![A chain with glowing lights

Description automatically generated]()S

**SAMPLE WEB APPLICATION VULNERABILITY ASSESSMENT REPORT**

Date: MONTH YEAR

A white letter with a red green yellow and black logo

Description automatically generated

www.anadata.com

**REPORT DETAILS**

|  |  |
| --- | --- |
| **Title** | Application Penetration Testing Report |
| **Version** | V 1.0 |
| **Author** | Vishal Pranav Thangaraj |
| **Tester(s)** | Vishal Pranav Thangaraj (OSCP)  Rahul Kalnarayan (ISO 27K LA, OSCP, eWPTX V2, eMAPT, CRTP) |
| **Classification** | Confidential |

**RECIPIENT**

|  |  |
| --- | --- |
| **Organization Name** | [Redacted] |
| **Contact Person** | [Redacted] |
| **Contact Number** | [Redacted] |
| **Email** | [Redacted] |
| **Type of test Requested** | Application Penetration Testing |

**VERSION CONTROL**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description** |
| 1.0 |  | Shanawaz Mohammed (CISSP, CISA, CCSK, CCISO, CEH, eJPT) | Initial Report |

**CONFIDENTIAL & PROPRIETARY**

This document contains information that is confidential and proprietary which shall not be disclosed, transmitted, duplicated, or used in whole or in part for any purpose other than its intended purpose. Any use or disclosure in whole or in part of this information without explicit written permission of [Redacted Organization] is prohibited. Ana-Datamakes no warranty that the information contained in this document is complete or error free.

This report is solely for the information of [Redacted Organization] and cannot be used outside [Redacted Organization] without the management permission, circulated, quoted, or otherwise referred to for any other purpose, nor included or referred to in whole or in part in any document.

The specific Devices/ IP addresses/ Domains / Applications were provided by [Redacted Organization]. Our subsequent test work, study of issues in detail and developing action plans are directed towards the issues identified. Consequently, this report may not necessarily comment on all the weaknesses perceived as important by [Redacted Organization] and/ or [Redacted Organization] management.

© Copyright 2024 Ana-Data Consulting Inc. All rights reserved. Ana-Data logo are trademarks of Ana-Data Consulting Inc. and are registered in the USA and other countries. All other trademarks contained in this document are the property of their respective owners.

**REPORT ANALYSIS & COMPLIANCE**

* The issues identified and proposed action plans in this report are based on our testing. We made specific efforts to verify the accuracy and authenticity of the information gathered only in those cases where it was felt necessary.
* The identification of the issues in the report is mainly based on the tests carried out during the limited time for conducting such an exercise. As the basis of selecting the most appropriate weaknesses/ vulnerabilities is purely judgmental in view of the time available, the outcome of the analysis may not be exhaustive and represents all possibilities, though we have taken reasonable care to cover the major eventualities.
* The vulnerabilities reported in this report are valid as of the **[end date]**. Any vulnerability which may have been discovered after this or any exploitation made available after **[end date]** does not come under the purview of this report.
* Any configuration changes or software/ hardware updates made on hosts/ machines on the application covered in this test after the date mentioned herein may impact the security posture either positively or negatively and hence invalidates the claims & observations in this report. Whenever there is an update on the application, we recommend that the organization conducts a penetration test to ensure compliance of the security posture with its security policies.
* Applications often store sensitive information such as personal details, credit card numbers, healthcare records, financial information, etc. Ana-Data Consulting Inc. assesses, and reports identified security vulnerabilities on a customer’s web and mobile application’s compliance to the most stringent security standards, such as OWASP, CWE, Application Security Verification Standards (ASVS) and other regulatory requirements.
* Ana-Data Consulting Inc. follows the industry standard such as Common Vulnerability Scoring System (CVSS) to calculate the severity score of the identified vulnerabilities and provide the customer with simple pass/fail status for a compliance regulation like OWASP Top 10.

