



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-04/26/0047
Report Version	v1.0
Web Application Name	Trading.lkpsec
Assessment Approach	Grey Box Web Application Security Assessment
Type of Audit Report	First Audit Report
Primary Assessment Period	04 May 2026 to 06 May 2026
Re-Assessment Period	Follow Up Audit Pending
Report Prepared by	Vivek Pawar
Reviewed by	Rushikesh Patil
Approved by	Rohit Soni
Released by	Pavan Saxena
Date of Release	06 May 2026

Document Change History		
Version	Date	Remarks / Reason of Change
v1.0	06 May 2026	First Audit Report

Document Distribution List			
Name	Organization	Role	Email Id
Dhruv Chauhan	TechDefence Labs	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 - Directory listing – {High} {Open}	12
TDL-002 - Missing Security Headers – {Low} {Open}.....	16
TDL-003 - Server name and Version – {Informational} {Open}	18
Annexure A - Engagement Limitations	20
Annexure B - Retesting Statement	20
Annexure C - Disclaimer and Precautions for Patch Implementation	21
Annexure D - CERT-In Reporting and Remediation Compliance.....	21

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	Trading.lkpsec
Web Application URL	https://trading.lkpsec.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 (ISC)2 - CC, AZ-900, CEHv12, eJPT-v2, CAP, CNSP, CAPen, KLCP, ISO-27001: Lead Auditor	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	v2025.10.2	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.

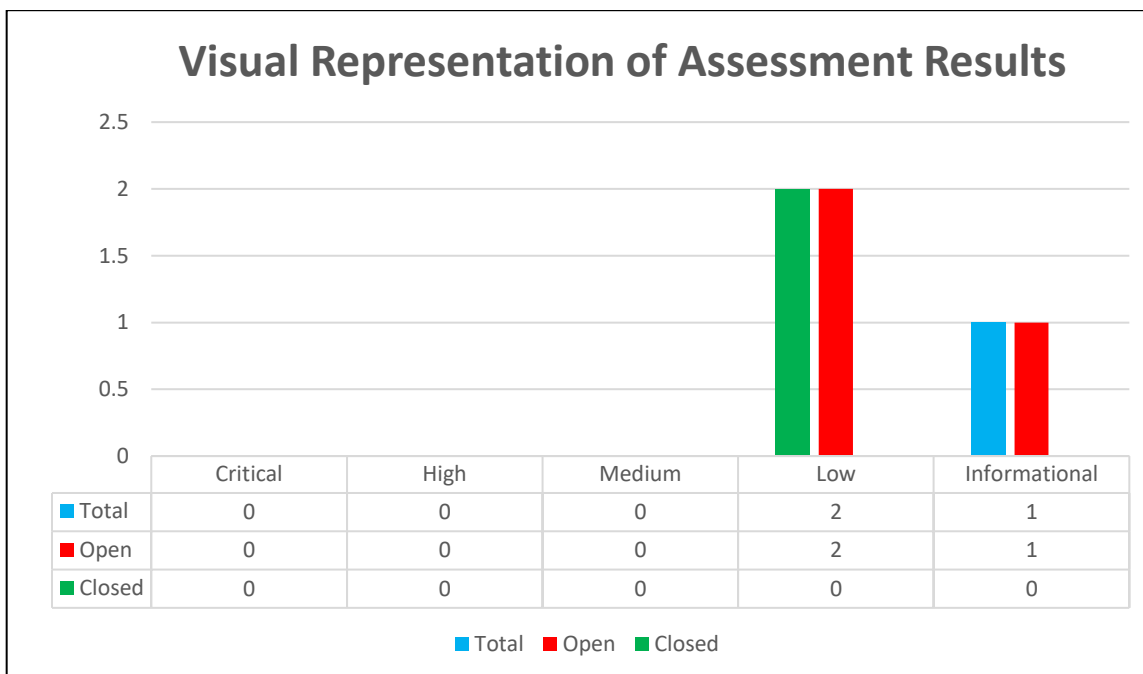
Risk Factors: Risk is assessed based on two primary factors: Likelihood and Impact.

