SYNERGYXR

IT Security Assessment Report

— Sune Wolff, CTO

24.03.2025

DATA CLASSIFICATION: PUBLIC

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this IT Security Assessment Report is to provide an overview of the security posture of our systems based on a series of scans and evaluations. By using industry-standard tools, including SSL Labs for SSL/TLS configuration analysis, Security Headers for HTTP header evaluations, and various penetration testing utilities, we aim to highlight key areas of strength and identify any potential areas for improvement.

This report aims to give our customers transparency and assurance regarding the security measures we have in place to protect their data and interactions with our services.

1.2 Scope

The scope of this IT Security Assessment are all online endpoints of the SynergyXR solution. This includes the web application SynergyXR Manager (https://portal.synergyxr.com/) as well as the underlying Azure-based infrastructure of our content backend.

1.3 Audience

The target audience of this IT Security Assessment Report is IT professionals, network administrators, business owners, technical leads, asset owners, and general users at our end-users who are interested in the security posture of SynergyXR.

1.4 Improvement

SynergyXR are committed to continuous improvement of the IT security offered by the SynergyXR platform. As new relevant tools are identified, the result of these will be added to the test suite to give as complete a picture of the security state as possible.

New scans will be performed quarterly, or upon request by individual customers. The latest report will always be available online for customers to download and assess.

2 Online Tool Suite

2.1 SSL Labs Report

We utilize the online SSL Server Test to perform a deep analysis of the configuration of our SSL web server. The tool is free and can be accessed from: https://www.ssllabs.com/ssltest/.

A high score in the Qualys SSL Labs report is important to us because it demonstrates our commitment to strong encryption, ensuring the security of our customers' data and reinforcing trust in our product's reliability.

The screenshot below shows the summary of the test. Please see the attached full report: 1.1_qualys_ssl_labs_report_20250324.pdf.

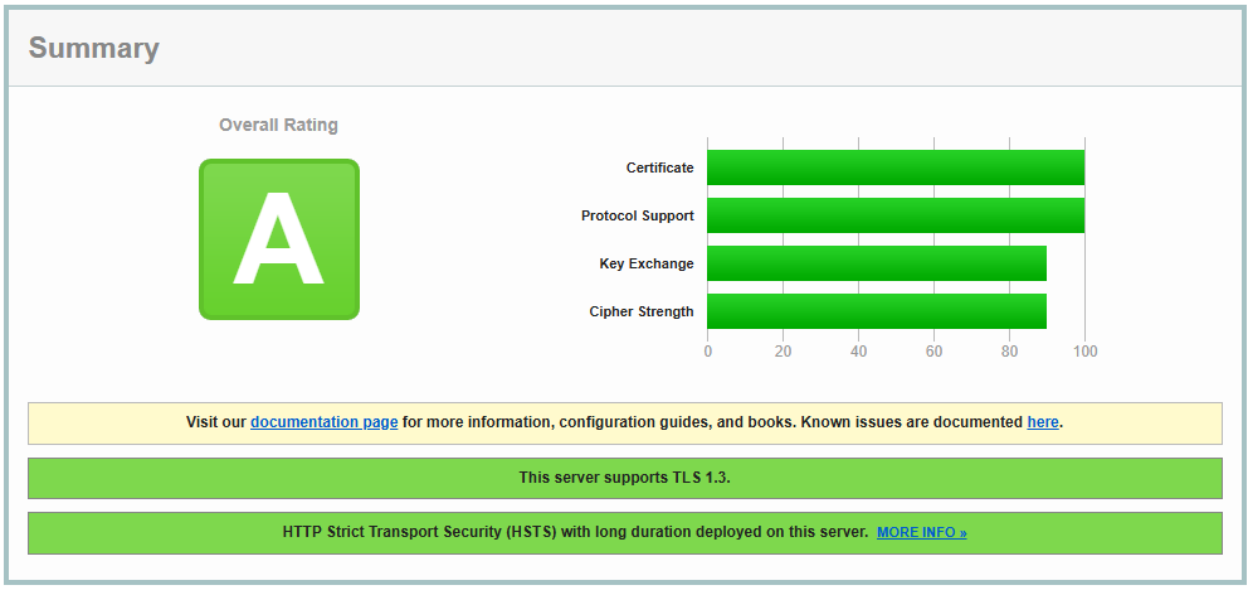

Figure 1: SSL Report from Qualys SSL Labs

2.2 Security Headers Report

We utilize the tool SecurityHeaders.com (https://securityheaders.com/) to evaluate our website's HTTP security headers, which help protect against common vulnerabilities. A strong score is important to us as

