



TECHDEFENCELABS

Your Trusted **Cyber Security** Partner

A CERT-In Empanelled Information Security Organisation

No:- 3(15)/2004-CERT-In



Document Authorization, Revision History, and Control

Document Preparation	
Document Title	Web Application Vulnerability Assessment & Penetration Testing Report
Evaluated Organization	LKP Securities Limited
Document ID	TDL-LSL-WG-04/26/0050
Report Version	v1.0
Web Application Name	rekyc.lkponline
Assessment Approach	Grey Box Web Application Security Assessment
Type of Audit Report	First Audit Report
Primary Assessment Period	18 May 2026 – 19 May 2026
Re-Assessment Period	Follow up Audit Pending
Report Prepared by	Harsh Sapariya
Reviewed by	Rushikesh Patil
Approved by	Rohit Soni
Released by	Pavan Saxena
Date of Release	21 May 2026

Document Change History		
Version	Date	Remarks / Reason of Change
v1.0	21 May 2026	First Audit Report

Document Distribution List			
Name	Organization	Role	Email Id
Dhruv Chauhan	TechD Cybersecurity Limited	Manager – Enterprise Business	dhruv.chauhan@techdefence.com
Umair Patel	LKP Securities Limited	Assistant manager information security	jotiba_patil@lkpsec.com

Confidentiality and Disclaimer

This report is prepared exclusively for the management of the Evaluated organization and is intended solely for internal use. TechD Cybersecurity Limited disclaims any liability to third parties for the unauthorized use or distribution of this document or its contents. The findings, information, data, advice, and recommendations are based on the cooperation of the Evaluated organization and the data provided during the assessment period. Any limitations due to environmental constraints, access restrictions, or insufficient information may have impacted the thoroughness of our analysis and could result in unidentified vulnerabilities.

The report assesses the initial security controls implemented by the Evaluated organization, specifically focusing on the security of the defined domain and systems in-scope. TechD Cybersecurity Limited highlights areas for potential improvement; however, the responsibility for implementing and maintaining robust security measures lies with the management of the Evaluated organization. The information provided in this document reflects the state of the security environment at the time of preparation and is not an exhaustive evaluation.

Note: *For the purpose of this report, the term “Evaluated organization” refers to the client organization for which this assessment was conducted.*

©TechD Cybersecurity Limited, 2026
9th Floor, Abhishree Adroit,
Near Mansi Circle, Vastrapur,
Ahmedabad-380015.

Table of Contents

Document Authorization, Revision History, and Control	2
Document Preparation	2
Document Change History	2
Document Distribution List	2
Confidentiality and Disclaimer	3
1. Assessment Details	5
1.1 Engagement Scope	5
1.2 Scope Exclusions	6
1.3 Project Team	6
1.4 Tools used during the assessment	7
2. VAPT Methodology and Standards	8
2.1 Phases of the Assessment	8
2.2 Standards and Methodologies	8
2.3 Vulnerability Risk Rating Metrics and Remediation SLA	9
3. Executive Summary	10
3.1 Visual Representation of Assessment Results	10
3.2 Vulnerability Overview Table	11
4. Detailed Vulnerability Observations	12
TDL-001 - OTP Bypass via Response Manipulation – {High } {Open}	12
TDL-002 - Insufficient Session Expiration – {Medium} {Open}	16
Annexure A - Engagement Limitations	19
Annexure B - Retesting Statement	19
Annexure C - Disclaimer and Precautions for Patch Implementation	20
Annexure D - CERT-In Reporting and Remediation Compliance	20

1. Assessment Details

The Evaluated organization engaged TechD Cybersecurity Limited to assess the security of its web application. The evaluation focused on identifying web application-level vulnerabilities, testing security mechanisms, and evaluating resilience against unauthorized access. The assessment followed recognized industry standards, including the OWASP Top 10, the SANS Top 25, and the Penetration Testing Execution Standard (PTES).

1.1 Engagement Scope

The following web applications provided by the Evaluated organization were identified as in scope for this security assessment, as defined during the engagement.

In Scope of Assessment	
Web Application Name	rekyc.lkponline
Web Application URL	https://rekyc.lkponline.com/v1/company/lkpsec/modification/login
Web Application Version	N/A
Assessment Approach	Grey Box
Testing Environment	Production
User Roles Provided for Testing	Normal User

Out-of-Scope Components			
Sr. No.	Component / Function	URL / Endpoint	Reason for Exclusion
N/A	N/A	N/A	N/A

1.2 Scope Exclusions

1. Infrastructure and server-level testing, including operating systems, databases, and hosting environments on which the web application is deployed, are outside the scope of this assessment unless explicitly specified.
2. Secure code review, static code analysis, and testing of the web application's source code are not included as part of this assessment.
3. Testing of third-party services, external integrations, API gateways not owned or controlled by the Evaluated organization, Denial-of-Service (DoS/DDoS) attacks, and social engineering activities such as phishing or physical security testing are excluded from the scope of this assessment.
4. When testing is conducted in a production environment, test cases that may cause service disruption, downtime, or instability may be intentionally avoided to maintain the availability of the Evaluated organization's systems.
5. Any web application endpoints or functions explicitly listed as "Out of Scope" for the assessment will not be tested.

1.3 Project Team

Below are the TechD Cybersecurity Limited Auditing team members who played a key role in this engagement:

Name	Designation	Email-ID	Qualifications/Certifications	Listed in CERT-In Snapshot? (Yes/No)
Pavan Saxena	Team Lead - VAPT	pavan@techdefence.com	BCA OSCP+, OSWP, KLCP, ISO 27001:2022 LA, CEH v12, eJPT v2, CCSP-AWS, CAPEN, CNSP, AZ-900	Yes
Rushikesh Patil	Sr. Security Analyst	Rushikesh.patil@techdefence.com	CEH Master, ISO27001	No
Pruthvirajsinh Parmar	Security Analyst	pruthviraj@techdefence.com	B.Tech, CompTIA A+, CompTIA N+, CompTIA Security+, RHCSA, ISO 27001, eJPT, ICCA	Yes

1.4 Tools used during the assessment

Sr. No.	Name of Tool /Software used	Version of the tool /Software used	Open Source /Licensed
01	Burp Suite Professional	v10.12.0	Licensed

2. VAPT Methodology and Standards

2.1 Phases of the Assessment

- **Pre-engagement Phase:** This is the stage where the logistics and the rules of engagement of the test are discussed.
- **Reconnaissance/ Discovery Phase:** To simulate a cyber-attack on a Web Application, the penetration tester needs access to information about the target. They gather this information in the reconnaissance stage.
- **Vulnerability Analysis:** This phase consists of testing the Web Application for known vulnerabilities. Using an automated and manual approach for uncovering new and hidden vulnerabilities in the Web Application.
- **Exploitation and Post Exploitation:** The goal here is establishing access to a system using the loopholes uncovered in the earlier phases of penetration testing. The penetration tester tries to identify an entry point and then look for assets that can be accessed through that.
- **Reporting and Recommendations:** All the previous penetration testing phases contribute to this phase where a VAPT report is created and shared with the client.
- **Remediation and Rescan:** Once the vulnerabilities are fixed, we would carry out the round of rescans to identify any security loopholes that might have been left unattended.

2.2 Standards and Methodologies

- **OWASP Security Top 10:** is a list of the most critical security risks related to Web Application. It highlights common vulnerabilities that can lead to data breaches, unauthorized access, and other security incidents, helping organizations prioritize Web Application security measures.
- **SANS Institute's Top 25:** The SANS Top 25 is a list of the most critical software vulnerabilities, identified by the SANS Institute, which pose significant risks to applications and systems. It serves as a guide for developers and security professionals to prioritize and address common vulnerabilities to improve overall security posture.
- **Penetration Testing Execution Standard (PTES):** The Penetration Testing Execution Standard (PTES) provides a structured methodology for conducting comprehensive penetration testing. It includes seven essential phases—planning, information gathering, threat modelling, vulnerability analysis, exploitation, post-exploitation, and reporting—ensuring thorough coverage of vulnerabilities and helping organizations enhance their security posture through systematic testing and analysis.

2.3 Vulnerability Risk Rating Metrics and Remediation SLA

This section outlines the methodology used to assess and classify vulnerabilities based on the Common Vulnerability Scoring System (CVSS), along with the corresponding risk ratings. In addition, it defines the recommended remediation timelines for identified vulnerabilities based on their severity and potential business impact.

The Recommended Remediation Timelines provided in this report are suggested by TechD Cybersecurity Limited, based on industry best practices, risk exposure, and experience from similar engagements. These timelines are intended to assist the Evaluated organization in prioritizing remediation efforts effectively and reducing overall security risk.

Risk Exposure	CVSS Score	Remediation Timeline	Description
Critical	9.0 – 10.0	Within 7 Days	Immediate risk of severe impact on confidentiality, integrity, or availability.
High	7.0 – 8.9	Within 15 Days	High risk of system or data compromise requiring urgent remediation.
Medium	4.0 – 6.9	Within 30 Days	Moderate risk with potential for exploitation under certain conditions.
Low	0.1 – 3.9	Within 60 Days	Low risk with limited impact and specific exploitation requirements.
Informational	0	As per Business Priority	No direct risk; improvement recommendations for security posture.

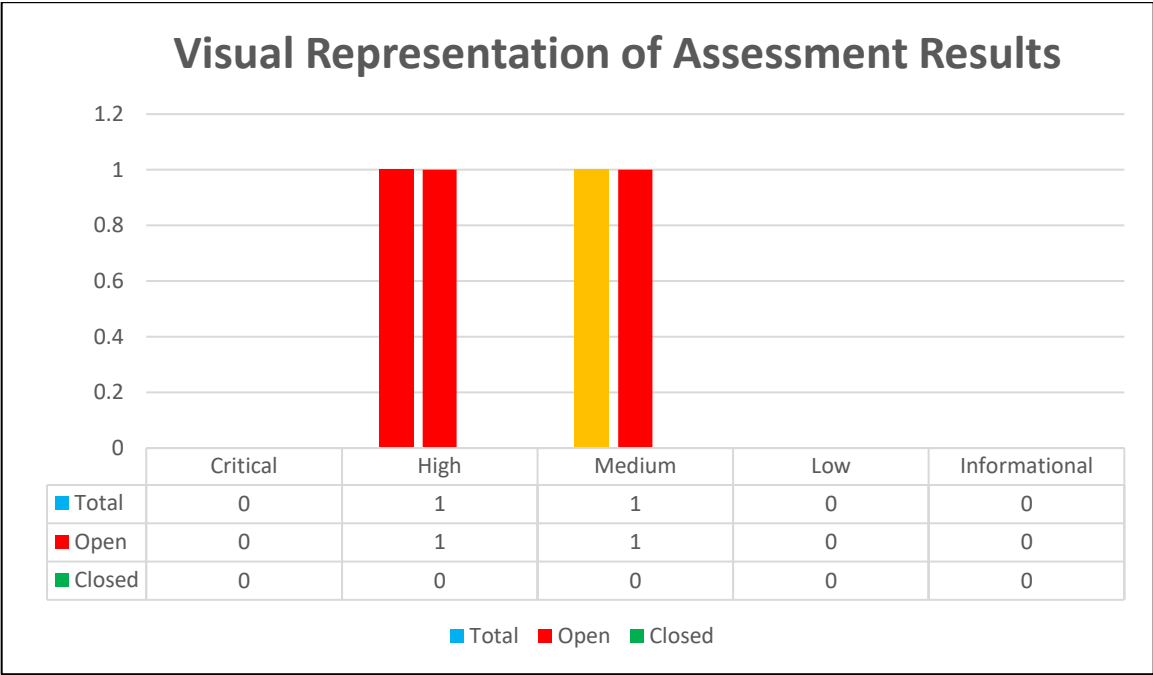
Risk Factors: Risk is assessed based on two primary factors: Likelihood and Impact.

- **Likelihood:** This factor measures the probability of a vulnerability being exploited. Ratings are determined by the attack difficulty, the availability of tools, the skill level of potential attackers, and the environment.
- **Impact:** This factor evaluates the potential consequences of a vulnerability on operations, including its effect on confidentiality, integrity, and availability of systems/data, as well as any reputational or financial damage.

3. Executive Summary

The following section provides an executive summary of the vulnerabilities identified during this security assessment.

3.1 Visual Representation of Assessment Results



3.2 Vulnerability Overview Table

The table below outlines the vulnerabilities discovered during the assessment, along with their associated risk severity. It provides an evaluation of both the potential impact and the likelihood of each vulnerability occurring.

ID	Vulnerable URL	Vulnerability Name	CVE/CWE	Severity	Status
TDL-001	https://rekyc.lkponline.com/v1/company/lkpsec/modification/login	OTP Bypass via Response Manipulation	CWE-287	High	Open
TDL-002	https://rekyc.lkponline.com/v1/user/Bank/page	Insufficient Session Expiration	CWE-613	Medium	Open

