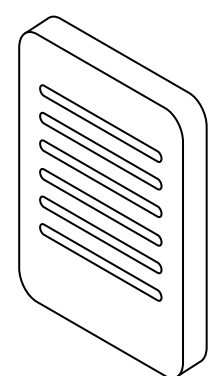




# Discordia

## Penetration Testing

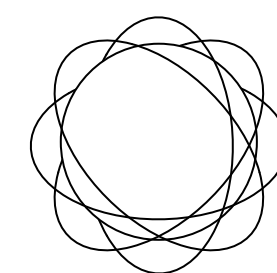


### Overview

DISCORDIA is the **largest transport and logistics company in Bulgaria**. Currently, the company is actively working with over 70 countries (40 of them are in Europe) and it is constantly expanding its global coverage.

Becoming a recognized **technological leader** in the industry is among the goals and ambitions of DISCORDIA. The company has already started working in this direction, investing in the integration of **digital and innovative software solutions** of the latest generation.

**Industry:** Transportation



### Challenge

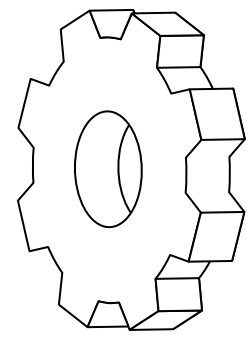
As a logistics provider, Discordia handles sensitive data, including customer information, delivery schedules, and financial transactions. Protecting this data from cyber threats is crucial to maintaining **customer trust and operational efficiency**.

Therefore, Discordia has sought the cooperation of Telelink Business Services requesting a professional **penetration testing service** to address the challenge of ensuring the security and integrity of their digital infrastructure.





# Discordia Penetration Testing

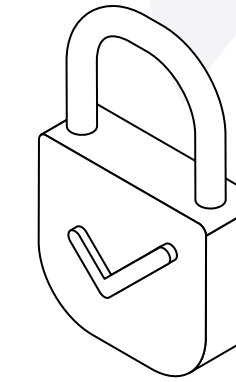


## Solution

During the pentest, all necessary measures were considered to avoid service disruption on the systems tested. An additional pentest was conducted to verify the security of the client's Wi-Fi networks.

### The pentest services included the following steps:

- **Defining and validating the scope** and requirements for a successful penetration test;
- **Preparation phase - gathering relevant information, outlining the steps;**
- **Security analysis** - penetration testing of Discordia's network infrastructure and Wi-Fi networks using the gray-box method;
- **Analysis and reporting of results** - creating a detailed report containing risk and impact assessment using the OWASP methodology, technical details of vulnerabilities found, remediation guidelines, etc.;
- **Follow-up meeting with the customer, presenting the report.**



## Results

**Pentest type:** Internal

**Pentest Model:** Gray-box

### Pentest Objectives:

- Tested overall security
- Tested attack detection
- Tested attack prevention
- Tested how well company data is protected
- Tested specific services, devices, or network