



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-04/26/0048
Report Version	v1.0
Web Application Name	ekyc.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 - Sensitive Information Disclosure – {High} {Open}	12
Annexure A - Engagement Limitations	14
Annexure B - Retesting Statement	14
Annexure C - Disclaimer and Precautions for Patch Implementation	15
Annexure D - CERT-In Reporting and Remediation Compliance	15

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	ekyc.lkponline
Web Application URL	https://ekyc.lkponline.com/lkpsec/individual_rm
Web Application Version	N/A
Assessment Approach	Grey Box
Testing Environment Configuration	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.

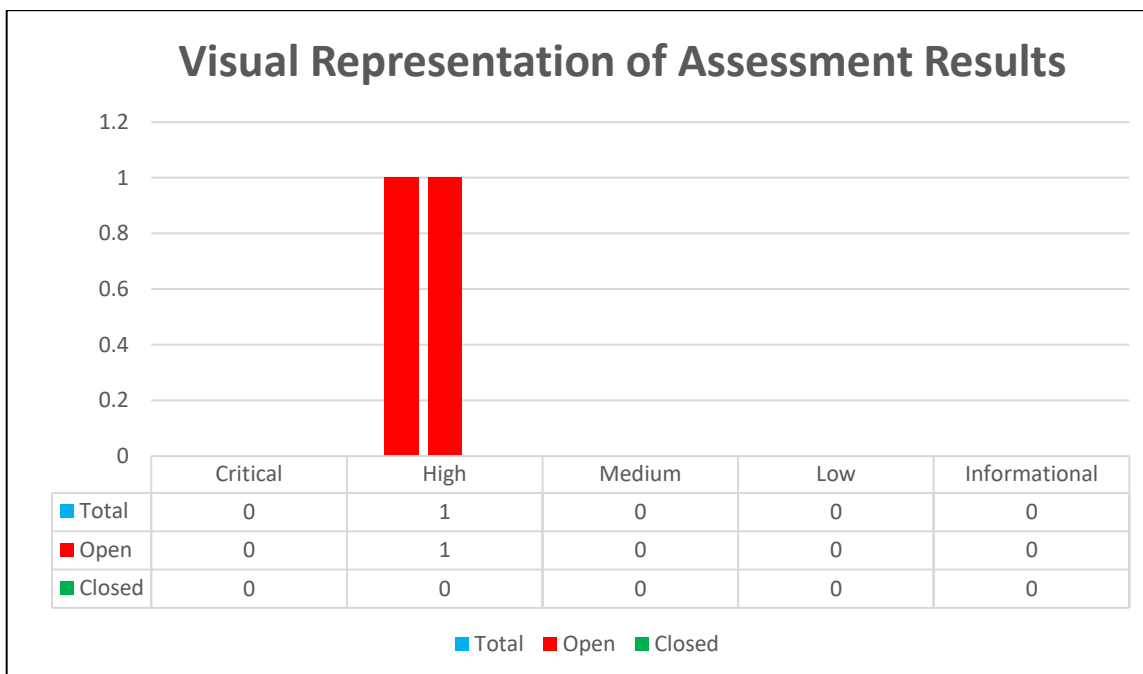
Risk Factors: Risk is assessed based on two primary factors: Likelihood and Impact.

- **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://ekyc.lkponline.com/lkpsec/individual_rm	Sensitive Information Disclosure	CWE-200	High	Open

