VEXTA INTELLIGENCE PLATFORM

HIGHLY CONFIDENTIAL

Vulnerability Assessment & Penetration Test

Automated Security Assessment Report

TARGET SCOPE	PREPARED FOR	REPORT DATE	ENGINE
*.example.com	Example Corp Inc.	Month Day, Year	Vexta

00 TABLE OF CONTENTS

REPORT SUMMARY

16	1	2	4
TOTAL FINDINGS	CRITICAL	HIGH	MEDIUM

01 AT A GLANCE

STATUS

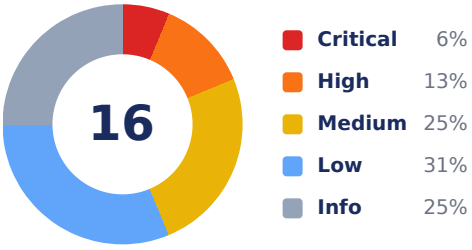
AT RISK

The target environment contains a **Critical SQL Injection** vulnerability enabling unauthorized database access, alongside **2 High** severity issues. Vexta autonomously verified all exploitation paths. Immediate remediation is required.

FINDINGS BY SEVERITY

CRITICAL	1
HIGH	2
MEDIUM	4
LOW	5
INFO	4

VULNERABILITY DISTRIBUTION



RECONNAISSANCE FOOTPRINT

14	3	247	10,482	42 min
SUBDOMAINS	EXPOSED SERVICES	URLS CRAWLED	PAYLOADS SENT	SCAN DURATION

FINDINGS BY CATEGORY (OWASP)

Injection (SQLi, NoSQLi, CMDi)	3
Cross-Site Scripting (XSS)	2
Security Misconfiguration	4
Broken Access Control	1
Cryptographic Failures	2
Information Disclosure	4

02 METHODOLOGY

Vexta employs a four-phase automated assessment pipeline. Each phase is executed autonomously and verified before proceeding. The methodology aligns with OWASP Testing Guide v4.2 and PTES standards.

01 RECONNAISSANCE

Passive and active discovery of subdomains, open ports, exposed services, technology fingerprinting, and API endpoint enumeration across the target perimeter.

02 ACTIVE SCANNING

Systematic probing against 25+ OWASP vulnerability classes using over 10,000 type-aware payload templates with smart parameter fuzzing.

03 PROOF-OF-EXPLOITATION

Safe, non-destructive exploitation verification via time-based inference, out-of-band callbacks (DNS/HTTP), and differential analysis to achieve 0% false positives.

04 AI VERIFICATION

LLM reasoning layer classifies each finding, generates contextual impact analysis, produces bespoke remediation guidance, and formats evidence for the final report.

TECHNOLOGIES DETECTED

Nginx 1.24 · Node.js · React · PostgreSQL · Redis · AWS CloudFront · Express.js · JWT Auth · REST API · GraphQL

SCAN CONFIGURATION

Scan Mode	Full – External Perimeter	**Authentication**	Unauthenticated + Guest Token
Rate Limiting	50 req/s (throttled)	**Out-of-Band Server**	oob.vexta.cloud (DNS + HTTP)
AI Model	Vexta Reasoning Engine v3.2	**Scan Duration**	42 minutes

SEVERITY
CRITICAL

Blind SQL Injection (Time-Based)

CVSS 9.8 · CWE-89

AFFECTED ASSET

https://api.example.com/v1/users/search?query=test · param: **query**

DESCRIPTION

The query parameter is directly interpolated into a SQL statement without parameterization. An attacker can use time-based blind techniques to extract the entire database schema and contents.

IMPACT

Full database read access. Attacker can exfiltrate user credentials, PII, financial records, and escalate to admin privileges via password hashes.

PROOF OF EXPLOITATION ● Verified

```
GET /v1/users/search?query=test' AND (SELECT SLEEP(5))-- HTTP/1.1
Host: api.example.com
► Response delayed by 5.012s — SQL INJECTION CONFIRMED
```

REMEDIATION

Use parameterized queries (prepared statements) for all database interactions. Apply input validation and deploy a WAF rule for SQL injection patterns.