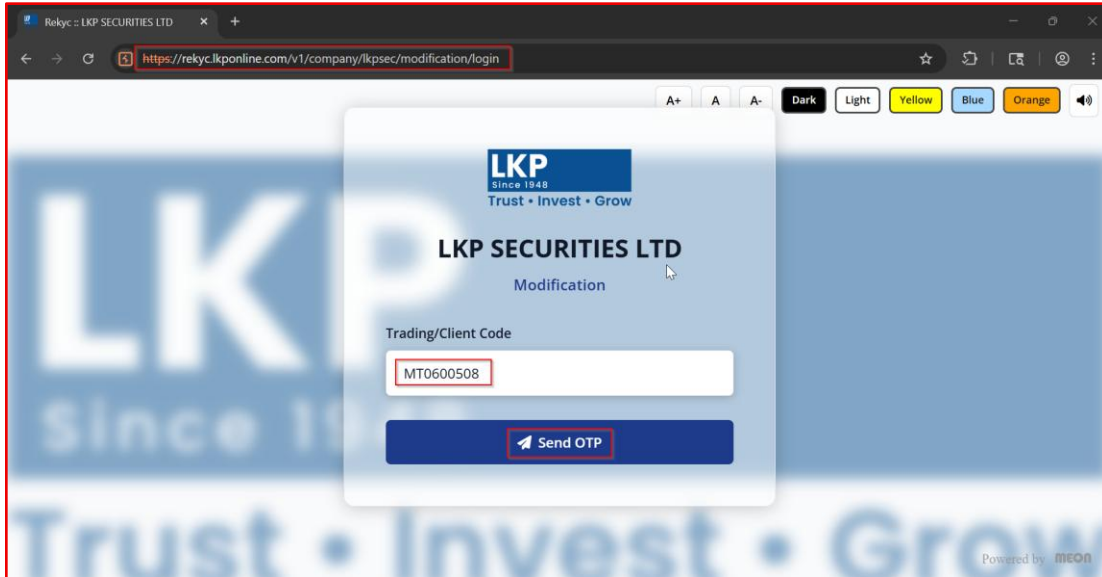
4. Detailed Vulnerability Observations

TDL-001 - OTP Bypass via Response Manipulation – {High} {Open}

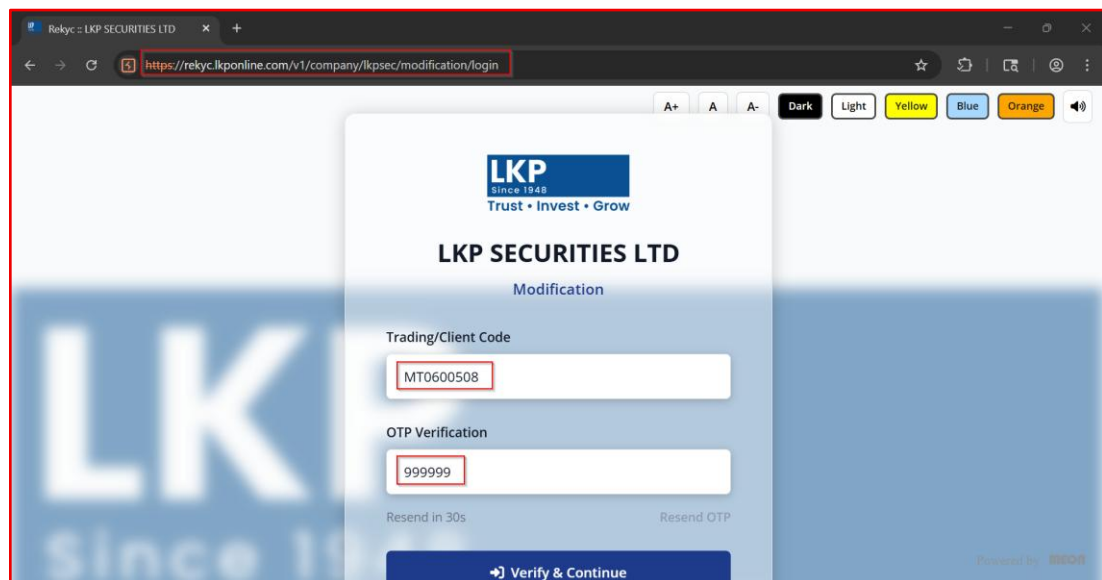
Vulnerable URLs	https://rekyc.lkponline.com/v1/company/lkpsec/modification/login
Vulnerable Parameter	{ "data": {}, "message": "invalid otp", "status": false }
Payload	{ "data": {}, "message": "valid otp", "status": true } (Manipulated Response)
OWASP Vulnerability Classification	A07:2021 – Identification and Authentication Failures
CVSS Score 3.1	High - 7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CWE-ID Mapping	CWE-287
Vulnerability Explanation:	The application validates OTP on the client side by trusting the server response intercepted via a proxy tool. An attacker can intercept the OTP verification response using Burp Suite and manipulate "status":false to "status":true and "message":"invalid otp" to "message":"valid otp", successfully bypassing OTP authentication without knowing the actual OTP.
Vulnerability Impact:	An attacker can bypass OTP authentication for any valid Trading/Client Code and gain unauthorized access to sensitive user accounts. This allows full account takeover, exposure of personal and financial data including PAN, CKYC, Bank details, and Date of Birth, and enables unauthorized modifications to KYC records of any user on the platform.
Remediation	OTP validation must be enforced strictly on the server side, never relying on client-side response values. The server should issue a session token only after successful OTP verification internally. Implement integrity checks so that tampering with responses does not affect authentication state. Rate-limit OTP attempts and invalidate OTPs after a single failed attempt.
Reference	https://cwe.mitre.org/data/definitions/287.html

Steps to Reproduce & Proof of Concept:

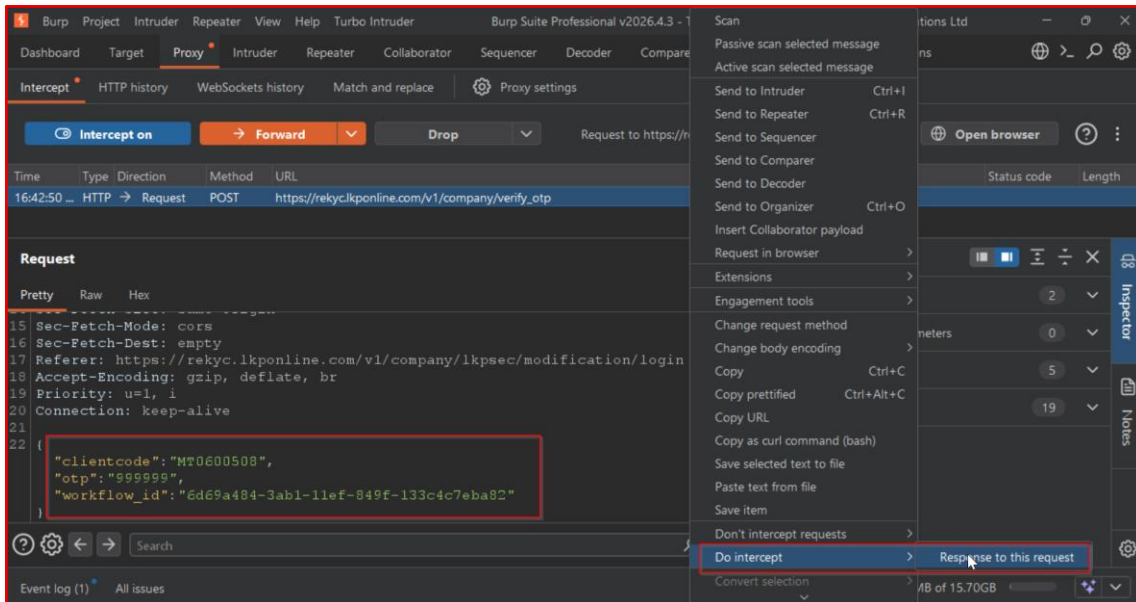
1. Navigate to <https://rekyc.lkponline.com/v1/company/lkpsec/modification/login>, enter a valid Trading/Client Code and click Send OTP.



2. Enter any random/incorrect OTP and click Verify & Continue.

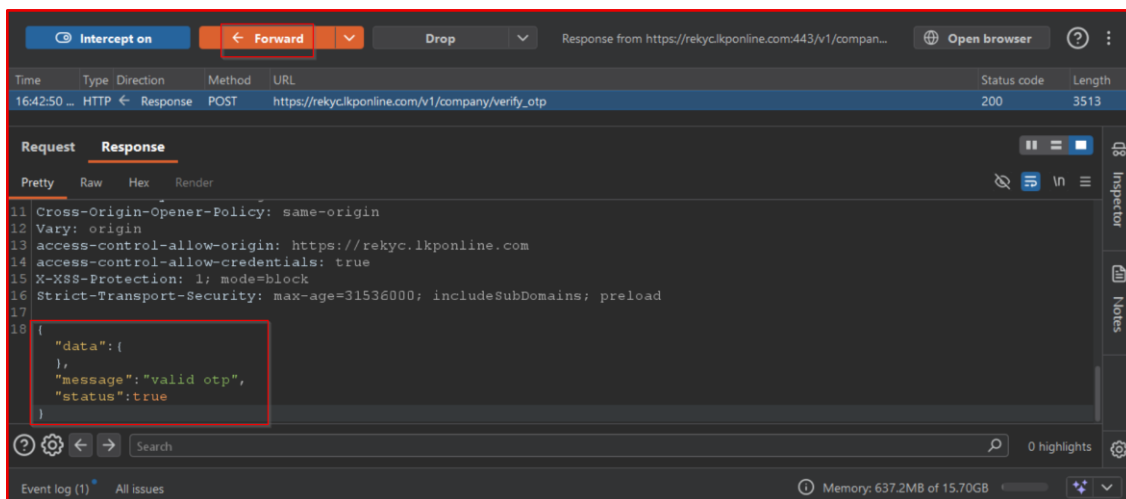


3. Intercept the request in Burp Suite — POST request goes to /v1/company/verify_otp.




4. Enable "Do Intercept → Response to this request" and forward the request.


5. In the intercepted response, change "status":false → "status":true and "message":"invalid otp" → "message":"valid otp", then forward — authentication is bypassed and account is accessed.





← → ↻ <https://rekyc.lkponline.com/v1/user/Personal/page> ☆ 📄 🗨️ 🌐


**LKP**
Since 1988
Trust • Invest • Grow


A+ A A- Dark Light Yellow Blue Orange 🔊 🔔 **LOGOUT**


 **Personal**

 Bank


 Segment

 Nominee

 Others




 Document

Account Details

Name 	Client ID	Account Status	PAN	CKYC No.
Hareshkumar S Darji	MT0600508	ACTIVE	ALAPD6986B	10012301677544

Personal Details

Updating e-mail and phone number will take up to 48 hours to reflect in your account post verification.

