

# SecureLayer7

Time and Again, Securing you



## Product Name Web Application

### Vulnerability Assessment and Penetration Testing Report

## Disclosure Statement

This document is subject to the terms and conditions of a non-disclosure agreement between SecureLayer7 and **Company Name**.

SecureLayer7 Technologies Private Limited has prepared this confidential document for the customer. This document shall be treated at all times as confidential. Portions of this document and the templates used in its production are SecureLayer7 Technologies Private Limited's property. No part of this document may be reproduced, copied, or modified (in whole or part) without SecureLayer7 Technologies Private Limited's or customer's consent.

While precautions have been taken in preparing this document, SecureLayer7 Technologies Private Limited, the publisher, and the author(s) assume no responsibility for errors, omissions, or damages resulting from the use of the information contained herein.

North America | South Asia | Middle-east  
00919762001337 | info@SecureLayer7.net | SecureLayer7.net

## Table of Contents

<b>Disclosure Statement.....</b>	<b>2</b>
Document Stakeholders .....	4
Document Version History.....	4
<b>Executive Summary .....</b>	<b>5</b>
<b>Objective .....</b>	<b>5</b>
<b>Scope .....</b>	<b>5</b>
<b>Penetration Test Details: .....</b>	<b>5</b>
<b>Disclaimer and Limitations.....</b>	<b>6</b>
<b>Penetration Testing Process .....</b>	<b>7</b>
<b>Approach and Methodology.....</b>	<b>7</b>
Identification of Vulnerabilities: .....	8
<b>Attack Narrative: .....</b>	<b>9</b>
<b>Graphical Representation of Vulnerabilities:.....</b>	<b>11</b>
<b>Summary of Key Findings .....</b>	<b>12</b>
<b>Detailed Finding .....</b>	<b>13</b>
1. #IIOG6Z Privilege Escalation Leads to Account Owner Disable via Low Data Owner User Account .....	13
<b>General Comments and Security Advice .....</b>	<b>15</b>
Implement Centralized Filtering Method Potential .....	15
Source Code Audit .....	15
<b>Conclusion and Roadmap .....</b>	<b>16</b>

## Document Details

### Document Stakeholders

Role	Name of Stakeholder	Designation
Reviewer - SecureLayer7	Stack holder 1	Service Delivery Head, SecureLayer7
Reviewer - SecureLayer7	Stack holder 2	CTO, SecureLayer7
Reviewer – <b>Company Name</b>	Customer 1	CEO, <b>Company Name</b>

### Document Version History

Document Version	Comment	Date
1.0	Final Report	10 <sup>th</sup> December 2022

## Executive Summary

The SecureLayer7 team inclusive of 1 Penetration Tester, 1 Team Lead, and 1 Project Manager, were allocated to accomplish this assessment. Penetration testers along with the team lead are accountable for the identification, analysis, and evaluation of the security issues found during the testing. The Project Manager is responsible for the project plan, project monitoring & controlling project documentation, and providing high-quality deliverables. This assessment was performed remotely by the SecureLayer7 team, and the assessment started on 1<sup>st</sup> December 2022 and concluded on 9<sup>th</sup> December 2022. The SecureLayer7 team and the **Company Name** team decided to use the grey box penetration testing methodology and approach for this assessment.

The tests were carried out by identifying vulnerabilities with the intent of gaining access to critical information. The objective of performing this activity was to assess the security risks associated with the developed application and service and identify vulnerabilities that could be leveraged by cybercriminals to compromise the application and its services.

The security test results and findings provided in this report are valid for the period during which the assessment was carried out and are based on the information provided for the assessment. The findings in this report reflect the conditions found during the assessment and do not necessarily reflect current conditions.

During the penetration testing, SecureLayer7 reported 06 different vulnerabilities which include the following:

- **High:** 01
- **Low:** 05

## Objective

The purpose of this assessment was to:

1. Test the Company Name Web Application to identify technical vulnerabilities and discover whether an attacker may leverage these flaws to compromise the security of Company Name Web Application.
2. Provide recommendations for risk mitigation that may arise on successful exploitation of these vulnerabilities.

## Scope

Following digital assets are considered as the scope of work. The security assessment was performed using the below scope information and agreed upon by the client.

