Project Completion Report – Draup Inc

Date: 26/02/2025

1. INTRODUCTION

Indusface is a SaaS company which secures critical Web applications of 2000+ global customers using its award-winning platform that integrates Web application scanner, Web application firewall, CDN and threat information engine.
The company has been mentioned in the Gartner Magic Quadrant and Forrester Tech Now reports, is CERT-In empaneled as a trusted scanning vendor and has been the recipient of many awards such as the Economic Times Top 25, NASSCOM DSCI Top Security Company of the year Award and is funded by Tata Capital Growth Fund.

Indusface has successfully completed the application assessment as per the scope.
Indusface WAS does not carry out any DOS attacks and makes the best effort to not run any exploits which can affect system vulnerability.
Indusface has conducted Application scan on web application using valid credentials.
Scope of Manual PT is to report only one instance of a type of vulnerability and does not cover identification of all instances of every vulnerability.

Scope of testing

https://draup.com/

Indusface was able to identify the findings below during the application audit.

The audit was concluded on 28/08/2024, the Re-audit was concluded on 30/09/2024.

Sr. No	Issue Description	Severity	Reval_Status
1	Application is vulnerable to OTP flooding attack	Medium	Closed
2	HTML Form Without Anti-CSRF Token Detected	Medium	Closed
3	Content Injection	Medium	Closed
4	HTTP Verb Tampering	Low	Closed
5	Predictable Resource Location	Info	Closed
6	Running Service (Open Port)	Info	Closed
7	Email Address Disclosure	Info	Closed

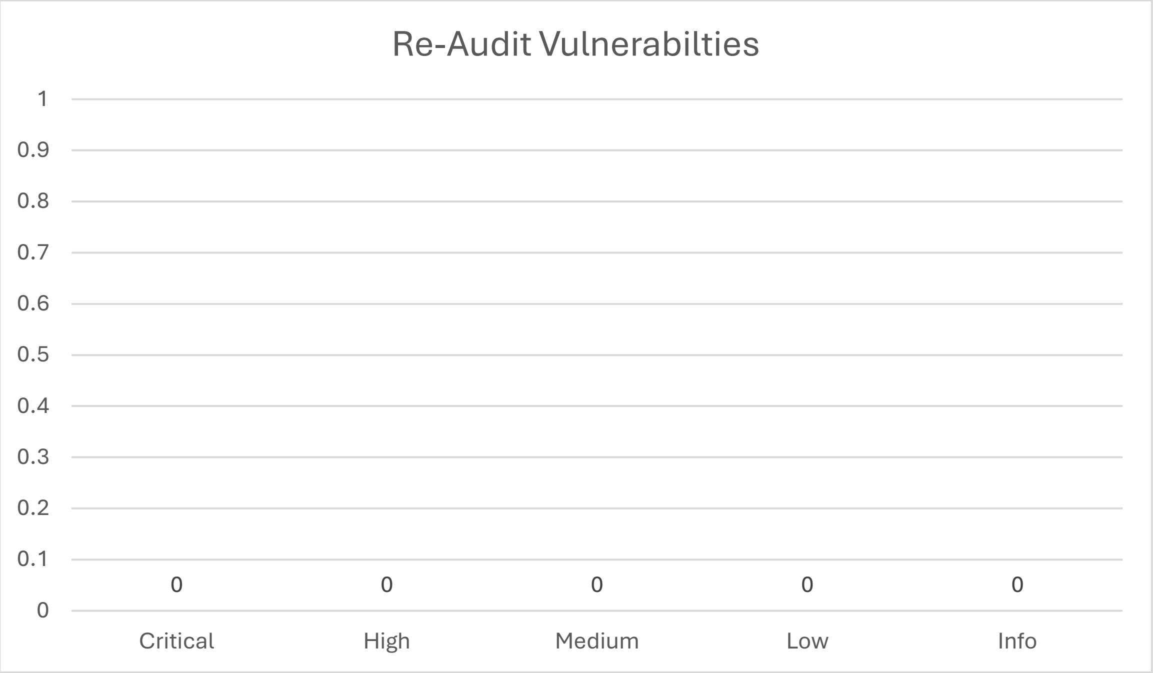
Conclusion:

The tested application hosted is free from any severe vulnerability/threat and safe to carry out transactions. The application has passed **Critical / High / Medium / Low** vulnerabilities for application security assessment tests.