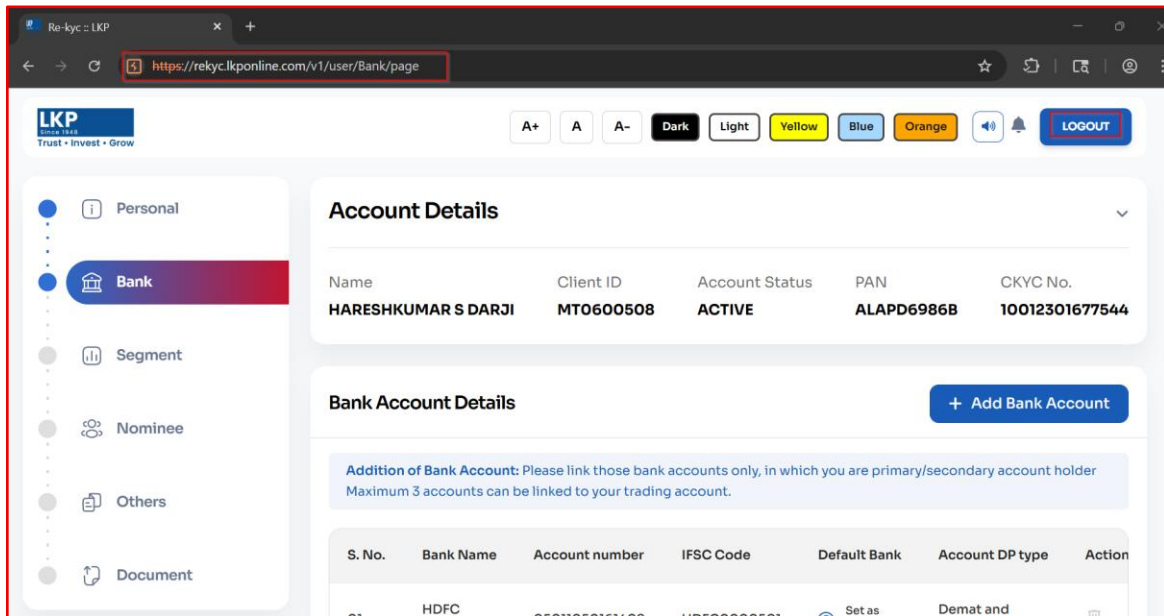
Father's Name / Spouse Name 	Mother's Name 	Date of Birth 
SURESHBHAI BABULAL DARJI	.	18-01-1984

TDL-002 - Insufficient Session Expiration – {Medium} {Open}

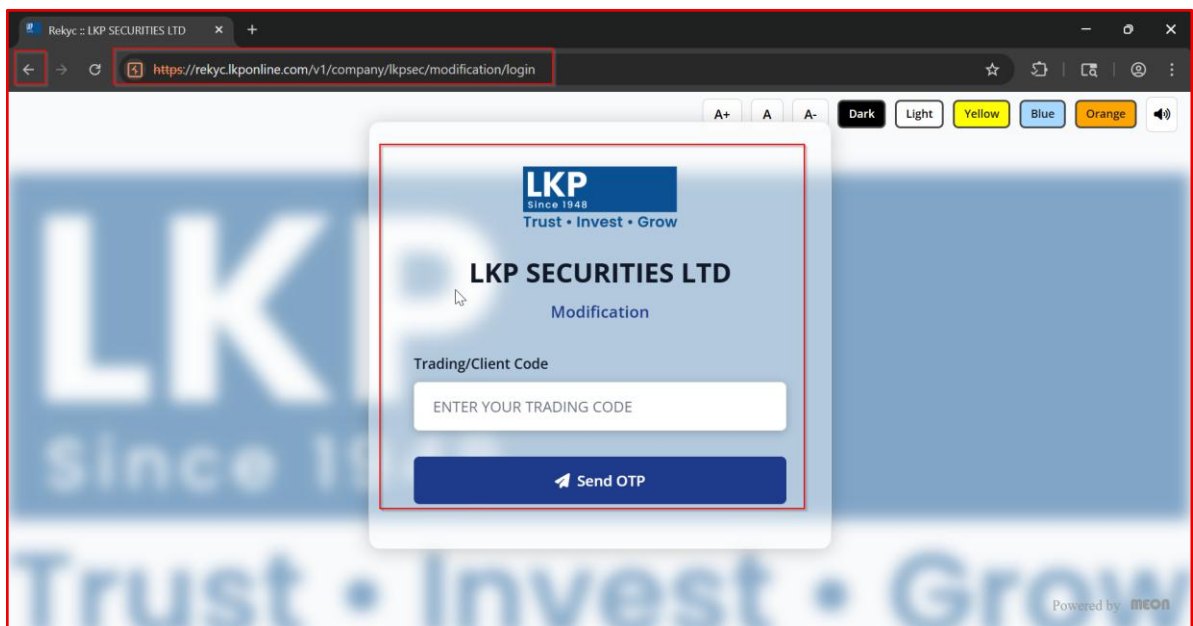
Vulnerable URLs	https://rekyc.lkponline.com/v1/user/Bank/page
Vulnerable Parameter	N/A
Payload	N/A
OWASP Vulnerability Classification	A07:2021 – Identification and Authentication Failures
CVSS Score 3.1	Medium - 4.3 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
CWE-ID Mapping	CWE-613
Vulnerability Explanation:	After a user logs out of the application, the browser caches previously visited authenticated pages. Due to insufficient session expiration and missing cache-control headers, pressing the browser's back button allows access to sensitive pages — such as Bank Details, Personal Details, and Segment Details — without re-authentication, exposing confidential user data.
Vulnerability Impact:	An attacker with physical or remote access to the browser can view sensitive financial and personal information including Name, PAN, CKYC Number, Bank Account details, and Brokerage/Segment data after logout. This poses serious risks of identity theft, financial fraud, and unauthorized account access, especially on shared or public devices.
Remediation	Implement proper cache-control headers (Cache-Control: no-store, no-cache, Pragma: no-cache) on all authenticated responses. Invalidate server-side session tokens immediately upon logout. Use client-side session checks to redirect unauthenticated users to the login page, preventing cached page access via browser back navigation.
Reference	https://cwe.mitre.org/data/definitions/613.html

