APPLICATION SECURITY REPORT

Prepared for

Redacted

Redacted Reports Web Application, Thick Client & VoIP Infrastructure

Application Security Assessment • Gray Box • UAT

DarkNext Cybersecurity

REPORT RELEASE DATE
26-April-2026

TYPE OF AUDIT
Application Security

TYPE OF AUDIT REPORT
First Audit Report

PERIOD
15-April-2026 to 26-April-2026

Issued by
Darknext LLP, 15A Fairlawn Diamond Garden, Chembur, Mumbai 400071
+91 9820380225 | www.darknext.com

DarkNext
Cybersecurity

SECTION 01

01

Document Control

Preparation, change history & distribution

SECTION 01

Document Control

Document Preparation

Document Title	Redacted_Application_Security_Report_v_1.0
Document ID	7392168460
Document Version	1.0
Prepared by	Harshad Lataye
Reviewed by	Lalit Vazirani
Approved by	Lalit Vazirani
Released by	Harshad Lataye
Release date	26-April-2026

Document Change History

Version	Date	Remarks / Reason of change
1.0	26-April-2026	First Audit Report

Document Distribution List

Name	Organization	Designation	Email Id
Mr. Redacted	Redacted	Redacted	Redacted@gmail.com

SECTION 02

02

Contents

What this report covers

SECTION 02

Contents

SECTION 03

03

Introduction

Engagement background, objectives & assumptions

SECTION 03

Introduction

CLIENT	TESTING APPROACH	ENVIRONMENT	ACCESS
Redacted	Gray Box	UAT	Authorized credentials provided

DarkNext was engaged by Redacted to conduct a comprehensive security assessment of their Redacted Reports Web Application, along with associated thick client and VoIP infrastructure. The assessment involved Gray Box testing, and authorized credentials were provided to facilitate the evaluation. It is important to note that all testing activities were carried out in the UAT environment.

The primary objective was to provide independent assurance regarding the security posture of the application's architecture and associated systems. This included evaluating whether communications and access between components were securely implemented and resilient against known threats.

This assessment is a snapshot in time and represents the findings found during testing and may not reflect the current state of the systems in question:

SECTION 03

Introduction - Scope

SCOPE OBJECTIVES

The assessment was conducted to evaluate the overall security posture of the web application, thick client, and VoIP system by identifying vulnerabilities that could potentially expose them to security threats. Redacted has tasked DarkNext for identifying security vulnerabilities across the web application, thick client, and VoIP infrastructure to assess their exposure to potential exploitation.

SCOPE ASSUMPTIONS

Based on the scope, only the agreed URL addresses, web application, thick client, and VoIP system were tested.

NOT COVERED IN THIS TEST

The following was not covered as part of the penetration test:

- Distributed Denial of Service testing.
- Quality Testing, Stress Testing, and Load Testing

SECTION 04

04

Engagement Scope

Application, URL's & thick client application's

SECTION 04

Engagement Scope

S. No	Application Name	Criticality	Hash Value	Version
1	Redacted	Medium	Not Applicable	1.0

URLs

S. No	URL's	Application Name
1	http://Redacted/	Redacted Reports
2	http://Redacted/	Redacted Reports
3	http://Redacted:8080/	Redacted Server

Thick Client Application's

S. No	Application Name
1	Redacted server
2	Redacted v1
3	Redacted (administrator)

SECTION 05

05

Details of the Auditing Team

The people behind this assessment

SECTION 05

Details of the Auditing Team

LV

Lalit Vazirani

DIRECTOR

EMAIL

Lalit.vazirani@darknext.com

QUALIFICATIONS / CERTIFICATIONS

B.E in Computer Engineering.

ISO 27001 LA

KJ

Krishna Jere

ASSOCIATE DIRECTOR

EMAIL

Krishna.jere@darknext.com

QUALIFICATIONS / CERTIFICATIONS

B.E. in Electronics & Communication

ISO 27001 LA

HL

Harshad Lataye

CONSULTANT

EMAIL

Harshad.lataye@darknext.com

QUALIFICATIONS / CERTIFICATIONS

B.E in Mechanical Engineering

CEH

DarkNext
Cybersecurity

SECTION 06

06

Audit Activities and Timelines

How the engagement was executed

SECTION 06

Audit Activities and Timelines

PHASE 1

Information Gathering

DATE

15-April-2026

PHASE 2

Assessment

DATE

15-April-2026 to 19-April-2026

PHASE 3

Reporting

DATE

23-April-2026 to 26-April-2026

Engagement period: **15-April-2026 to 26-April-2026**

SECTION 07

07

Audit Methodology and Criteria

Web, thick client & VoIP assessment approach

SECTION 07

Audit Methodology and Criteria

The audit methodology is designed to systematically evaluate the security posture of critical digital assets, including web applications, thick client applications, and VoIP systems. This process uses a combination of manual inspection and automated tools to identify vulnerabilities that may be exploited by malicious actors. The primary audit criteria focus on assessing risks that could affect the confidentiality, integrity, and availability of data and services.

