40 Factory MAT - VAPT Report (PUBLIC)

Revision	***Author***	**Reviewer**	***Date***	***Notes***
v01	Federico Gorla	Alberto Battistello	30 ott 2025	Initial version
v01.1	Federico Gorla	Alberto Battistello	5 dic 2025	Updated with retest results

1. List of Abbreviations

General Security & Testing

- **VAPT** – Vulnerability Assessment and Penetration Testing
- **VA** – Vulnerability Assessment
- **PT** – Penetration Testing
- **PoC** – Proof of Concept
- **PTES** – Penetration Testing Execution Standard
- **OWASP** – Open Web Application Security Project
- **CVSS** – Common Vulnerability Scoring System
- **CVE** – Common Vulnerabilities and Exposures
- **CVSS** – Common Vulnerability Scoring System
- **CWE** – Common Weakness Enumeration
- **MITRE ATT&CK** – MITRE Adversarial Tactics, Techniques, and Common Knowledge

Web Application & Network

- **URL** – Uniform Resource Locator
- **URI** – Uniform Resource Identifier
- **HTTP / HTTPS** – Hypertext Transfer Protocol / Secure
- **API** – Application Programming Interface
- **REST** – Representational State Transfer
- **JWT** – JSON Web Token
- **CORS** – Cross-Origin Resource Sharing
- **DNS** – Domain Name System
- **IP** – Internet Protocol
- **SSL / TLS** – Secure Sockets Layer / Transport Layer Security

Attack Types & Vulnerabilities

- **XSS** – Cross-Site Scripting
- **CSRF / XSRF** – Cross-Site Request Forgery
- **SQLi** – SQL Injection
- **RCE** – Remote Code Execution
- **LFI / RFI** – Local File Inclusion / Remote File Inclusion
- **IDOR** – Insecure Direct Object Reference
- **SSRF** – Server-Side Request Forgery
- **XXE** – XML External Entity Injection
- **SSTI** – Server-Side Template Injection
- **DOS / DDOS** – Denial of Service / Distributed Denial of Service
- **ACL** – Access Control List
- **AuthN / AuthZ** – Authentication / Authorization

2. Introduction

40 Factory 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 40 Factory MAT platform, businesses can achieve significant improvements in operational efficiency, data management, and overall productivity.

Security Pattern has conducted a Vulnerability Assessment and 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 40 Factory MAT platform
- Perimeter of the web application and of its API
- Authentication mechanisms
- Business logic
- System configurations
- Use of cryptography

The assessment activities have been executed between 13 ott 2025 and 3 nov 2025.

A session of retest has been performed between 1 dic 2025 and 5 dic 2025 after which, the majority of the security impactful vulnerabilities have been resolved.

2.1. 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.

2.1.1. MAT

Testing dates: from 13 ott 2025 and 3 nov 2025.

Endpoints:

- MAT portal: https://matdev.40mat.com/
- IP: 4.210.142.189

Admin Users:

- f.gorla@securitypattern.com

Regular users:

- fg_pentest_user@securitypattern.com

2.2. 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 40 Factory 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
- Vulnerability analysis
    - CVE Discovery with the ARIANNA platform
    - CVE Analysis

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	Severity Score Range	Description
CRITICAL	9.0-10.0	Weaknesses which impact the entire system, and which can compromise its essential functions. Attackers (even if inexperienced) can easily exploit these weaknesses to cause damage. **It is strongly recommended to take immediate corrective actions.**
HIGH	7.0-8.9	Weaknesses which impact large portions of the system, and which can compromise its essential functions. Attackers with some experience can easily exploit these weaknesses to cause damage. **It is recommended that corrective actions for resolution are planned to be executed within a few days.**
MEDIUM	4.0-6.9	Weaknesses 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 weaknesses to cause damage. **It is recommended that corrective actions for resolution are planned to be executed within a few weeks.**
LOW	0.1-3.9	Weaknesses 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 weaknesses 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	0.0-0.0	These items do not represent weaknesses 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.**

3. Executive summary

The analyses performed by Security Pattern on the Customer device was framed as follows:

Device name	40Factory MAT
Samples received	https://matdev.40mat.com
Review start date	13 ott 2025
Review end date	3 nov 2025
Expertise of the tester	Senior Security Engineer
Scope of the analysis	Vulnerability Analysis and Penetration Test of a Web Application

The security evaluation of the 40Factory MAT platform revealed a small number of non-critical issues that can be addressed through standard security improvements.