Scope Details
<b>Company Portal</b> <a href="https://securelayer7">https://securelayer7</a> <a href="https://api.securelay">https://api.securelay</a>

## Penetration Test Details:

Activity Date(s)	1 <sup>st</sup> December 2022 – 7 <sup>th</sup> December 2022
------------------	---

## Disclaimer and Limitations

No major blockers were encountered for accessing the application. SecureLayer7 does not constitute any form of representation, warranty, or guarantee that the systems are 100% secure from every form of a cyber-attack. While SecureLayer7's methodology includes both automated and manual testing to identify and attempt exploitation of the most common security issues, testing was limited to an agreed-upon timeframe. The application was tested for all known vulnerabilities or public vulnerabilities and not every vulnerability may be identified.

1. Denial of service issues that could potentially disrupt the Client environment was not tested.
  - A. SecureLayer7 did not test vulnerabilities that would intentionally lead to denial of service issues in an effort to prevent operational disruptions to the Client environment.
2. Social Engineering
  - B. Social Engineering attacks were not in scope for this assessment.

## Penetration Testing Process

SecureLayer7 follows a penetration testing methodology that aligns with industry best practices including the following:

- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment of Federal Information
- OWASP Top Ten and OWASP ASVS 4.0.2
- Penetration Testing Execution Standard (PTES)
- Payment Card Industry Information Supplement: Requirement 11.3 Penetration Testing

SecureLayer7 Vulnerability Assessments and Penetration tests are scaled to meet the needs of the organization and help the organization in identifying the high business risk vulnerabilities in the provided scope of work.

## Approach and Methodology

The assessment was completed as per SecureLayer7's proprietary standard security best practices including OWASP, SANS, and NIST standards and frameworks. SecureLayer7 penetration testing is scaled to meet the needs of the organization and helps the organization identify the high business risk vulnerabilities in the given scope of work. The below section describes the approach and methodology followed during the penetration testing.

The general overview of our methodology is as follows:



The OWASP Top Ten/ OWASP ASVS 4.0.2 list of vulnerabilities that are included for this pentest assessment:

- A01:2021 - Broken Access Control
- A02:2021 - Cryptographic Failures
- A03:2021 - Injection
- A04:2021 - Insecure Design
- A05:2021 - Security Misconfiguration
- A06:2021 - Vulnerable and Outdated Components
- A07:2021 - Identification and Authentication Failures
- A08:2021 - Software and Data Integrity Failures
- A09:2021 - Security Logging and Monitoring Failures
- A10:2021 - Server-Side Request Forgery

#### Identification of Vulnerabilities:

SecureLayer7 uses industry frameworks such as OWASP ASVS 4.0, SANS, NIST 800-115, and out of box test cases for identifying the critical to low vulnerabilities in the agreed scope of work. Company Name can be sure that the most recent and common web application vulnerabilities are identified during the penetration testing.

#### Evaluation of Vulnerability:

After understanding the vulnerability next step is to evaluate or rank the vulnerability by determining the risk magnitude, which is the combination of likelihood and consequence. Evaluate the vulnerability on the 5-level Severity scale from Informational, Low, Medium, High and Critical. In addition, the report also provides but is not limited to decisions about whether the vulnerability is acceptable or whether it is serious enough to warrant treatment.

The following priority matrix was used to classify the structure of assessment findings:

Priority Level	Severity Scale	CVSS Score	Description of Vulnerability
P1	Critical	9.0-10.0	Vulnerabilities that affect all users of the platform, and/or affect the security of the platform or host system(s).
P2	High	7.0-8.9	Vulnerabilities that affect more than one user of the platform, and that require little or no user interaction to trigger.
P3	Medium	4.0-6.9	Vulnerabilities that affect more than one user but may also require interaction or a specific configuration.
P4	Low	0.1-3.9	Issues that affect individual users and require interaction or significant prerequisites (MITM) to trigger.
P5	Informational	0.0	Issues that leaking very basic information which might lead to information disclosure.



## Attack Narrative:

### Overview

This document provides information on the narrative and description of the weaknesses which were exploited to gain unauthorized access to sensitive data or protected systems in the Client environment via Web Application Penetration Testing. The intent was to closely simulate an adversary and provide sufficient details to Company Name Team.

### Research and Exploitation

The information below describes the tests and coverage achieved for the Web Application Penetration Testing of the given Product Application scope. The section comments on enumerated approaches taken to investigate various components and areas of the items in scope. SecureLayer7 began the Web Application Penetration Test by passively reviewing the application's underlying public infrastructure and architecture. The following are the details of the testing:

### Scope URLs:

In an attack scenario, the application was tested for an unintended proxy issue, such as blind server-side request forgery adding the Burp collaborator link in the Referrer header. This attack aimed to check and observe whether the application backend validates the request via the Referrer header value by interacting with it to check whether any hit back onto the Burp collaborator client. If it happens, then open ports and services can be enumerated using this scenario. SecureLayer7 did not observe any hit back from the server, and the server returned the 200 Ok onto the burp collaborator client, invalidating any test scenario for blind server-side request forgery.

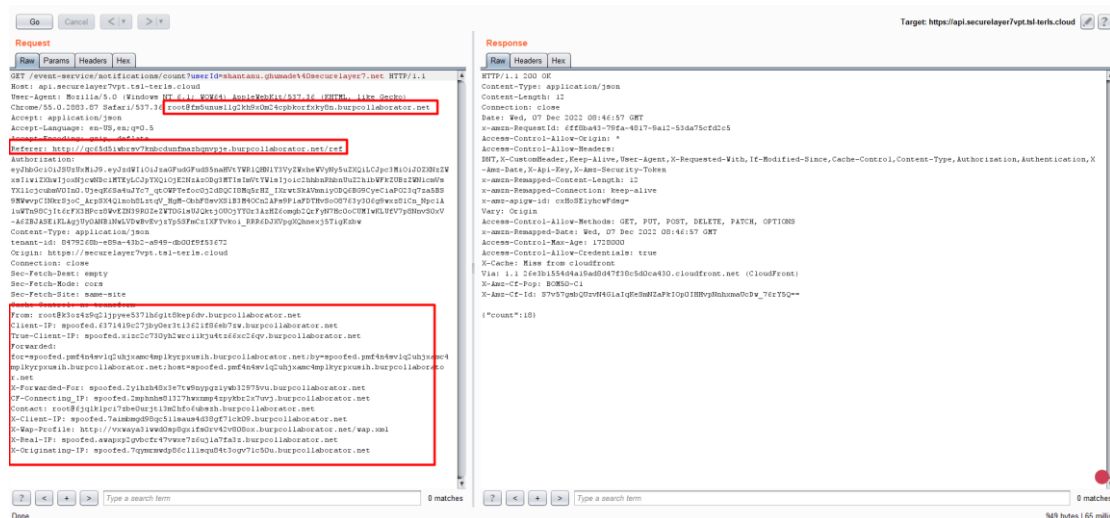
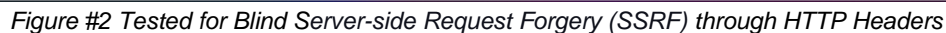


Figure #1 Tested for Blind Server-side Request Forgery (SSRF) through HTTP Headers



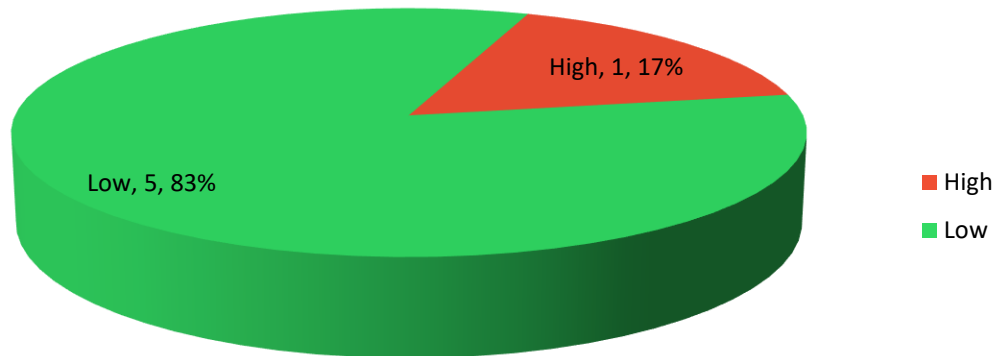
Summarizing the attack narrative, SecureLayer7 used the Burp Proxy Suite of tools to record, intercept, and replay the requests to the application. Once the application had been mapped out with general requests, Burp was also used to identify the classic vulnerabilities.

As for the approach chosen for the assessment, the involved parties agreed upon the benefits of a Grey Box methodology. This means that the SecureLayer7 team was provided full access to all relevant infrastructure. With this focus and scope in mind, SecureLayer7 conducted extensive tests against Tessell Web application running on these. It should also be noted that the parts of the software involving web front ends were specifically tested and checked for Blind Server-side Request Forgery (SSRF) through HTTP Headers, CRLF Injection, Insufficient Session Expiration, Information Disclosure via Directory Bruteforce, Cross-site Request Forgery, Unrestricted File Upload, Privilege Escalation, Cross-Site Scripting (XSS), SQL Injection, Unauthenticated Access on Ticket Files, Account Takeover via Set New Password, Sensitive Information Disclosure via JS Files, and similarly dangerous attacks.

