mirror 172.31.31.3:3000)

Критическая

Отчёт

4

Русский отчет PDF 1.8 MB · 09 окт. 2026 г., 01:45

Русский отчет MARKDOWN 146.2 KB · 09 окт. 2026 г., 01:45

Английский отчет PDF 1.8 MB · 09 окт. 2026 г., 01:40

Английский отчет MARKDOWN 94.1 KB · 09 окт. 2026 г., 01:40

Находки

62
находки

58
подтверждено

4
требуют проверки

IDOR: чужая запись без авторизации

Успешно

Расширенная

Отчёт готов

Параметры

← К запускам

🔗 Сравнить

🔄 Повторный запуск

Широкое покрытие #a945c57d · 08 окт. 2026 г., 23:02

🕒 2ч 43м Прошло

🛡️ 62 Находки

Подготовка

Разведка

Согласование контура

Проверки

Отчёт

🔍 Обзор

📊 Охват 15

🧩 Вспомогательные модули 18

🛡️ Находки 62

🔑 Секреты 29

📁 Ма

Находки этого запуска

Находки, включенные в основные итоги отчета и метрики критичности.

Подтвержденные 58

Неподтвержденные 4

От модулей проверки 78

🔍 IDOR in Node API /api/users/2

1 / 58

Свернуть все

📌 Высокие 1

✓ IDOR in Node API /api/users/2 exposes administrative password hash, SSN and flag CG{id0r_admin_record}

172.31.20.5:3000 /api/users/2

ОПИСАНИЕ

The API exposes user records via IDOR without authentication: /api/users/2 leaks the admin passwordHash, ssn and the flag CG{id0r_admin_record}.

ЦЕЛЬ

172.31.20.5:3000 /api/users/2

ДОКАЗАТЕЛЬСТВА

credentialed-lateral-movement-evidence.txt, recovered-cg-flags.txt

ВЛИЯНИЕ

Exposure of user password hashes, PII and an administrative flag to unauthenticated attackers.

Высокая

</>

GET /api/users/2

👤

Запись администратора без аутентификации

📄

Сохранены доказательства

IDOR: из карточки — в отчёт

Та же находка: `/api/users/2`

НАХОДКА F-38

IDOR в Node API `/api/users/2` раскрывает хеш административного пароля, SSN и флаг `CG{idor_admin_record}`

ВЫСОКАЯ

ПОДТВЕРЖДЕНО

ЦЕЛЬ

172.31.20.5:3000 `/api/users/2`

АГЕНТЫ-ИСТОЧНИКИ

pentest-net1-ftp-pivot

Описание

API раскрывает записи пользователей через IDOR без аутентификации: `/api/users/2` утекает административные `passwordHash`, `ssn` и флаг `CG{idor_admin_record}`.

Влияние

Раскрытие хешей паролей пользователей, PII и административного флага неаутентифицированным атакующим.

Воспроизведение

1. GET `/api/users/2` -> запись администратора, включая `passwordHash`, `ssn` и `CG{idor_admin_record}`

Рекомендации

Добавьте проверки авторизации для `/api/users/:id` и никогда не возвращайте хеши паролей, SSN или флаги в ответах.



Влияние

Раскрытие хешей паролей пользователей, PII и административного флага неаутентифицированным атакующим.



Воспроизведение

GET `/api/users/2` ->
запись администратора,
включая `passwordHash`, `ssn`
и `CG{idor_admin_record}`.



Рекомендация

Добавьте проверки авторизации для `/api/users/:id` и никогда не возвращайте хеши паролей, SSN или флаги в ответах.

JWT: доступ с поддельной ролью

Успешно Расширенная Отчёт готов

Широкое покрытие · #a945c57d · 08 окт. 2026 г., 23:02

2h 43m Прошло 62 Находки

Подготовка Разведка Согласование контура Проверки Отчёт

Обзор Охват 15 Вспомогательные модули 18 Находки 62 Секреты 29 М...

Находки этого запуска

Находки, включенные в основные итоги отчета и метрики критичности.

