# **CTF Challenge: SSL/TLS Configuration Assessment Using CryptCheck**



# **1. Introduction**

CryptCheck is a tool designed to evaluate the SSL/TLS configuration of websites and identify potential security issues. This challenge will introduce you to using CryptCheck to assess the SSL/TLS configuration of a specific website.



# **2. Tools and Requirements**

Access to the internet and search for cryptcheck.fr

# **3. Scenario**

You are a security consultant tasked with evaluating the SSL/TLS configuration of a client's website using CryptCheck. Your objective is to determine the overall grade of the SSL/TLS configuration and identify one specific issue that needs to be addressed.



# **4. Process to Follow while Performing CTF**

1. Go to CryptCheck: [**https://cryptcheck.fr/**](https://cryptcheck.fr/)

2. Enter the URL [**www.daraz.com.np**](http://www.daraz.com.np)in the search bar and start the performance test.

3. Solve the CTF.

# **5. Let’s Begin the Challenge**

**Question**

**Flag 1: What key exchange mechanisms are used in the TLSv1.2 connections listed for** [**www.daraz.com.np**](http://www.daraz.com.np)**?**

*Answer: ECDHE-ECDSA and ECDHE-RSA*

**Flag 2: What encryption algorithms and their respective key sizes are used in the provided TLSv1.2 connections?**

*Answer: AES 128, 256*

**Hint:**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated