



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-LS-WB-01/26/1992
Report Version	v1.0
Web Application Name	Lkpsec
Type of Audit	Black Box Web Application VAPT Audit
Type of Audit Report	First Audit Report
Assessment Period	12-01-2026 to 13-01-2026
Report Prepared by	Kunal Patil
Reviewed by	Heet Kakadiya
Approved by	Rohit Soni
Released by	Pavan Saxena
Date of Release	19-01-2026

Document Change History		
Version	Date	Remarks / Reason of Change
v1.0	19-01-2026	First Audit Report

Document Distribution List			
Name	Organization	Designation	Email Id
Pavan Saxena	TechDefence Labs	Team - Lead	pavan@techdefence.com
Rohit Soni	TechDefence Labs	Team – Manager	rohit.s@techdefnce.com
Kunal Patil	TechDefence Labs	Security Analyst	kunal.p@techdefene.com
Dhruv Chauhan	TechDefence Labs	Manager – Enterprise Business	dhruv.chauhan@techdefence.com
Jotiba Patil	LKP Securities Limited	Manager IT	jotiba_patil@lkpsec.com

Confidentiality and Disclaimer

This report is prepared exclusively for the management of **LKP Securities Limited** 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 **LKP Securities Limited** and the data provided during the assessment period. Any limitations due to environment 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 **LKP Securities Limited**, specifically focusing on the security of the defined domain and systems in-scope. TechDefence Labs highlights areas for potential improvement; however, the responsibility for implementing and maintaining robust security measures lies with the management of **LKP Securities Limited**. 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: Wherever the name “**TechDefence Labs**” appears in this report, it should be understood as referring to “**TechD Cybersecurity Limited**.”

© Techdefence Labs, 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 VAPT Assessment Timeline	6
1.4 Project Team	7
2. VAPT Audit Methodology and Standards.....	8
2.1 Phases of the Assessment.....	8
2.2 Standards and Methodologies	8
2.3 Vulnerability Metrics	9
2.4 Tools used during the assessment.....	10
3. Executive Summary	11
3.1 Visual Representation of Assessment Results	11
3.2 Vulnerability Overview Table.....	12
4. Detailed Vulnerability Observations.....	13
TDL-001 -Clickjacking – {Low} {Open}	13
TDL-002 – Vulnerable and Outdated Components – {Low} {Open}	15
TDL-003 – Missing Security Headers – {Low} {Open}	17
TDL-004 – Server Name and Version Disclosure– {Low} {Open}.....	19
TDL-005 – Unnecessary ports open - {Informational} {Open}	21
Disclaimer and Precautions for Patch Implementation	23
Appendices	23

1. Assessment Details

LKP Securities Limited engaged TechDefence Labs to assess the security of its Web Application. The evaluation focused on identifying Web Application-level vulnerabilities, testing security mechanisms, and resilience against unauthorized access. The assessment followed industry standards, including OWASP Security Top 10, SANS Institute's Top 25 and Penetration Testing Execution Standard (PTES).

1.1 Engagement Scope

The following web application provided by **LKP Securities Limited** have been identified as in-scope for this security assessment, as defined and specified by **LKP Securities Limited**:

In Scope of Assessment	
Web Application Name	Lpksec
Web Application URL	https://lkpsec.com/
Version of Web Application	Not Provided
Audit Type	Black Box
Testing Environment Configuration	Production Environment
User Roles Configured for Testing	N/A

Out of the Scope of Assessment			
Sr. No	Application Function Name	Application Function URL	Reason
N/A	N/A	N/A	N/A

1.2 Scope Exclusions

1. Server testing on which the Web Application is hosted is outside the scope of this assessment.
2. The source code review of the Web Application is not included in the scope of this assessment.
3. Any API gateways connected to the Web Application but not owned by LKP Securities Limited are outside the scope of this assessment.
4. For production environments provided during testing, vulnerabilities or test cases that may cause damage, or downtime will be excluded from the security audit.
5. Any Web Application endpoints or functions explicitly listed as "Out of Scope" for the assessment will not be tested.

1.3 VAPT Assessment Timeline

Events	Dates
Initial Security Assessment Start Date	12-01-2026
Initial Security Assessment End Date	13-01-2026
Initial Security Assessment Reports Shared Date	19-01-2026

1.4 Project Team

Below are the TechDefence Labs Auditing team members who played a key role in this engagement:

Name	Designation	Email-ID	Qualifications/ Certifications	Has the resource been listed on CERT-In's published Snapshot? (Yes/No)
Pavan Saxena	Team Lead - VAPT	pavan@techdefence.com	BCA, OSCP (ISC)2 - CC, AZ-900, CEHv12, eJPT-v2, CAP, CNSP, CAPen, KLCP, ISO-27001: Lead Auditor	Yes
Kunal Patil	Security Analyst	kunal.p@techdefence.com	Bsc, CAP, CNSP	No
Kalpesh Patil	TechDefence Labs	Kalpesh.p@techdefence.com	B.Tech OSCP, eWPTXV2, CNSP	No

2. VAPT Audit 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 Pen 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 Metrics

This section outlines the CVSS Scoring System used to calculate the severity of vulnerabilities, determined using leading security practices and TechDefence Labs' experience in similar projects. Each vulnerability is assigned a qualitative impact factor—Critical, High, Medium, Low, or Informational to help **LKP Securities Limited** prioritize remediation efforts effectively and enhance their risk management strategy.