- **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://trading.lkpsec.in/ftp/ https://trading.lkpsec.in/autoupd ate/ https://trading.lkpsec.in/ftp/APIL ogs_27-10-2025.txt	Directory listing	CWE-548	High	Open
TDL-002	https://trading.lkpsec.in/	Missing Security Headers	CWE-693	Low	Open
TDL-003	https://trading.lkpsec.in/	Server name and Version	CWE-200	Informational	Open

4. Detailed Vulnerability Observations

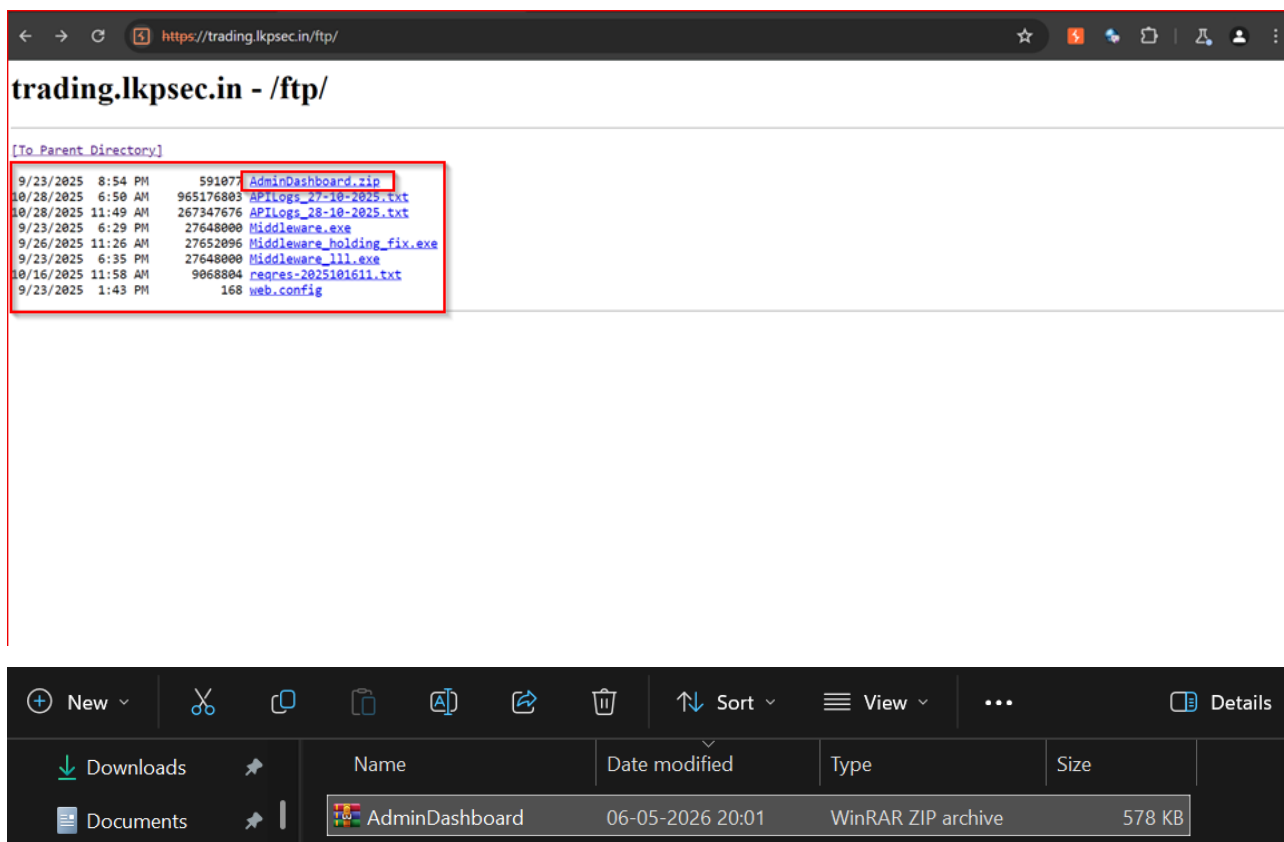
TDL-001 - Directory listing – {High} {Open}

Vulnerable URLs	https://trading.lkpsec.in/ftp/ https://trading.lkpsec.in/autoupdate/ https://trading.lkpsec.in/ftp/APILogs_27-10-2025.txt
Vulnerable Parameter	N/A
Payload	N/A
OWASP Vulnerability Classification	A05:2021-Security Misconfiguration
CVSS Score 3.1	Security Misconfiguration
CWE-ID Mapping	CWE-548
Vulnerability Explanation:	The application server is configured with directory listing enabled, allowing unauthenticated users to browse internal directories and access sensitive files directly through the browser. Exposed directories contain application logs, ZIP archives, executable files, configuration files, and update-related resources. Additionally, accessible log files disclose internal application activity and user-related information. This issue occurs due to insecure web server configuration and lack of proper access restrictions on sensitive directories hosted under the web root.
Vulnerability Impact:	Attackers can enumerate internal files and download sensitive resources without authentication. Exposed content such as API logs, executables, backup archives, and configuration files may reveal application structure, operational details, usernames, device identifiers, and internal business logic. Such information can facilitate targeted attacks, credential enumeration, phishing campaigns, reverse engineering, or exploitation of additional vulnerabilities. Public exposure of executable and configuration files may also increase the likelihood of unauthorized access and compromise of backend systems.
Remediation	Disable directory browsing/indexing on the web server immediately to prevent unauthorized file enumeration. Restrict access to sensitive directories such as /ftp/ and /autoupdate/ using proper authentication and authorization controls. Remove unnecessary files including logs, executables, archives, and configuration files from publicly accessible locations. Store sensitive resources outside the web root wherever

	possible. Additionally, implement strict access-control policies on IIS and perform periodic audits to identify and remove exposed internal files.
Reference	https://cwe.mitre.org/data/definitions/552.html

Steps to Reproduce & Proof of Concept:

1. Access the target URL.
2. Verify that directory listing/indexing is enabled.
3. Observe that publicly accessible files and directories can be browsed.



The screenshot shows a web browser at the URL <https://trading.lkpsec.in/ftp/>. The page displays a directory listing for the /ftp/ directory. The listing includes a link to the parent directory and a list of files and directories. The file **AdminDashboard.zip** is highlighted with a red box. Below the screenshot, a Windows File Explorer window shows the downloaded file **AdminDashboard** with the following details:

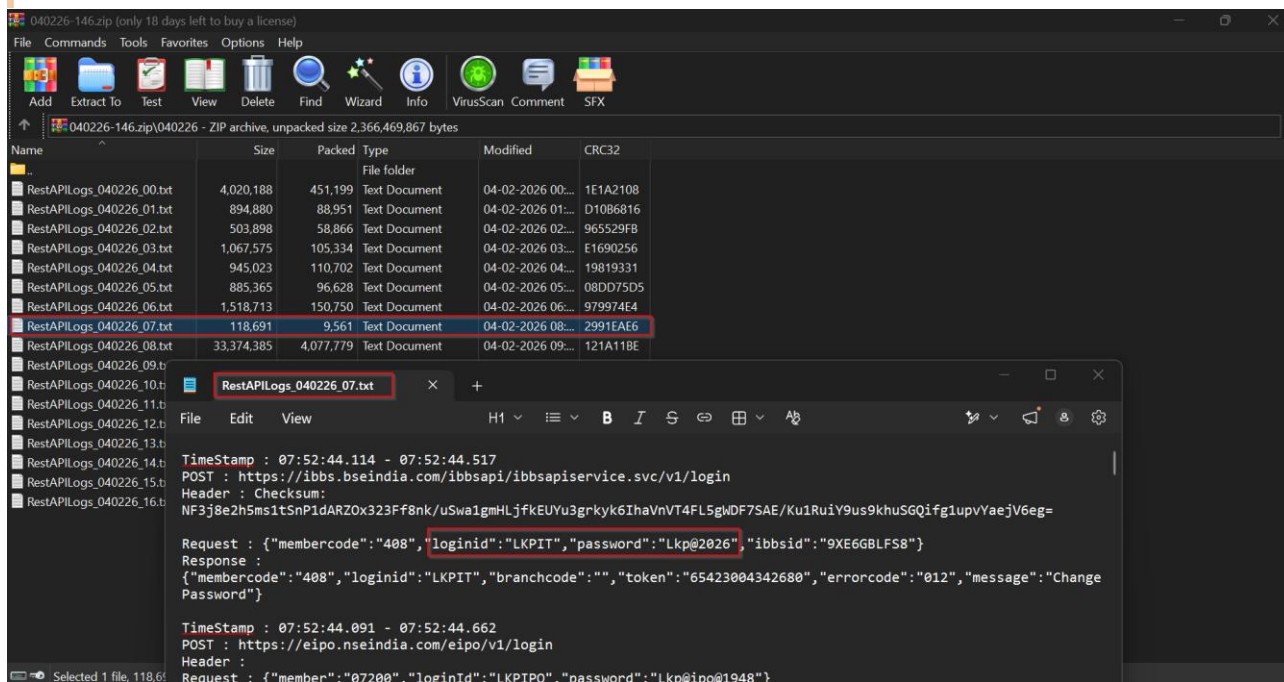
Name	Date modified	Type	Size
AdminDashboard	06-05-2026 20:01	WinRAR ZIP archive	578 KB

