MAT Penetration Testing Report

Revision	***Author***	***Date***	***Notes***
01	F. Gorla	10 gen 2025	Version released to the client
02	F.Gorla	7 feb 2025	Update after retest
03	F.Gorla	11 feb 2025	Final clean version

1. Introduction

40Factory has developed the MAT platform, a comprehensive solution designed to enhance the efficiency and effectiveness of industrial operations. It offers a suite of tools and services tailored to meet the specific needs of various industries, focusing on optimizing processes, improving productivity, and ensuring seamless integration with existing systems.
By leveraging the 40Factory MAT platform, businesses can achieve significant improvements in operational efficiency, data management, and overall productivity.

Security Pattern has conducted a Penetration Testing activity on the MAT platform, with the aim of identifying any vulnerabilities that could potentially affect the security of the entire system.

The analyses done by Security Pattern have covered the following areas:

- Interfaces of the 40Factory MAT platform
- Perimeter of the web application and of its API
- Authentication mechanisms
- Business logic
- System configurations

The assessment activities have been executed between 04/12/2024 and 16/12/2024.

1.1. Scope

The testing scope of the web application included the following targets:

- The MAT platform
    - Backend APIs
    - Frontend pages

Security Pattern tested each target separately. The aggregate results are provided in this document.

1.1.1. MAT

Testing dates: from 04/12/2024 and 16/12/2024.

Endpoints (DEMO environment):

- MAT portal: https://matdev.40mat.com/

Admin Users:

- f.gorla@securitypattern.com
- s.cristalli@securitypattern.com

Regular users:

- fg_pentest_user@securitypattern.com
- sc_pentest_user@securitypattern.com

1.2. Methodology

For their Penetration Testing activities, Security Pattern follows a mixed approach, with both automated and manual tests.

For designing and selecting the specific tests, their relevance is evaluated in comparison with industry-standard guidelines, such as, but not limited to, the ones from OWASP; in particular, the tests from the OWASP Web Security Testing Guide are taken into consideration. Also, the selection of tests is always adapted to the particular target being tested; Security Pattern is making sure that the tests are suitable for the system, with an *ad hoc* evaluation of:

- documentation about the system received from the client
- information about the system discovered by Security Pattern experts during testing
- the agreed perimeter for the assessment activities

For the testing of the 40Factory MAT Platform, Security Pattern has performed tests that include, but are not limited to, the following categories and items:

- Information gathering
    - HTTP header analysis
    - Cookie analysis
    - Entry point identification
    - Collection of relevant API and resources
    - Functional mapping of web application
    - Information disclosure by errors
- Authentication/authorization
    - Testing of authentication mechanisms
    - Tests on JWT tokens
    - Analysis of roles and permissions

    - Privilege escalation
- Session management
    - Session timeout
    - Logout management
- Data validation testing
    - Reflected XSS
    - Stored XSS
    - SQL injection
    - HTTP parameter pollution/manipulation
- Error handling
    - Analysis of error codes
    - Analysis of error messages
- Business logic testing
    - Business logic data validation
    - Integrity checks
    - Abuse of functionality
    - File upload vulnerabilities
- Cryptography
    - Testing of proper TLS configuration

The tests performed by Security Pattern are extensive, focusing on *breadth* and *coverage* (i.e. trying to find a high number of vulnerabilities in the various aspects that compose the target's security, without leaving any part not analyzed). However, it is worth noting that the results of this penetration testing cannot guarantee *completeness*; namely, it is not possible to guarantee the absence of:

- any vulnerability with a type that has not been found in this assessment
- vulnerabilities that are similar to the ones that have been found in this assessment

Regarding the second point, given the fact that single vulnerabilities can indicate the presence of underlying design or implementation flaws, it is strongly suggested to review the vulnerabilities that have been identified and to correct the underlying causes, searching for other entry points where the same issues could potentially be present.

To evaluate the impact of detected vulnerabilities, Security Pattern considers various factors, including the criteria evaluated within the CVSSv3 scoring system, and the assets of the particular system under analysis. In this document, the qualitative evaluation associated with each vulnerability is reported. The table below summarizes the meaning of each severity level.

Level	Description
CRITICAL	Vulnerabilities which impact the entire system, and which can compromise its essential functions. Attackers (even if inexperienced) can easily exploit these vulnerabilities to cause damage. **It is strongly recommended to take immediate corrective actions.**
HIGH	Vulnerabilities which impact large portions of the system, and which can compromise its essential functions. Attackers with some experience can easily exploit these vulnerabilities to cause damage. **It is recommended that corrective actions for resolution are considered urgent and planned to be executed within a short period of time.**
MEDIUM	Vulnerabilities which impact restricted portions of the system, and which can compromise its essential functions. It is possible that, under the right conditions, expert attackers may exploit these vulnerabilities to cause damage. **It is recommended that corrective actions for resolution are planned to be executed, although they are not to be considered urgent.**
LOW	Vulnerabilities which impact restricted portions of the system, and which cannot singularly impact its essential functions. It is possible that, under the right conditions, expert attackers may exploit these vulnerabilities to cause damage; however, such an event is expected to occur with low likelihood. **It is recommended to evaluate whether it is necessary to take corrective actions for resolving these problems, considering the system context and its threat modeling.**
INFORMATIVE	These items do not represent vulnerabilities per se, but rather inform about implementation choices for which some improvement is possible (referring to industry best practice). **It is recommended to evaluate whether it is necessary to take actions for implementing the suggested improvements, considering the system context and its threat modeling.**

2. Results

Security Pattern has executed two rounds of vulnerability assessment and penetration testing on the 40Factory MAT Platform.

After every iteration, the results have been shared with 40Factory, which has performed the adequate corrective actions.

At the end of the testing activities, Security Pattern reports no relevant vulnerabilities.

CRITICAL: 0

HIGH: 0

MEDIUM: 0

LOW: 0

INFORMATIVE: 1