Cyber Security Penetration Test Report

<Company Logo>

Web Application

<Date>

Table of Contents

Executive Summary

Security is not always a simple choice as sometimes it is a balance between security and usability. This Penetration Testing report aims to highlight security concerns and provide plenty of information so the best decision can be made.

The combined list of vulnerabilities by group is below:

Type	Insignificant	Low	Medium	High	Critical
Authentication Result				2	

Introduction

The Cyber Security Penetration test is to identify security vulnerabilities or items of concerns that either does not comply with best practice or could be used either individually or in combination with other items to impact the availability, confidentiality or integrity.

Security is not always a simple choice as sometimes it is a balance between security and usability. This Cyber Security Penetration Testing Report aims to highlight security concerns and provide recommendations based on the gathered information to balance security and usability. This means recommendations may be less secure in order to avoid impacting usability.

It is worth understanding the complexity of components in security. Some security controls may individually have minimal or limited security improvement; however, the combination of the security controls provide a significant amount of defense. Furthermore, each security control may have weaknesses individually that allow it to be defeated but combined with multiple security controls it can provide secure protection. This approach is called Defense in depth and the reason layers of controls are recommended.

Scope

Organization	
Test Type	
Application	
URL	
Date Tested	

Penetration Testing Result

1. Authentication Security

Authentication is important as it is the method of securing a user account and their data. Authentication has many aspects such as the login of users and the session used to keep them logged in.

1.1. Insecure Direct Object Reference

Impact	Risk	Fix Effort
High	High	High

Vulnerability	Insecure Direct Object Reference
Reason	Is a vulnerability that arises when attackers can access or modify objects by manipulating identifiers used in a web application's URLs or parameters.
Action	1. GET - /invoices/id/[invoices_id] 2. POST - /xendit/create By changing the parameters in each API end point. You can access and modify other user's data.
Further Information	https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html
Evidence	
Status	Pending

Notes and Legal

1. Recommendation

Before implementing any actions, appropriate impact assessment and testing should be performed to ensure no existing functionality is impacted. Many changes will require a restart of the service or server to apply to ensure this occurs to properly identify any issues early. All actions should be implemented unless they impact with any functionality.

2. Re-penetration Testing

Once the key vulnerabilities have been corrected it is important to initiate a re-testing to ensure they have been correctly closed. Furthermore, testing should be performed regularly after code changes or at least annually to help identify considerable bugs.

3. Legal

This report provides no promises that the penetration testing finds all, or even substantially all vulnerabilities, misconfigurations, security concerns, information, evidence, causes of the incident or security best practices. The person/s providing "Permission for Investigation" takes full Ownership and liability for any "harm" or "damage" resulting from the investigation activity including ordinary, third-party, other systems but also consequential and incidental associated with conducting the investigation and other activities associated including this report.