**TABLE OF CONTENTS**

[1 EXECUTIVE SUMMARY 6](#_Toc170998495)

[**1.1** **Scope of work** 6](#_Toc170998496)

[**1.2** **Timeline** 6](#_Toc170998497)

[2 SUMMARY OF FINDINGS 7](#_Toc170998498)

[3 METHODOLOGY 8](#_Toc170998499)

[4 INFORMATION GATHERING 9](#_Toc170998500)

[5 THREAT MODELLING 10](#_Toc170998501)

[6 VULNERABILITY ASSESSMENT 13](#_Toc170998502)

[**6.1** **Automated Vulnerability Assessment** 13](#_Toc170998503)

[**6.2** **Manual Vulnerability Assessment** 13](#_Toc170998504)

[7 VULNERABILITIES EXPLAINED 15](#_Toc170998505)

[7.1 Name of Vulnerability 15](#_Toc170998506)

[8 CONCLUSION 16](#_Toc170998507)

[**8.1** **Summary of Findings** 16](#_Toc170998508)

[**8.2** **Summary of Recommendations & Best Practices** 16](#_Toc170998509)

[9 APPENDIX 17](#_Toc170998510)

# **EXECUTIVE SUMMARY**

Ana-Data Consulting Inc. (We/Us/Our/Ana-Data), has conducted Internal Application Penetration Test on [Redacted Organization] ([Redacted Organization]/Client’s/ You/ Your), application to ensure security of the application and end user’s information that is processed and stored by the application. The test was performed to identify the potential vulnerabilities in the internal web application and to provide security advisory services. The objective is to validate the security mechanisms of the application and identify all (if any) vulnerabilities exist on the target in scope. Ana-Data performed Application Penetration Test with validated credentials using a methodological and standardized approach. This document summarizes the findings, analysis and recommendations from the penetration test conducted and included in Sections 4 to 10.

## **Scope of work**

The scope of the security assessment included internal web application penetration testing of the items listed below, in table 1. This information was provided by “[Redacted]” who works with [Redacted], this information was shared through email on [Date].

|  |  |  |
| --- | --- | --- |
| S. No | URL | Target Description |
| 1 | [Redacted] | [Redacted] |

Table 1 – Scope of the work

This assessment focuses on the [Redacted] Application, an internal application designed for [Redacted]. Conducted as a Grey box scan, the evaluation provided insights into the application's security posture and user access controls. Five different roles - [Redacted], [Redacted], [Redacted], [Redacted] and [Redacted]—were analyzed. To facilitate assessment, VPN access via [Redacted] VPN was granted to securely connect to the internal network. We conducted tests from both unauthenticated and authenticated contexts. Unauthenticated testing focused on assessing and identifying vulnerabilities that could be exploited without authentication. Authenticated testing delved into internal application components accessible only after successful authentication. Assessors were provided with multiple user accounts with varying permissions to evaluate internal security controls.

## **Timeline**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type of Testing | Start Date | End Date | Total hours | Status |
| Application VAPT (Grey Box) |  |  |  |  |

Table 2 – Timeline

# SUMMARY OF FINDINGS

Following both automated and manual techniques to identify vulnerabilities and simulating a real-world attack for target in scope, it is observed that applications have few existing vulnerabilities.

Based on our understanding of the applications, we have assessed and analyzed the level of risk on the application, based on the nature of the vulnerabilities discovered, their exploitability and potential impact. We discovered, investigated, and verified many vulnerabilities during this assessment. These weaknesses were categorized into four general threat levels based on the Common Vulnerability Scoring System (CVSS) ratings scale.

|  |  |  |
| --- | --- | --- |
| **Severity Level** | **Color Indicator** | **CVSS Category** |
| Critical | Maroon | 9.0 – 10.0 |
| High | Red | 7.0 – 8.9 |
| Medium | Orange | 4.0 – 6.9 |
| Low | Green | 0.1 – 3.9 |
| Informational | Blue | NA |

Below will the list of vulnerabilities that will identified during the assessment:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No** | **Vulnerabilities** | **Vulnerable Endpoint Count** | **CVSS** | **Severity** |
|  |  |  |  |  |
|  |  |  |  |  |

# **METHODOLOGY**

Timeline

Description automatically generatedThe **Penetration Testing Execution Standard (PTES)** consists of seven (7) main sections. These cover everything related to a penetration test - from the initial communication and reasoning behind a penetration test, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it. OWASP is a globally accepted framework designed to enable the execution of effective penetration testing consistent with best practice while ensuring a holistic and comprehensive evaluationof web applications. The application is manually tested following OWASP testing guide v4 for potential known vulnerabilities. This method of testing provides a wider approach to verify security of the applications accurately and efficiently. The OWASP guide evolves continually to keep pace with fast moving application security threat landscape ensuring that your application is secure. This approach to test the applications is consistent, repeatable, and defined. We have tailored the testing guide to match your organization’s technologies, processes, and organizational structure.