← → ↻ 🔒 https://trading.lkpsec.in/ftp/

trading.lkpsec.in - /ftp/

[\[To Parent Directory\]](#)

2/4/2026	4:30 PM	246076679	040226-148.zip
9/23/2025	7:31 PM	698371	23-09-2025.txt
10/28/2025	6:50 AM	1312055175	APILogs_27-10-2025.txt
10/28/2025	11:33 AM	302675703	APILogs_28-10-2025 - Copy.txt
10/16/2025	11:58 AM	9068804	regres-2025101611.txt
9/23/2025	7:42 PM	168	web.config



040226-148.zip (only 18 days left to buy a license)

File Commands Tools Favorites Options Help

Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX

040226-148.zip(040226 - ZIP archive, unpacked size 2,366,469,867 bytes)

Name	Size	Packed	Type	Modified	CRC32
RestAPILogs_040226_00.txt	4,020,188	451,199	Text Document	04-02-2026 00:...	1E1A2108
RestAPILogs_040226_01.txt	894,880	88,951	Text Document	04-02-2026 01:...	D10B6816
RestAPILogs_040226_02.txt	503,898	58,866	Text Document	04-02-2026 02:...	965529F8
RestAPILogs_040226_03.txt	1,067,575	105,334	Text Document	04-02-2026 03:...	E1690256
RestAPILogs_040226_04.txt	945,023	110,702	Text Document	04-02-2026 04:...	19819331
RestAPILogs_040226_05.txt	885,365	96,628	Text Document	04-02-2026 05:...	08DD75D5
RestAPILogs_040226_06.txt	1,518,713	150,750	Text Document	04-02-2026 06:...	979974E4
RestAPILogs_040226_07.txt	118,691	9,561	Text Document	04-02-2026 08:...	2991EAE6
RestAPILogs_040226_08.txt	33,374,385	4,077,779	Text Document	04-02-2026 09:...	121A11BE
RestAPILogs_040226_09.txt					
RestAPILogs_040226_10.txt					
RestAPILogs_040226_11.txt					
RestAPILogs_040226_12.txt					
RestAPILogs_040226_13.txt					
RestAPILogs_040226_14.txt					
RestAPILogs_040226_15.txt					
RestAPILogs_040226_16.txt					

RestAPILogs_040226_07.txt

File Edit View H1 B I S A

TimeStamp : 07:52:44.114 - 07:52:44.517
 POST : https://ibbs.bseindia.com/ibbsapi/ibbsapiservice.svc/v1/login
 Header : Checksum:
 NF3j8e2h5ms1tSnP1dARZ0x323Ff8nk/uSwa1gmHLjfkEUy3grkyk6IhaVnVT4FL5gwDF7SAE/Ku1RuiY9us9khuSGQifg1upvYaejV6eg=
 Request : {"membercode":"408","loginid":"LKPIIT","password":"Lkp@2026","ibbsid":"9XE6GBLFS8"}
 Response : {"membercode":"408","loginid":"LKPIIT","branchcode":"","token":"65423084342680","errorcode":"012","message":"Change Password"}
 TimeStamp : 07:52:44.091 - 07:52:44.662
 POST : https://eipo.nseindia.com/eipo/v1/login
 Header :
 Request : {"member":"07208","loginId":"LKPIPO","password":"Lkp@ipo@1948"}
 Selected 1 file, 118,691 bytes

```
← → ↻ https://trading.lkpsec.in/ftp/APILogs\_27-10-2025.txt ☆ ⚙ 📄 🗑 📌 👤 ⋮
```