The pentest activities began the engagement by using the application the same way a typical user would. This exercise was proxied through the Burp Suite proxy and included passive analysis for identification of any misconfigurations and various different vulnerabilities. By visiting each page, SecureLayer7 created a record of the Application in the Burp Suite proxy for use with manual and automated testing techniques later in the engagement.

## Graphical Representation of Vulnerabilities:

This section highlights the graphical representation of the vulnerability severity discovered during the assessment:



## Summary of Key Findings

The assessment uncovered several security flaws and some of them required urgent attention.

Finding ID #	Vulnerability Title	Severity Level	CVSS Score	Status
#IIOG6Z	Privilege Escalation Leads to Account Owner Disable via Low Data Owner User Account	High	7.1	Open
#TAVX49	Missing of Strict Transport Security Response Header	Low	3.7	Open

## Detailed Finding

The below sections list the detailed technical description of the identified vulnerabilities, possible mitigation strategies with references, security risk, and step-by-step details to reproduce the vulnerabilities.

### 1. #ILOG6Z Privilege Escalation Leads to Account Owner Disable via Low Data Owner User Account

Description
The application is vulnerable to privilege escalation vulnerability on the application IAM user module. This vulnerability allows an attacker to disable an account owner account via the low-level user role of Data Owner, which doesn't intend to happen.

CVSS	Vector String	Risk Rating
7.1	3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N	High

Module Name	Affected Resource
<ul style="list-style-type: none"><li>Sample</li></ul>	<a href="https://securelayer">https://securelayer</a>

Security Risk
<p>The security impact of this vulnerability is reported as <b>High</b>, considering the exploitability. The following are the considerable security impacts:</p> <ul style="list-style-type: none"><li>Low-Level users Data Owner users can perform high-privilege actions via low-level user permission.</li><li>Data owner users can disable any user account with a privilege escalation vulnerability.</li></ul>

Workaround/Mitigation
<p>It is strongly recommended to fix this vulnerability and implement the following:</p> <ul style="list-style-type: none"><li>Validate user permissions before giving access to resources.</li><li>Redirect the user to the home page /login page if they try to access a high-privilege endpoint.</li></ul>

References
<a href="https://capec.mitre.org/data/definitions/233.html">https://capec.mitre.org/data/definitions/233.html</a>

Proof of Details(POC)

## General Comments and Security Advice

### Implement Centralized Filtering Method Potential

It is recommended to use a centralized filtering method for all values that can be tampered by adversaries and actors other than the potentially affected user. This holds for the user name, the conversation name as well as values being sent by a potentially rogue communication server instance. The instances might be tampered with by motivated attackers. Therefore, a centralized filter tool that would continuously ensure proper output filtering for any incoming byte-string is urged, as it would assist in keeping the Application and any upcoming versions of the tool as safe and secure as possible.

### Source Code Audit

Source Code Audit/Review is a process to identify source code errors and find the un-sanitized portions in the source code of the application which can be a threat to the application security and can compromise the application and user information.

Our innovative methodology to audit source code for an application provides a comprehensive framework to identify the flaws and security issues inside the code of the application. In our source code audit methodology, we don't rely only upon the automated tools for the code audits. We do automate as well as manual source code review to cover all the problematic areas of the code. We at SecureLayer7 ensure the thorough auditing and reviewing of the source code of the application according to the defined standard

## Conclusion and Roadmap

The primary goals of this penetration test were to identify whether or not the **Product name** Web Application has adequate controls in place to protect against unauthorized access to sensitive information by both external and internal attackers and to identify any vulnerabilities that could present a risk to **Company Name** or its customers. To achieve these goals, we performed an extensive array of tests, using both manual techniques and commercial scanning tools in order to paint a comprehensive picture of the application's security posture. We conclude the target application security posture as below:

Application	Overall Security Posture
<b>Product Name</b>	Medium

In the above table, the overall security posture is calculated at medium level for the scope application service. This evaluation depends upon the vulnerability impact on the business objectives.

It should be noted that this was a point-in-time assessment and that **Company Name** Team should perform regular security assessments as changes are made to the application and supporting infrastructure. The actual risk posed by these findings may be less than what is indicated due to mitigating factors such as use case, technical, and administrative controls.