Risk Exposure	CVSS Score	Description
Critical	9.0 – 10.0	Exploitation of such vulnerabilities can lead to unauthorized access to sensitive information, data manipulation, and service disruptions, severely impacting Confidentiality, Integrity, and Availability (CIA) of the data, operations, business continuity and security posture.
High	7.0 – 8.9	Exploitation can lead to significant system or data compromise, with the potential for unauthorized access or privilege escalation. Prompt action is needed to mitigate risks before they escalate.
Medium	4.0 – 6.9	Exploitation may result in localized impact or reduced security but does not immediately threaten the overall system. These should be addressed in a timely manner to prevent potential exploitation.
Low	0.1 – 3.9	Exploitation has a minimal impact on system security and generally requires specific conditions. These can be addressed after higher-priority issues are resolved.
Informational	0	Findings that do not pose a direct risk but suggest improvements or optimizations to security practices. These should be reviewed for the best practices and continuous improvement.

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.

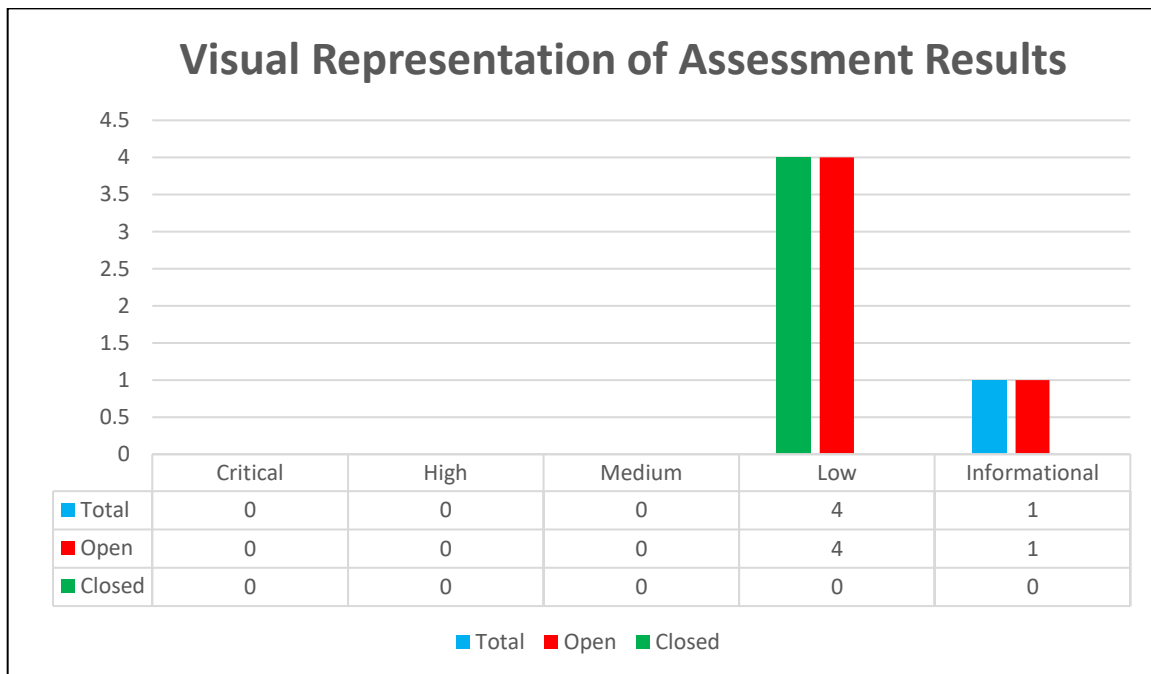
2.4 Tools used during the assessment

Sr. No	Name of Tool /Software used	Version of the tool /Software used	Open /Licensed	Source
01	Burp Suite Professional	v2025.10.2	Licensed	

3. Executive Summary

The following section provides an Executive Summary of the vulnerabilities identified during this Security Audit. Detailed recommendations for each observation are outlined in Section 4 of this report.

