Web Penetration Testing Report

Report For :

Organization Name	:	SampleCorp LLC
Report Date	:	Jan 23rd 23

Report By :

Organization Name	:	Xiarch Solutions Pvt Ltd
Report Date	:	Jan 23rd 23
Address	:	Suite 352, 2nd floor, Tarun, Outer Ring Road, Pitampura, New Delhi, Delhi 110034
Tel	:	+91-999999999
Email	:	info@xiarch.com
Web	:	www.xiarch.com

Disclaimer

All the information contained in this document is confidential to said company, disclosure and use of any information contained in this document by photographic, electronic or any other means, in whole or part, for any reason other than security enhancement is strictly prohibited without written consent of auditee organization.

Whilst all due care and diligence has been taken in the preparation of this document it is not impossible that document of this nature may contain errors or omissions because of a misunderstanding of Clients requirements. Any recommendations are made in good faith as guidelines to assist the client in evaluation and must not be construed as warranties of any kind. Findings in this report are based on various tests conducted using manual techniques and third-party tools and Xiarch Solutions Pvt Ltd has put its best efforts to eliminate all the false positives reported by these tools.

Xiarch Solutions Pvt Ltd shall assume no liability for any changes, omissions, or errors in this document. Xiarch Solutions Pvt Ltd shall not be liable for any damages financial or otherwise arising out of use/misuse of this report by any general member of public.

Table Of Content

1. Document Control

2. Introduction

3. Scope

4. Terms, Definition & Legends

This section describes the format in which the identified vulnerabilities are reported in the later section of the report. “Vulnerability Table” shown below is used to provide the details of the vulnerability, its impact and the recommendations.

4.1 Vulnerability Table

1. Title of the Vulnerability	
Risk Level	
Description :	
Impact :	
Recommendations :	
Affects :	
Status	

Title of the Vulnerability	-	A short title that describes the vulnerability
Risk Level	-	It describes the risk level. The title bar of each vulnerability table is colour coded for quick identifications of the severity level of the vulnerabilities
Description	-	It provides a brief description of the vulnerability.
Impact	-	Describes the probable impact if the vulnerability is successfully exploited.
Recommendations	-	Provide the recommendations to fix the vulnerability.
Affects	-	Provide the information where vulnerability is present.
Status	-	Provides the information whether the vulnerability is closed or not.

4.2 Findings Ranking System

In order to prioritize the assessment results, each finding was categorized based on severity classifications. Final analysis of the risk or impact to the application will require an internal evaluation. Xiarch Labs has developed classifications using the severity nomenclature for ranking the issues identified within the various severity categories.

4.2.1 Severity Categories

Based on Xiarch Lab analysis of the particular finding and assets affected, a finding will fall into one of the following severity level categories:

Critical Vulnerabilities require an immediate response through mitigating controls, direct remediation or a combination thereof. Exploitation of critical severity vulnerabilities results in privileged access to the target system, application or sensitive data and enables further access to other hosts or data stores within the environment. Findings with a critical ranking will cause significant losses when they are exploited, although the total cost is difficult to quantify in advance. In general, a critical severity ranking is warranted when the issue has a direct impact on regulatory or compliance controls imposed on the environment, accesses personally identifiable information (PII) or financial data or could cause significant reputational or financial harm.

High Findings with a high severity ranking require immediate evaluation and subsequent resolution. Exploitation of high severity vulnerabilities leads directly to an attacker gaining privileged, administrative-level access to the system, application or sensitive data. However, it does not enable further access to other hosts or data stores within the environment. If left unmitigated, high severity vulnerabilities can pose an elevated threat that could affect business continuity or cause significant financial loss.

Medium A finding with a medium severity ranking requires review and resolution within a short time. From a technical perspective, vulnerabilities that warrant a medium severity ranking can lead directly to an attacker gaining non-privileged or user-level access to the system, application or sensitive data. Findings that can cause a denial-of-service (DoS) condition on the host, service or application are also classified as medium risk. Alternately, the vulnerability may provide a way for attackers to gain elevated levels of privilege. From a less technical perspective, observations with this ranking are significant, but they do not pose as much of a threat as high or critical severity exposures.

Low Low severity findings should be evaluated for review and resolution once the remediation efforts for critical, high and medium severity issues are complete. From a technical perspective, vulnerabilities that warrant a low severity ranking may leak information to unauthorized or anonymous users used to launch a more targeted attack against the environment. From a process perspective, observations with this ranking provide awareness and should be addressed over time as part of a comprehensive information security program, but do not presently pose a substantial threat to business operations or have any significant loss associated with the exposure.

Informational An informational finding presents no direct threat to the confidentiality, integrity or availability of the data or systems supporting the environment. These issues pose an inherently low threat to the organization and any proposed resolution should be considered as an addition to the information security procedures already in place.

5. Assessment Methodology

6. Executive Summary

7. Assessment Findings Overview

The table below provides a summary of the assessment findings categorized by group and ranked by severity. The table provides an overview of all of the findings from the assessment and allows the remediation team to focus efforts on the areas of highest severity as determined by Xiarch Labs. Click the individual link below to go directly to that finding.

S. No.	Vulnerability Title	Severity	Status

8. Assessment Findings Details

9. Tools & Reference