



# 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-04/26/0051
Report Version	v1.0
Web Application Name	pay.lkp.net.in
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 - Outdated Components – {Low} {Open} .....	12
TDL-002 - Directory Listing Enabled– {Low} {Open} .....	14
TDL-003 - Default IIS Page Exposure– {Low} {Open} .....	16
Annexure A - Engagement Limitations .....	18
Annexure B - Retesting Statement .....	18
Annexure C - Disclaimer and Precautions for Patch Implementation .....	19
Annexure D - CERT-In Reporting and Remediation Compliance .....	19



## 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	pay.lkp.net.in
Web Application URL	https://pay.lkp.net.in
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.

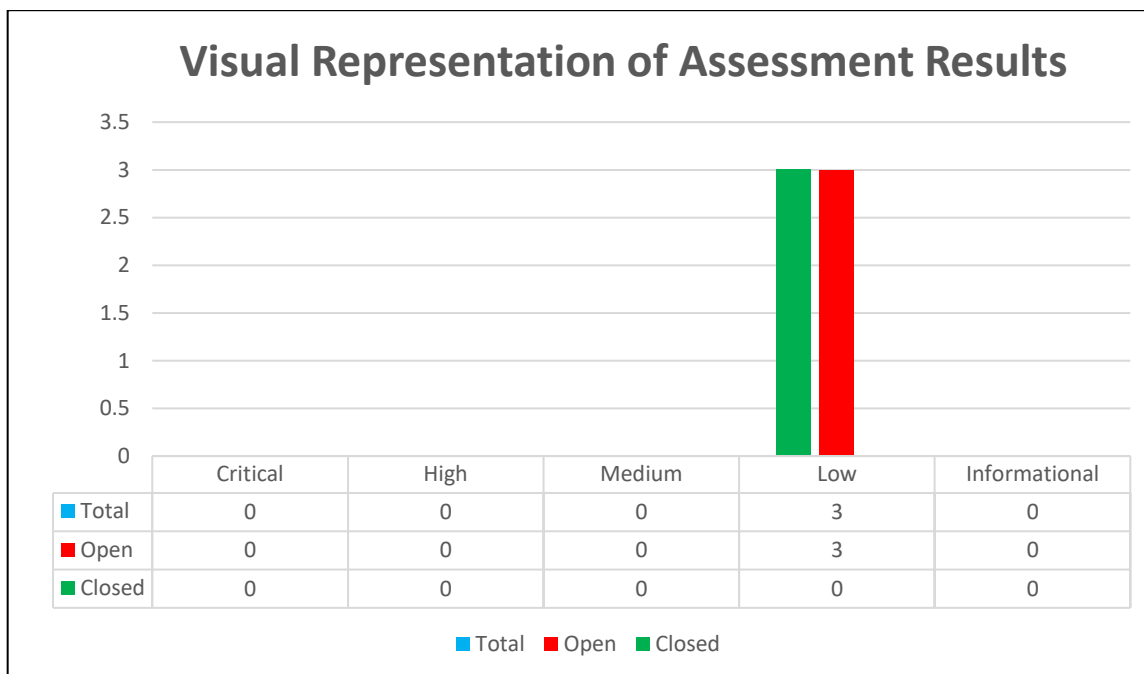
**Risk Factors:** Risk is assessed based on two primary factors: Likelihood and Impact.

- **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	<a href="https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js">https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js</a> <a href="https://maxcdn.bootstrapcdn.com/bootstrap/3.4.1/js/bootstrap.min.js">https://maxcdn.bootstrapcdn.com/bootstrap/3.4.1/js/bootstrap.min.js</a>	Outdated Components	<b>CWE-1104</b>	<b>Low</b>	<b>Open</b>
TDL-002	<a href="https://pay.lkp.net.in/FundTransfer/img/">https://pay.lkp.net.in/FundTransfer/img/</a>	Directory Listing Enabled	<b>CWE-548</b>	<b>low</b>	<b>Open</b>
TDL-003	<a href="https://pay.lkp.net.in">https://pay.lkp.net.in</a>	Default IIS Page Exposure	<b>CWE-756</b>	<b>Low</b>	<b>Open</b>

## 4. Detailed Vulnerability Observations

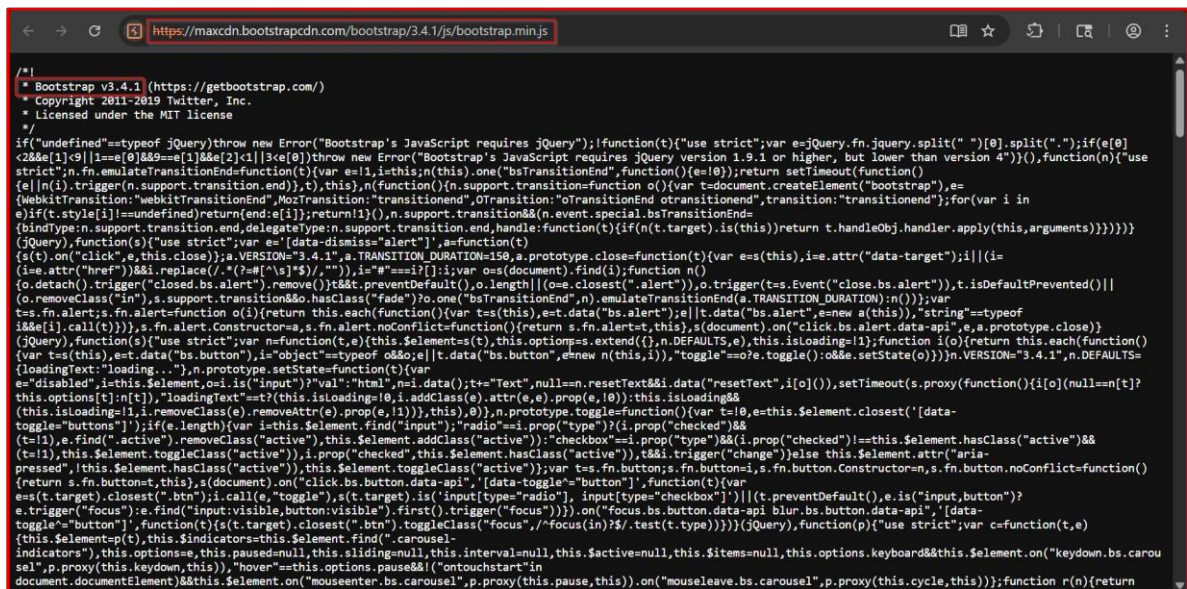
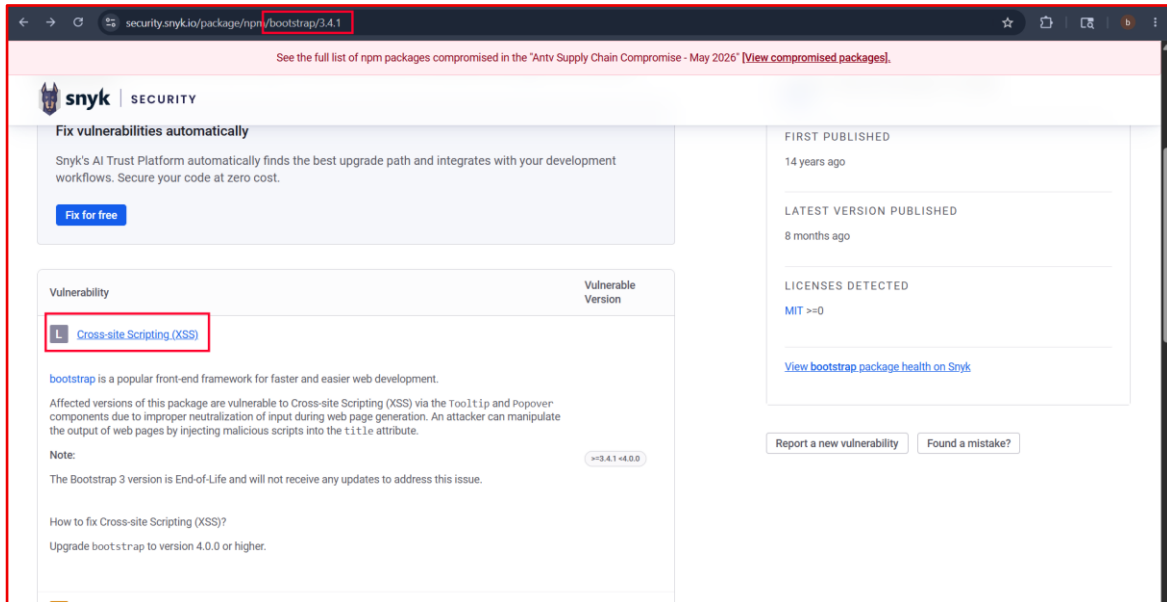
### TDL-001 - Outdated Components – {Low} {Open}


<b>Vulnerable URLs</b>	<a href="https://maxcdn.bootstrapcdn.com/bootstrap/3.4.1/js/bootstrap.min.js">https://maxcdn.bootstrapcdn.com/bootstrap/3.4.1/js/bootstrap.min.js</a>
<b>Vulnerable Parameter</b>	N/A
<b>Payload</b>	N/A
<b>OWASP Vulnerability Classification</b>	A06:2021 – Vulnerable and Outdated Components
<b>CVSS Score 3.1</b>	Security Misconfiguration
<b>CWE-ID Mapping</b>	CWE-1035
<b>Vulnerability Explanation:</b>	The application loads Bootstrap v3.4.1, which are outdated and contain publicly disclosed vulnerabilities. Bootstrap 3.4.1 has known XSS vulnerabilities in its tooltip and popover components. Using these versions exposes the application to client-side attacks.
<b>Vulnerability Impact:</b>	Attackers can exploit known flaws in these outdated libraries to execute Cross-Site Scripting (XSS) attacks, potentially stealing session cookies, performing unauthorized actions, redirecting users to malicious sites, or defacing web content. Since CVEs are publicly documented, exploitation is straightforward for any attacker with basic knowledge.
<b>Remediation</b>	Upgrade Bootstrap to version 5.x or the latest patched 4.x release. Implement a Software Composition Analysis (SCA) tool such as Snyk or OWASP Dependency-Check in the CI/CD pipeline to automatically detect and flag vulnerable third-party components before deployment.
<b>Reference</b>	<a href="https://cwe.mitre.org/data/definitions/1104.html">https://cwe.mitre.org/data/definitions/1104.html</a> <a href="https://owasp.org/Top10/2021/A06_2021-Vulnerable_and_Outdated_Components/index.html">https://owasp.org/Top10/2021/A06_2021-Vulnerable_and_Outdated_Components/index.html</a>



## Steps to Reproduce & Proof of Concept:

1. Open the target web application and launch Developer Tools (F12) → Network tab.
2. Identify and navigate to the loaded JavaScript library URLs:  
<https://maxcdn.bootstrapcdn.com/bootstrap/3.4.1/js/bootstrap.min.js>
3. Confirm outdated versions from file headers — Bootstrap v3.4.1.
4. Cross-reference confirmed versions against known CVEs on NVD or Snypk.
5. Validated vulnerabilities confirm the application is using components with publicly known exploits.

Vulnerability	Vulnerable Version
 Cross-site Scripting (XSS)	3.4.1 to 4.0.0

**bootstrap** is a popular front-end framework for faster and easier web development.

Affected versions of this package are vulnerable to Cross-site Scripting (XSS) via the Tooltip and Popover components due to improper neutralization of input during web page generation. An attacker can manipulate the output of web pages by injecting malicious scripts into the title attribute.