2. OVERALL VULNERABILITY DETAILS

Overall vulnerability details of the OPEN Vulnerabilities.

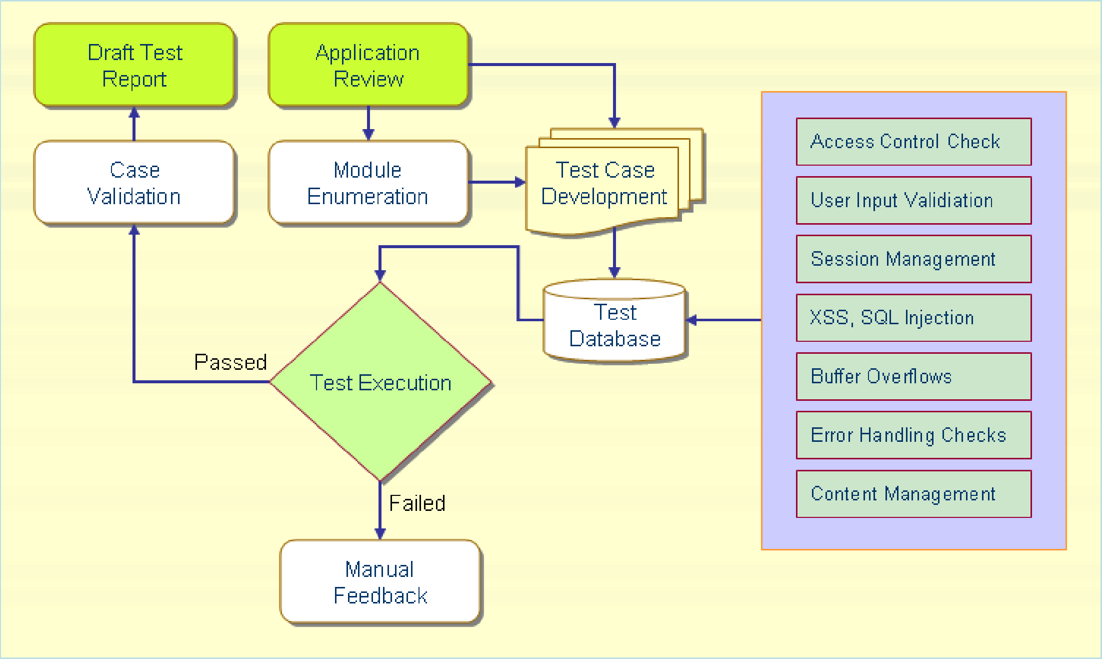
Sr No	Application Name	Critical	High	Medium	Low	Info	Total
1.	Web App - Audit https://draup.com/	0	0	3	1	3	7
2.	Web App – Reaudit https://draup.com/	0	0	0	0	0	0



3. APPLICATION AUDIT METHODOLOGY

Indusface Application Security expert would assess the Web Application by performing a range of application vulnerability tests and checks using a combination of manual testing techniques and automated tools testing. Indusface follows OWASP, OSSTMM & SANS Top-25 guidelines for carrying out Web application vulnerability assessment. The details of the same are given below:

Project shall be initiated with a kick-off meeting with the concerned persons of the Customer. Indusface consultants shall gather all relevant information with respect to the scope of work before initiating the actual audit. Indusface uses a combination of manual and automated techniques to perform an application audit. Customer has a defined approach on auditing its critical / non-critical application and hence Indusface defines an approach which will be a combination of threat profiles defined by Customer and Indusface.
Following is the block representation of the Web application testing process:



Module Enumeration
Following our approach towards module enumeration:

- Understanding the module operations and its features
- Creating a data and process flow map
- Discovering visible and hidden modules manually or using tools
- Understanding data paths and in some cases initialization process
- Discovering the underlying development programing languages, frameworks, CRMs and the versions

Test Case Development

Following is our approach towards test case development:

- Enumerate the various input, data, exchange fields used in each module!
- Identifying the data types accepted by each of these fields.
- Enlisting each permutation and combination that could be used in these fields.
- Creating a case that could be used to test the application.