Despite these minor findings, the platform exhibited strong core security principles, including robust authentication through Microsoft SSO, effective access controls, proper input validation, and secure business logic implementation. Overall, the 40Factory MAT platform demonstrates a solid level of security maturity and a robust foundation for protecting data and operations.

Security Pattern established that it is very unlikely for an attacker to impact the security of the 40Factory MAT (namely, to compromise both confidentiality and integrity properties) leveraging the most serious of these vulnerabilities.

The table below summarized the lists of tests performed:

ID	Description	Pass condition	Result
T1	**Validation of previous fixes**	All the previously discovered issues have been correctly fixed	**PASS**
T2	**Services enumeration and discovery**	The web application must not disclose unnecessary, sensitive, or undocumented interfaces or endpoints that could aid an attacker in reconnaissance or unauthorized access.	**PASS**
T3	**SQL Injection**	The web application must not be vulnerable to SQL injection via any input channel (web forms, URL parameters, headers, cookies, API parameters, JSON/XML bodies, etc.).	**PASS**
T4	**TLS Tests**	The web application or associated services must enforce secure, up-to-date TLS configurations that protect the confidentiality and integrity of data in transit.	**PASS**
T5	**SSH**	The SSH service must be securely configured to resist unauthorized access, downgrade attacks, and cryptographic weaknesses.	**PASS**
T6	**Client side**	The web application must ensure that no client-side vulnerabilities expose sensitive data, enable unauthorized actions, or compromise user sessions or browser integrity.	**PASS**
T7	**API & Business logic**	The application's API endpoints and business logic must be secure, enforce proper access control, and prevent manipulation or abuse of functional workflows.	**PASS**

T8	**Vulnerability analysis**	All components, dependencies, operating systems, frameworks, and third-party libraries used in the environment must be free from known, unpatched vulnerabilities as identified in public vulnerability databases (e.g., NVD, MITRE CVE, vendor advisories).	**PASS**

The following is a summary of the issues found:

Test ID	Vulnerability	CVSS	Severity
T2	Unnecessary open port	2.2	**LOW**
T4	Certificate Validity Too Long	—	**INFORMATIVE**
T5	SSH Deprecated Algorithms	4.8	**MEDIUM**
T7	Session Validity too long	3.3	**LOW**
T7	Missing Web Application Firewall	2.2	**LOW**

After a session of fixes, the following are the only issues left:

Test ID	Vulnerability	CVSS	Severity
T4	Certificate Validity Too Long	—	**INFORMATIVE**
T7	Missing Web Application Firewall	2.2	**LOW**

Given their low security impact, the related tests can be considered a PASS.

4. Conclusions

The security evaluation of the 40Factory MAT platform revealed a small number of non-critical issues that can be addressed through standard security improvements.

The absence of a Web Application Firewall (WAF) was observed; deploying a WAF would provide an extra layer of protection against common web-based attacks by filtering and monitoring HTTP requests.

Finally, the platform's SSL/TLS certificate was configured with a slightly longer validity period than advised, and reducing this duration would align better with current best practices for certificate lifecycle management.

Despite these minor findings, the platform exhibited strong core security principles, including robust authentication through Microsoft SSO, effective access controls, proper input validation, and secure business logic implementation. Overall, the 40Factory MAT platform demonstrates a solid level of security maturity and a robust foundation for protecting data and operations.