4. Detailed Vulnerability Observations

TDL-001 - Sensitive Information Disclosure – {High} {Open}

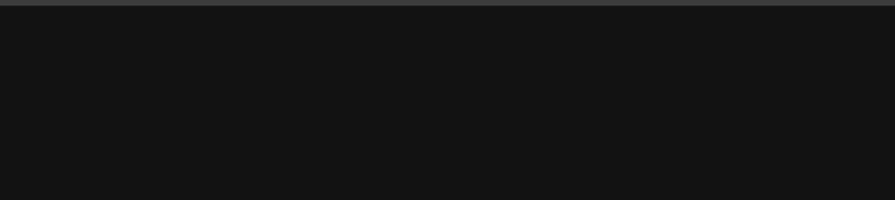
Vulnerable URLs	https://ekyc.lkponline.com/lkpsec/individual_rm
Vulnerable Parameter	N/A
Payload	N/A
OWASP Vulnerability Classification	A02:2021 – Cryptographic Failures
CVSS Score 3.1	7.5 - High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CWE-ID Mapping	CWE-200
Vulnerability Explanation:	The application exposes sensitive information such as access tokens, backend API endpoints, usernames, passwords, and database-related parameters within the client-side source code and URL query parameters. An attacker can simply inspect the page source or observe network requests to retrieve these details without authentication bypass. Exposing credentials and tokens in publicly accessible content significantly weakens application security and may allow unauthorized access to internal systems, APIs, or sensitive backend resources.
Vulnerability Impact:	Sensitive information disclosure can allow attackers to gain unauthorized access to backend systems, internal APIs, or protected resources. Exposed credentials and access tokens may be reused for privilege escalation, account compromise, API abuse, or further attacks against internal infrastructure. Disclosure of database names and backend endpoints also assists attackers during reconnaissance activities. Successful exploitation could result in data leakage, unauthorized transactions, service disruption, or complete compromise of connected systems and applications.
Remediation	Sensitive information such as access tokens, usernames, passwords, database identifiers, and internal API details should never be exposed in client-side source code or URL parameters. Store secrets securely on the server side and use secure session management mechanisms. Remove hardcoded credentials and implement token rotation with short expiration periods. Use environment variables or secret management solutions for sensitive configurations. Additionally, apply least-privilege access controls, disable verbose information exposure, and regularly review application responses for unintended data leakage.
Reference	https://cwe.mitre.org/data/definitions/200.html

1. Open the target URL in a web browser.
2. Right-click on the webpage and select “View Page Source”.
3. Search for sensitive keywords such as `access_token` or `UrlPassword`.
4. Observe exposed tokens, credentials, and backend API details in the source code.
5. Verify that the sensitive information is accessible without authentication.

```

156 </head>
157
158 <body>
159   <input type="hidden" id="titleHead" value="">
160   <input type="hidden" id="primary_color" value="#0a5193">
161   <input type="hidden" id="secondary_color" value="#0a5193">
162   <input type="hidden" id="tertiary_color" value="#0d28e">
163   <input type="hidden" id="quaternary_color" value="#ccee6f">
164   <input type="hidden" id="access_token" value=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJjb2MiZGFzaC6ImSc2UsImhhdChGtH4EjD0tE4MDIwOSwiZW5jaWkiOiJyZS2zM3MmQmQtN2E0M0YlODkxLWVhcnVhbnQCOEw%
165
166   <input type="hidden" id="workFlow_Key" value=9758871127>
167   <input type="hidden" id="workFlow_name" value=individual_rm>
168   <input type="hidden" id="token_revoke_time" value=60>
169
170   <input type="hidden" id="companyname" value=lkpsec>
171   <input type="hidden" value=image_path>
172   <input type="hidden" id="logo_path" value=static/backend/lkpsec/images/9758871127/logo.png>
173   <input type="hidden" value=under_Construction>
174   <input type="hidden" id="AllField" value={&#39;i&#39;; &#39;l&#39;; &#39;data&#39;; {&#39;label&#39;; &#39;mobile&#39;; &#39;moduleName&#39;; &#39;mobile&#39;;}, &#39;nam
175
176   <input type="hidden" id="Position" value=mobile>
177   <input type="hidden" value=>
178   <input type="hidden" data-step="1" value=1>
179   <input type="hidden" value=lkpsec-9758871127-69>
180   <input type="hidden" id="popUpValidation" value=False>
181   <input type="hidden" class="xyz" data-APIMethod="json" value=json>
182   <input type="hidden" id="secret_token_get" value="">
183   <input type="hidden" id="digilocker_company" value="">
184   <input type="hidden" id="digilocker_url" value="">
185   <input type="hidden" id="logoditch" value="159">
186   <input type="hidden" id="textloader" value=static/backend/lkpsec/images/9758871127/loader.gif>
187   <input type="hidden" id="logoHeight" value="90">
188   <input type="hidden" class="setLength" name="staticOtpField" InputLength="">
189   <input type="hidden" id="is_renderer_msg" value=False>
190   <input type="hidden" id="render_msg" value="">
191   <input type="hidden" id="saveFilesAPI" value="">
192   <input type="hidden" id="generated_data" value={}>

```



The screenshot shows a web browser window with the address bar displaying 'view-source:https://ekyc.lkponline.com/lkpsc/individual_rm'. The main content area is dark, and the source code is visible. A red box highlights a URL within the source code: 'https://backoffice.lkp.net.in:8080/techexcelapi/index.cfm/Searchpan/Searchpan1?&Ur1Username=TECHAPI&Ur1Password=TECH0123&Ur1Database=CAPSFO&Ur1DataYear=2025&...'.

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.