WEB APPLICATIONS

For web applications, the audit examines vulnerabilities such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), insecure authentication mechanisms, and misconfigurations. The methodology includes penetration testing, vulnerability scanning, and secure code reviews. The audit evaluates both client-side and server-side components to verify that data validation, encryption, and access control mechanisms are implemented in accordance with industry standards, such as the OWASP Testing Guide.

THICK CLIENT APPLICATIONS

Thick client applications are audited using techniques tailored to their architecture, which typically involves local execution with remote server interaction. The audit criteria focus on risks including insecure local data storage, insufficient encryption, and unprotected client-server communication channels. The methodology applies static and dynamic analysis, reverse engineering, and traffic inspection to uncover weaknesses that may lead to privilege escalation, data leakage, or application tampering.

VoIP SYSTEMS

For VoIP systems, the audit assesses the security of signalling and media transport protocols (such as SIP and RTP), access controls, and system configurations. Key risks include call interception, denial of service, and credential compromise. Audit techniques include protocol fuzzing, packet capture analysis, and authentication testing, aligned with VoIP-specific security standards and threat models.

Organizations are advised to conduct regular security audits using updated methodologies and threat intelligence. This ensures ongoing compliance with best practices and mitigates exposure to emerging threats. A thorough and repeatable audit methodology supports long-term security maturity and operational resilience.

DarkNext
Cybersecurity

SECTION 08

08

Tools / Software Used

Licensed & open-source tooling

SECTION 08

Tools / Software Used

S. No	Name of Tool/Software used	Version	Open Source/Licensed
1	Tenable Nessus Pro	10.8	Licensed
2	Burp Suite Professional	1.7	Licensed
3	Nmap	7.95	Open Source
4	Nikto	2.5	Open Source
5	Dirbuster	1.0-RC1	Open Source
6	Editthiscookie	1.0	Open Source
7	TamperData Extension	1.0	Open Source

S. No	Name of Tool/Software used	Version	Open Source/Licensed
8	Xnip	2.2.6	Open Source
9	Sqlmap	1.9-1	Open Source
10	Github Scripts	N/A	Open Source
11	Metasploit	6	Open Source
12	OWASP ZAP	2.16.1	Open Source
13	Wireshark	4.4	Open Source

DarkNext
Cybersecurity

SECTION 09

09

Executive Summary

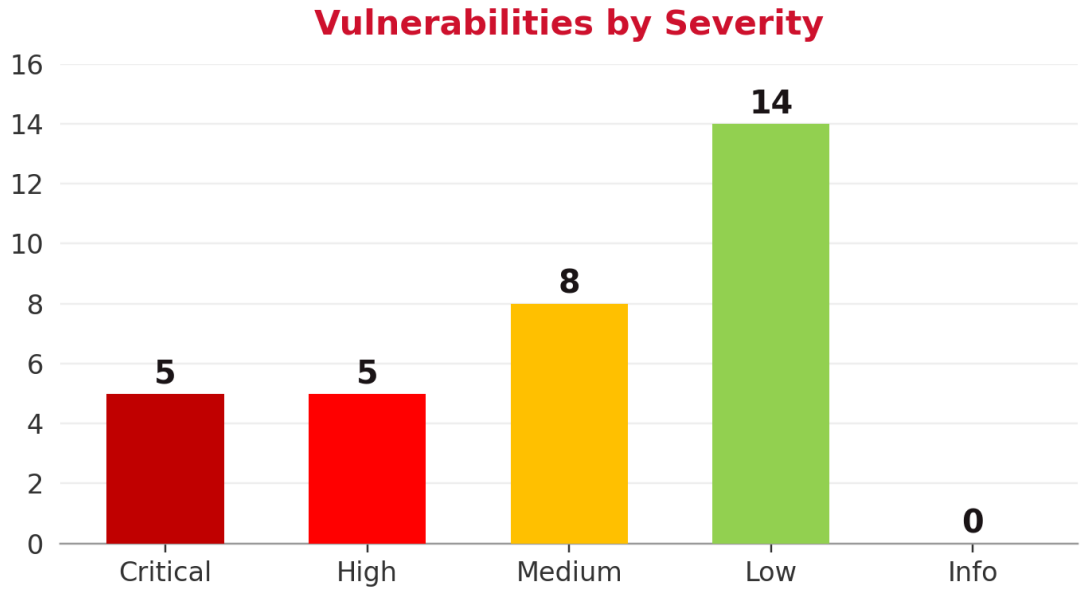
Overall security posture at a glance

SECTION 09

Executive Summary

Darknext LLP performed Application Security Assessment on Redacted. The test was performed using industry-standard tools, framework and technologies to assess the overall security posture of the application by providing this report comprising of all identified vulnerabilities, their impact and steps for mitigation of the same.

