OPENIDL

Web Application Pentest

Executive Report

Created On

August 3rd, 2022

Prepared By

ITPEOPLE CORPORATIONS

CONTENTS

Version	Modification	Date	Author
1.0	Initial Report	11/02/2022	Snehil Khare
1.1	Final report after issue remediation	03/08/2022	Snehil Khare

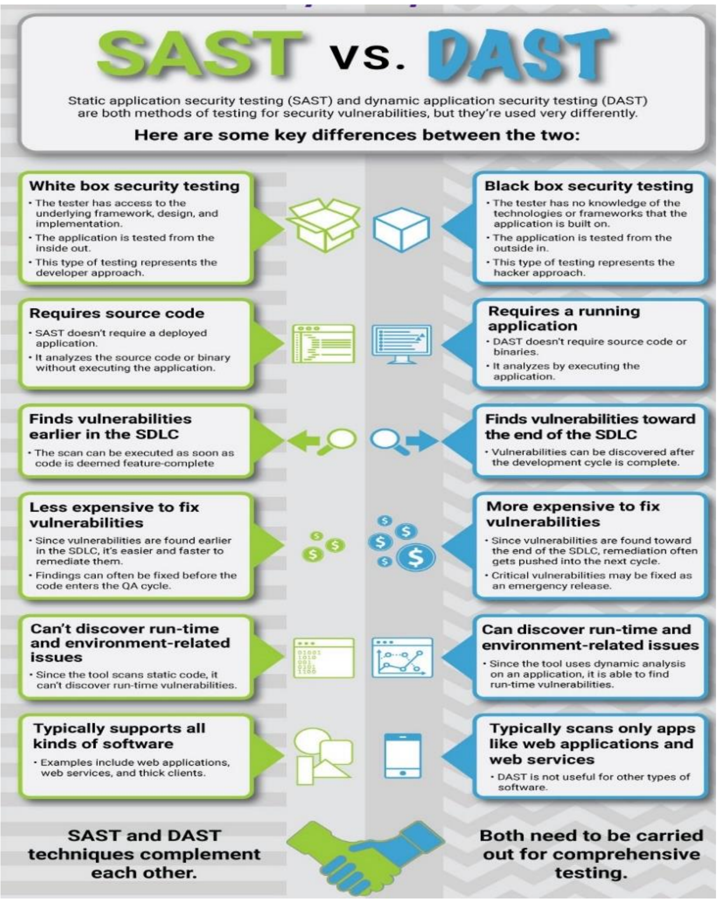
SCOPE SUMMARY

Targets & Scope

The assessment was carried out to understand the existing security posture of OPENIDL application and how it can be abused by a malicious actor to disrupt the operations and compromise critical insurance data of OPENIDL customers.

It was identified during the initial scoping discussion that there are multiple components in place such as RDBMS integration to store & interact with application data, front end and back-end stack and third-party libraries which was incorporated within the application. It was agreed that all the components will be thoroughly tested to ensure no loose ends for data & environment compromise

Target	Category	Scope	Type
https://openidl.dev.openidl.aaisdirect.com/#/login	Frontend & application server	In-Scope	DAST
GitHub - openidl-org/openidl-main	Code repository	In-Scope	SAST



SAST vs. DAST

Static application security testing (SAST) and dynamic application security testing (DAST) are both methods of testing for security vulnerabilities, but they're used very differently.

Here are some key differences between the two:

White box security testing
- The tester has access to the underlying framework, design, and implementation.
- The application is tested from the inside out.
- This type of testing represents the developer approach.

Black box security testing
- The tester has no knowledge of the technologies or frameworks that the application is built on.
- The application is tested from the outside in.
- This type of testing represents the hacker approach.

Requires source code
- SAST doesn't require a deployed application.
- It analyzes the source code or binary without executing the application.

Requires a running application
- DAST doesn't require source code or binaries.
- It analyzes by executing the application.

Finds vulnerabilities earlier in the SDLC
- The scan can be executed as soon as code is deemed feature-complete

Finds vulnerabilities toward the end of the SDLC
- Vulnerabilities can be discovered after the development cycle is complete.

Less expensive to fix vulnerabilities
- Since vulnerabilities are found earlier in the SDLC, it's easier and faster to remediate them.
- Findings can often be fixed before the code enters the QA cycle.

More expensive to fix vulnerabilities
- Since vulnerabilities are found toward the end of the SDLC, remediation often gets pushed into the next cycle.
- Critical vulnerabilities may be fixed as an emergency release.

Can't discover run-time and environment-related issues
- Since the tool scans static code, it can't discover run-time vulnerabilities.

Can discover run-time and environment-related issues
- Since the tool uses dynamic analysis on an application, it is able to find run-time vulnerabilities.

Typically supports all kinds of software
- Examples include web applications, web services, and thick clients.

Typically scans only apps like web applications and web services
- DAST is not useful for other types of software.

SAST and DAST techniques complement each other.

Both need to be carried out for comprehensive testing.