Steps to Reproduce & Proof of Concept:

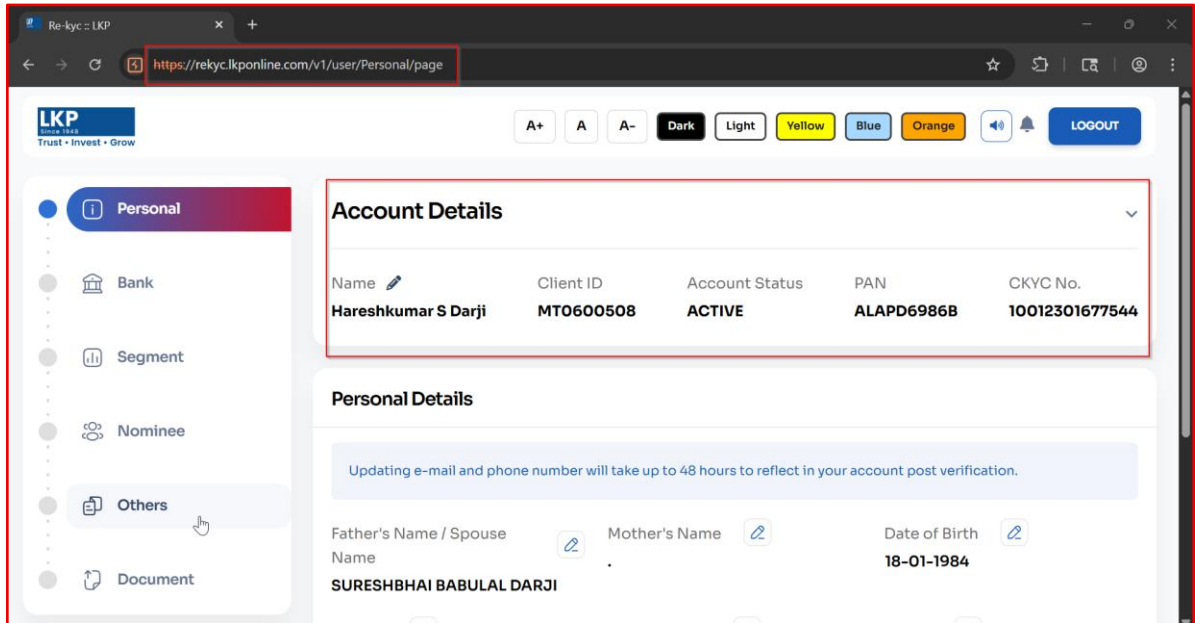
1. Login to <https://rekyc.lkponline.com> and navigate through pages like Bank, Personal, and Segment.



2. Click the Logout button to end the session.



3. After logout, press the browser's Back button.
4. Observe that sensitive authenticated pages (Bank, Personal, Segment details) are accessible without re-login.
5. Confirm PAN, CKYC, Bank Account, and other sensitive data is visible without any authentication.