The graphical representation of vulnerabilities is shown below.



5	Critical
5	High
8	Medium
14	Low
0	Info

SECTION 10

10

Table of Observations

All identified vulnerabilities by severity

SECTION 10

Table of Observations

Sr No	Vulnerabilities	Severity
1	Forced Browsing	Critical
2	Sensitive data exposed	Critical
3	Potential Privilege Escalation through DLL Hijacking	Critical
4	Cleartext Credentials	Critical
5	Hardcoded Credentials	Critical
6	Authentication Bypass via Reverse Engineering	High
7	Unencrypted Credentials Stored in Database	High

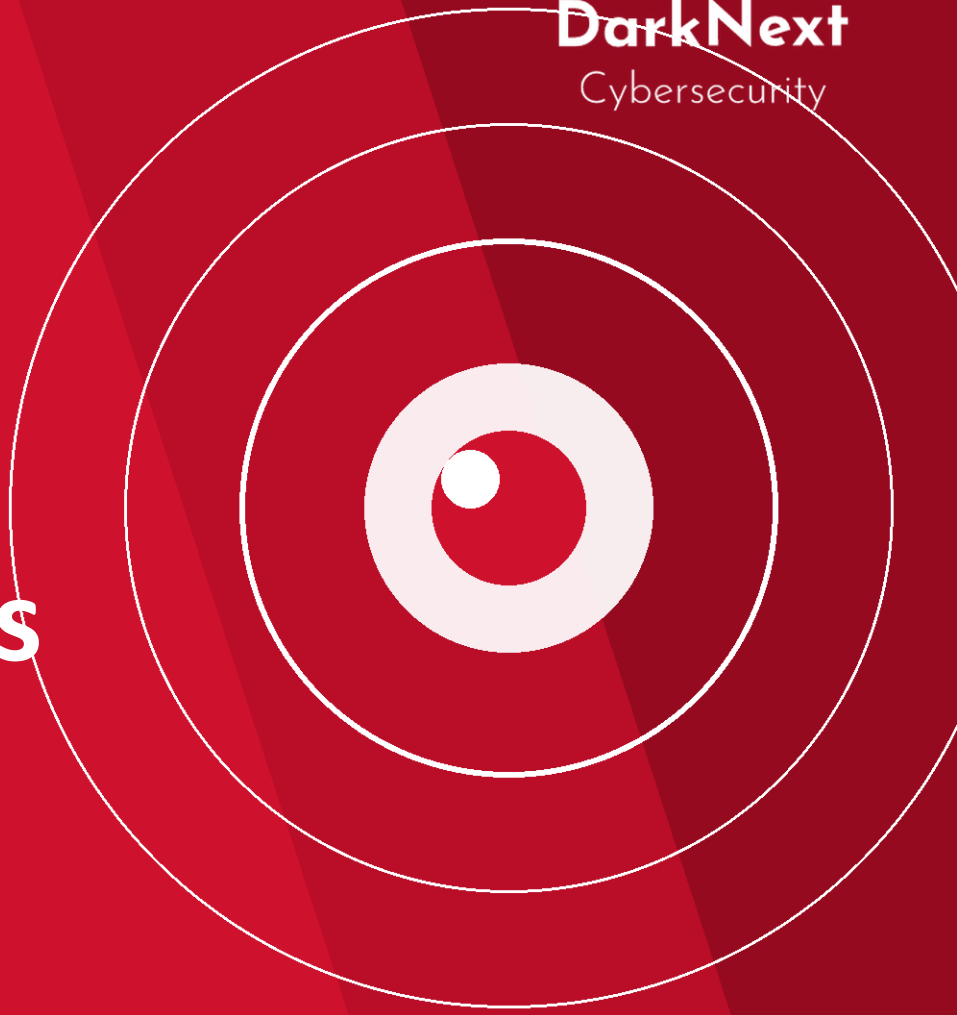
Sr No	Vulnerabilities	Severity
8	VoIP Flood Attack	High
9	SIP User Enumeration	High
10	Rate Limiting not implemented	Medium
11	Internal Path disclosure	Medium
12	Session Fixation	Medium
13	SIP Server Configured with POP3	Medium
14	Brute Force Attack Against SIP Credentials	Medium