Fig 1: Ana-Data’s Methodology for conducting Penetration Testing Assessments.

# **INFORMATION GATHERING**

In the information gathering phase, a thorough exploration of the internal application's environment was conducted to gather critical insights and identify potential vulnerabilities. Various techniques and tools were employed to extract valuable information, laying the groundwork for subsequent penetration testing activities.

**[Compiles all gathered information essential for aiding the assessment.]**

This comprehensive approach to information gathering included both theoretical knowledge acquisition and practical exploration, resulting in a thorough understanding of the application. All gathered information will be utilized for threat modeling. This approach ensures that threat assessments prioritize vulnerabilities specific to the application's features, enhancing targeted security measures and mitigations.

# **THREAT MODELLING**

This section examines every potential threat to the application, leveraging its existing features as a foundation. Through this process, it identifies and assesses various risks that could compromise the application's security and functionality. By anticipating and understanding these threats, the section enables the adoption of a systematic approach to penetration testing.

In this process, the OWASP Top 10 served as a valuable reference point. The OWASP Top 10 is a widely recognized list of the most critical web application security risks, highlighting common vulnerabilities that attackers frequently exploit. By aligning the threat modelling process with the OWASP Top 10, a comprehensive coverage of potential vulnerabilities was ensured, and prioritization of their assessment was based on the likelihood and impact of exploitation.

Furthermore, the 10 most frequently found vulnerabilities identified by OWASP directly informed the threat modelling process. By considering these vulnerabilities, such as injection flaws, broken authentication, sensitive data exposure, XML external entities (XXE), broken access control and much more, tailored approaches to identifying and addressing specific security risks within the application were developed.

Performed threat modeling systematically by integrating information gathered during the “Information Gathering” phase with the OWASP Top 10, identifying potential threats to the application. Each feature was individually analyzed to comprehensively assess associated risks and vulnerabilities.

Overall, the combination of comprehensive understanding, meticulous analysis, and alignment with the OWASP Top 10 ensured a robust threat modelling process, enabling effective anticipation and addressing of potential security risks during the vulnerability assessment of the target application.

**INJECTION**

Injection vulnerabilities occur when user input is not properly sanitized or validated before being used in dynamic queries, commands, or interpreted by the application. Attackers can exploit input injection vulnerabilities to execute arbitrary commands, inject malicious code, or manipulate application behavior. The mentioned features, which has searching, adding, and editing functionalities reliant on user input, pose potential risks of input injection attacks:

* [Redacted]

All input points were tested with multiple payloads. Validation mechanisms have been implemented across all input points to ensure the proper sanitization and validation of user inputs, mitigating the risk of exploitation.

**FILE UPLOAD**

This vulnerability occurs when a web application allows users to upload files without proper validation and sanitization. Attackers can exploit this vulnerability by uploading malicious files, such as scripts or malware, which can then be executed on the server or by other users. The inclusion of attachment functionality in the specified features introduces the potential risk of file upload vulnerabilities:

* [Redacted]

**CSV INJECTION**

CSV (Comma-Separated Values) injection occurs when user-controlled data is improperly inserted into CSV files. Attackers can exploit this vulnerability by injecting formulas or special characters into CSV data, leading to arbitrary code execution when the file is opened by a spreadsheet application. The presence of export functionality within the specified features enables users to export current information into Excel sheets, creating a potential risk of CSV injection vulnerability if input data passed to the Excel sheet is not properly sanitized:

* [Redacted]

**BROKEN ACCESS CONTROL**

The application was checked to detect any instances lacking authentication measures, potentially allowing unauthorized access for attackers. These vulnerabilities could result in unauthorized access to sensitive data or systems, posing risks to confidentiality, integrity, and availability.

**Vulnerable and Outdated Components**

The application was enumerated to determine the components used and their versions, and if identifiable, they were examined to determine if it had reached its end of life. The components were scrutinized for known vulnerabilities. Relying on vulnerable third-party components exposes systems to various exploits, potentially leading to system compromise, data breaches, and disruption of services.