Подтвержденные 58 Неподтвержденные 4 От модулей проверки 78

Node/Express API JWT forgery via

1 / 58 Свернуть все

Критические 1

Node/Express API JWT forgery via weak HS256 secret secret and accepted alg:none (172.31.20.5:3000)

172.31.20.5:3000

ОПИСАНИЕ

The API signs HS256 JWTs with the literal secret 'secret' (verified by reproducing a /api/login token signature) and also accepts unsigned alg:none tokens. A forged HS256 token with username admin and role admin is accepted by /api/admin returning CG{jwt_weak_secret_forged}, and an unsigned token with role admin is accepted by /api/account returning CG{jwt_alg_none_trusted}.

ЦЕЛЬ

172.31.20.5:3000

ДОКАЗАТЕЛЬСТВА

net2-node-api-flags-and-sqli.txt

ВЛИЯНИЕ

Any user able to reach the API can forge administrative JWTs and access privileged functionality without

Критическая

Отчёт

Русский отчет PDF 1.8 MB · 09 окт. 2026 г., 01:45 ↓

Русский отчет MARKDOWN 146.2 KB · 09 окт. 2026 г., 01:45 ↓

Английский отчет PDF 1.8 MB · 09 окт. 2026 г., 01:40 ↓

Английский отчет MARKDOWN 94.1 KB · 09 окт. 2026 г., 01:40 ↓

01 —

Слабый ключ
HS256

02 —

Принимается
alg:none

03 —

Два
контрольных флага

JWT: тот же обход в русском отчёте

Карточка JWT → находка F-10 в отчёте

НАХОДКА F-10

Подделка JWT API Node/Express через слабый секрет HS256 secret и принимаемый alg:none (172.31.20.5:3000)

КРИТИЧЕСКАЯ

ПОДТВЕРЖДЕНО

ЦЕЛЬ

172.31.20.5:3000

АГЕНТЫ-ИСТОЧНИКИ

pentest-net2-estate

Описание

API подписывает JWT алгоритмом HS256 с буквальным секретом 'secret' (проверено воспроизведением подписи токена /api/login) и также принимает неподписанные токены alg:none. Поддельный токен HS256 с username admin и role admin принимается /api/admin, возвращая CG{jwt_weak_secret_forged}, а неподписанный токен с role admin принимается /api/account, возвращая CG{jwt_alg_none_trusted}.

Влияние

Любой пользователь, способный достичь API, может подделывать административные JWT и получать доступ к привилегированному функционалу без учётных данных.



Права
администратора



Слабый ключ
HS256



Принятие
alg:none



Подтверждённое
влияние

От результата — к повторной проверке

Находка F-10: воспроизведение, исправление, доказательства

Воспроизведение

1. Подделайте JWT HS256 с payload username=admin, role=admin, подписанный ключом 'secret'
2. GET /api/admin с Authorization: Bearer -> {"ok":true,"flag":"CG{jwt_weak_secret_forged}"}
3. GET /api/account с неподписанным токеном header {"alg":"none"} payload {"role":"admin"} -> {"ok":true,"flag":"CG{jwt_alg_none_trusted}"}

Рекомендации

Используйте высокоэнтропийный секрет из окружения, фиксируйте принимаемый алгоритм, никогда не принимайте alg:none и определяйте роли на стороне сервера, а не из утверждений токена.

Доказательства

НАЗВАНИЕ	ТИП	ИСТОЧНИК	РАЗМЕР	SHA-256
net2-node-api-flags-and-sqli.txt	Evidence	pentest-net2-estate	1.8 KB	eb3896b91ac12b7f01585d5b75a880 db806436cabf16dab7af131371d93b 678f

1 Запрос и ответ

Показываем, как воспроизвести находку: последовательность запросов и полученные ответы с флагами.

2 Что исправить

Краткие рекомендации по устранению: безопасный секрет, фиксация алгоритма, запрет alg:none, определение ролей на сервере.

3 Где доказательство

Файл с результатами и флагами: название, тип, источник, размер и SHA-256.