SECTION 11

11

Detailed Observations

Description, solution, references & proof of concept



SECTION 11

Detailed Observations

OBS-01	VULNERABILITY Forced Browsing	RISK Critical

DESCRIPTION

Forced Browsing is an attack technique used to gain access to restricted pages or other sensitive resources in a web server by forcing the URL directly. If the restricted URLs, scripts, or files that reside in the web server directory are not enforced with appropriate authorization, they can be vulnerable to forced browsing attacks.

SOLUTION

Avoid common file names and disable directory listing on the webserver. Verify user authentication and enforce access controls before granting access to sensitive functions.

CWE	CWE-425	Ref	N/A

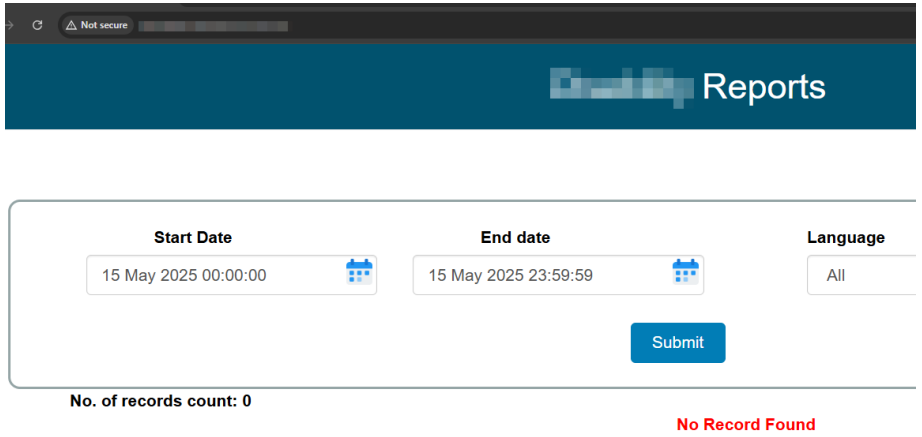
SECTION 11

Proof of Concept - OBS-01

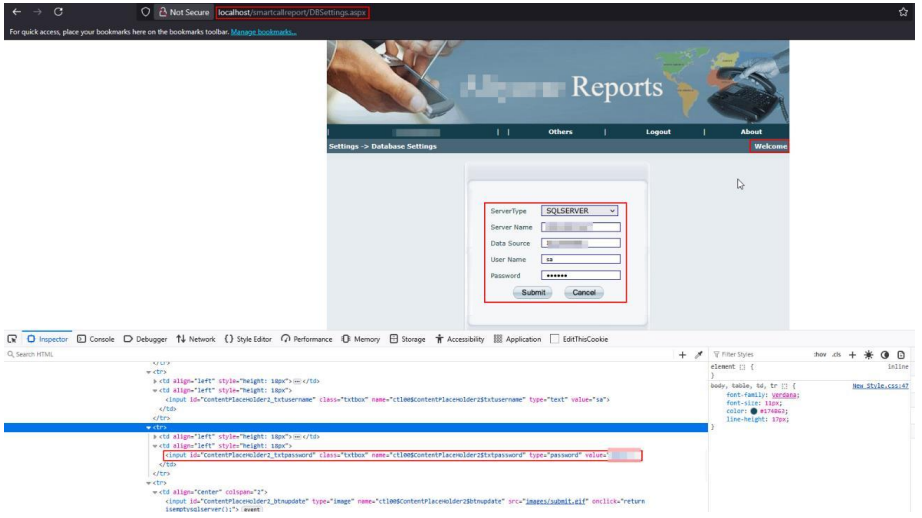
Forced Browsing

OBSERVATION

The application allows access to a sensitive or restricted page without requiring user authentication, potentially exposing functionality or data to unauthorized users.



Step 1: Users can access Redacted Reports without logging in.



Step 2: The Database Settings page is accessible without authentication, allowing unauthorized individuals to view database credentials.

SECTION 11

Detailed Observations

OBS-02	VULNERABILITY	RISK
	Sensitive data exposed	**Critical**

DESCRIPTION

If an application's source code is exposed, it can reveal sensitive information like credentials, API keys, and security configurations. Attackers can analyze the code to find vulnerabilities and exploit them. This can lead to unauthorized access, data breaches, or complete system compromise.

