Client – Confidential

Project	Date
Vulnerability Assessment	14/10/25
Document Classification	Version
Client Confidential	1
Prepared By	Suvhankar Dutta

RECON ON **CODELOGICX**

1. **Legally registered in India**

- The company is **CODELOGICX TECHNOLOGIES PRIVATE LIMITED** with CIN **U72300WB2013PTC191145**. (ZaubaCorp)
- It was incorporated on **4th March 2013**. (InstaFinancials)
- It is currently **Active** in the Ministry of Corporate Affairs (MCA) registry. (InstaFinancials)
- Its authorized share capital is ₹2,00,00,000 and paid-up capital is same (₹2 Crores) per some company info sites. (InstaFinancials)
- They have two listed directors: **Amitabh Roy** and **Meghamala Roy**. (ZaubaCorp)
- They have an **LEI (Legal Entity Identifier)** registration: 984500J9C92EV02EA451, validating their legal identity in trade / finance contexts. (LEI Register)

2. **Employee feedback / reviews exist**

- On Glassdoor, they have an average employee rating of ~4.5 / 5 (based on ~50+ reviews). (Glassdoor)
- Many reviews cite *"friendly work environment," "learning opportunities," "salary on time."* (Glassdoor)
- But there are also negative / cautionary reviews: complaints about management, favoritism, pressure, weekend work, etc. (Glassdoor)
- On Indeed, some reviews describe a good work environment and learning exposure. (Indeed)

3. **Third-party profile / credibility in agency directories**

- DesignRush gives them a profile, people estimate their hourly rate ~$15/hr, employee size 100-249. (DesignRush)
- JustDial (a local directory) shows them in Kolkata with ~4.4 rating from ~78 reviews. (Justdial)

4. **Claims & self-presented achievements**

- They claim awards like "SaaS Company of the Year" at TechMeet 2024 (by ASSOCHAM) for their in-house product TeamTrace. (CodelogicX)
- They list many technology capabilities, global offices, and a narrative of growth since 2013. (CodelogicX)

Weaknesses, red flags, or areas needing more verification

1. **Marketing claims without strong evidence**

- "Nearly 100% client retention," "95% project success rate," etc. are self-claims. Need to verify via client references or third-party reviews. (CodelogicX)
- Awards / recognitions need verification: local awards and event claims are easier to self-promote. Always ask for proof (certificates, press releases).

2. **Employee reviews contain serious criticisms**

- Some reviews allege *"incompetent managers," "favoritism," "weekend work is expected/enforced,"* etc. (Glassdoor)
- These negative reviews suggest potential cultural / management risks, especially for long term or sensitive projects.

3. **Financials / revenue not transparent in public domain**

- The public registries mention capital / balance sheet filing, but I did not find reliable recent revenue, profit, or audited reports in open sources. (InstaFinancials)
- The "revenue < $1 million USD" mention on Glassdoor (as a profile estimate) is a signal that they may be small in scale compared to big IT firms. (Glassdoor)

4. **Client feedback / independent references lacked in my search**

- I did not find many case studies from independent sources about their completed projects, client testimonials outside their website, or press coverage verifying their claims.
- No significant negative news / litigation (in my search) surfaced, but absence of evidence is not proof of absence.

5. **Local directory mixing of business types**

- On JustDial, some descriptions may misclassify the company (as an installation services provider). That could be generic or outdated listings. (Justdial)
- Some directories may show mixed or mistaken categories. Be cautious on directory data.

SQL-injection tools

1) Automated scanners & enterprise tools

These run wide checks automatically and are good for broad coverage / scheduled scans.

- sqlmap — CLI automation for discovering and exploiting SQLi

(fingerprinting DB, extracting data). Great for fast, deep checks in a lab. (Cross-platform, Python).

Defender note: watch for automated, repetitive query patterns.

- Acunetix — Commercial web scanner with built-in SQLi checks and enterprise reporting/CI integrations.

Defender note: use for scheduled scans in pre-prod and triage false positives manually.

- Netsparker / Invicti — Commercial scanner focused on accuracy and proof-based detection to reduce false positives.

Defender note: integrates with ticketing to push fixes to dev teams.