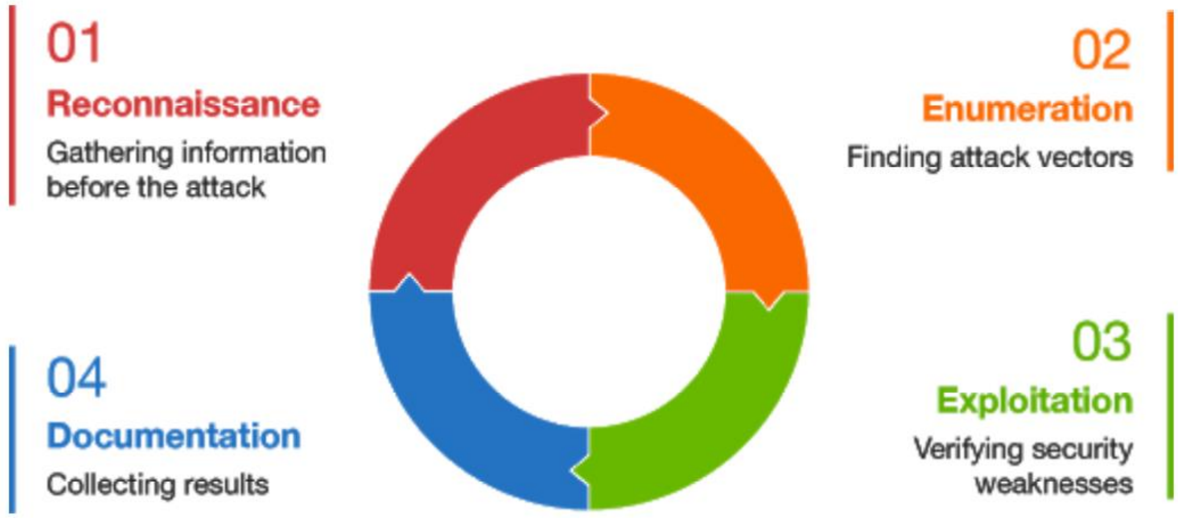
REPORTING & METHODOLOGY

ITPEOPLE CORPORATIONS Pen Test service was designed, and independently assessed by qualified security professionals to ensure alignment with key compliance and regulatory standards

By leading with a best-in-class testing approach, our methodology provides enhanced risk reduction while supporting critical compliance initiatives. A review of these standards follows.

Organizational Methodology Standards

Executing a penetration test involves a proven workflow that is split up into phases. Each one of these phases is executed in a cyclical manner allowing penetration testers to build upon findings and potentially uncover significant risk. An organizational methodology also ensures that high-level coverage of testing is done. When reviewing common organizational methodologies ITPEOPLE CORPORATIONS found similarities in general workflow. ITPEOPLE CORPORATIONS pen testers adhere to these standards in a common workflow outlined below:



Reviewed organizational methodology standards

PCI DSS Requirement 11.2, 11.3.1, 11.3.3, 11.3.4

NIST 800-115 - Technical Guide to Information Security Testing and Assessment 2.1 “Information Security Assessment Methodology”

Open-Source Security Testing Methodology Manual (OSSTMM)

Penetration Testing Execution Standard (PTES)

Operational Methodology Standards

Many penetration testing models fail to provide both results and coverage. In order to bring value to the customer ITPEOPLE CORPORATIONS has reviewed the most common and in-depth Operational Pentest methodologies. Operational methodologies provide detail on what exactly needs to be tested in a security assessment on each endpoint. For external assets the most complete, documented and adhered to methodology is the OWASP Testing Guide Methodology.

Included in the appendix is a detailed table describing checks from this and several other methodologies covered in testing. In order to create a complete testing methodology ITPEOPLE CORPORATIONS has pulled from the following industry standard operational methodologies:

• OWASP Testing Guide (OTG)

• Web Application Hacker Handbook Methodology (WAHHM)

• Others where applicable (SANS Top 25, CREST, WASC, PTES)

OSSTMM
CREST
PTES
Technical Guidelines
The Web Application Hacker's Handbook 2
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
CWE and SANS Institute
TOP 25
MOST DANGEROUS SOFTWARE ERRORS

EXECUTIVE SUMMARY

OPENIDL is open blockchain network that streamlines regulatory reporting and provides new insights for insurers, while enhancing timeliness, accuracy, and value for regulators**.** As a requirement of their business, OPENIDL is responsible for collecting and processing insurance data of their customers.

OPENIDL has a requirement and obligation to ensure that their application is resilient to cyber-attack to protect the data of their customers. To assist with this, OPENIDL employed ITPEOPLE CORPORATIONS to perform a ***Hybrid Penetration Test (HPT) which took place from 1st of Feb 2022 until the 10th of Feb 2022 followed by reporting of identified vulnerabilities to Openidl development team and then conducting retest of application on 08-07-2022 to verify the patches.***

ITPEOPLE CORPORATION'S HPT is an on-demand methodology-driven penetration test that delivers real-time results.