SOLUTION

Restrict access to sensitive files by ensuring only authorized users can view them. Store configuration files securely and avoid hardcoding credentials or API keys in the source code. Use code scanning tools to detect and remove exposed sensitive information.

CWE	CWE-540	Ref	N/A

SECTION 11

Proof of Concept - OBS-02

Sensitive data exposed

STEPS TO REPRODUCE

- *[Add step 1]*
- *[Add step 2]*
- *[Add step 3]*

EVIDENCE

[Insert POC screenshot(s) here]

SECTION 11

Detailed Observations

OBS-03	VULNERABILITY **Potenial Privilege Escalation through DLL Hijacking**	RISK **Critical**

DESCRIPTION

DLL hijacking occurs when an attacker places a malicious DLL in a directory where a vulnerable application loads it instead of the legitimate one, due to improper search order or missing DLL path validation. This can lead to code execution under the context of vulnerable application.

SOLUTION

- Always load DLLs using the full absolute path instead of relying on Windows' default search order (which looks in potentially unsafe directories first like the current working directory).
- Sign your DLLs and verify their signatures at runtime before loading them. This ensures only trusted, unaltered DLLs are used.
- Place your DLLs in secure, access-controlled directories (like C:\Program Files) and ensure the folder is not writable by non-admin users.
- Avoid LoadLibrary when not necessary.
- Limit dynamically loading DLLs at runtime unless essential.
- Validate and sanitize all inputs used in DLL loading logic.

CVE	CVE-2019-0859	Ref	N/A

SECTION 11

Proof of Concept - OBS-03

Potential Privilege Escalation through DLL Hijacking

STEPS TO REPRODUCE

- *[Add step 1]*
- *[Add step 2]*
- *[Add step 3]*

EVIDENCE

[Insert POC screenshot(s) here]

SECTION 11

Detailed Observations

OBS-04

VULNERABILITY

Cleartext Credentials

RISK

Critical

DESCRIPTION

Cleartext credentials occur when usernames and passwords are transmitted or stored without encryption, making them easily readable by attackers through network sniffing or local file access. This exposes sensitive information and increases the risk of unauthorized access.

SOLUTION

Always encrypt sensitive credentials at rest using strong encryption or hashing algorithms. Hash passwords using strong, modern algorithms like bcrypt, scrypt, or Argon2. Never store passwords in plain text. Use encryption (e.g., AES-256) for storing other sensitive credentials (e.g., API keys, tokens) and keep encryption keys in a secure location (e.g., a Hardware Security Module or a secure key vault). Avoid storing any sensitive credentials in plain text or reversible formats in the database

CWE	CWE-319	Ref	N/A

SECTION 11

Proof of Concept - OBS-04

Cleartext Credentials

STEPS TO REPRODUCE

- *[Add step 1]*
- *[Add step 2]*
- *[Add step 3]*

EVIDENCE

[Insert POC screenshot(s) here]

SECTION 12

12

Risk Rating

CVSS-aligned rating methodology

SECTION 12

Risk Rating

Within each report, every finding is given a rating that is based upon CVSS. The Common Vulnerability Scoring System provides an open framework for communicating the characteristics and impacts of IT related vulnerabilities, this is summarized in the table below. We have aligned the CVSS ratings to the OSB Internal Audit ratings, which have been used for reporting purposes in this document.

CVSS Rating	Description	Features
Critical	Findings that represents vulnerabilities that could lead to significant data breaches, complete system compromise, or severe financial loss if exploited. These are typically highpriority issues requiring immediate attention.	▪ Loss of (confidentiality / integrity / availability) is likely to have a catastrophic effect on the organisation's operations and reputation. ▪ Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit
High	Findings that are fundamental to the management of risk in the business area, representing a weakness in control that requires the immediate attention of management	▪ Loss of (confdentiality / integrity / availability) is likely to have a catastrophic effect on the organisation ▪ Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit
Medium	Important findings that are to be resolved by management.	▪ Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited ▪ Authentication is required to exploit the vulnerability ▪ The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit
Low	Findings that identify an area for review with established services and good practice	▪ There is reduced performance or interruptions in resource availability ▪ There is little to no impact to the integrity of the system ▪ There is informational disclosure
Info	Findings that are limited in affect but are worthy of being noted for review- for example future proofing.	▪ Information for department management ▪ Very limited risk - something that could be utilised with the relevant skillsets and resources to gather information

THANK YOU

Darknext LLP, 15A Fairlawn Diamond Garden, Chembur, Mumbai 400071

+91 9820380225 | www.darknext.com

DarkNext

Cybersecurity