- OWASP ZAP — Open-source scanner + proxy; good for automated baseline scans and CI pipeline integration. (Java)

Defender note: run in staging to catch regressions early.

2) Manual testing & proxy tools

Used by testers to craft, manipulate, and validate payloads interactively.

- Burp Suite (Proxy / Repeater / Intruder / Scanner) — Industry standard for manual web testing; craft requests, fuzz, and validate SQLi.

(Community & Pro)

Defender note: manual probing often leaves long sequences of similar requests — monitor for that.

- Tamper Data / browser devtools — Browser tools/addons for

intercepting and editing requests manually. Essential for quick proofs-of- concept.

Defender note: strong server-side validation prevents these manual attacks.

- curl / HTTPie — Command-line HTTP clients for crafting custom requests; good for reproducible POCs or scripts.

Defender note: logs will show unusual content in parameters when attacks occur.

3) DB-specific exploitation tools

Target particular DB engines or provide DB-centric post-exploitation features.

- sqlninja — Focused on Microsoft SQL Server exploitation and post- exploit actions.

Defender note: harden MSSQL (disable dangerous extended procedures, enforce least privilege).

- sqlsus — Tool aimed at MySQL SQLi exploitation and extraction (CLI).

Defender note: separate DB accounts and remove unnecessary privileges.

- jSQL Injection — Java GUI tool that automates detection/extraction across many DB types (beginner-friendly).

Defender note: GUI tools are noisy — WAFs often have signatures.

- Havij — Automated Windows GUI SQLi tool (historically popular). Use only in safe labs — it's often detected by security controls.

Defender note: rely on secure coding rather than only WAF signatures.

4) Fuzzers & blind SQLi helpers

Designed to enumerate injection points, brute-force payloads, or extract data via blind channels.

- BBQSQL — A blind SQLi fuzzer and extraction tool (Python) designed for time/boolean based blind attacks.

Defender note: blind attacks generate many slow, patterned requests — watch for timing anomalies.

- WFuzz — Generic web fuzzer useful to brute force parameter values and test payloads.

Defender note: rate-limit and alert on high request bursts.

- SQLiv — Automated SQL injection scanner that helps find injectable URLs from lists (CLI).

Defender note: scanning tools often probe many parameters; block or throttle unauthenticated scanning.

5) Recon / enumeration / supporting tools

Not pure SQLi tools but useful in the discovery phase to find targets, endpoints, versions, and configurations.

- Nmap (with NSE scripts) — Network/service discovery and scripts that can fingerprint DB services and versions. Useful pre-engagement recon. Defender note: minimize exposed DB ports; use network segmentation.

- Nikto — Web server scanner to find outdated software, CGI scripts, and misconfigurations that might lead to injection vectors.

Defender note: patch and reduce server info exposure.

- DirBuster / Dirsearch — Directory and file bruteforcers to discover hidden endpoints/parameters that could be injectable.

Defender note: hide or protect admin/endpoints and require auth.

6) NoSQL & non-SQL injection tools

For apps using NoSQL databases (different injection patterns).

- NoSQLMap — Automated tool for detecting/exploiting NoSQL injection (MongoDB, etc.). Targets operator injection and JSON payload issues. Defender note: validate types and use safe query builders; don't build queries from raw JSON from users.

7) Exploitation frameworks & post-exploit tools

Used when SQLi can be chained to further compromise (authorized red-team).