**Note:**  
The Bootstrap 3 version is End-of-Life and will not receive any updates to address this issue.

**How to fix Cross-site Scripting (XSS)?**  
Upgrade bootstrap to version 4.0.0 or higher.

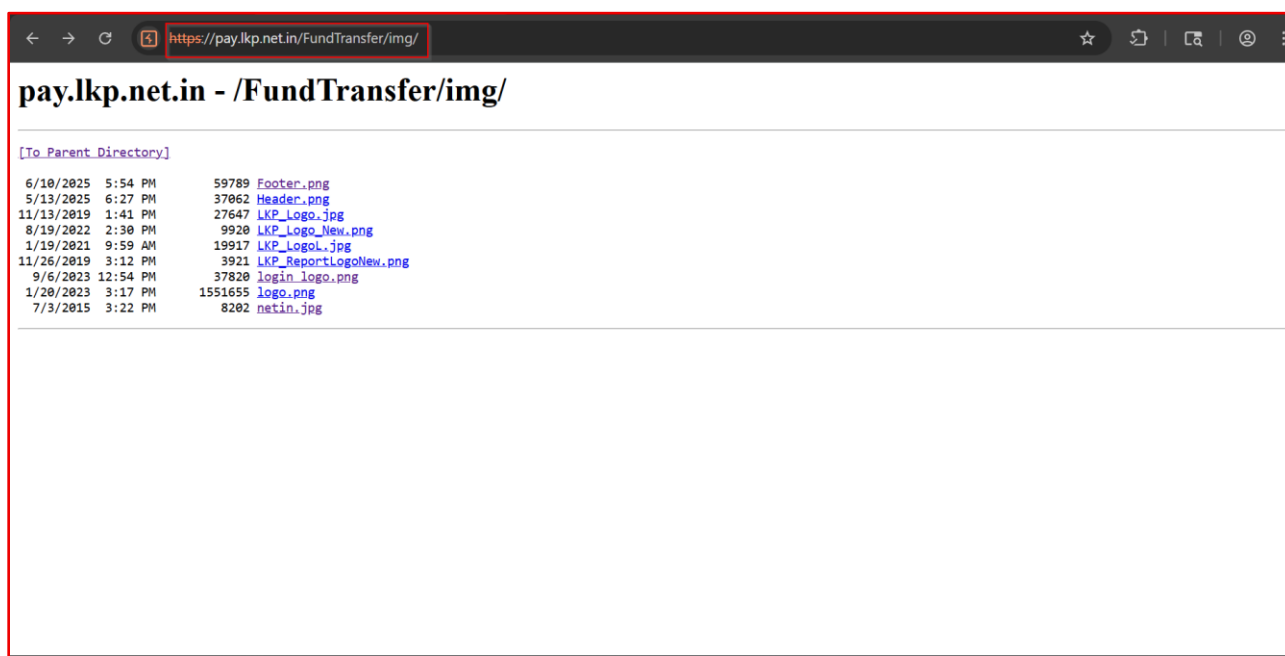


## TDL-002 - Directory Listing Enabled– {Low} {Open}

<b>Vulnerable URLs</b>	<a href="https://pay.lkp.net.in/FundTransfer/img/">https://pay.lkp.net.in/FundTransfer/img/</a>
<b>Vulnerable Parameter</b>	N/A
<b>Payload</b>	N/A
<b>OWASP Vulnerability Classification</b>	A05:2021 – Security Misconfiguration
<b>CVSS Score 3.1</b>	<b>Security Misconfiguration</b>
<b>CWE-ID Mapping</b>	<b>CWE-548</b>
<b>Vulnerability Explanation:</b>	The web server is configured with directory browsing enabled, allowing users to directly access and enumerate files stored within the /FundTransfer/img/ directory. An attacker can view internal resources, image files, filenames, timestamps, and directory structure information without authentication. Such exposure may assist attackers in reconnaissance activities and provide valuable information about the application's internal structure, resources, and naming conventions.
<b>Vulnerability Impact:</b>	Directory listing exposure allows attackers to enumerate accessible files and folders hosted on the server. This may reveal sensitive resources, backup files, hidden application components, or internal naming structures that can assist in further attacks. Attackers can use the disclosed information to identify vulnerable components, gather reconnaissance data, or discover unintentionally exposed files that could lead to unauthorized access or additional information disclosure.
<b>Remediation</b>	Disable directory browsing on the web server to prevent unauthorized users from listing directory contents. Configure proper access controls for sensitive directories and restrict public access wherever unnecessary. Remove unused or sensitive files from publicly accessible locations. Regularly audit exposed directories and server configurations to ensure only intended resources are accessible to external users.
<b>Reference</b>	<a href="https://cwe.mitre.org/data/definitions/548.html">https://cwe.mitre.org/data/definitions/548.html</a>

## Steps to Reproduce & Proof of Concept:

1. Open the target URL in a web browser.
2. Navigate to /FundTransfer/img/.
3. Observe that directory contents are publicly accessible.
4. View listed files, timestamps, and resources.
5. Verify that authentication is not required.