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://lkpsec.com/	Clickjacking	CWE-1021	Low	Open
TDL-002	https://lkpsec.com/_next/static/chunks/main-306b02f0f74abccd.js	Vulnerable and Outdated Components	CWE-1104	Low	Open
TDL-003	https://lkpsec.com/	Missing Security Headers	CWE-693	Low	Open
TDL-004	https://lkpsec.com/	Server Name and Version Disclosure	CWE-200	Low	Open
TDL-005	https://lkpsec.com/	Unnecessary ports open	CWE-693	Informational	Open

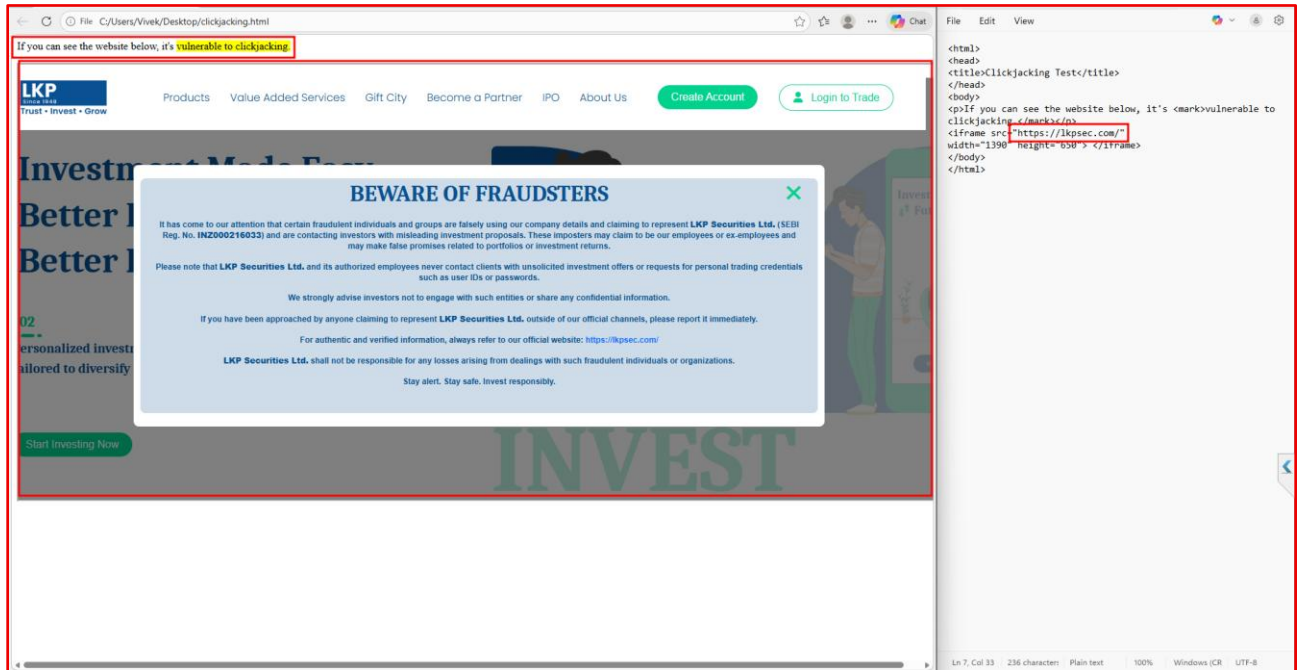
4. Detailed Vulnerability Observations

TDL-001 - Clickjacking – {Low} {Open}

Vulnerable URLs	https://lbpsec.com/
Vulnerable Parameter	Missing X-frame Options header
Payload	N/A
Vulnerability Class	A05:2021 – Security Misconfiguration
CVSS Score 3.1	Security Misconfiguration
CWE-ID	CWE-1021
Vulnerability Explanation:	Clickjacking is a UI redress attack where a malicious actor overlays transparent or opaque layers on a trusted webpage to trick users into clicking hidden elements, such as buttons or links. This can lead users to unknowingly perform unintended actions, such as submitting sensitive data, enabling permissions, or initiating transactions. The attack leverages HTML iframes and CSS styling to conceal the true nature of the clickable element.
Vulnerability Impact:	If exploited, clickjacking can result in unauthorized actions being performed on behalf of the victim, such as changing account settings, transferring funds, or enabling malicious features. This can compromise confidentiality, integrity, and even lead to full account compromise. When combined with other attacks like CSRF, clickjacking can significantly amplify the damage and impact on both the user and the web application.
Remediation	Implement HTTP response headers like X-Frame-Options set to DENY or SAMEORIGIN to prevent the site from being embedded in iframes on malicious domains. Alternatively, use the Content-Security-Policy (CSP) frame-ancestors directive to define allowed embedding sources. Regularly audit the application for framing vulnerabilities, apply proper access control on sensitive actions, and ensure all browsers are tested for compliance with the implemented protections. This layered defense minimizes the risk of clickjacking attacks.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

Steps to Reproduce & Proof of Concept:

1. Load the given URL in a iframe and save it in a HTML file, now run the file and observe that site is vulnerable to clickjacking.