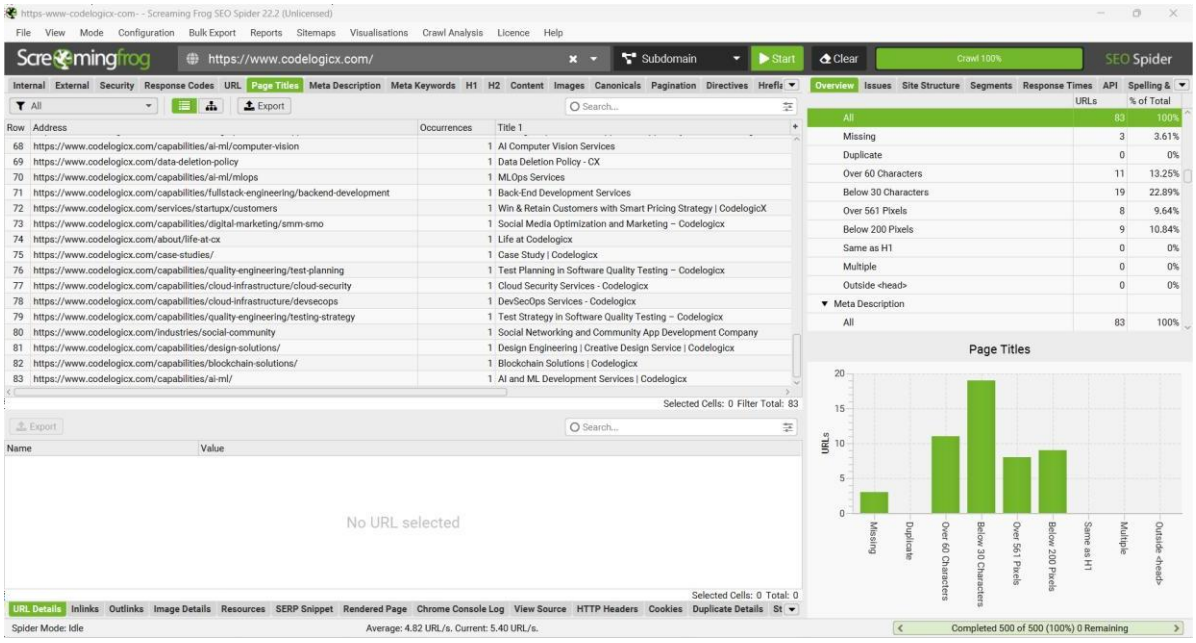
- Metasploit Framework — Large exploitation framework with modules useful for post-exploitation after gaining DB access or a shell.

Defender note: monitor for lateral movement and abnormal process/command activity.

8) Other SQLi helpers / one-offs you may see

- SQLi Dumper / SQLi tools — Various smaller or less reputable tools exist; they often automate extraction but may be outdated or malicious.

Defender note: WAF signatures often include such tool fingerprints — but do not rely solely on signatures.



No of Web pages:- 83 Proof of concept:-

1. https://www.codelogicx.com/
2. https://www.codelogicx.com/capabilities/design-solutions/social-media- creatives-design
3. https://www.codelogicx.com/capabilities/quality-engineering/ci-cd-testing
4. https://www.codelogicx.com/capabilities/mobile-engineering/ios-app- development
5. https://www.codelogicx.com/services/maintenance-upgrades
6. https://www.codelogicx.com/capabilities/quality-engineering/specialized- testing
7. https://www.codelogicx.com/privacy-policy
8. https://www.codelogicx.com/industries/fintech-app-development
9. https://www.codelogicx.com/terms-of-service
10. https://www.codelogicx.com/services/staff-augmentation
11. https://www.codelogicx.com/capabilities/fullstack-engineering/web-app- development
12. https://www.codelogicx.com/capabilities/quality-engineering/functional- testing
13. https://www.codelogicx.com/capabilities/ai-ml/edge-ai
14. https://www.codelogicx.com/industries/healthcare-software-development
15. https://www.codelogicx.com/about/locations
16. https://www.codelogicx.com/contact
17. https://www.codelogicx.com/capabilities/ai-ml/agent-chatbots
18. https://www.codelogicx.com/capabilities/cloud-infrastructure/dr-solutions
19. https://www.codelogicx.com/about/safe-workplace
20. https://www.codelogicx.com/cookie-policy
21. https://www.codelogicx.com/industries/transport-software-development
22. https://www.codelogicx.com/capabilities/quality-engineering/manual- testing
23. https://www.codelogicx.com/capabilities/cloud-infrastructure/kubernetes- solutions
24. https://www.codelogicx.com/industries/retail-ecommerce
25. https://www.codelogicx.com/capabilities/quality-engineering/test- automation
26. https://www.codelogicx.com/services/startupx/planning
27. https://www.codelogicx.com/capabilities/cloud-infrastructure/devops- enablement