Артефакты связаны с результатами

Успешно Расширенная Отчёт готов

Широкое покрытие · #a945c57d · 08 окт. 2026 г., 23:02

2h 43m Прошло 62 Находки

Подготовка Разведка Согласование контура Проверки Отчёт

Обзор Охват 15 Вспомогательные модули 18 Находки 62 Секреты 29 **Материалы 216** Сравнение Журнал

Все категории

Все источники

216 / 216

Файл и доступ	Источник	Размер	Обновлено
Отчёты 12			
application-attack-hypotheses.md Связи · 4 находок · 4 отчётов	recon-ext-web	8.1 KB	8 окт. 2026 г.
external-attack-surface-report.172.23.10.19.md	recon-ext-perimeter	12.5 KB	8 окт. 2026 г.
internal-pivot-target-map.md	recon-internal-topology	24.3 KB	8 окт. 2026 г.
net3-ssh-credential-chain-investigation-report.md Связи · 2 находок · 4 отчётов	pentest-net3-ssh-credential-chain	6.6 KB	9 окт. 2026 г.
net31-ssrf-assessment-summary.md	pentest-net31-ssrf-ingress	2.7 KB	9 окт. 2026 г.
restoration-and-cleanup-final.txt	pentest-net31-ssrf-ingress	3.2 KB	9 окт. 2026 г.
restoration-and-cleanup.txt	pentest-net31-ssrf-ingress	2.3 KB	9 окт. 2026 г.
security-report-en-2026-10-09T01-40-04Z.md	report-en	94.1 KB	9 окт. 2026 г.



Категории материалов



Источник — агент



Связь с находкой



Просмотр и скачивание

Учётные данные в отдельном каталоге

Успешно

Расширенная

Отчёт готов

Широкое покрытие · #a945c57d · 08 окт. 2026 г., 23:02

🕒 2ч 43м Прошло

🔍 62 Находки

Подготовка

Разведка

Согласование контура

Проверки

Отчёт

🔗 Обзор

📊 Охват 15

🛠️ Вспомогательные модули 18

🔍 Находки 62

🔗 Секреты 29

📁 Ма

🔗 Секреты запуска 29

Учётные данные, сохранённые этим запуском. Значения доступны только через отдельное защищённое скачивание.

Ограниченный доступ

🔗 node-api-jwt-secret-and-token node-api-jwt-secret-and-token.txt	Задача #af0f3b8c 09 окт. 2026 г., 01:08	Размер 862 B	📄
🔗 internal-pivot-recovered-credentials internal-pivot-recovered-credentials.txt	Задача #af0f3b8c 09 окт. 2026 г., 01:08	Размер 2.6 KB	📄
🔗 net31-node-api-jwt-and-shop-admin net31-node-api-and-shop-credentials.txt	Задача #9816245a 09 окт. 2026 г., 01:00	Размер 2.2 KB	📄
🔗 net1-net2-db-postgres-smb-monitor-credentials net1-net2-recovered-credentials.txt	Задача #ce71eb0e 09 окт. 2026 г., 00:54	Размер 1.6 KB	📄
🔗 net2-smb-fileadmin-monitor-and-node-jwt smb-fileadmin-share-and-monitor-account.txt	Задача #34814e77 09 окт. 2026 г., 00:54	Размер 932 B	📄
🔗 net2-monitor-and-smb-private-credentials net2-monitor-and-smb-private-credentials.txt	Задача #19c0b3a7 09 окт. 2026 г., 00:37	Размер 1.2 KB	📄
🔗 internal-segment-credentials internal-segment-credentials.txt	Задача #cba29068 09 окт. 2026 г., 00:35	Размер 2.7 KB	📄

Отчёт 4

📄 Русский отчет PDF
1.8 MB · 09 окт. 2026 г., 01:45

📄 Русский отчет MARKDOWN
146.2 KB · 09 окт. 2026 г., 01:45

📄 Английский отчет PDF
1.8 MB · 09 окт. 2026 г., 01:40

📄 Английский отчет MARKDOWN
94.1 KB · 09 окт. 2026 г., 01:40



Найденные доступы



Источник и контекст



Связь с проверкой

История действий остаётся доступной

Успешно

Расширенная

Отчёт готов

Параметры

К запуском

Сравнить

Повторный запуск

Широкое покрытие · #a945c57d · 08 окт. 2026 г., 23:02

2h 43m Прошло · 62 Находки

Подготовка

Разведка

Согласование контура

Проверки

Отчёт

Модули 18

Находки 62

Секреты 29

Материалы 216

Сравнение

Журнал

Журнал исполнения

Сводные события синхронизации из контура управления.