- Version specific test cases for the Underlying development programming languages, frameworks, CRMs

Consultants would take detailed step-by-step POCs for vulnerabilities found during audits and re-audits with highlighting required areas such as parameters that are targeted; with date-time.

Consultants would take Safe and Unsafe POCs for the test cases while performing a fresh assessment or a re-assessment. For each application; upon completion of the assessment; the following would be saved to the share drive – Report (Word and PDF), POCs, Burp State and video for any Critical / High / business flaw vulnerability; especially during re-audits and complete application Video.

For initiating a re-audit of the application; verify the scanning from IG. Validate each automated finding for eliminating any FPs.

Case Validation

Each test result may be further validated and verified by completing an attack cycle. This is done to reconfirm the process and to understand the flaws in the application. Validating a case may also be useful to recommend an accurate recommendation procedure.

Test Database

Following is our approach towards test database:

- Each test case created will be matched against the possible attacks in the list of attacks in the attacks database.
- A permutation of each case and attack is created and added to the test database
- Sample values and or ranges are entered in each of the test cases in the test database
- A test success criterion is also documented in each of the test cases

Application Assessment

To conduct a comprehensive Application Assessment, it is vital to have a broad and flexible testing methodology to uncover the most stubborn vulnerabilities.

The Indusface Application Testing methodology leverages dozens of grey-box and black-box tests to better understand the workings of the applications, while identifying vulnerabilities. Combined, these services offer the consultants the framework required to conduct the most thorough assessment possible.
It is important that Indusface fully understands the unique circumstances around each application, and what the primary concerns are. For example, the Indusface testing methodology examines risk related to each of the following areas (the engagement can be tailored to focus on any particular area):

- Exposure and integrity of confidential information
- Exposure and integrity of confidential employee information
- Denial of service risk to application or application components
- Network infrastructure exposure via application vulnerabilities

Detailed Application Risk Assessment Methodology

The standard Indusface Application Assessment methodology focuses primarily on the following testing classes:

- Architecture
- Business Logic
- Development procedures
- Authentication
- Transmission security
- Session management
- Information or data leakage
- Input validation
- Logic flow and authorization
- Data corruption
- Application deployment

Overall examination of the applications deployed and security configuration from perceived threat models. Advice is given on secure deployment methodologies for the application type based upon market trends, new vulnerability developments and attack methodologies.

Reporting
Audit Report should include all the details of audit, tools, manual process, findings, prioritization, sampling decisions, manpower involved and exemptions. Version control, change management and hash value should be maintained properly. Auditee must mention the hash value of application in report.

Once testing is completed, consultant needs to report vulnerabilities on production URL so make sure to change Host Name entry in Request/Response Header and URL, Injected URL and Response URL while doing reporting.

Report single instances for all issues unless you find any critical case as per your judgement.

During revalidation, reported instances would be verified and if is not open; then only the vulnerability would be marked as safe / closed. While reporting in the injected URL mention the affected URL. For the open vulnerabilities, ensure to update the POCs, request/response headers, injected URL.

Severity of any vulnerability reported (either in WAS or in manual reports), need to be calculated thru the CVSS scores and vectors. It should be based on the consultant's judgement about the attack scenario and be reviewed with respective report reviewers and should be confirmed before publishing report.

WAS Portal: Ensure to get the authenticated scan of the URL in case of grey box testing. Verify the scanners vulnerabilities for false positives. If those are FP whitelist those vulnerabilities and if not, then add POCs for the same.

For the open vulnerabilities, ensure to update the POCs, request/response headers, injected URL. Ensure to elaborate the vulnerability in the report; with a simple language; not using too many technical jargons and detailing on the description, impact, recommendations, and references. The reference links would include – OWASP links; or any other reliable / verified link but make sure we do not add any competitor company's link.

If same vulnerability is reported by both Manual and Automated scan; then only automated scan instance needs to be placed in report. POC, business impact should be updated in that.