**Identification and Authentication Failures**

Identification and authentication failures occur when applications inadequately verify or manage user identities and sessions. These vulnerabilities are tied to fault authentication system and flaws in session management, such as insufficient session expiration or predictable session tokens. Attackers exploit these weaknesses to gain unauthorized access, manipulate user sessions, or escalate privileges.

# **VULNERABILITY ASSESSMENT**

We have conducted both manual testing and automated scans on the application in scope. Automated scans serve as a valuable addition to manual penetration testing by offering a systematic and efficient approach to identifying prevalent vulnerabilities across extensive codebases and web applications. While manual penetration testing provides detailed analysis and human expertise to uncover subtle vulnerabilities, automated scans specialize in repetitive tasks and promptly identify well-known vulnerabilities. This automation not only saves time but also creates opportunities for more thorough testing. This section is divided into two parts – 6.1 Automated Scans and 6.2 Manual Testing.

## **Automated Vulnerability Assessment**

For automated scanning, we have utilized Burp Suite Pro version to conduct a thorough scanning. Burp Suite Pro is a software security application used for penetration testing of web applications. The software is developed by the company Portswigger and is the world's most popular tool for application security testing.

The issues identified by Burp Suite Pro are detailed below.

**Summary of scan results**

This section contains a list of all vulnerabilities reported by Burp Suite Pro. Please find the results of Burp Suite Pro in Appendix 1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S. No** | **Vulnerability Classification** | **Vulnerabilities** | **Instance Count** | **CVSS** | **Severity** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

We've manually validated the scan results. These vulnerabilities were confirmed to exist in the infrastructure, while all others mentioned in the scan results (Appendix 1) are to be considered false positives.

## **Manual Vulnerability Assessment**

A manual vulnerability assessment was conducted, utilizing gathered information and performed threat modeling. This approach helps in identifying vulnerabilities that necessitate additional attention and are often overlooked by automated scanners.

**Summary of manual assessment results**

This section summarizes all the vulnerabilities identified through manual assessment.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S.No** | **Vulnerability Classification** | **Vulnerabilities** | **Vulnerable Endpoint Count** | **CVSS** | **Severity** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# **VULNERABILITIES EXPLAINED**

Name of Vulnerability

**Description**  
This section provides a detailed account of the identified vulnerability or issue within the web application. It includes specifics such as affected functionalities and technical details to ensure clarity and understanding among stakeholders.

**Impact**

This section outlines the potential consequences and risks associated with the identified vulnerability. It describes how the issue could be exploited by attackers and the resulting impact on the confidentiality, integrity, and availability of the web application and its data.

**Vulnerable Endpoint(s)**

The "Vulnerable Endpoints" section identifies specific endpoints or URLs within the web application that are susceptible to security vulnerabilities.

**Severity Details**

* **Severity**:
* **CVSS Score:**

**Steps to Reproduce**

This section details the sequence of actions or conditions required to demonstrate the presence and exploitation of the identified vulnerability. It serves as a practical guide for validating the findings and verifying the effectiveness of remediation measures.

**Recommendation**

This section offers actionable guidance and best practices to mitigate or eliminate the identified vulnerability. It includes specific steps, configurations, or practices recommended to enhance the security posture of the web application and prevent future occurrences of similar issues.

**References**

This section provides citations, links, or acknowledgments for external sources, standards, or methodologies referenced throughout the VAPT report. It offers additional context and supplementary resources relevant to the assessment findings and recommendations.

# **CONCLUSION**

Ana-Data Consulting Inc. (Ana-Data) has successfully completed a comprehensive Internal Application Penetration Test on [Redacted]'s internal web application. The primary aim of this assessment was to ensure the security of the application and the protection of end user information processed and stored by the application. Concluding the assessment, we have provided our list of findings and recommendations from the assessment. Please find them below:

## Summary of Findings

Our penetration testing identified multiple vulnerabilities using manual and automated penetration testing on the [Redacted] Application.

This section will list vulnerabilities identified during the assessment with their respective severity and reference links.

## Summary of Recommendations & Best Practices

This section provides a concise overview of actionable steps and guidelines derived from the assessment findings. It outlines specific measures to enhance the security posture of the web application, addressing identified vulnerabilities and risks.

# **APPENDIX**

This section compiles automated scan reports and additional attachments essential for a detailed understanding of the assessment findings. It enhances transparency and facilitates further analysis and validation of the web application's security posture beyond the core report content.