Elizabeth Velikova Koleva

Security Assessment Report

Penetration Test

Active Information Security 2023/2024

Report Issued: 10.01.2024

## Confidentiality Notice

*This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to AIS (Ivan Zlatanov) or facilitate attacks AIS (Ivan Zlatanov). Elizabeth Velikova Koleva shall not be held liable for special, incidental, collateral, or consequential damages arising out of the use of this information.*

## Disclaimer

*Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made on AIS (Ivan Zlatanov)’s environment. Any changes made to the environment during the period of testing may affect the results of the assessment.*

**TABLE OF CONTENTS**

[Confidentiality Notice 2](#_Toc155741640)

[Disclaimer 2](#_Toc155741641)

[1. Introduction 5](#_Toc155741642)

[1.1 Purpose 5](#_Toc155741643)

[1.2. Scope of this risk assessment 5](#_Toc155741644)

[2. Risk Assessment Approach 5](#_Toc155741645)

[2.1 Participants 5](#_Toc155741646)

[2.2 Techniques Used 6](#_Toc155741647)

[2.3 Risk Model 6](#_Toc155741648)

[3. System Characterization 6](#_Toc155741649)

[3.1 Technology components 6](#_Toc155741650)

[3.2 Physical Location(s) 7](#_Toc155741651)

[3.3 Data Used By System 7](#_Toc155741652)

[3.4 Users 7](#_Toc155741653)

[3.5 Flow Diagram 7](#_Toc155741654)

[4. Vulnerability Statement 8](#_Toc155741655)

[5. Threat Statement 8](#_Toc155741656)

[5. Risk Assessment Results 1](#_Toc155741657)

[EXECUTIVE SUMMARY 2](#_Toc155741658)

[<Optional - Big Issue> Recommendation 2](#_Toc155741659)

[HIGH LEVEL ASSESSMENT OVERVIEW 3](#_Toc155741660)

[Observed Security Strengths 3](#_Toc155741661)

[Areas for Improvement 3](#_Toc155741662)

[Short Term Recommendations 3](#_Toc155741663)

[Long Term Recommendations 3](#_Toc155741664)

[SCOPE 5](#_Toc155741665)

[Networks 5](#_Toc155741666)

[Other 5](#_Toc155741667)

[Provided Credentials 5](#_Toc155741668)

[TESTING METHODOLOGY 6](#_Toc155741669)

[CLASSIFICATION DEFINITIONS 7](#_Toc155741670)

[Risk Classifications 7](#_Toc155741671)

[Exploitation Likelihood Classifications 7](#_Toc155741672)

[Business Impact Classifications 8](#_Toc155741673)

[Remediation Difficulty Classifications 8](#_Toc155741674)

[ASSESSMENT FINDINGS 9](#_Toc155741675)

[APPENDIX A - TOOLS USED 12](#_Toc155741676)

[APPENDIX B - ENGAGEMENT INFORMATION 13](#_Toc155741677)

[Client Information 13](#_Toc155741678)

[Version Information 13](#_Toc155741679)

[Contact Information 13](#_Toc155741680)

# 

# 1. Introduction

## Purpose

[Describe the purpose of the risk assessment in context of the organization’s overall security program]

## 1.2. Scope of this risk assessment

[Describe the scope of the risk assessment including system components, elements, users, field site locations (if any), and any other details about the system to be considered in the assessment]

# 2. Risk Assessment Approach

## 2.1 Participants

|  |  |
| --- | --- |
| **Role** | **Participant** |
| System Owner |  |
| System Custodian |  |
| Security Administrator |  |
| Database Administrator |  |
| Network Manager |  |
| Risk Assessment Team |  |

## 2.2 Techniques Used

|  |  |
| --- | --- |
| **Technique** | **Description** |
| [List techniques used e.g., questionnaires, tools] | [Describe the technique used and how it assisted in performing the risk assessment] |

## 2.3 Risk Model

[Describe the risk model used in performing the risk assessment. For an example risk model refer NIST publication SP-800-30]

# 3. System Characterization

## 3.1 Technology components

|  |  |
| --- | --- |
| **Component** | **Description** |
| Applications | [Describe key technology components including commercial software] |
| Databases |  |
| Operating Systems |  |
| Networks |  |
| Interconnections |  |
| Protocols |  |

## 3.2 Physical Location(s)

|  |  |
| --- | --- |
| **Location** | **Description** |
| [Include locations included in scope] |  |

## 3.3 Data Used By System

|  |  |
| --- | --- |
| **Data** | **Description** |
| [Detail data elements included in scope] | [Describe characteristics of data elements] |

## 3.4 Users

|  |  |
| --- | --- |
| **Users** | **Description** |
| [Detail categories of users] | [Describe how users access the system and their intended use of the system] |

## 3.5 Flow Diagram

[Provide connectivity diagram or system input and output flowchart to delineate the scope of this risk assessment effort].