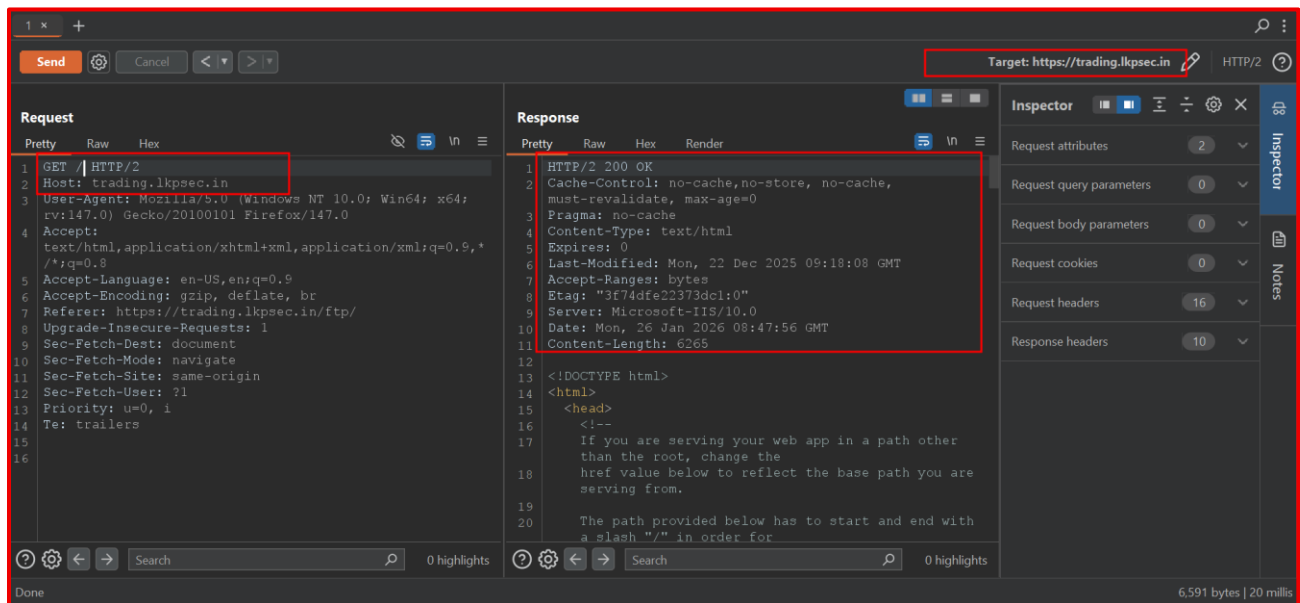
```
mpinlogin>42.108.77.113>>23170010>>>07:34:02>07:34:03>1425.482 sec>{"logindevice":"Android","deviceid":"GSG_a312cc3ce669c600","userid":"23170010","code":"85067c60-397d-4cf7-9ea5-82f18f81c928","source":"MOB","ApkVersion":"","mPin":"","clientCategory":"GSG"}>Accept-Encoding: gzip,Host: trading.lkpsec.in,User-Agent: Dart/3.9 (dart:io),>{"status":false,"message":"Not_Ok","errorCode":"400","msg":"Login Unsuccessful.Please try again after sometime.","data":null}>biometriclogin>219.91.178.15>>14001499>>>07:34:11>07:34:11>950.990 sec>{"logindevice":"Android","deviceid":"GSG_f1e7c436c714f6ea","userid":"14001499","code":"616a6715-001a-4fb4-b575-e11931df82e2","source":"MOB","ApkVersion":"","mPin":"","clientCategory":"GSG"}>Accept-Encoding: gzip,Host: trading.lkpsec.in,User-Agent: Dart/3.9 (dart:io),>{"status":false,"message":"Not_Ok","errorCode":"400","msg":"Login Unsuccessful.Please try again after sometime.","data":null}>mpinlogin>219.91.178.15>>14001499>>>07:34:21>07:34:21>940.573 sec>{"logindevice":"Android","deviceid":"GSG_f1e7c436c714f6ea","userid":"14001499","code":"616a6715-001a-4fb4-b575-e11931df82e2","source":"MOB","ApkVersion":"","mPin":"","clientCategory":"GSG"}>Accept-Encoding: gzip,Host: trading.lkpsec.in,User-Agent: Dart/3.9 (dart:io),>{"status":false,"message":"Not_Ok","errorCode":"400","msg":"Login Unsuccessful.Please try again after sometime.","data":null}>biometriclogin>49.36.184.125>>468100020>>>07:34:56>07:34:57>941.692 sec>{"logindevice":"IOS","deviceid":"GSG_F229AAF9-AF69-48FD-ABEC-815B0DA1D28D","userid":"468100020","code":"000df288-a116-4526-83cd-e05e155346d3","source":"MOB","ApkVersion":"","clientCategory":"GSG"}>Accept-Encoding: gzip,Host: trading.lkpsec.in,User-Agent: Dart/3.9 (dart:io),>{"status":false,"message":"Not_Ok","errorCode":"400","msg":"Login Unsuccessful.Please try again after sometime.","data":null}>biometriclogin>152.58.177.156>>SAR010>>>07:35:07>07:35:08>929.090 sec>{"logindevice":"Android","deviceid":"GSG_bde70d9251b81e2a","userid":"SAR010","code":"3ed571a0-870a-4861-aa2f-3473e6ea9e16","source":"MOB","ApkVersion":"","clientCategory":"GSG"}>Accept-Encoding: gzip,Host: trading.lkpsec.in,User-Agent: Dart/3.9 (dart:io),>{"status":false,"message":"Not_Ok","errorCode":"400","msg":"Login Unsuccessful.Please try again after sometime.","data":null}>mpinlogin>152.58.177.156>>SAR010>>>07:35:21>07:35:22>928.857 sec>{"logindevice":"Android","deviceid":"GSG_bde70d9251b81e2a","userid":"SAR010","code":"3ed571a0-870a-4861-aa2f-3473e6ea9e16","source":"MOB","ApkVersion":"","mPin":"","clientCategory":"GSG"}>Accept-Encoding: gzip,Host: trading.lkpsec.in,User-Agent: Dart/3.9 (dart:io),>{"status":false,"message":"Not_Ok","errorCode":"400","msg":"Login Unsuccessful.Please try again after sometime.","data":null}>mpinlogin>1.38.96.6>>11000591>>>07:35:31>07:35:32>948.562 sec>{"logindevice":"Android","deviceid":"GSG_c820a6d93707208f","userid":"11000591","code":"05860f4e-8a31-4e73-a69c-17e171cbc512","source":"MOB","ApkVersion":"","mPin":"","clientCategory":"GSG"}>Accept-Encoding: gzip,Host: trading.lkpsec.in,User-Agent: Dart/3.9 (dart:io),>{"status":false,"message":"Not_Ok","errorCode":"400","msg":"Login Unsuccessful.Please try again after sometime.","data":null}>mpinlogin>1.38.96.6>>11000591>>>07:35:38>07:35:39>931.640 sec>{"logindevice":"Android","deviceid":"GSG_c820a6d93707208f","userid":"11000591","code":"05860f4e-8a31-4e73-a69c-17e171cbc512","source":"MOB","ApkVersion":"","mPin":"","clientCategory":"GSG"}>Accept-Encoding: gzip,Host: trading.lkpsec.in,User-Agent: Dart/3.9 (dart:io),>{"status":false,"message":"Not_Ok","errorCode":"400","msg":"Login Unsuccessful.Please try again after sometime.","data":null}>biometriclogin>49.37.39.118>>CLS10>>>07:36:15>07:36:16>941.071 sec>{"logindevice":"Android","deviceid":"GSG_c2af95669b210884","userid":"CLS10","code":"41fd5b86-30fe-4699-b883-e0f4b9245853","source":"MOB","ApkVersion":"","clientCategory":"GSG"}>Accept-Encoding: gzip,Host: trading.lkpsec.in,User-Agent: Dart/3.9 (dart:io),>{"status":false,"message":"Not_Ok","errorCode":"400","msg":"Login Unsuccessful.Please try again after sometime.","data":null}>biometriclogin>49.37.39.118>>CLS10>>>07:36:27>07:36:28>924.640 sec>{"logindevice":"Android","deviceid":"GSG_c2af95669b210884","userid":"CLS10","code":"41fd5b86-30fe-4699-b883-e0f4b9245853","source":"MOB","ApkVersion":"","clientCategory":"GSG"}>Accept-Encoding: gzip,Host: trading.lkpsec.in,User-Agent: Dart/3.9 (dart:io),>{"status":false,"message":"Not_Ok","errorCode":"400","msg":"Login Unsuccessful.Please try again after sometime.","data":null}>biometriclogin>49.37.39.118>>CLS10>>>07:36:41>07:36:42>938.065 sec>{"logindevice":"Android","deviceid":"GSG_c2af95669b210884","userid":"CLS10","code":"41fd5b86-30fe-4699-b883-e0f4b9245853","source":"MOB","ApkVersion":"","clientCategory":"GSG"}>Accept-Encoding: gzip,Host: trading.lkpsec.in,User-Agent: Dart/3.9 (dart:io),>{"status":false,"message":"Not_Ok","errorCode":"400","msg":"Login Unsuccessful.Please try again after sometime.","data":null}>getmappedidbymob>125.62.206.231>>>>>07:38:59>07:38:59>176.996 sec>{"MobileNo":"9701759666","DeviceId":"","Source":"MOB","ClientCategory":"GSG"}>Accept-Encoding: gzip,Host:
```