Below are the variables used while reporting

- Methodology used to carry our audit
- Standards followed
- Tools used
- List of vulnerabilities identified
- Descriptions of vulnerabilities
- Risk rating or severity vulnerabilities
- Proof of Concept
- Recommendations

- **QA and Report Review Process:**

For getting the report reviewed; the consultant needs to share the reviewer with the URL details to be reviewed.

The consultant needs to share the details with the reviewer – Audit/ Re-Audit, No of re-audit cycle, any explanation/ exception details shared by the client, Black-Box/Grey-Box.

- **Safe To Host Certificate:**

Upon final completion of the project, it is the consultant’s responsibility to share the sample Safe-to-host certificate with the client and get the initial details filled and then forward it to the RO for further processing.

4. WEB APPLICATION ASSESSMENT STANDARDS

OWASP Top 10

A1 - Broken Access Control

Testing for unauthorized functionality

Insecure Data Object Reference

A2 – Cryptographic Failures

Test for Sensitive data exposure

Testing for critical data management

A3 – Injection

SQL Injection

LDAP Injection

OS Command Injection

SSI Injection

X-path Injection

A4 – Insecure Design

Check for the error message revealing sensitive information,

unprotected storage credentials

A5 – Security Misconfiguration

Insecure cryptygraphy storage,

Insufficient transport layer

A6 – Vulnerable and outdated Components

Known vulnerable framework and Library.

Check for vulnerable software modules, product CVEs

A7 – Identification and Authentication Failures

Session Management

Privilege Escalation

Insufficient Session Expiration

A8 – Software and Data Integrity Failures

Verify the integrity check support

Check for the verification of data authenticity

A9 - Security Logging & Monitoring Failure

Check for warnings and errors generate no, inadequate, or unclear log messages.

A10 – Server-Side Request Forgery

attacker can influence the server to make requests to arbitrary domains or resources.

Some Logical and Indusface Define Checks	
Abuse of Functionality	Check for Encoding
Insufficient Anti-automation	Password Auto-Complete
Insufficient Authentication	Improper implementation of SSL (cipher, version)
Email ids can be harvested for spamming	Service enumeration
Bypass Authentication	Port scanning
Insufficient password recovery	Hidden iframe detection
Insufficient process validation	Malicious file can be uploaded on the server
Application does not display last login time	Steal password from browser memory
Server-side validation	Check HTTP methods
	Check for Cookie Attributes

Application specific business logic checks
Application specific business logical checks are carried out by security experts. These experts shall undergo a walkthrough of the web application to understand various threat scenarios and functionality of the application before a business logic test can be performed.

5. SEVERITY RATING – CVSS

Indusface Application Security Assessment (Web and Mobile) produces reports with severity based on the industry standard of using the Common Vulnerability Scoring System – CVSS Scores.

The Common Vulnerability Scoring System (CVSS) is an open framework maintained by the Forum of Incident Response and Security Teams (FIRST), a US-based non-profit organization globally. It provides a numerical (0-10) representation of the severity of an information security vulnerability.

Base Score Calculation:

Publicly available CVSS scores are Base Scores only.

They represent the severity of a vulnerability. The Basic Metric Group is classified into Three Sub-Groups:

- Scope
- Exploitability
- Impact

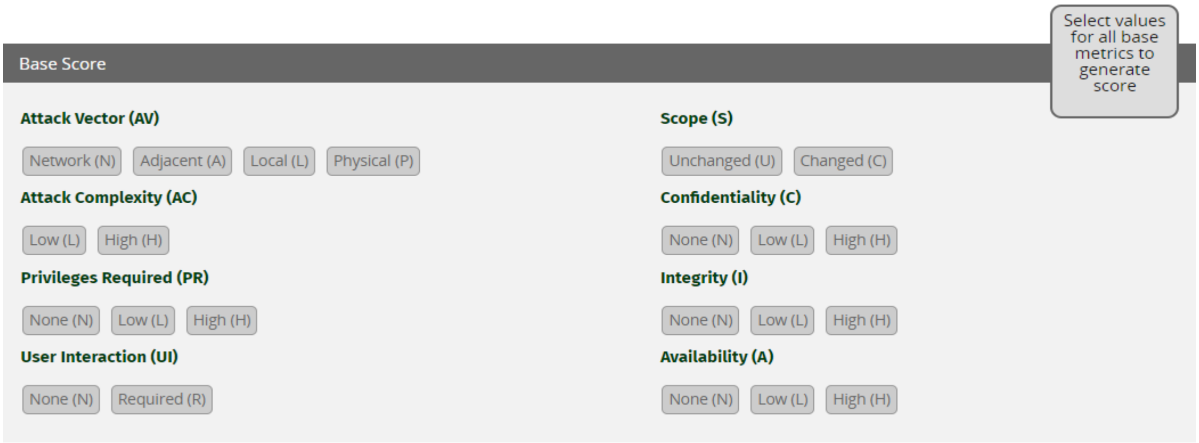
Scope: Scope relates to whether a vulnerability in one component can propagate to other components.