# 4. Vulnerability Statement

[Compile and list potential vulnerabilities applicable to the system assessed].

|  |  |
| --- | --- |
| **Vulnerability** | **Description** |
| [List vulnerabilities] | [Describe vulnerability and its impact] |

# 5. Threat Statement

[Compile and list the potential threat-sources applicable to the system assessed].

|  |  |
| --- | --- |
| **Threat-Source** | **Threat Actions** |
| [List threat sources] | [List and/or describe actions that can be taken by threat source e.g., identity theft, spoofing, system intrusion] |

# 5. Risk Assessment Results

[List the observations (vulnerability/threat-source pairs). Each observation should include—

* Observation number and brief description of observation (e.g., Observation 1: User system passwords can be guessed or cracked)
* A discussion of the threat-source and vulnerability pair
* Identification of existing mitigating security controls
* Likelihood discussion and evaluation (e.g., High, Medium, or Low likelihood)
* Impact analysis discussion and evaluation (e.g., High, Medium, or Low impact)
* Risk rating based on the risk-level matrix (e.g., High, Medium, or Low risk level)
* Recommended controls or alternative options for reducing the risk].

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Item Number** | **Observation** | **Threat-Source/**  **Vulnerability** | **Existing controls** | **Likelihood** | **Impact** | **Risk Rating** | **Recommended controls** |
|  |  |  |  |  |  |  |  |

# EXECUTIVE SUMMARY

<TEAM NAME> performed a security assessment of the internal corporate network of <CLIENT NAME> on <TEST DATE>. <TEAM NAME>’s penetration test simulated an attack from an external threat actor attempting to gain access to systems within the <CLIENT NAME> corporate network. The purpose of this assessment was to discover and identify vulnerabilities in <CLIENT NAME>’s infrastructure and suggest methods to remediate the vulnerabilities. <TEAM NAME> identified a total of <VULN TOTAL NUM> vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| **CRITICAL** | **HIGH** | **MEDIUM** | **LOW** |
| **1** | **2** | **2** | **1** |

The highest severity vulnerabilities give potential attackers the opportunity to <BAD ACTIONS THAT COULD OCCUR HERE - FULL PARAGRAPH WITH HIGH-LEVEL DETAIL>. In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

## <Optional - Big Issue> Recommendation

This is an optional paragraph that discusses a very critical series of business failures (e.g. failure to adhere to applicable legal regulations) that isn’t a technical vulnerability but still should be brought to the attention of the executive team.

# HIGH LEVEL ASSESSMENT OVERVIEW

## Observed Security Strengths

<TEAM NAME> identified the following strengths in <CLIENT NAME>’s network which greatly increases the security of the network. <CLIENT NAME> should continue to monitor these controls to ensure they remain effective.

<Strength Category>

* Great thing we saw here that causes us issues (which is a good thing)
* Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

## Areas for Improvement

<TEAM NAME> recommends <CLIENT NAME> takes the following actions to improve the security of the network. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack <CLIENT NAME>’s information systems and/or reduce the impact of a successful attack.

### Short Term Recommendations

<TEAM NAME> recommends <CLIENT NAME> take the following actions as soon as possible to minimize business risk.

<Recommendation Category>

* <Individual Recommendation>
* Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

### Long Term Recommendations

<TEAM NAME> recommends the following actions be taken over the next <NUM> months to fix hard-to-remediate issues that do not pose an urgent risk to the business.

<Recommendation Category>

* <Individual Recommendation>
* Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

# 

# SCOPE

All testing was based on the scope as defined in the Request For Proposal (RFP) and official written communications. The items in scope are listed below.

## Networks

|  |  |
| --- | --- |
| **Network** | **Note** |
| 10.0.1.0/24 | Network for Corporate HQ |
| 10.0.2.0/24 | Gotham, NY, branch site |

## Other

|  |  |  |
| --- | --- | --- |
| **Name** | **System Type** | **Note** |
| IVR System | Phone | 555-555-1234 |

## Provided Credentials

<CLIENT NAME> provided <TEAM NAME> with the following credentials and access to facilitate the security assessment listed below.