it shows our dedication to secure web practices, safeguarding user data and reinforcing trust in our platform's safety.

The screenshot below shows the summary of the test. Please see the attached full report: 1.2_security_headers_report_20250324.pdf.

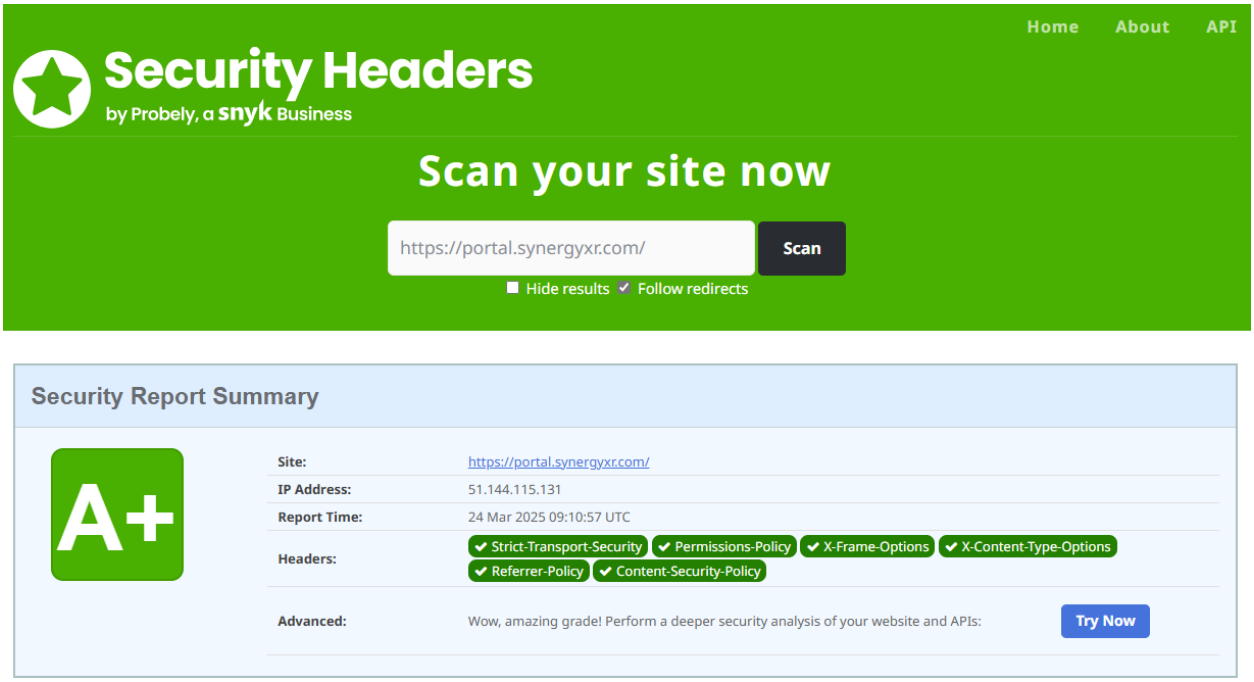

Figure 2: HTTP Security header analysis summary

2.3 Mozilla MDN Observatory Report

Launched in 2016, the HTTP Observatory (https://developer.mozilla.org/en-US/observatory) enhances web security by analyzing compliance with best security practices. It has provided insights to over 6.9 million websites through 47 million scans.

The screenshot below shows a summary of the security scan report. Please see the attached full report: 1.3_mdn_report_20250324.pdf.