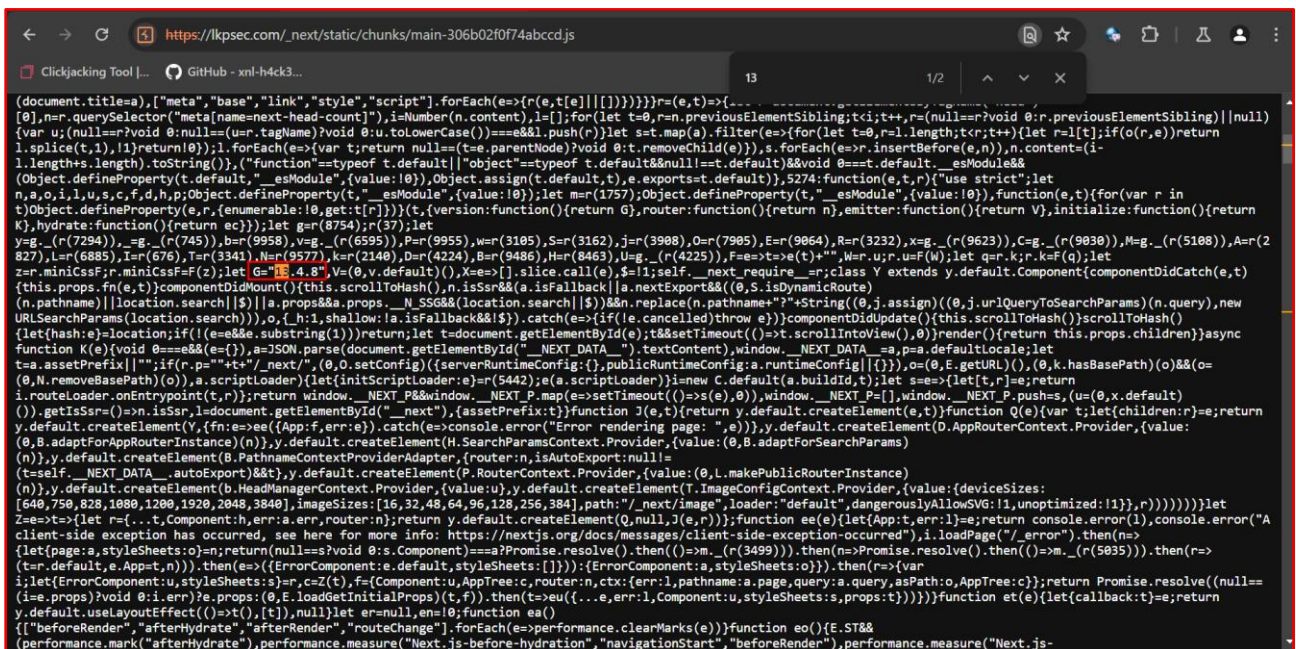
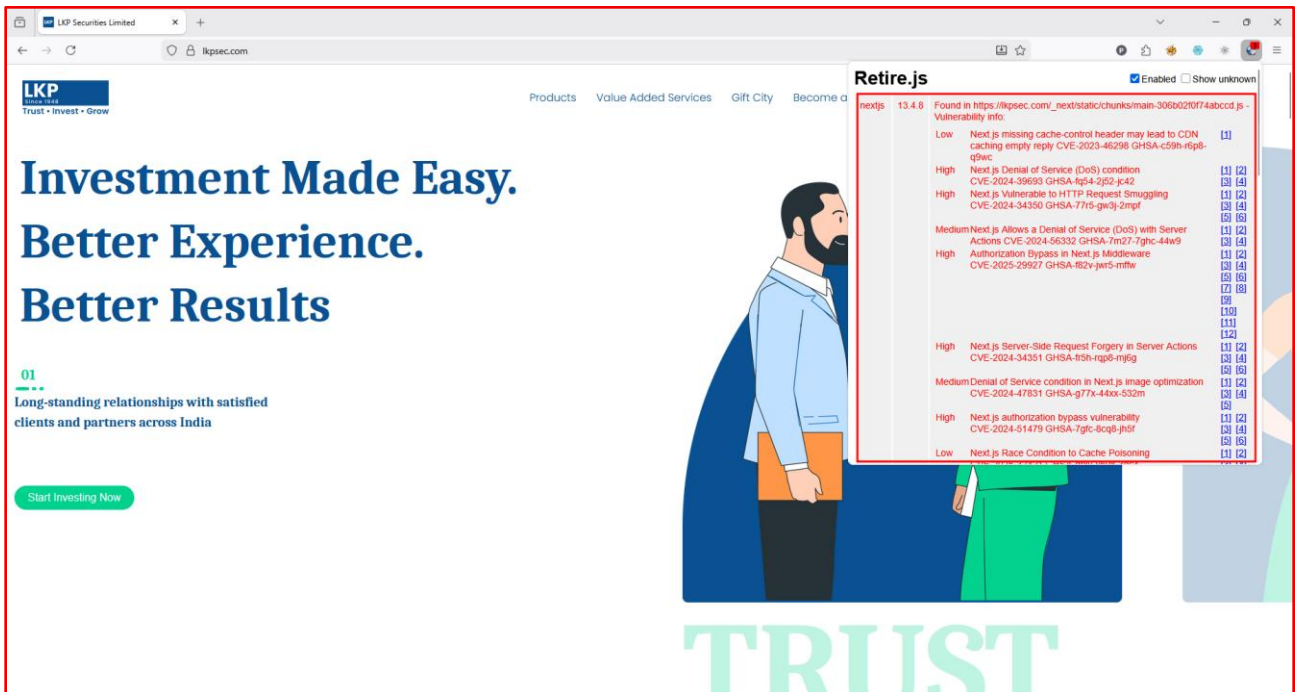