SEVERITY
HIGH

Reflected Cross-Site Scripting (XSS)

CVSS 7.1 · CWE-79

AFFECTED ASSET

https://www.example.com/search?q=%3Cscript%3E · param: **q**

DESCRIPTION

User input in the search parameter is reflected into the HTML response without sanitization or encoding, enabling script injection in the victim's browser context.

IMPACT

Session hijacking via cookie theft. Attacker can impersonate any user, inject phishing forms, or redirect to malware distribution sites.

REMEDIATION

HTML-encode all user input before rendering. Implement Content-Security-Policy headers. Use framework-level auto-escaping (React JSX, Go html/template).

SEVERITY
HIGH

Insecure Direct Object Reference (IDOR)

CVSS 7.5 CWE-639

AFFECTED ASSET

https://api.example.com/v1/invoices/1042 · param: **id**

DESCRIPTION

Sequential invoice IDs are directly exposed in the API. Any authenticated user can access or download invoices belonging to other organizations by incrementing the numeric identifier.

IMPACT

Unauthorized access to financial data of other tenants. Breach of customer confidentiality and potential regulatory violation (GDPR, DPDP Act).

REMEDIATION

Replace sequential IDs with UUIDs. Implement server-side authorization checks verifying the requesting user owns the requested resource. Add rate-limiting on enumeration attempts.

SEVERITY
MEDIUM

Missing Security Headers

CVSS 5.3 CWE-693

AFFECTED ASSET

https://www.example.com/

DESCRIPTION

The application does not set critical security headers: Content-Security-Policy, X-Frame-Options, Permissions-Policy, and Referrer-Policy. This increases the attack surface for XSS, clickjacking, and data leakage.

IMPACT

Enables clickjacking attacks, facilitates XSS exploitation, and allows browser feature abuse. Lowers the overall security baseline.

REMEDIATION

Configure the web server or CDN to return: Content-Security-Policy, X-Frame-Options: DENY, Strict-Transport-Security, Referrer-Policy: strict-origin-when-cross-origin, and Permissions-Policy.

REMAINING FINDINGS (SUMMARY)

SEVERITY	TITLE	CWE	ASSET
MEDIUM	TLS Certificate Weak Cipher Suites	CWE-326	mail.example.com:443
MEDIUM	Directory Listing Enabled	CWE-548	/assets/uploads/
MEDIUM	CORS Misconfiguration	CWE-942	api.example.com

04 SCOPE & DISCLAIMER

SCOPE OF ASSESSMENT

In Scope
*.example.com – all subdomains, web applications, and API endpoints accessible from the public internet.

Out of Scope
Internal networks, third-party SaaS integrations, mobile applications, and physical infrastructure.

Testing Window
July 22, 2026 — single automated assessment cycle.

Authorization
Written authorization received from Example Corp Inc. security team prior to engagement.

SEVERITY CLASSIFICATION (CVSS 3.1)

RATING	CVSS RANGE	DESCRIPTION
Critical	9.0 – 10.0	Exploitation is trivial and leads to full system compromise. Immediate action required.
High	7.0 – 8.9	Exploitation is likely and causes significant impact. Remediate within 7 days.
Medium	4.0 – 6.9	Exploitation requires specific conditions. Remediate within 30 days.
Low	0.1 – 3.9	Limited impact or unlikely exploitation. Remediate in next release cycle.
Info	0.0	Best-practice recommendation. No direct exploitability.

DISCLAIMER & LIMITATIONS

This report is a point-in-time assessment. New vulnerabilities may emerge after the testing window due to code deployments, configuration changes, or newly disclosed CVEs.

All testing was performed non-destructively. No data was modified, deleted, or exfiltrated during the assessment. Proof-of-exploitation techniques were designed to confirm exploitability without impacting availability or integrity.

Findings are based on automated scanning and AI verification. While Vexta achieves near-zero false positive rates, manual expert review is recommended for critical findings before production remediation.

This document is classified as **Highly Confidential** and is intended solely for the authorized recipient. Do not distribute without written consent from VITI Security LLP.

VERSION HISTORY

VERSION	DATE	AUTHOR	CHANGES
1.0	July 22, 2026	Vexta AI Engine	Initial automated assessment report

VITI Security LLP
security@vitisecurity.com · vitisecurity.com