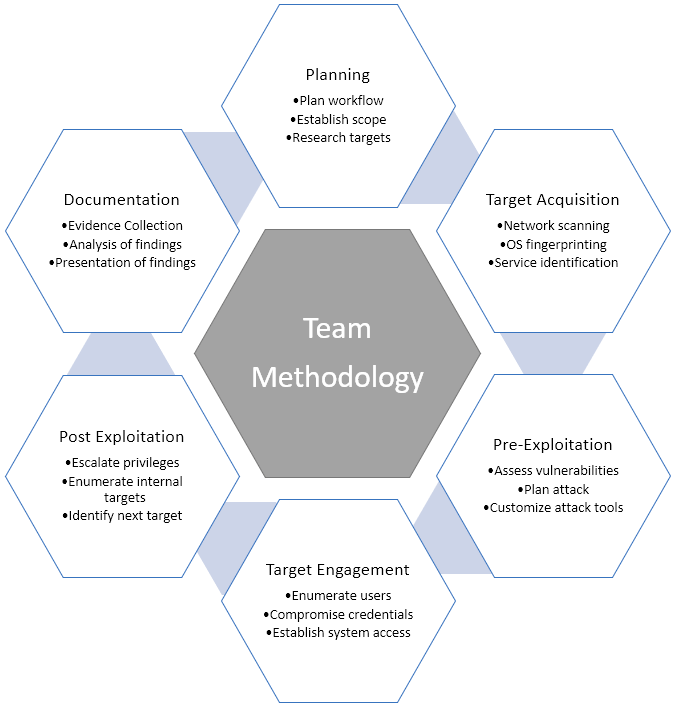
|  |  |
| --- | --- |
| **Item** | **Note** |
| Customer Account | (testuser@example.com) A fake customer account in the XXXX application for testing functionality that requires authentication. |
| IVR Testing Phone | (555-555-5678) Specific phone to use for IVR system testing. |

# 

# TESTING METHODOLOGY

<TEAM NAME GOES HERE>’s testing methodology was split into three phases: *Reconnaissance*, *Target Assessment*, and *Execution of Vulnerabilities*. During reconnaissance, we gathered information about <CLIENT NAME>’s network systems. <TEAM NAME GOES HERE> used port scanning and other enumeration methods to refine target information and assess target values. Next, we conducted our targeted assessment. <TEAM NAME GOES HERE> simulated an attacker exploiting vulnerabilities in the <CLIENT NAME> network. <TEAM NAME GOES HERE> gathered evidence of vulnerabilities during this phase of the engagement while conducting the simulation in a manner that would not disrupt normal business operations.

The following image is a graphical representation of this methodology.



# CLASSIFICATION DEFINITIONS

## Risk Classifications

|  |  |  |
| --- | --- | --- |
| **Level** | **Score** | **Description** |
| **Critical** | **10** | The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed. |
| **High** | **7-9** | The vulnerability poses an urgent threat to the organization, and remediation should be prioritized. |
| **Medium** | **4-6** | Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible. |
| **Low** | **1-3** | The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible. |
| **Informational** | **0** | These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company. |

## Exploitation Likelihood Classifications

|  |  |
| --- | --- |
| **Likelihood** | **Description** |
| **Likely** | Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty. |
| **Possible** | Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation. |
| **Unlikely** | Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation. |

## Business Impact Classifications

|  |  |
| --- | --- |
| **Impact** | **Description** |
| **Major** | Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage. |
| **Moderate** | Successful exploitation may cause significant disruptions to non-critical business functions. |
| **Minor** | Successful exploitation may affect few users, without causing much disruption to routine business functions. |

## Remediation Difficulty Classifications

|  |  |
| --- | --- |
| **Difficulty** | **Description** |
| **Hard** | Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions. |
| **Moderate** | Remediation may require minor reconfigurations or additions that may be time-intensive or expensive. |
| **Easy** | Remediation can be accomplished in a short amount of time, with little difficulty. |

## 

# ASSESSMENT FINDINGS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Number** | **Finding** | **Risk Score** | **Risk** | **Page** |
| 1 | Example Vulnerability Finding | **9** | **High** | 11 |
| 2 | Firewall Rule Set Not Best Practice | **8** | **High** | 12 |
| 3 | Outdated Software | **6** | **Medium** | 69 |
| 4 | Multiple XYZ Vulnerabilities | **5** | **Medium** | 420 |
| 5 | Fake Finding | **2** | **Low** | 6969 |