TDL-002 - Missing Security Headers – {Low} {Open}

Vulnerable URLs	https://trading.lkpsec.in/
Vulnerable Parameter	N/A
Payload	N/A
OWASP Vulnerability Classification	A05:2021-Security Misconfiguration
CVSS Score 3.1	Security Misconfiguration
CWE-ID Mapping	CWE-693
Vulnerability Explanation:	The application response is missing multiple important HTTP security headers that help protect users against common web-based attacks. The response does not include headers such as Content-Security-Policy (CSP), X-Frame-Options, X-Content-Type-Options, Strict-Transport-Security (HSTS), and Referrer-Policy. Without these protections, browsers are not instructed to enforce additional security controls, increasing exposure to attacks including clickjacking, MIME-type confusion, insecure transport usage, and client-side injection-related risks.
Vulnerability Impact:	Missing security headers weaken the browser-side security posture of the application and increase the attack surface available to attackers. An attacker may exploit the absence of these headers to perform clickjacking attacks, content injection, MIME-sniffing abuse, or downgrade attacks against users accessing the application. Although the issue may not directly lead to compromise independently, it significantly reduces defense-in-depth protections and can assist attackers in chaining other vulnerabilities for more severe exploitation scenarios.
Remediation	Configure the web server and application to include recommended HTTP security headers for all responses. Implement headers such as Content-Security-Policy to mitigate injection attacks, X-Frame-Options to prevent clickjacking, X-Content-Type-Options to disable MIME sniffing, and Strict-Transport-Security to enforce HTTPS communication. Additionally, implement Referrer-Policy and Permissions-Policy headers to reduce unnecessary data exposure and restrict browser features. Regularly validate security header configurations through automated security assessments and hardening reviews.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP-Headers_Cheat_Sheet.html

Steps to Reproduce & Proof of Concept:

