List of tools used:



1. Vulnerability Name

|  |  |
| --- | --- |
| **Critical Risk** | |
| **Likelihood** | Likely |
| **Impact** | Severe |
| **Remediation** | Hard |

Affected Scope



Description

Description of the vulnerability

Steps to Reproduce

How you determined there was a vulnerability, what you saw, proof of concept, detailed steps

Technical Impact

Technical consequences that would result due to exploitation.

Business Impact

Business consequences that would result due to exploitation.

Remediation Recommendation

Sdffsdafsdfsdfsdaf

References

Ref 1

END OF FINDING

1. High Vulnerability

|  |  |
| --- | --- |
| **High Risk** | |
| **Likelihood** | Possible |
| **Impact** | Severe |
| **Remediation** | Hard |

Affected Scope



Description

Description of the vulnerability

Steps to Reproduce

How you determined there was a vulnerability, what you saw, proof of concept, detailed steps

Technical Impact

Technical consequences that would result due to exploitation.

Business Impact

Business consequences that would result due to exploitation.

Remediation Recommendation

Sdffsdafsdfsdfsdaf

References

Ref 1

END OF FINDING

1. Medium Vulnerability

|  |  |
| --- | --- |
| **Medium Risk** | |
| **Likelihood** | Unlikely |
| **Impact** | Severe |
| **Remediation** | Hard |

Affected Scope



Description

Description of the vulnerability

Steps to Reproduce

How you determined there was a vulnerability, what you saw, proof of concept, detailed steps

Technical Impact

Technical consequences that would result due to exploitation.

Business Impact

Business consequences that would result due to exploitation.

Remediation Recommendation

Sdffsdafsdfsdfsdaf

References

Ref 1

END OF FINDING

1. Low Vulnerability

|  |  |
| --- | --- |
| **Low Risk** | |
| **Likelihood** | Unlikely |
| **Impact** | Moderate |
| **Remediation** | Hard |

Affected Scope



Description

Description of the vulnerability

Steps to Reproduce

How you determined there was a vulnerability, what you saw, proof of concept, detailed steps

Technical Impact

Technical consequences that would result due to exploitation.

Business Impact

Business consequences that would result due to exploitation.

Remediation Recommendation

Sdffsdafsdfsdfsdaf

References

Ref 1

END OF FINDING

1. Informational Vulnerability

|  |  |
| --- | --- |
| **Informational Risk** | |
| **Likelihood** | Unlikely |
| **Impact** | Minor |
| **Remediation** | Hard |

Affected Scope



Description

Description of the vulnerability

Steps to Reproduce

How you determined there was a vulnerability, what you saw, proof of concept, detailed steps

Technical Impact

Technical consequences that would result due to exploitation.

Business Impact

Business consequences that would result due to exploitation.

Remediation Recommendation

Sdffsdafsdfsdfsdaf

References

Ref 1

END OF FINDING

## Risk Matrix

TEAM-## utilized the following 3x3 risk matrix for determining the severity level of each finding uncovered during the assessment. After determining the impact and likelihood classifications for the finding, they are used to select the appropriate severity level based on the risk matrix.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | **Impact** | | |
|  |  | Severe | Moderate | Minor |
| **Likelihood** | Likely | Critical | High | Medium |
| Possible | High | Medium | Low |
| Unlikely | Medium | Low | Informational |

## Classification Definitions & Scales

TEAM-## utilized the following definitions and scales for classifying impact, likelihood, and remediation for each finding.

### Impact

**Definition:** With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII.

|  |  |
| --- | --- |
| **Scale** | **Description** |
| Severe | Successful exploitation of the vulnerability may result in wide-spread disruption of critical business functions and significant financial damage. |
| Moderate | Successful exploitation of the vulnerability may cause significant disruptions to non-critical business functions. |
| Minor | Successful exploitation of the vulnerability may affect a few users without causing much disruption to routine functions. |

### Likelihood

**Definition:** A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.

|  |  |
| --- | --- |
| **Scale** | **Description** |
| Likely | Exploitation methods are well-known and can be performed with minimal difficulty using publicly available tools. |
| Possible | Exploitation methods are well-known and may be performed using public tools with configuration changes. Understanding of the underlying system is required for successful exploitation. |
| Unlikely | Exploitation requires deep understanding of the underlying system or advanced technical skills. Precise conditions may be required for successful exploitation. |

### Remediation

**Definition:** The act of mitigating a vulnerability or a threat.

|  |  |
| --- | --- |
| **Scale** | **Description** |
| Hard | Remediation may require extensive reconfiguration of the underlying systems and disruption of normal business functions. |
| Medium | Remediation may require minor reconfigurations or additions that may be time-intensive or expensive. |
| Easy | Remediation may be accomplished within a short amount of time and with little difficulty. |