The objective of this assessment was to assess the overall security posture of the application from a grey-box perspective. This includes determining the application's ability to resist common attack patterns and identifying vulnerable areas in the internal or external interfaces that may be exploited by a malicious user.

Throughout the course of this HPT engagement multiple findings were identified and reported to team from different areas which was further verified and fixed on priority basis to strengthen the security posture of application.

Statement of Attestation (03-08-2022)

Security team at ITPEOPLE tested the application in following manner

- DAST (Dynamic application security testing)
- SAST (Static application security testing)

Multiple findings were identified in both the areas, details of which can be read in findings table section of the report.

Findings were reported to Openidl team for remediation and triage. Upon verification and further investigation approved issues were taken into consideration and fixed asap.

ITPEOPLE has verified the robustness of patches and found the fix to be implemented strongly.

Vulnerability ID	Current Status	Date
D001	CLOSED	08/07/2022
D002	CLOSED	08/07/2022
S001	CLOSED	08/07/2022
S002	CLOSED	08/07/2022

The above information represents a point-in-time snapshot of Openidl's overall security posture. Additionally, please note that as of August 03, 2022, all reported issues are fixed.

RISK & PRORITY MARKERS

The following guideline is used to explain how ITPEOPLE CORPORATIONS rates valid vulnerability submissions and their technical severity.

Technical Severity	Example Vulnerability Types
Critical severity submissions (also known as "P1" or "Priority 1") are submissions that are escalated to OPENIDL as soon as they are validated. These issues warrant the highest security consideration and should be addressed immediately. Commonly, submissions marked as Critical can cause financial theft, unavailability of services, large-scale account compromise, etc.	• Remote Code Execution • Vertical Authentication Bypass • XML External Entities Injection • SQL Injection • Insecure Direct Object Reference for a critical function
High severity submissions (also known as "P2" or "Priority 2") are vulnerability submissions that should be slated for fix in the very near future. These issues still warrant prudent consideration but are often not availability or "breach level" submissions. Commonly, submissions marked as High can cause account compromise (with user interaction), sensitive information leakage, etc	• Lateral authentication bypass • Stored Cross-Site Scripting • Cross-Site Request Forgery for a critical function • Insecure Direct Object Reference for an important function • Internal Server-Side Request Forgery
Medium severity submissions (also known as "P3" or "Priority 3") are vulnerability submissions that should be slated for fix in the major release cycle. These vulnerabilities can commonly impact single users but require user interaction to trigger or only disclose moderately sensitive information.	• Reflected Cross-Site Scripting with limited impact • Cross-Site Request Forgery for an important function • Insecure Direct Object Reference for an unimportant function
Low severity submissions (also known as "P4" or "Priority 4") are vulnerability submissions that should be considered for fix within the next six months. These vulnerabilities represent the least danger to confidentiality, integrity, and availability.	• Cross-Site Scripting with limited impact • Cross-Site Request Forgery for an unimportant function • External Server-Side Request Forgery
Informational submissions (also known as "P5" or "Priority 5") are vulnerability submissions that are valid but out-of-scope or are "won't fix" issues, such as best practices.	• Lack of code obfuscation • Autocomplete enabled • Non-exploitable SSL issues

Findings Table

DAST RESULTS

Index	Vulnerability	Vulnerability Category (OWASP TOP 10-2021)	Severity	Status
D001	Aws cognito misconfiguration leading to arbitrary user creation on the cognito user pool which gives attacker UserToken to interact with application.	A5: Security Misconfiguration	**P1**	CLOSED 08/07/2022
D002	Reverse tabnabbing	A5: Security Misconfiguration	**P2**	CLOSED 08/07/2022

SAST RESULTS

Index	Vulnerability	Vulnerability Category (OWASP TOP 10-2021)	Severity	Status
S001	User controlled URL in http client libraries can result in Server-Side Request Forgery (SSRF)	A1: Injection	**P1**	CLOSED 08/07/2022
S002	Multiple cookie issues • Same site attribute missing • Secure path attribute missing • HttpOnly attribute missing	A5: Security Misconfiguration	**P3**	CLOSED 08/07/2022

Conclusion

ITPEOPLE CORPORATIONS Systems

One Copley Parkway, Suite 216,
Morrisville, NC 27560, USA.
Telephone: 919.806.3535

03rd Aug 2022

Introduction

This report shows testing of OPENIDL between the dates of Feb 1st, 2022 – Feb 10th, 2022. The purpose of this assessment was to identify security issues that could adversely affect the confidentiality, integrity & authenticity of OPENIDL. The assessment was performed as per guidelines laid down in OWAS TOP 1O and PTES.

Testing Methods

This security assessment leveraged researchers that used a combination of proprietary, public, automated, and manual test techniques throughout the assessment. Commonly tested vulnerabilities include code injection, cross-site request forgery, cross-site scripting, insecure storage of sensitive data, authorization/authentication vulnerabilities, business logic vulnerabilities, and more.

Current Security Posture

OPENIDL has a strong security posture as of 3rd August 2022. No critical vulnerability was found during the latest assessment.

All the identified issues from the initial assessment stands fixed as of now.