1. Visit the targeted URL.
2. Intercept the request in Burp-suite.
3. Send to Repeater.

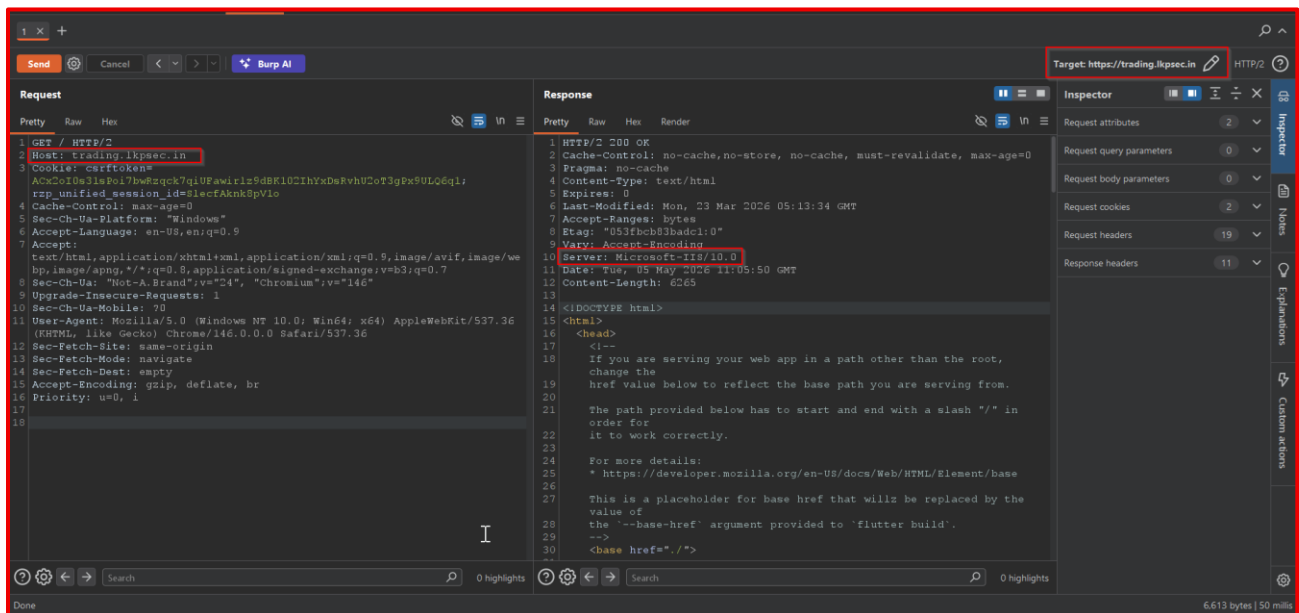


TDL-003 - Server name and Version – {Informational} {Open}

Vulnerable URLs	https://trading.lkpsec.in/
Vulnerable Parameter	N/A
Payload	N/A
OWASP Vulnerability Classification	A05:2021-Security Misconfiguration
CVSS Score 3.1	Security Misconfiguration
CWE-ID Mapping	CWE-200
Vulnerability Explanation:	The application exposes its web server name and version through the HTTP response header "Server: Microsoft-IIS/10.0". This disclosure reveals the exact web server software and version running on the target system. Such information is not required for normal application functionality and provides attackers with insights into the backend infrastructure, making it easier to identify potential vulnerabilities associated with the disclosed server version.
Vulnerability Impact:	Attackers can use the disclosed server version to correlate known vulnerabilities and publicly available exploits specific to Microsoft IIS 10.0. This significantly reduces reconnaissance effort and enables more targeted and efficient attack strategies. Although this issue alone does not lead to direct exploitation, it increases the overall risk posture by facilitating vulnerability chaining and targeted attacks against outdated or misconfigured server components.
Remediation	Suppress or modify the "Server" response header to prevent disclosure of server details. In IIS, configure URL Rewrite rules or use registry settings to remove or obfuscate the server banner. Ensure that unnecessary headers revealing backend technologies are disabled. Regularly review response headers as part of security hardening practices and keep the server updated with the latest patches to reduce exposure to known vulnerabilities.
Reference	https://cwe.mitre.org/data/definitions/200.html

Steps to Reproduce & Proof of Concept:

1. Visit the targeted URL.
2. Intercept the request in Burp-suite.
3. Send to Repeater.



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.