28. https://www.codelogicx.com/services/startupx/product

29. https://www.codelogicx.com/services/startupx/launch

30. https://www.codelogicx.com/capabilities/quality-engineering/api-testing

31. https://www.codelogicx.com/capabilities/mobile-engineering/app- maintenance

32. https://www.codelogicx.com/capabilities/cloud-infrastructure/cost- optimization

33. https://www.codelogicx.com/capabilities/mobile-engineering/app- modernization

34. https://www.codelogicx.com/capabilities/mobile-engineering/flutter-app-development

35. https://www.codelogicx.com/capabilities/mobile-engineering/web-app- development

36. https://www.codelogicx.com/capabilities/digital-marketing/seo

37. https://www.codelogicx.com/capabilities/design-solutions/ui-ux-design

38. https://www.codelogicx.com/capabilities/digital-marketing/ppc

39. https://www.codelogicx.com/capabilities/mobile-engineering/react-app- development

40. https://www.codelogicx.com/services/startupx/

41. https://www.codelogicx.com/capabilities/design-solutions/product-design

42. https://www.codelogicx.com/services/software-rescue-services

43. https://www.codelogicx.com/capabilities/ai-ml/generative-ai

44. https://www.codelogicx.com/industries/hr-payroll-software-development

45. https://www.codelogicx.com/capabilities/quality-engineering/performance- testing

46. https://www.codelogicx.com/capabilities/fullstack-engineering/frontend- development

47. https://www.codelogicx.com/capabilities/fullstack-engineering/ai- integration

48. https://www.codelogicx.com/industries/travel-hospitality-software- development

49. https://www.codelogicx.com/capabilities/mobile-engineering/android-app-development

50. https://www.codelogicx.com/about/values

51. https://www.codelogicx.com/services/startupx/scale

52. https://www.codelogicx.com/capabilities/ai-ml/nlp-llm

53. https://www.codelogicx.com/capabilities/cloud-infrastructure/cloud- managed-service

54. https://www.codelogicx.com/capabilities/cloud-infrastructure/site- reliability

55. https://www.codelogicx.com/capabilities/design-solutions/brand-design

56. https://www.codelogicx.com/capabilities/fullstack-engineering/api- integration
57. https://www.codelogicx.com/capabilities/cloud-infrastructure/cloud- migration
58. https://www.codelogicx.com/capabilities/ai-ml/recommender-systems
59. https://www.codelogicx.com/industries/education
60. https://www.codelogicx.com/services/code-infrastructure-audits
61. https://www.codelogicx.com/services/product-engineering
62. https://www.codelogicx.com/capabilities/digital-marketing/content- marketing
63. https://www.codelogicx.com/capabilities/cloud-infrastructure/cloud- modernization
64. https://www.codelogicx.com/capabilities/digital-marketing/email- marketing
65. https://www.codelogicx.com/capabilities/ai-ml/deep-learning
66. https://www.codelogicx.com/capabilities/ai-ml/computer-vision
67. https://www.codelogicx.com/services/scaling-optimization-support
68. https://www.codelogicx.com/capabilities/quality-engineering/mobile-app- testing
69. https://www.codelogicx.com/capabilities/ai-ml/mlops
70. https://www.codelogicx.com/capabilities/fullstack-engineering/backend- development
71. https://www.codelogicx.com/data-deletion-policy
72. https://www.codelogicx.com/capabilities/digital-marketing/smm-smo
73. https://www.codelogicx.com/about/life-at-cx
74. https://www.codelogicx.com/capabilities/quality-engineering/test-planning
75. https://www.codelogicx.com/services/startupx/customers
76. https://www.codelogicx.com/case-studies/
77. https://www.codelogicx.com/capabilities/cloud-infrastructure/cloud- security
78. https://www.codelogicx.com/capabilities/cloud-infrastructure/devsecops
79. https://www.codelogicx.com/capabilities/quality-engineering/testing- strategy
80. https://www.codelogicx.com/industries/social-community
81. https://www.codelogicx.com/capabilities/design-solutions/
82. https://www.codelogicx.com/capabilities/blockchain-solutions/
83. https://www.codelogicx.com/capabilities/ai-ml/