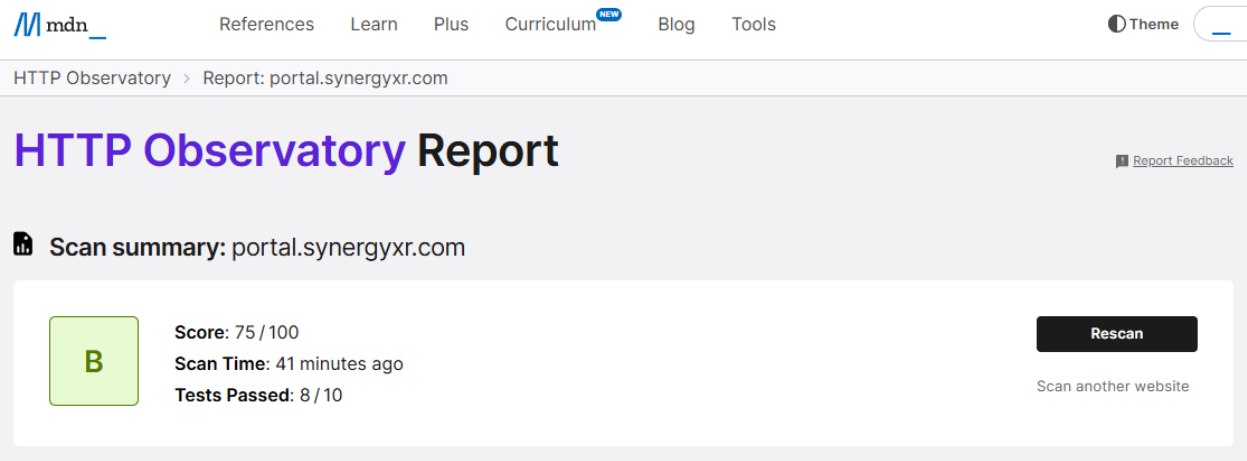

Figure 3: Summary of the security scan performed by the HTTP Observatory

2.4 Pentest Tools Automatic Report

The Pentest Tools report (https://pentest-tools.com/usage/pentest-reporting-tool) scans for vulnerabilities in web applications and networks, identifying potential security risks. Trusted by high-profile companies like Vodafone and ROLEX, using this tool is important to us as it validates our security efforts and ensures we proactively address threats, further building trust with our customers.

The screenshot below shows a summary of the report. Please see the attached full report: 1.4_pentest_tools-20250324-1000.pdf.

