**Genpact Internal Penetration Testing Report**

**PCI DSS Re-Certification**

**Asahi Beverages Badshahpur**

**WFO + WFH Environment**

**Nov’2021**

The assessment is performed in two distinct stages,

# Vulnerability Assessment

This stage identifies the security issues considered to be the 'low hanging fruit' and lays the foundations for the manual assessment.

The following objectives are included as part of the vulnerability assessment.

* Identification of open ports
* Fingerprinting of operating system and service versions
* Identification of software (missing patch) related vulnerabilities

# Penetration Testing

This stage manually confirms vulnerabilities and identifies additional security issues that are only highlighted when hosts are compromised.

The following objectives were included as part of the Penetration Test. This list is not exhaustive.

* Identification of application configuration vulnerabilities
* Analysis of network traffic
* Identification of high-level Web application vulnerabilities
* Assessment of infrastructure devices
* Password strength analysis
* Assessment of database access restrictions
* Assessment of sensitive information disclosure vulnerabilities

# Assessment Scope

## Assessment Drivers

The results of this assessment will form the basis for retests, remediation actions and spearhead a continued improvement in overall information security.

## Submitted Scope



# Testing Methodology

This is the assessment methodology that is followed by our testing team.

The testing consists of four phases. These phases start with the PCI requirements and it finishes the results back to the Owner, along with any recommendations for remedial action. These four steps are:

1. Initial Scooping
2. Assessment
3. Reporting
4. Presentation

Assessment results are used to support the determination of security control effectiveness over time.

This publication addresses technical testing and examination techniques that can be used to identify, validate, and assess technical vulnerabilities and assist organizations in understanding and improving the security posture of their systems and networks.

Security testing and examination is required by many regulations. It is not meant to take the place of implementing security controls and maintaining system security, but to help organizations confirm that their systems are properly secured and identify any organization security requirements that are not met as well as other security weaknesses that should be addressed.

# Information Security Assessment Methodology

A repeatable and documented security assessment methodology is beneficial in that it can:

* Provide consistency and structure to security testing, which can minimize testing risks
* Expedite the transition of new assessment staff
* Address resource constraints associated with security assessments

### Planning

Critical to a successful security assessment, the planning phase is used to gather information needed for assessment execution—such as the assets to be assessed, the threats of interest against the assets, and the security controls to be used to mitigate those threats—and to develop the assessment approach. A security assessment should be treated as any other project, with a project management plan to address goals and objectives, scope, requirements, team roles and responsibilities, limitations, success factors, assumptions, resources, timeline, and deliverables.

### Execution

Primary goals for the execution phase are to identify vulnerabilities and validate them when appropriate. This phase should address activities associated with the intended assessment method and technique. Although specific activities for this phase differ by assessment type, upon completion of this phase assessors will have identified system, network, and organizational process vulnerabilities.

### Post-Execution

The post-execution phase focuses on analysing identified vulnerabilities to determine root causes, establish mitigation recommendations, and develop a final report.

# Management Summary

No Critical Vulnerabilities appeared during the test, team was not able to find any vulnerability on the systems, servers were not be able to be compromised , all systems were correctly patched and well protected with the latest updates installed.

The report found to be Compliant with PCI DSS Requirements for Penetration testing.

# Identified Vulnerability Details

The following pages cover all identified vulnerabilities – if exist- along with remediation advice and any evidence gathered during the assessment. Each will include a 'RISK' rating and a 'CVSS' score in order that any identified issues can be prioritized. Genpact sort these issues by severity, so that the more significant issues can be seen first. The following sections cover each vulnerability from a CVSS score of 0.1 to 10.

* Summary - A breakdown of the vulnerability, any affected services and operating systems and any other pertinent information. The summary section may also include a proof of concept screenshot as evidence of the identified issue, though it may not always be feasible to include this.
* Business Impact & Exposure - This section covers the potential ramifications should an attacker successfully exploit the issue. As an example, this section could have indicated whether the system could be fully compromised or not.
* Vulnerability Evidence - The vulnerability evidence could be service or software versions which were found in use on the system, and any fixed version that may be available. There may not always be further evidence available dependent on the type of issue found.
* Remediation - Any available remediation advice will be covered under this heading. This could range from operating system patching to configuration changes. This section will often contain links to vendor security update sites so that any relevant patches can be downloaded. Any remediation should be undertaken with great care. This can mean testing the suggestions on systems that are not live, testing the advice out of hours, or testing on virtual images of live hardware.
* External References - All vulnerabilities identified will have external references available. One of the most prevalent is the CVE or 'Common Vulnerabilities & Exposures'.
* Affected Hosts - The affected hosts table lists all hosts and ports on which the vulnerability was identified.
* Report Navigation - A list of identified vulnerabilities per host can be located in the 'Identified Vulnerability Summary Table (if exist).

# Running Services Assessment

During this stage the team performed a port mapping and manual verification for the systems in scope to identify any weak protocol or unused services.

No weak protocols detected, services are protected and secured with proper access list and segmentation

Vulnerability Assessment / Penetration Test

# No vulnerability noted

# Conclusion:

Performing a thorough penetration test security assessment is a complex task which should be approached like any other software analysis – with a methodology, testing procedures, skills, knowledge and accept a vast amount of input from users, in many different locations. This requires the person assessing the application to go over each script and each parameter, and to test it for numerous possible security flaws.

Once applying the remediation instruction for each finding (if exist) in this report, the risk will be reduced and protect against any attacks and the environment will be secured.

# Appendix A - Explanation of Severities

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Two common uses of CVSS are prioritization of vulnerability remediation activities and in calculating the severity of vulnerabilities discovered on one's systems. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

The five tiers of the used model are CRITICAL, HIGH, MEDIUM, LOW, and Informational.

|  |  |
| --- | --- |
| Severity | CVSS v2.0 Base Score |
| Critical | 10 |
| High | 7.0 - 9.9 |
| Medium | 4.0 - 6.9 |
| Low | 0.0 - 3.9 |
| Informational | N/A |