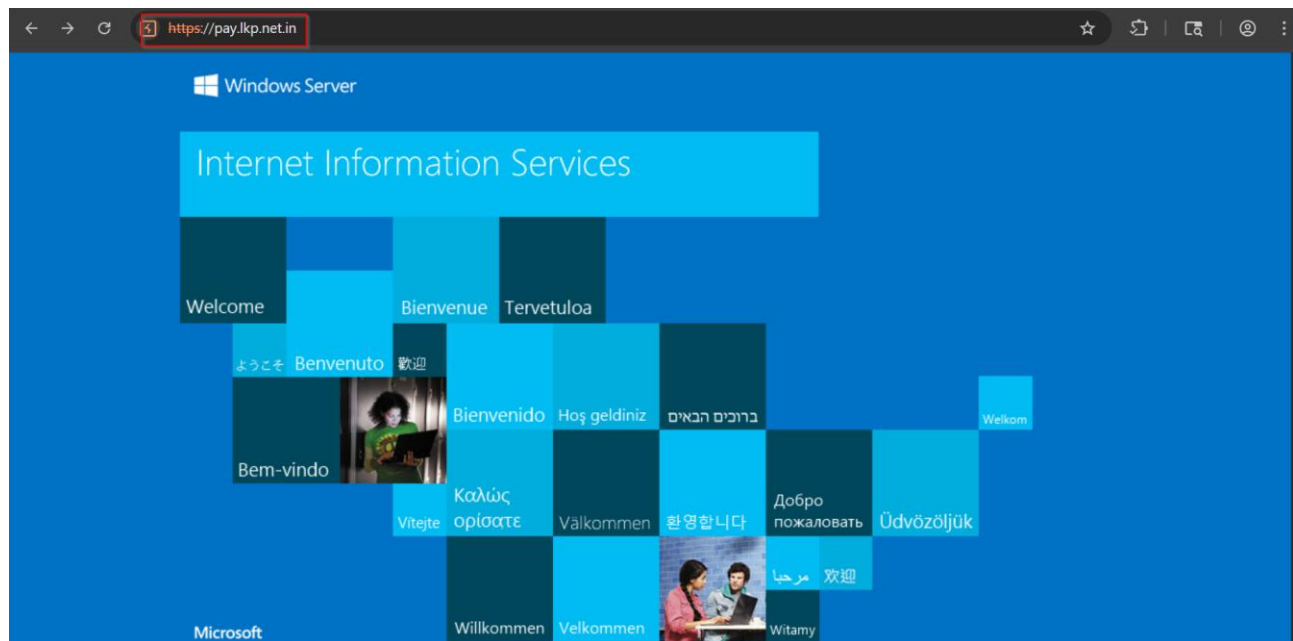


### TDL-003 - Default IIS Page Exposure– {Low} {Open}

<b>Vulnerable URLs</b>	<a href="https://pay.lkp.net.in/FundTransfer/img/">https://pay.lkp.net.in/FundTransfer/img/</a>
<b>Vulnerable Parameter</b>	N/A
<b>Payload</b>	N/A
<b>OWASP Vulnerability Classification</b>	A05:2021 – Security Misconfiguration
<b>CVSS Score 3.1</b>	<b>Security Misconfiguration</b>
<b>CWE-ID Mapping</b>	<b>CWE-200</b>
<b>Vulnerability Explanation:</b>	The application server exposes the default Microsoft IIS welcome page instead of a properly configured production landing page. This disclosure reveals the underlying web server technology being used by the application infrastructure. Exposure of default server pages indicates incomplete server hardening and may provide attackers with useful reconnaissance information regarding the hosting environment, server configuration, and deployed technologies.
<b>Vulnerability Impact:</b>	Exposed default server pages assist attackers in fingerprinting the underlying infrastructure and identifying the web server technology in use. Such information can be leveraged to target server-specific vulnerabilities, known exploits, or misconfigurations. Although the issue alone may not directly compromise the application, it increases the overall attack surface and supports further reconnaissance and targeted exploitation attempts against the environment.
<b>Remediation</b>	Remove default IIS pages from the production environment and configure a custom application landing page or error page. Harden the web server configuration to minimize technology disclosure and disable unnecessary default content. Regularly review publicly accessible pages and server responses to ensure no default configurations or unnecessary information are exposed to external users.
<b>Reference</b>	<a href="https://cwe.mitre.org/data/definitions/756.html">https://cwe.mitre.org/data/definitions/756.html</a>

### Steps to Reproduce & Proof of Concept:

1. Open the target domain in a web browser.
2. Access <https://pay.lkp.net.in>.
3. Observe the default Microsoft IIS welcome page.
4. Verify that the application landing page is not configured.
5. Confirm server technology disclosure through the default page.



## **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.