Safe to Host Certificate

Date: 13/06/2024

Auditor Name: Gaurav Gera

Reviewed by: Kandarp Shah

E-mail Address: gaurav.gera@indusface.com

kandarp.shah@indusface.com

Address: A-2/3, 3rd Floor Status Plaza, Akshar Chowk, Atladra Old Padra Road, Vadodara.Pin – 390020, Gujarat, India.

1st Audit Completion Date : 04/03/2024
Last Revalidation Completion Date: 30/04/2024

To whomsoever it may concern

Company Name: Cactus Communications Pvt. Ltd

Application Name: Researcher Life

Purpose of the Application: Researcher Life is an ecosystem of solutions that assist the researchers in every step of their research life. It helps researchers from creating projects to manage everything around research, making manuscript ready for journal submission, reading the latest and most relevant research, finding the right journals to submit to, up skilling, and building researchers community.

Audit Performed on URL: https://www.researcher.life

Production URL (If any): https://www.researcher.life

UAT URL: Yes

Certificate Validity: This certificate is valid for the instance provided at the time of 1st Audit.

Audit Methodology: OWASP Top 10 2021 & OWASP Web Security Testing Guide (WSTG)

Tool Used: Burpsuite Professional, Nmap, OSINT Tools, Manual Test Methodologies, Exploit DB etc.
Out Of Scope: Security audit of the hosting infrastructure (servers, network, database, etc) and the source code of the application.

The tested application hosted of the mentioned version is free from any severe vulnerability/threat. The application has passed Critical / High / Medium vulnerabilities for application security assessment tests. For a detailed description of other security assessment-related details, please refer to the audit report shared with **Cactus Communications Pvt. Ltd**

The application may be hosted with the privilege of read and write access for the public with an exact replica of the audited URL in the production environment.

Name: Kandarp Shah
Head of Services & Compliance

Safe to Host Certificate

Date: 06/06/2024

Auditor Name: Kali Prasad Reddipalli

Reviewed by: Kandarp Shah

E-mail Address: kaliprasad.reddipalli@indusface.com

kandarp.shah@indusface.com

Address: A-2/3, 3rd Floor Status Plaza, Akshar Chowk, Atladra Old Padra Road,

Vadodara.Pin – 390020, Gujarat, India.

1st Audit Completion Date: 06/03/2024
Last Revalidation Completion Date: 20/05/2024

To whomsoever it may concern

Company Name: Cactus Communication

Application Name: Discovery Android Application

Application Hash value: 19D55E1DD33FA507430BD2C33BA56848

Purpose of the Application: Application is used by researchers to access related information about their research topics.

Audit Performed on Android package name and version: com.rdiscovery & V-3.3.6

Certificate Validity: This certificate is valid for the instance provided at the time of 1st Audit.

Audit Methodology: OWASP Mobile Top 10 2024 & OWASP Mobile Application Security

Tool Used: Burpsuite Professional, APK Tool, Frida, Magisk, Manual Test Methodologies etc.
Out Of Scope: Security audit of the hosting infrastructure (servers, network, database, etc) and the source code of the application.

The tested application hosted of the mentioned version is free from any severe vulnerability/threat. The application has passed Critical / High vulnerabilities for application security assessment tests. For a detailed description of other security assessment-related details, please refer to the audit report shared with Cactus Communication.

The application may be hosted with the privilege of read and write access for the public with an exact replica of the audited URL in the production environment.

Name: Kandarp Shah
Head of Services & Compliance

Safe to Host Certificate

Date: (23rd January 2024)

Auditor Name: Kalpesh Patil

Reviewed by: Kandarp Shah

E-mail Address: kalpesh.patil@indusface.com

kandarp.shah@indusface.com

Address: A-2/3, 3rd Floor Status Plaza, Akshar Chowk, Atladra Old Padra Road, Vadodara.Pin – 390020, Gujarat, India.

Project Start: 18th January 2024 **Project Finish:** 29th February 2024

To whomsoever it may concern

Company Name: Cactus Communications Ltd

Application Name: Editage Web Application

Purpose of the Application: Online Editage System (EOS), the application provides users actionable insights on their business needs such as manuscripts submission, tracking, order download, payments, and various self-service actions**.**

Audit Performed on URL: https://app.editage.com

Production URL (If any): https://app.editage.com

UAT URL: (available or not): No

Audit Methodology: OWASP Top 10 2021 & OWASP Web Security Testing Guide (WSTG)

Tool Used: Burpsuite Professional, Nmap, OSINT Tools, Manual Test Methodologies, Exploit DB etc.

The tested application hosted of the mentioned version is free from any severe vulnerability/threat. The application has passed Critical / High / Medium vulnerabilities for application security assessment tests. For a detailed description of other security assessment-related details, please refer to the audit report shared with (Cactus Communications Ltd).

The application may be hosted with the privilege of read and write access for the public with an exact replica of the audited URL in the production environment.

The Audit was concluded on (23rd January 2024) and the 1st Re-audit was concluded (29th February 2024).