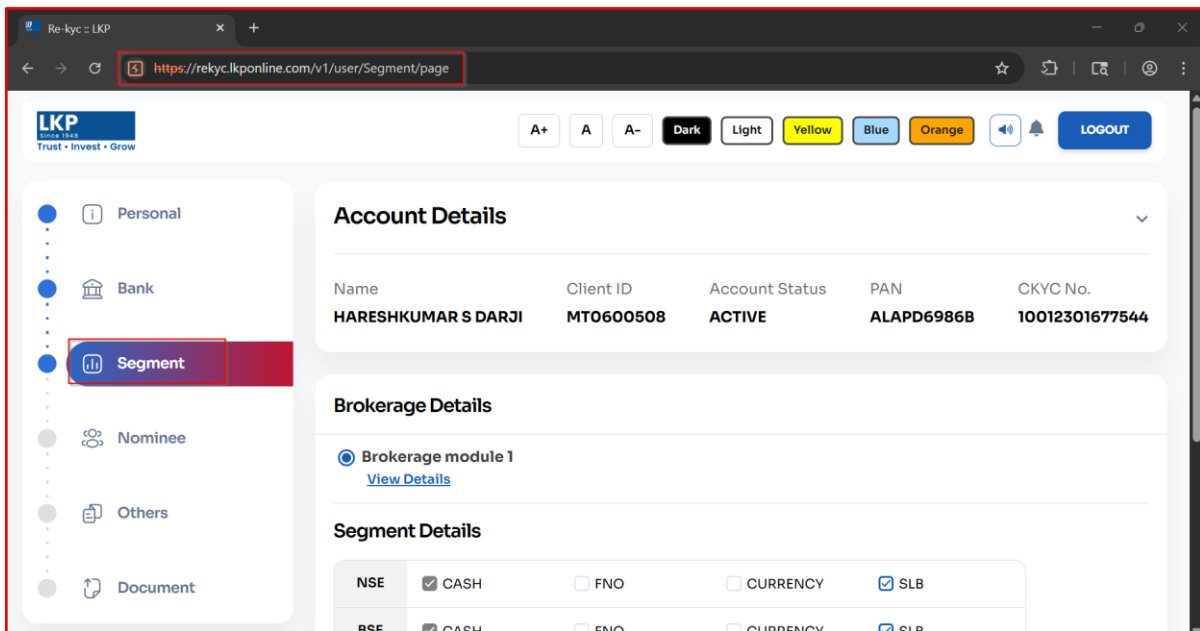


The screenshot shows the LKP Re-kyc LKP portal. The URL bar displays <https://rekyc.lkponline.com/v1/user/Personal/page>. The page features a sidebar with navigation options: Personal, Bank, Segment, Nominee, Others, and Document. The main content area is divided into two sections: Account Details and Personal Details. The Account Details section shows the following information:

Name	Client ID	Account Status	PAN	CKYC No.
Hareshkumar S Darji	MT0600508	ACTIVE	ALAPD6986B	10012301677544

The Personal Details section shows the following information:

Father's Name / Spouse Name	Mother's Name	Date of Birth
SURESHBHAI BABULAL DARJI		18-01-1984



The screenshot shows the LKP Re-kyc LKP portal. The URL bar displays <https://rekyc.lkponline.com/v1/user/Segment/page>. The page features a sidebar with navigation options: Personal, Bank, Segment, Nominee, Others, and Document. The main content area is divided into three sections: Account Details, Brokerage Details, and Segment Details. The Account Details section shows the following information:

Name	Client ID	Account Status	PAN	CKYC No.
HARESHKUMAR S DARJI	MT0600508	ACTIVE	ALAPD6986B	10012301677544

The Brokerage Details section shows the following information:

Brokerage module 1
View Details

The Segment Details section shows the following information:

NSE	CASH	FNO	CURRENCY	SLB
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Annexure A - Engagement Limitations

The security assessment was conducted within the scope and timeline agreed upon during the engagement with the Evaluated organization. Due to time limitations and operational constraints, it may not have been possible to identify every potential vulnerability present within the environment.

Testing activities were limited to the systems, endpoints, and functionalities that were made accessible by the Evaluated organization during the defined assessment period. The findings presented in this report represent the security posture of the evaluated systems at the time of testing and should not be interpreted as a guarantee that no additional vulnerabilities exist.

Annexure B - Retesting Statement

Upon completion of remediation activities by the Evaluated organization, a re-assessment may be conducted to verify whether the identified vulnerabilities have been successfully mitigated. The purpose of the re-assessment is limited to validating the remediation of the specific findings documented in this report.

The Evaluated organization is expected to address the identified vulnerabilities within a period of ninety (90) days from the date of report issuance, in accordance with the agreed remediation service level timelines. Re-assessment requests submitted within this period will be accommodated as part of the engagement to verify the implemented fixes.

Requests for re-assessment submitted after the ninety (90) day remediation window may be subject to a separate engagement or additional scope, as the validity and relevance of the original findings may change over time due to updates in the application environment.

Annexure C - Disclaimer and Precautions for Patch Implementation

Before implementing any remediation, actions based on this report, the following precautions should be observed:

- **Backup & Recovery:** Ensure complete backups of systems, applications, and data are taken prior to changes, along with a defined rollback plan to restore services in case of failure.
- **Controlled Testing:** Validate all fixes in a UAT or staging environment before deploying to production to avoid service disruption.
- **Third-Party References:** External links provided for remediation guidance are for reference only; their accuracy and availability are not guaranteed.
- **Assessment Limitations:** Findings are based on testing performed within the defined scope, timeline, and accessible environment. Certain vulnerabilities, especially those requiring intrusive testing, may not have been identified.
- **Point-in-Time Evaluation:** This report reflects the security posture at the time of assessment. New vulnerabilities may emerge due to system changes or evolving threats.
- **Ongoing Security Responsibility:** Security is a continuous process. The responsibility for implementing fixes and maintaining security controls rests with the Evaluated organization.

Annexure D - CERT-In Reporting and Remediation Compliance

As a CERT-IN empanelled organization, we have received communication stating that all CERT-IN empanelled organizations are required to submit audit-related data (including Cyber Audits, IS Audits, Regulatory audits, and VAPT audits) to CERT-IN starting from the fiscal year 2024. We will be sharing this VAPT Audit Reports or related details with CERT-IN. According to CERT-IN regulations, a period of 90 days is provided for the remediation/patching process from the release date of the audit reports. Therefore, we kindly request you to address all mentioned vulnerabilities within the 90-day timeframe and to inform us for the follow-up audit.