Cybersecurity and Information Resilience

January 12, 2021

Mursion X Application Penetration Test Executive Summary Report

Prepared for: Mursion Inc. | **Attention**: Tomer Ben-Evi, Head of Security/DPO

Table of Contents

Project Details

Project Name: **Mursion X Application Penetration Test Executive Summary Report**

Testing Date: December 7, 2020 - January 12, 2021

Customer Name and Address:	**Consultant Name and Address:**
Mursion Inc. 682 Schofield Rd San Francisco, CA 94129	**BSI Cybersecurity and Information Resilience** 6110 Hellyer Avenue, Suite 100 San Jose, CA 95138

Project Engagement Team

Customer Project Manager:	Tomer Ben-Evi | tomer.benevi@mursion.com | Ph: 415.746.9631 ext. 2201
Consultant Project Manager:	Tracy Tran | tracy.tran@bsigroup.com | Ph: 408.425.2038 Thuy Vu | thuy.vu@bsigroup.com | Ph: 408.439.0195
Consultant Account Manager:	Scott Simmons | scott.simmons@bsigroup.com | Ph: 408.439.5405 Ryan Hogan | ryan.hogan@bsigroup.com | Ph: 408.391.1638
Security Consultant:	Brandon Wilson | brandon.wilson@bsigroup.com | Ph: 408.444.1852

Executive Summary

In September of 2020, BSI Cybersecurity and Information Resilience ("BSI") performed a penetration test of the Mursion X application. This test focused on features, such as authentication, session management, and web server security. This was a detailed application-level test that employed a combination of manual testing by experienced professionals and automated testing tools.

During the initial test, BSI identified 21 distinct vulnerabilities, with the following breakdown of severity levels: 1 Medium, 8 Low, and 12 Best Practice. Mursion is working on remediating these vulnerabilities and will engage BSI to retest the application.

Objectives

This penetration test was conducted against the Mursion X application with the following primary objectives:

- Identify and assess the controls in place to protect against both external and internal threats.
- Identify thick client, web application and server configuration vulnerabilities that put sensitive information at risk.
- Test the application from the standpoint of unauthorized users attempting to gain access as well as authorized users trying to escalate access.
- Provide a detailed risk analysis and remediation advice for each vulnerability identified.

Methodology and Tools Used

Methodology

BSI performed this test following a CREST-certified methodology based on OWASP's Application Security Verification Standard (ASVS). BSI performed the following steps when conducting this web application penetration test.

1. **Preparation** – BSI verified that it had received the following information from Mursion in preparation for the penetration test.
    a. Application name
    b. Brief description of the application and its purpose
    c. Starting URL(s) for testing the application and URLs or IP addresses for accessing each web server included in the scope of the penetration test
    d. Two sets of login credentials for each level of access that the application provides. For example, if the application provides User and Admin roles, a total of four sets of login credentials will be required (two Users and two Admins).
    e. Time windows for when the automated scanning portion of the penetration test can be run without risk of disrupting other users of the application.
2. **Exploration** – BSI manually explored the entire application in order to become familiar with the application's functionality, purpose, and the sensitivity of information handled by the application.
3. **Automated Vulnerability Scanning** – High-quality commercial vulnerability scanning tools were used to thoroughly scan the application. This scanning process included:
    a. A non-authenticated scan, simulating a user without any login credentials.
    b. An authenticated scan, simulating a logged-in User and a logged-in Administrator.

   c. A server-level scan was run against all web servers included in the scope of the penetration test for server configuration vulnerabilities.
   d. A manual review and analysis was conducted on all scan results, removing any false positives from the results before presenting them to Mursion.
4. **Manual Penetration Testing** – The application was manually tested by experienced web application security professionals using BSI's systematic testing process. This manual testing process covers all major aspects of web application security, including:
   a. Authentication
   b. Authorization
   c. Session Management
   d. Input/Output Validation
   e. Configuration
   f. Sensitive Data Handing
   g. Privilege Escalation
   h. Logical Vulnerability Checks
5. **Report Preparation –** BSI took the results of both the automated and manual penetration testing and compiled a consolidated report, detailing all vulnerabilities uncovered during the testing process along with severity levels and recommendations for how to remediate each vulnerability that was identified.

Tools Used

The following tools were used when conducting this penetration test:

- Burp Suite Professional
- Nessus network vulnerability scanning tool
- The Firefox web browser
- YAWAST automated SSL scanning tool
- PE Viewer
- JetBrains dotPeek
- Notepad++
- Qualys SSL Labs

Scope

Application

The assessment was conducted per the following details:

Engagement Date(s)	*Initial Testing* December 7. 2020 – January 12, 2021
Location	Amazon Web Services
URL(s)	https://staging.portal.mursion.com https://ml3assetbundles.s3.amazonaws.com https://mursioncloudvideos.s3.amazonaws.com
Web Server	Nginx
Application Language	C#, Java
Environment	Staging Environment
Internet Facing?	Yes

Tests

The application was tested for the following categories of technical vulnerabilities:

Platform-level	Application-level
1. Server misconfigurations 2. Published vulnerabilities 3. Forceful browsing 4. Stealth commanding 5. Buffer overflow vulnerabilities 6. Email input/output issues 7. File upload/download concerns	1. Authentication 2. Authorization 3. Parameter tampering 4. Hidden field manipulation 5. Cross-site scripting 6. Cookie manipulation 7. Permissions escalation 8. Session management

Conclusion

The primary goals of this penetration test were to identify whether or not the Mursion X application has adequate controls in place to protect against unauthorized access to sensitive information by both external and internal attackers and to identify any vulnerabilities that could present risk to Mursion or its customers. To achieve these goals, we performed an extensive array of tests, using both manual techniques and commercial scanning tools in order to paint a comprehensive picture of the application's security posture.

There were a number of vulnerabilities identified during the initial assessment. However, the actual risk posed by these findings may be less than what is indicated due to mitigating factors such as use case, technical, and administrative controls. Mursion is working to remediate these vulnerabilities and will engage BSI to perform a remediation test.

It should be noted that this was a point-in-time assessment and that Mursion should perform regular security assessments as changes are made to the application and supporting infrastructure. BSI has detailed security assessment reports on file that back up the information provided in this Executive Summary report.