Name: Kandarp Shah
Head of Services & Compliance

Safe to Host Certificate

Date: 25/04/2024

Auditor Name: Mr. Kush Sharma
Reviewed by: Kandarp Shah
E-mail Address: kandarp.shah@indusface.com

Address: A-2/3, 3rd Floor Status Plaza, Akshar Chowk, Atladra Old Padra Road, Vadodara.
Pin – 390020, Gujarat, India.

Project Start: 11/02/2024 **Project Finish:** 24/04/2024.

To whomsoever it may concern

Company Name: Cactus Communications Pvt. Ltd.

Application Name: PaperPal

Purpose of the Application: Paperpal is a comprehensive AI academic writing assistant that empowers authors to write better, faster, and more responsibly. Harnessing 21+ years of STM expertise and trained on millions of language corrections by professional academic editors, Paperpal's AI delivers human precision at machine speed.

Audit Performed on URL: https://edit.paperpal.com/

Production URL (If any): https://edit.paperpal.com/

The tested application hosted of the mentioned version is free from any severe vulnerability/threat. The application has passed Critical / High / Medium vulnerabilities for application security assessment tests. For a detailed description of other security assessment-related details, please refer to the audit report shared with **Cactus Communications.**

The application may be hosted with the privilege of read and write access for the public with an exact replica of the audited URL in the production environment.

The Audit was concluded on 16th Febraury-24 and the 1*st* Re-audit was concluded on 24th April-24.

Name: Kandarp Shah
Head of Services & Compliance

Safe to Host Certificate

Date: 12/02/2024

Auditor Name: Ms. Priyanka Revar
Reviewed by: Kandarp Shah
E-mail Address: priyanka.revar@indusface.com
kandarp.shah@indusface.com
Address: A-2/3, 3rd Floor Status Plaza, Akshar Chowk, Atladra Old Padra Road, Vadodara.
Pin – 390020, Gujrat, India.

Project Start: 04/01/2024 **Project Finish:** 12/01/2024.

To whomsoever it may concern

Company Name: Cactus Communications Ltd

Application Name: Paperpal Preflight.

Purpose of the Application: Preflight can help authors to remedy technical issues and improve language quality which assists you to write, revise, and perfect academic text instantly. It is powered by machine learning and trained on millions of published articles.

Audit Performed on URL: https://preflight.paperpal.com/partner/paperpal/generic
Production URL (If any):
https://preflight.paperpal.com/partner/paperpal/generic

The tested application hosted of the mentioned version is free from any severe vulnerability/threat. The application has passed Critical / High / Medium vulnerabilities for application security assessment tests. For a detailed description of other security assessment-related details, please refer to the audit report shared with **Cactus Communications Ltd.**

The application may be hosted with the privilege of read and write access for the public with an exact replica of the audited URL in the production environment.

Name: Kandarp Shah
Head of Services & Compliance

Safe to Host Certificate

Date: 17/06/2020

Auditor Name: Mr. Suresh Chittimalli
Reviewed by Mr. Tushar Malhotra, Manager, Client Services - Indusface Pvt. Ltd.
E-mail Address: Tushar.malhotra@indusface.com
Address: A-2/3, 3rd Floor Status Plaza, Akshar Chowk, Atladra Old Padra Road, Vadodra. Pin – 390020, Gujrat, India.

Project Start: 05/01/2020 **Project Finish:** 16/06/2020

To whomsoever it may concern

Company Name: **Cactus Communications Ltd.**
Application Name: **CRM (Internal work-flow system)**
Purpose of the Web Application: **Workflow Management**
Audit Performed on Temporary URL: https://crm.cactusglobal.com/
Production URL: https://crm.cactusglobal.com/
The tested application hosted of the mentioned version is free from any severe vulnerability/threat and safe to carry out transaction. The application has passed Critical / High / Medium vulnerabilities for application security assessment tests.
For detailed description of Low severity vulnerabilities and other security assessment related details, please refer to the audit report shared with Cactus Communications Ltd
The application may be hosted with the privileges of read and write access for public with exact replica of the audited URL in the production environment.

Name: Tushar Malhotra
Manager – Client Services, Indusface Pvt Ltd

Vulnerabilities Addressed During Audit

OWASP Top 10

A1 – Injection

SQL injection
LDAP injection
OS commanding
SSI injection
X path injection

A2 – Broken Authentication

Session management
Privilege escalation
Insufficient session expiration

A3 – Sensitive Data Exposure

Test for sensitive data exposure
Testing for critical data management

A4 - XML External Entities (XXE)

Testing for XML external entities

A5 - Broken Access Control

Testing for unauthorized functionality
Insecure data object reference

A6 - Security Misconfiguration

Insecure cryptographic storage, Insufficient transport layer protection, Check for SSL certificate attributes
Misconfiguration of OS, libraries, frameworks etc.

