Penetration Testing Certificate

Client Facing Document
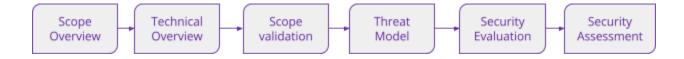
Approach

The security assessment carried out by Sayfer targets the Request Finance application. Particularly, the assessment displays the security posture review for the web application and its surrounding infrastructure and process implementations.

This review was commissioned by Sayfer, and the project was carried out in collaboration with the Request Finance team.

The project life cycle:

Scope Overview → Technical Overview → Scope validation → Threat Model → Security Evaluation → Security Assessment

About Sayfer

Sayfer is a leading consultant and software solutions company. We specialize in making organizations safer with ad-hoc solutions that close the gaps common security products fail to reach.

By being professional but lean and open to customer desires, we are able to provide our clients with fast, valuable solutions that prevent major security breaches.

Sayfer specializes in offensive defense, by leveraging approaches that imitate the attacker's behavior, like reverse engineering and vulnerability research, we are able to find novel security breaches in our client's products and prevent the real bad guys from threatening our clients.

Scope Overview

During our kickoff meeting and after understanding the company's needs, we defined the scope of the penetration testing project.

Project scoping is an essential step in a penetration testing project as it helps to define the boundaries and objectives of the project. It allows the testing team to understand the client's requirements, expectations, and objectives, and to focus their testing efforts on the most critical areas of the application or network.

We defined the **web application of Request Finance** to be the scope of the project. In addition to it, we also conducted multiple reconnaissance techniques to identify external network security risks for the company.

Certification

Request Finance contacted Sayfer Security in order to perform a black-box penetration test in June 2022.

Before assessing the system, we held a kickoff meeting with Request Finance's technical team and received an overview of the system and the goals for this assessment.

Over the assessment period of 4 weeks, we conducted research that aimed to find security vulnerabilities in the system.

After the Request Finance team deployed their fixes for the findings presented by Sayfer, we conducted an additional iteration to validate that the findings were fixed successfully. This is part of a healthy security process, which validates that the system was patched correctly.

We found that all the vulnerabilities found in our initial report were fixed during our second iteration.

Request Finance's systems that were evaluated in the scope of this penetration testing are certified OWASP WSGT version 4.2

We are available at security@sayfer.io

If you want to encrypt your message please use our public PGP key:

https://sayfer.io/3D4A560F984C41BE.asc

Key ID: 3D4A560F984C41BE

Website: https://sayfer.io

Public email: info@sayfer.io

Phone: +972-559139416