TDL-002 – Vulnerable and Outdated Components – {Low} {Open}

Vulnerable URLs	https://ljkpsec.com/_next/static/chunks/main-306b02f0f74abccd.js
Vulnerable Parameter	N/A
Payload	N/A
Vulnerability Class	A06:2021 – Vulnerable and Outdated Components
CVSS Score 3.1	Security Misconfiguration
CWE-ID	CWE-1104
Vulnerability Explanation:	Vulnerable and Outdated Components occur when a web application uses libraries, frameworks, or software components with known security flaws. These components may contain publicly disclosed vulnerabilities that attackers can easily exploit. The issue commonly arises due to lack of patch management or dependency monitoring. Since such components are often deeply integrated, their vulnerabilities directly impact the application's security. Attackers can identify these components through version disclosure or fingerprinting techniques.
Vulnerability Impact:	Exploitation of vulnerable components can lead to serious attacks such as remote code execution, SQL injection, authentication bypass, or data leakage. Attackers may gain unauthorized access to the server or application data. This can compromise sensitive user information and impact application availability. Additionally, using outdated components increases the risk of automated attacks, regulatory non-compliance, and reputational damage to the organization.
Remediation	Maintain an up-to-date inventory of all third-party libraries and frameworks used in the application. Regularly update and patch components to the latest stable and secure versions. Remove unused or unsupported dependencies to reduce attack surface. Monitor vulnerability databases and security advisories for component-related issues. Implement automated dependency scanning tools as part of the development and deployment process.
Reference	https://owasp.org/Top10/2021/A06_2021-Vulnerable_and_Outdated_Components/

Steps to Reproduce & Proof of Concept:

1. Visit the URL



TDL-003 – Missing Security Headers – {Low} {Open}

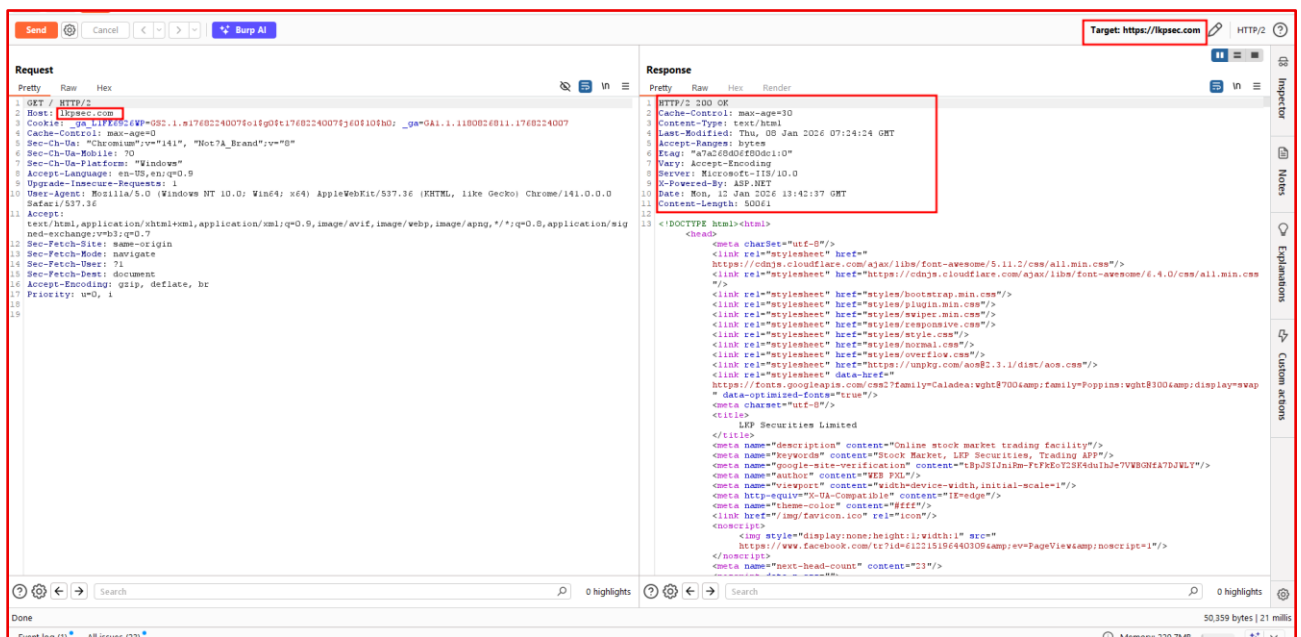
Vulnerable URLs	https://lbpsec.com/
Vulnerable Parameter	N/A
Payload	N/A
Vulnerability Class	A05:2021-Security Misconfiguration
CVSS Score 3.1	Security Misconfiguration
CWE-ID	CWE-693
Vulnerability Explanation:	Missing security headers occur when a web application does not implement standard HTTP response headers that help protect against common attacks. Headers such as Strict-Transport-Security, X-Content-Type-Options, X-Frame-Options, Referrer-Policy, and Content-Security-Policy play a key role in mitigating risks like clickjacking, MIME-type sniffing, mixed content, and cross-site scripting (XSS). Without these headers, browsers cannot enforce certain security policies, leaving the application more exposed to exploitation.
Vulnerability Impact:	The absence of security headers increases the attack surface by removing browser-enforced protections. Attackers may exploit this to execute clickjacking attacks, steal sensitive data via content injection, or manipulate page rendering. It can also allow the loading of insecure or malicious external resources. While missing headers alone may not directly compromise the system, they often weaken the overall security posture and can be combined with other vulnerabilities for more impactful attacks.
Remediation	Configure the web server or application framework to include recommended HTTP security headers in every response. Common best practices include enabling Strict-Transport-Security to enforce HTTPS, setting X-Content-Type-Options: nosniff to prevent MIME sniffing, using X-Frame-Options: DENY or SAMEORIGIN to block clickjacking, implementing a strict Content-Security-Policy to control allowed resources, and applying Referrer-Policy to limit referrer data exposure. Test header configurations regularly to ensure they are present, correctly set, and compatible with application functionality.

Reference

<https://www.invicti.com/blog/web-security/missing-http-security-headers/>

Steps to Reproduce & Proof of Concept:

1. Visit the given URL and capture the request in burpsuite, in response observe that Security Headers are missing.

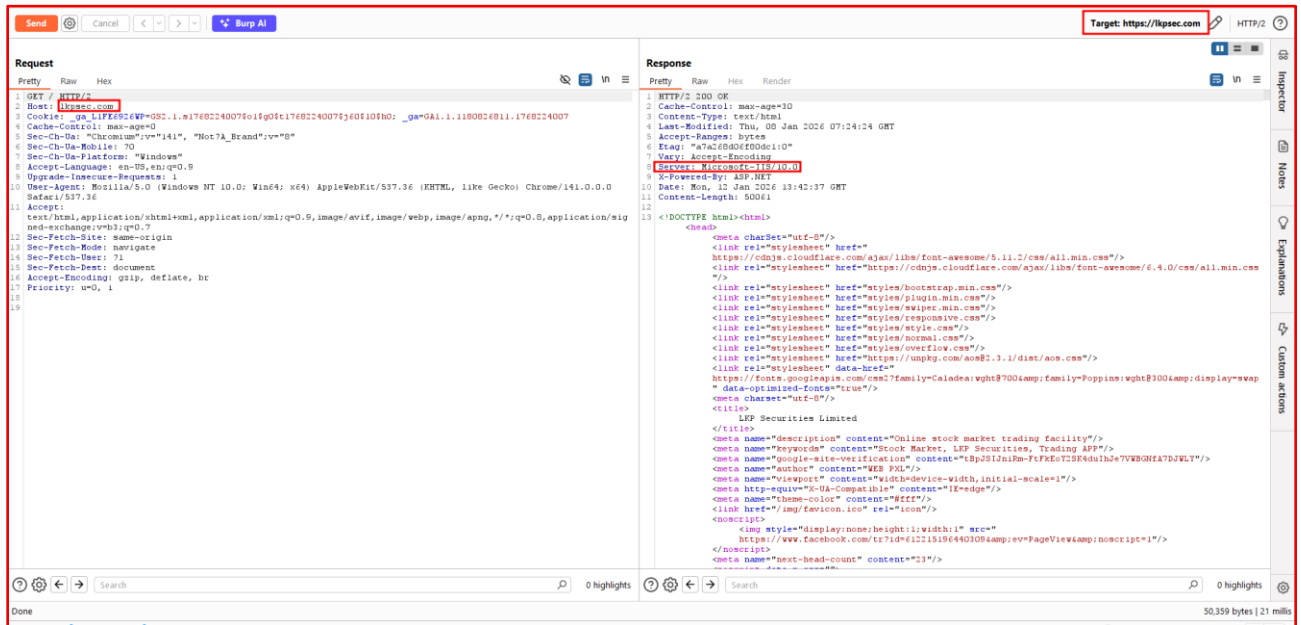


TDL-004 – Server Name and Version Disclosure– {Low} {Open}

Vulnerable URLs	https://lkpsec.com/
Vulnerable Parameter	N/A
Payload	N/A
Vulnerability Class	A05:2021-Security Misconfiguration
CVSS Score 3.1	Security Misconfiguration
CWE-ID	CWE-200
Vulnerability Explanation:	Server name and version disclosure occurs when a web application or server reveals its software type and version details through HTTP headers, error messages, or banners. This information can be retrieved using tools like curl, browser developer tools, or vulnerability scanners. Exposing server details gives attackers valuable intelligence about the technology stack, which they can leverage to identify known vulnerabilities and craft targeted attacks against specific server versions.
Vulnerability Impact:	If an attacker knows the exact server software and version in use, they can search for related exploits and security flaws. This reduces the effort required for reconnaissance and increases the likelihood of a successful targeted attack. For example, outdated or vulnerable versions of Apache, Nginx, or IIS may have publicly available exploits that could allow remote code execution, privilege escalation, or denial-of-service attacks. Even if the system is patched, disclosure still increases the attack surface.
Remediation	Disable or obfuscate server banner information in HTTP responses by modifying the server configuration. For Apache, use <code>ServerTokens Prod</code> and <code>ServerSignature Off</code> . In Nginx, use <code>server_tokens off;</code> . For IIS, remove or modify the X-Powered-By header. Additionally, ensure that custom error pages do not reveal software or framework details. Employ a security gateway or WAF to sanitize headers before sending them to clients. Regularly update and patch server software to minimize the risk of exploitation even if some details are inadvertently disclosed.
Reference	https://www.acunetix.com/blog/articles/configure-web-server-disclose-identity/

Steps to Reproduce & Proof of Concept:

1. Go to the given URL and capture the request in burpsuite, in response observe that server name is disclosed.



TDL-005 – Unnecessary ports open - {Informational} {Open}

Vulnerable URLs	https://lkpsec.com/
Vulnerable Parameter	N/A
Payload	nmap -sC -Pn -p- <IP Address>
Vulnerability Class	A05:2021 - Security Misconfiguration
CVSS Score 3.1	Security Misconfiguration
CWE-ID	CWE-693
Vulnerability Explanation:	Leaving unnecessary ports open increases the attack surface, providing potential entry points for attackers. Open ports might expose services that have vulnerabilities, allowing unauthorized access or providing reconnaissance data. This can lead to deeper network penetration if these services are not adequately secured.
Vulnerability Impact:	Open ports can lead to unauthorized access, increasing the likelihood of an attack. Attackers can use open ports to gain valuable insights into network configurations and potentially exploit exposed services. It raises the risk of network compromise through vulnerabilities associated with exposed applications or services.
Remediation	Implement network filtering to restrict open ports to only essential ones. Regularly scan the network to identify and close unnecessary ports. Apply strict firewall rules and ensure only the ports required for business functionality are open. Additionally, periodically review configurations to maintain a minimal attack surface.
Reference	https://www.e2enetworks.com/blog/is-open-port-vulnerable

Steps to Reproduce & Proof of Concept:

