**CTF Topic: GraphQL Security**

****

**Introduction**

****

In this CTF challenge, you will explore the security aspects of GraphQL, a popular query language for APIs. While GraphQL provides powerful capabilities for querying data, it can also introduce security risks if not properly implemented. Your task is to identify and exploit common security vulnerabilities in a GraphQL API.

**Tools and Requirements**

A computer with internet access

Web browser

**Link**

**Scenario**

****

You have been given access to a GraphQL API endpoint that is suspected to have security vulnerabilities. Your task is to perform various security assessments to identify and exploit these vulnerabilities, ensuring the API is secure against common attacks.

**Process to follow while performing CTF.**

**Step 1:** Go to your browser and open the provided link: <https://graphql.security/>

**Step 2:** Enter the URL <https://kavyaschool.edu.np/> in the field and click on the **start scan** option.

**Questions**

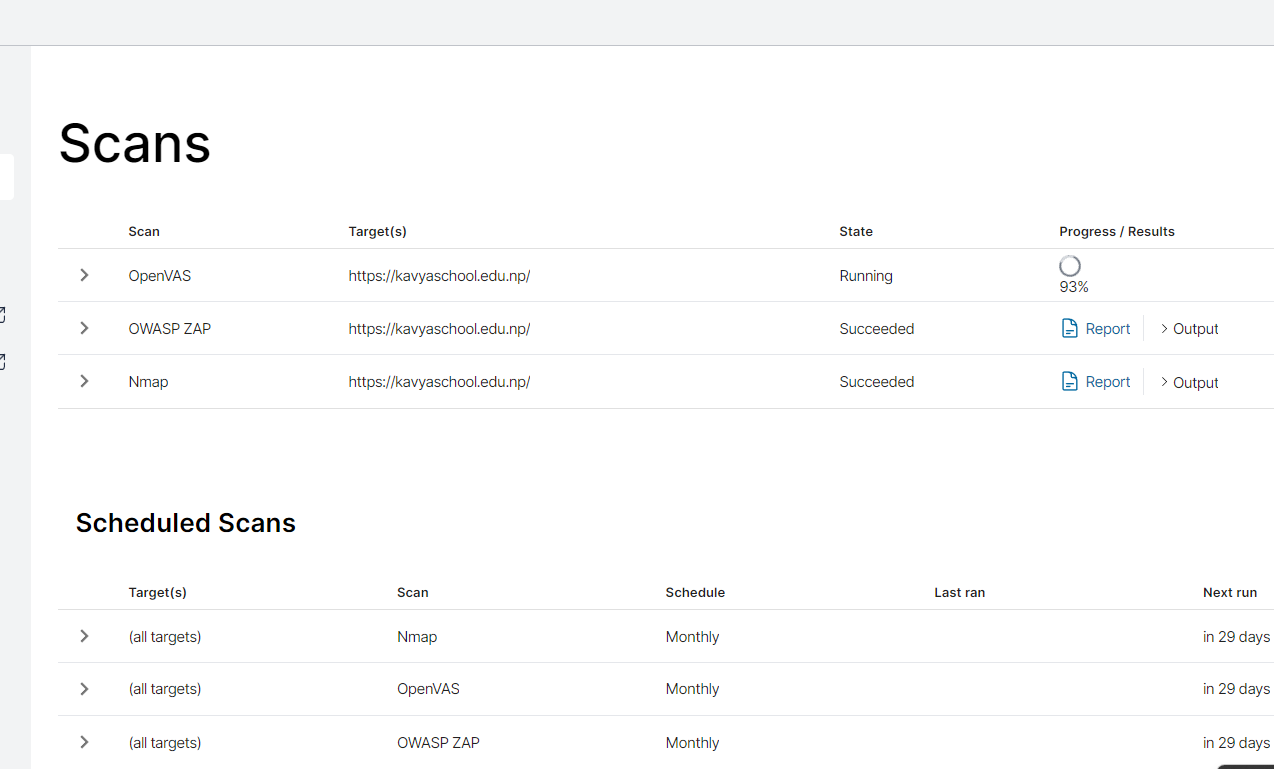
**Flag 1 : What is the scan that was performed by the graphql security?**

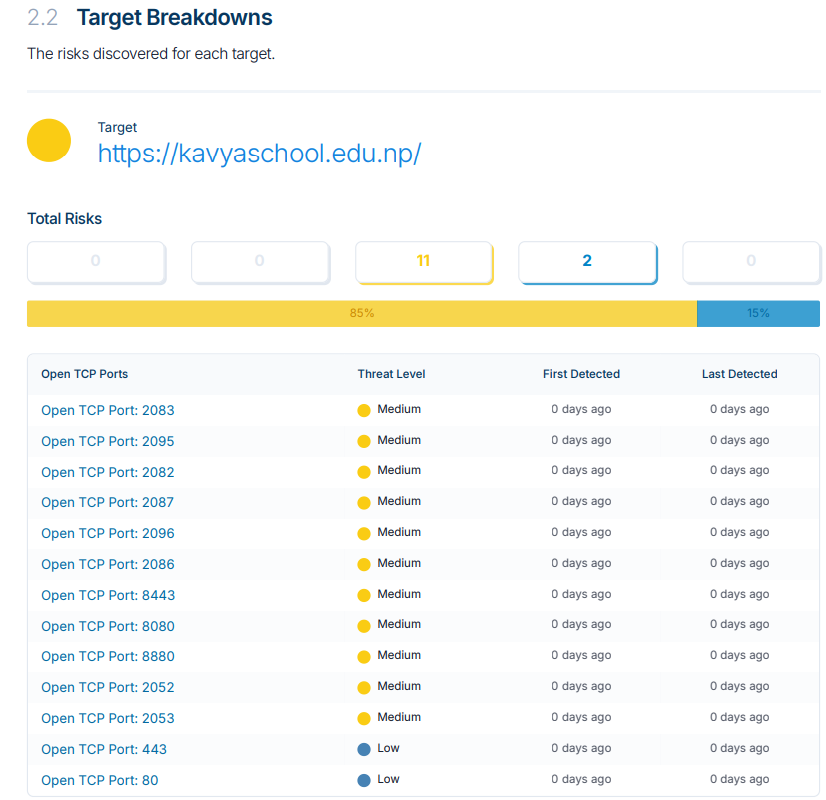
**Ans:** OpenVAS, OWASP ZAP and Nmap

**Flag 2 : What is the total risk for each target?**

**Ans:** 13

**Hint**

****

****