TEMPLATE NOTE: (Sorting by descending risk score)

**1 - Example Vulnerability Finding**

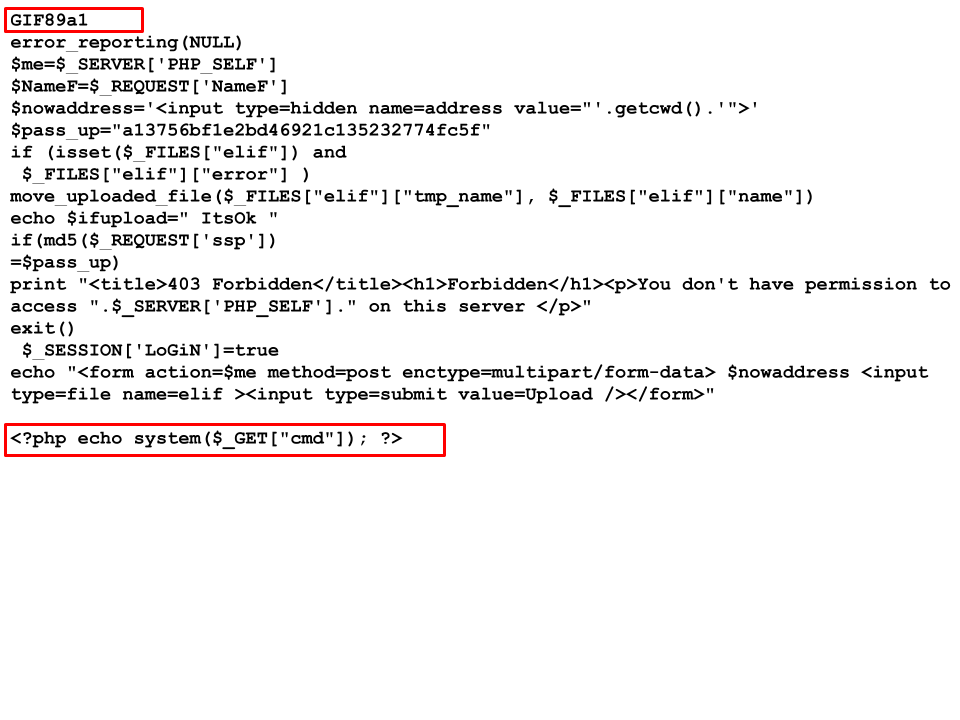
|  |  |
| --- | --- |
| **HIGH RISK (8/10)** | |
| **Exploitation Likelihood** | **Possible** |
| **Business Impact** | **Severe** |
| **Remediation Difficulty** | **Easy** |

**Security Implications**

This is where you give a 1-2 sentence description about the major impact of the finding. This finding is very important because it can destroy the entire business if left unchecked.

**Analysis**

Longer discussion of the finding. Includes screenshots. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum (see Appendix 1).



***Figure 2.3.1****: A php webshell uploaded to XYZ Application*

**Recommendations**

* Remove XYZ to make things more secure
* If you can not remove XYZ do this…

**References (opt)**

* <https://github.com/Sevaarcen/RADAR/tree/master/radar/playbooks>
* <https://owasp.org/www-project-top-ten/>

# APPENDIX A - TOOLS USED

|  |  |
| --- | --- |
| **TOOL** | **DESCRIPTION** |
| **BurpSuite Community Edition** | Used for testing of web applications. |
| **Metasploit** | Used for exploitation of vulnerable services and vulnerability scanning. |
| **Nmap** | Used for scanning ports on hosts. |
| **OpenVAS** | Used to scan the networks for vulnerabilities. |
| **PostgreSQL Client Tools** | Used to connect to the PostgreSQL server. |

***Table A.1:*** *Tools used during assessment*

# APPENDIX B - ENGAGEMENT INFORMATION

## Client Information

|  |  |
| --- | --- |
| **Client** | <CLIENT NAME> |
| **Primary Contact** | <Person Name>, <Person’s Title> |
| **Approvers** | The following people are authorized to change the scope of engagement and modify the terms of the engagement   * <PERSON NAME 1> * <PERSON NAME 2> |

## Version Information

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description** |
| 1.0 | <DATE HERE> | Initial report to client |

## Contact Information

|  |  |
| --- | --- |
| **Name** | <TEAM NAME> Consulting |
| **Address** | 1001 Fake Street, Gotham, NY 11201 |
| **Phone** | 555-185-1782 |
| **Email** | <REPLACE WITH PROVIDED EMAIL> |