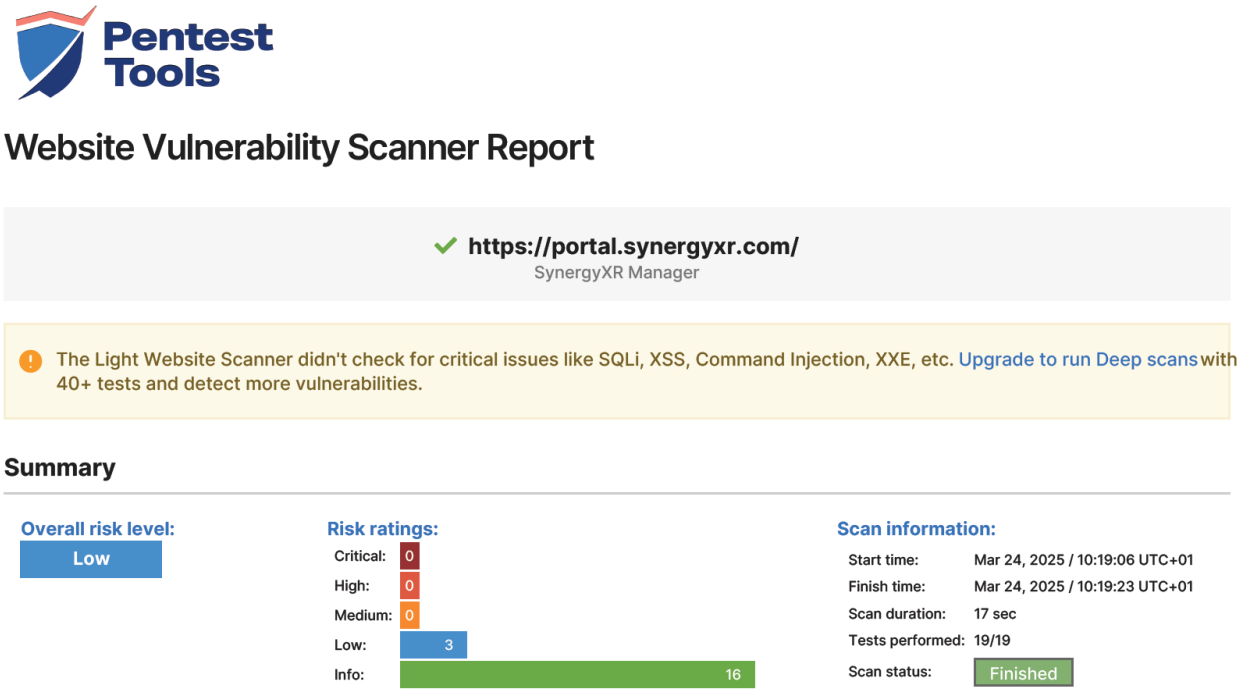

Figure 4: Summary of the Pentest Tools vulnerability scanner report

3 Certified Security Engineers

This is a list of the certifications held by our Azure security-certified engineers. We strive to always have qualified personnel overseeing security.

Figure 5: Gill Lumer-Klabbers (authentic certificate: 2.2_1_Credentials - gilllumer _ Microsoft Learn.pdf)

Figure 6: Jonas Tuemand Mortensen (authentic certificate: 2.2_2_Credentials - jonastuemand _ Microsoft Learn.pdf)

4 NuGet Packages Used

We want to have full transparency regarding the libraries and packages we use to help our partners assess potential risks.

- AspNetCore.Proxy - Version 4.4.0
- Azure.Messaging.EventGrid - Version 4.21.0
- Azure.Storage.Blobs - Version 12.16.0
- IdentityModel - Version 5.1.0
- IdentityModel.AspNetCore - Version 3.0.0
- IdentityModel.OidcClient - Version 4.0.0
- Microsoft.ApplicationInsights.AspNetCore - Version 2.22.0
- Microsoft.AspNetCore.Authentication.OpenIdConnect - Version 6.0.12
- Microsoft.AspNetCore.Mvc.Razor.RuntimeCompilation - Version 6.0.12
- Microsoft.AspNetCore.SpaServices.Extensions - Version 3.1.30
- Microsoft.Extensions.Logging.AzureAppServices - Version 5.0.10
- Microsoft.VisualStudio.Web.BrowserLink - Version 2.2.0
- Microsoft.VisualStudio.Web.CodeGeneration.Design - Version 6.0.11
- NWebsec.AspNetCore.Middleware - Version 3.0.0
- RestSharp - Version 112.1.0
- UAParser - Version 3.1.47
- glTF2Loader - Version 1.1.4-alpha

A vulnerability check reveals that none of these packages have vulnerabilities.

```
The given project `UnityStudios.Synergy.WebPortal` has no vulnerable packages given the current sources.
```

5 Compliance and Best Practices

We are committed to maintaining high standards of security and compliance. As part of our ongoing efforts, we are currently implementing the ISMS ISO/IEC 27001:2022 framework to establish a robust Information Security Management System. This framework will guide our practices in risk management, data protection, and compliance with industry standards, ensuring that we consistently safeguard our customers' information and uphold their trust.

6 Regular Security Practices

Our regular security practices are designed to ensure a proactive approach to safeguarding our applications and data. We follow the principle of least privilege, ensuring that users and systems have only the permission necessary to perform their tasks, minimizing potential security risks. We are also committed to following OWASP guidelines, regularly reviewing our code and applications for common vulnerabilities and security weaknesses. This includes conducting code reviews, implementing automated testing for security, and maintaining an ongoing process for identifying and addressing vulnerabilities. By integrating these practices into our development lifecycle, we enhance our overall security posture and protect our customers’ sensitive information.


SYNERGYXR