Все 333

Агенты 98

Подтверждения 15

Материалы 217

Система 3

ВРЕМЯ	СОБЫТИЕ	АГЕНТ	СОСТОЯНИЕ
09 окт. 2026 г., 01:45	Материал сохранён	security-report-ru-2026-10-09T01-45-53Z.md	user
09 окт. 2026 г., 01:45	Материал сохранён	security-report-ru-2026-10-09T01-45-53Z.pdf	user
09 окт. 2026 г., 01:40	Отчёт сформирован	report	Готово
09 окт. 2026 г., 01:40	Материал сохранён	security-report-en-2026-10-09T01-40-04Z.pdf	user
09 окт. 2026 г., 01:40	Материал сохранён	security-report-en-2026-10-09T01-40-04Z.md	user
09 окт. 2026 г., 01:40	Материал сохранён	findings.json	user
09 окт. 2026 г., 01:32	Формирование отчета начато	runner	Формируется отчет
09 окт. 2026 г., 01:32	Run deadline reserve reached; finalize committed evidence	Master	Решение

Отчёт 4

Русский отчет PDF

1.8 MB · 09 окт. 2026 г., 01:45

↓

Русский отчет MARKDOWN

146.2 KB · 09 окт. 2026 г., 01:45

↓

Английский отчет PDF

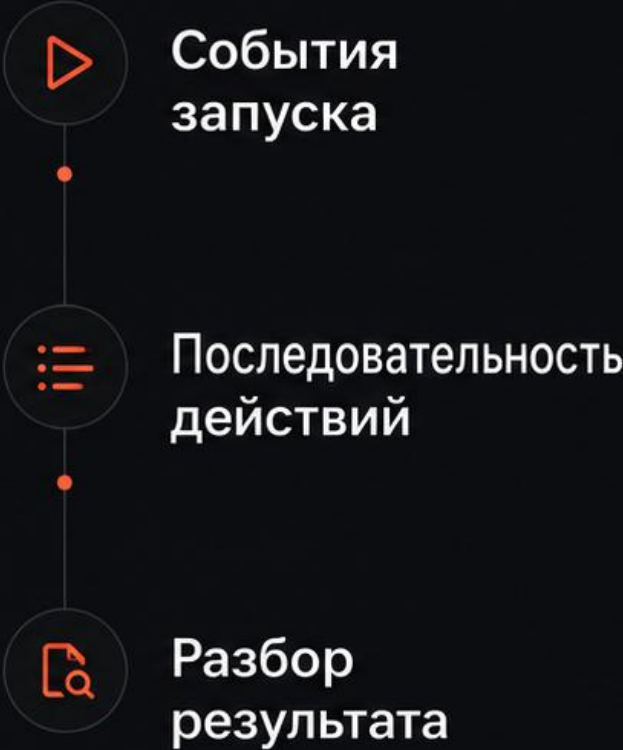
1.8 MB · 09 окт. 2026 г., 01:40

↓

Английский отчет MARKDOWN

94.1 KB · 09 окт. 2026 г., 01:40

↓



Всё исследование — **В ИТОГОВОМ ОТЧЁТЕ**

Находки + материалы + история → сводка результатов

Обзор результатов

В снимок включено находок: 62.
Подтверждено: 58; не подтверждено: 4.

НАИВЫСШАЯ КРИТИЧНОСТЬ

Критическая

62

НАХОДОК

58

ПОДТВЕРЖДЕНО

4

НЕ ПОДТВЕРЖДЕНО

211

МАТЕРИАЛОВ

Распределение по критичности



КРИТИЧЕСКАЯ **15**

ВЫСОКАЯ **42**

СРЕДНЯЯ **4**

НИЗКАЯ **0**

ИНФОРМАЦИОННАЯ **1**

Итог проверки

62

находки

58

подтверждены

4

требуют проверки

211

материалов

Результаты нашего бенчмарка

Cunning Goose · сравнение запусков

Инструмент	Реализовано критических событий	Время	Использование токенов
Triadix	22 / 30 73,3%	2 ч 40 мин	298,75 млн Измерено: работники + оркестратор
PentAGI	11 / 30 36,7%	11 часов	1,246 млрд токенов (оценка)

В 2 раза больше событий · в 4,1 раза меньше времени

Сканер

Известные CVE

Ручной пентест

Индивидуальный подход, но
дорого и редко

AI-пентест

Всегда доступен и готов к работе
любому сценарию проверки

Покажем, на что способна наша система



triadix.ru

Пилотный запуск на вашем скоупе