A7 - Cross-Site Scripting (XSS)

Testing for Cross Site Scripting

A8 - Insecure Deserialization

Testing for Insecure deserialization

A9 - Using Components with Known Vulnerabilities

Known vulnerable framework and Library Check for vulnerable software modules, product CVEs

A10 - Insufficient Logging & Monitoring

Secure Communication, API authentication, Data formats, Access control, Injection attack in API,
Insufficient logging and monitoring

Logical Checks

Abuse of Functionality
Insufficient Anti-automation
Insufficient Authentication
Email ids can be harvested for spamming
By Pass Authentication
Insufficient password recovery
Insufficient process validation
Application does not display last
login time
Server-side validation

SANS TOP 25

SQL Injection
OS Command Injection
Cross Site Scripting
Malicious File Upload
Uncontrolled Format String
Integer Overflow or Wraparound
Missing Authentication for Critical
Function
Missing Authorization
Cross Site Request Forgery (CSRF)
Buffer Overflow
Path Traversal
Download of code without integrity
Check
Inclusion of Functionality from Untrusted Control
Sphere
Use of Potentially Dangerous Function
Incorrect Calculation of Buffer Size
Use of Hard-coded Credentials
Missing Encryption of Sensitive Data
Reliance on Untrusted Inputs in a
Security Decision
Execution with Unnecessary Privileges
Incorrect Authorization
Incorrect Permission Assignment
for Critical Resource
Use of a Broken or Risky Cryptographic
Algorithm
Improper Restriction of Excessive
Authentication Attempts
Use of a One-Way Hash without a
Salt

Indusface Defined Checks

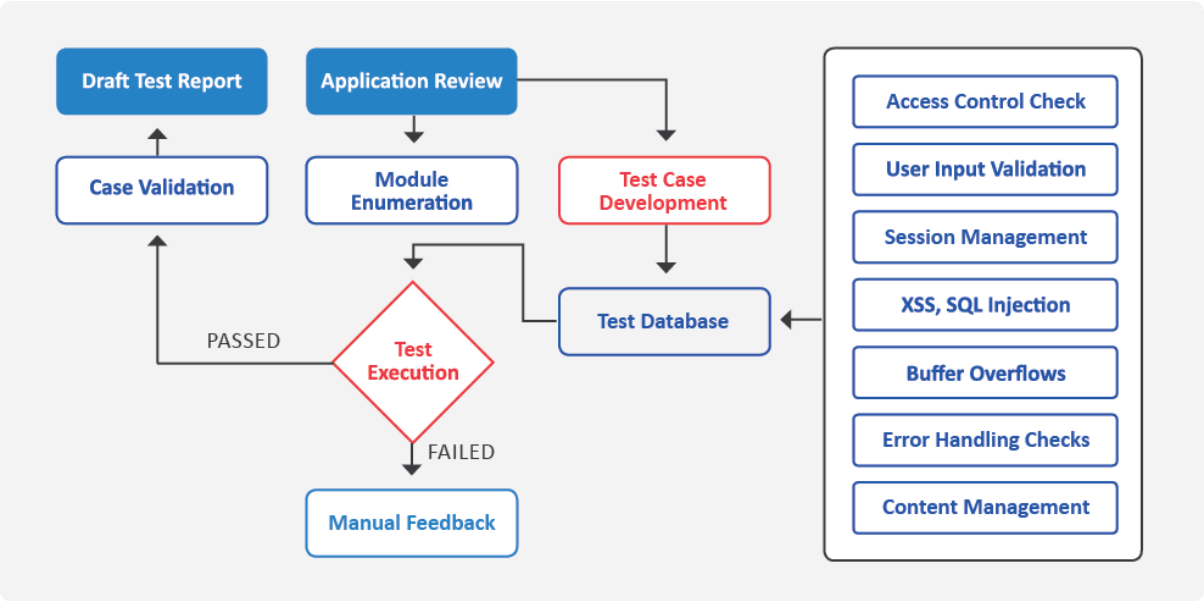
Check for Encoding
Password Auto-Complete
Improper implementation of SSL
(cipher, version)
Service enumeration
Port scanning
Hidden iframe detection
Malicious file can be uploaded on
the server
Steal password from browser memory
Check HTTP methods
Check for cookie attributes

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/Mobile application testing process:



Module Enumeration

Following is 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

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

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.

Application Audit Methodology (Continuation)

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

In order 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

At the end of the assessment, Indusface Application Security Expert will deliver a report on

- 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

Tools Used for Penetration Testing, Vulnerability Assessment & Application Penetration Testing

Following table depicts the partial list of tools used during the Project by IndusFace Pvt Ltd. Information Security Consultants.

Web Applications:

Combination of proprietary tool Indusface WAS, custom scripts and any of the below tools:

Tools	Details
Tamper IE	Http Tamper tool
Paros proxy	A web application vulnerability assessment proxy
WebScarab	A web application vulnerability assessment proxy
Burpproxy	A web application vulnerability assessment proxy
Link checker	Broken Links checker
Real Link checker	Broken Links checker
Crawler	Web Site Crawler
Sam Spade	Multipurpose tool
Indusface WAS	In-house Application scanner tool

Web Applications:

Tools	Details
Netcat	The network Swiss army knife
Nmap	Open source utility for network exploration or security auditing
Hping/Hping2	PingSweep
Firewalk	Firewall Evasion
Superscan	Port Scan
WS_pingpropack	Network Discovery
GetAccount	Windows Accounts Enumeration