1. Go to CMD
2. After that Run give command in cmd.

```
Microsoft Windows [Version 10.0.26280.7462]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Vivek> nmap -sC -sV -Tl -A lkpsec.com
Starting Nmap 7.92 ( https://nmap.org ) at 2026-01-12 18:57 India Standard Time
Nmap scan report for lkpsec.com (51.162.178.250)
Host is up (0.0063s latency).
Not shown: 786 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp   open  https
444/tcp   open  http
445/tcp   open  smb
4481/tcp  open  http
80/tcp    open  http
Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: LKP Securities Limited
|_ http-server-header:
|_ Microsoft-IIS/10.0
|_ Microsoft-IIS/10.0
82/tcp    open  tcpwrapped
89/tcp    open  tcpwrapped
189/tcp   open  tcpwrapped
113/tcp   closed ident
119/tcp   open  tcpwrapped
|_ _ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ _ssl-v2: ERROR: Script execution failed (use -d to debug)
|_ _tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ _tls-alpn: ERROR: Script execution failed (use -d to debug)
|_ _ssl-date: ERROR: Script execution failed (use -d to debug)
125/tcp   open  tcpwrapped
186/tcp   open  tcpwrapped
211/tcp   open  tcpwrapped
254/tcp   open  tcpwrapped
259/tcp   open  tcpwrapped
425/tcp   open  tcpwrapped
443/tcp   open  ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ _ssl-cert: Subject: commonName=www.lkp.net.in/organizationName=LKP SECURITIES LIMITED/stateOrProvinceName=Maharashtra/countryName=IN
|_ Subject Alternative Name: DNS:www.lkp.net.in, DNS:www.lkpfinance.com, DNS:uattrading.lkponline.com, DNS:www.lkpsec.com, DNS:trading.lkponline.com, DNS:ekyc.lkponline.com, DNS:lkpsec.com, DNS:uatekyc.lkponline.com, DNS:uat.lkpsec.com, DNS:trading.pennypal.in, DNS:ekyc.pennypal.in, DNS:rekye.pennypal.in, DNS:uat.pennypal.in, DNS:uatweb.pennypal.in, DNS:pennypal.in, DNS:demo.pennypal.in, DNS:referral.pennypal.in, DNS:notification.lkponline.com, DNS:notification.pennypal.in, DNS:admin.pennypal.in, DNS:uatspip.lkponline.com, DNS:spip.lkponline.com, DNS:druat.pennypal.in, DNS:uatgetsetgrow.lkponline.com, DNS:getsetgrow.lkponline.com, DNS:lkpconnect.net.in, DNS:pay.lkp.net.in, DNS:ekyc.lkp.net.in, DNS:bo.lkp.net.in, DNS:les.lkp.net.in, DNS:ia.lkp.net.in, DNS:welcome.lkp.net.in, DNS:hms.lkp.net.in, DNS:devtrade.lkp.net.in, DNS:ap.lkp.net.in, DNS:aims.lkp.net.in, DNS:backoffice.lkp.net.in, DNS:devtrade.lkp.net.in, DNS:spip.lkp.net.in, DNS:ekycuat.lkp.net.in, DNS:uatbackoffice.lkp.net.in, DNS:wealth.lkp.net.in, DNS:middleware.lkp.net.in, DNS:middlewareapi.lkp.net.in, DNS:ra.lkp.net.in, DNS:ipo.lkp.net.in, DNS:uat.lkp.net.in, DNS:allocation.lkp.net.in, DNS:trilogy.lkp.net.in, DNS:lkp.net.in
|_ Not valid before: 2025-04-21T10:26:13
|_ Not valid after: 2026-05-23T10:26:12
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: LKP Securities Limited
|_ _ssl-date: 2026-01-12T13:33:44+00:00; 0s from scanner time.
```


Disclaimer and Precautions for Patch Implementation

Before initiating any patching, updates, or remediation work based on the vulnerabilities identified in the following report, please ensure the following precautions are in place:

- **Backups:** Confirm that comprehensive backups of the systems, code, and relevant data are created prior to making any changes. This ensures that you can restore the environment if needed.
- **Rollback Plan:** Have a clear rollback plan ready in case the patching or remediation leads to unexpected issues. This plan should outline steps to return the system to its previous state with minimal downtime.
- **Testing in UAT Environment:** Prior to implementing any hotfixes, service packs, or patches in the production environment, ensure thorough testing is conducted in a User Acceptance Testing (UAT) environment. This step helps verify that the fixes do not cause unforeseen issues or downtime.
- **Third-Party Links Disclaimer:** The following report includes third-party links to resources for vulnerability remediation. Please note that TechDefence Labs does not assume responsibility for the accuracy, availability, or content of these external sites, as they may change overtime.
- **Vulnerability Report Limitations:** The vulnerabilities listed in this report are based on security scans and tests conducted on the specified date using a non-intrusive approach within the tested environment. Please be aware that new vulnerabilities may be discovered after the report is generated. Additionally, certain vulnerabilities that could lead to system instability or downtime were not assessed in this report. The assessment was conducted within the timeline constraints of the audit, which may have excluded some potential test cases.
- **Ongoing Security:** This Vulnerability Assessment and Penetration Testing (VAPT) report should not be construed as an assertion of absolute security for the system or applications. Security is an ongoing process, and the system's security posture can evolve over time. The penetration tester does not accept responsibility for new risks that may arise after the assessment period due to changes in the target system or other unforeseen factors.

Appendices

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 this 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.