Exploitability: Exploitability metrics are made up of characteristics of the vulnerable component, with Exploitability being made up of four further sub-components.

- **Attack Vector**—Based on the level of access required to exploit a vulnerability.
- **Attack Complexity**—Based on the factors outside of the attacker's control that are required to exploit the vulnerability.
- **Privileges Required**—this score varies based on the privileges required for the attacker to conduct the exploit.
- **User Interaction**—this score varies based on whether the attacker must recruit either a willing or unwitting participant in order to complete their task.

Impact: Impact focuses on the actual outcome that an attacked can achieve as a result of exploiting the vulnerability in question. Impact metrics are comprised of three sub-metrics.

- **Confidentiality**—Based on the amount of data that the attacker gains access to.
- **Integrity**—Based on the ability of the attacker to alter or change data on the impacted system.
- **Availability**—Based on the loss of availability of the exploited system.



Select values for all base metrics to generate score

Base Score

Attack Vector (AV)

Network (N) Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) Required (R)

Scope (S)

Unchanged (U) Changed (C)

Confidentiality (C)

None (N) Low (L) High (H)

Integrity (I)

None (N) Low (L) High (H)

Availability (A)

None (N) Low (L) High (H)

CVSS QUALITATIVE RATINGS:

Severity Rating	CVSS Score	Description
Critical	**9.0 - 10.0**	A vulnerability wherein an attacker might have the ability to execute commands on the server or retrieve and modify private information.
High	**7.0 - 8.9**	Security issues are defined as a risk that puts the system and / or data related to the system in immediate danger.
Medium	**4.0 - 6.9**	Findings indicate a more serious security matter that should be remedied appropriately within a short amount of time.
Low	**1.0 - 3.9**	Findings usually indicate a minor security risk that does not pose immediate or short-term danger. An observational point in the site, or detection of certain applications or web servers.
Informational	**0.0**	An observational point in the site, or detection of certain applications or web servers.

6. TOOLS USED FOR PENETRATION TESTING & VULNERABILITY ASSESSMENT

The following table depicts the partial list of tools used during the Project by Indusface Consulting Information Security Consultants.

Password Cracker

Tools	Details
Cain and Abel	Password Cracker as well as Network Enumeration
John the Ripper	A powerful, flexible and fast multi-platform password hash cracker
Aircrack	802.11 WEP Encryption Cracking tool
Airsnort	802.11 WEP Encryption Cracking tool
Solarwinds	A plethora of network discovery/monitoring/attack tools
Brutus	A network brute-force authentication cracker
Web Cracker	Web Application Password Brute Force Tool
Lopht	Windows Hash Cracker

Sniffers

Tools	Details
TCPDump	The classic sniffer for network monitoring and data acquisition
Ettercap	In case you still thought switched LANs provide much extra security
Dsniff	A suite of powerful network auditing and penetration-testing tools
Winhex	Reads memory
Wireshark	Network Tool

Penetration Testing: Combination of proprietary tool WAS, custom scripts; for web and API testing.

Tools	Details
Nikto	Web Vulnerability Scanner
Burp proxy Professional	A web application vulnerability assessment proxy
Crawler	Web Site Crawler
WAS	In-house Application scanner tool
WPScan	Wordpress vulnerability scanner
Nuclei	Open source, fast, extensible, and covers a wide range of weaknesses.

Other tools used.

Tools	Details
Nmap	Open-source utility for network exploration or security auditing