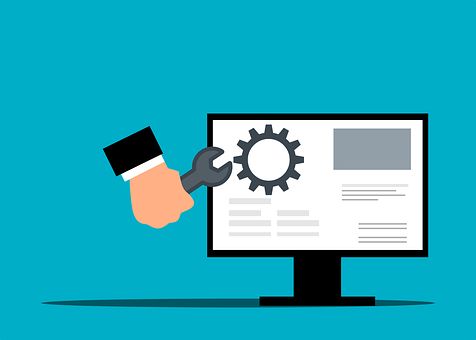
# **CTF Challenge: Website Security Assessment - Using Hardenize**



# **1. Introduction**

Hardenize is a comprehensive platform that provides a detailed analysis of website security configurations, including HTTPS, DNS, email, and other protocols. This challenge will introduce you to using Hardenize to gather information about the security posture of a specific domain.

# **2. Tools and Requirements**

Access to the internet and search for **Hardenize**

# **3. Scenario**



You are a cybersecurity consultant hired to perform a security assessment of a client's new domain. Your task is to use Hardenize to determine the security configurations and identify one relevant security issue associated with the domain.

# **4.Process to follow while performing CTF**

1. Go to **Hardenize**: [**https://www.hardenize.com/**](https://www.hardenize.com/)

2. Search: Enter the domain[**http://www.itsecgames.com/**](http://www.itsecgames.com/)in the search bar and click on run option.

3. Solve the CTF.

# **5. Let’s Begin the Challenge**

**Question**

**Flag 1: Which Transport Layer Security Version has been used?**

*Answer: TLS 1.2*

**Flag 2: Is TLS 1.2 supported or not supported?**

*Answer: Supported*

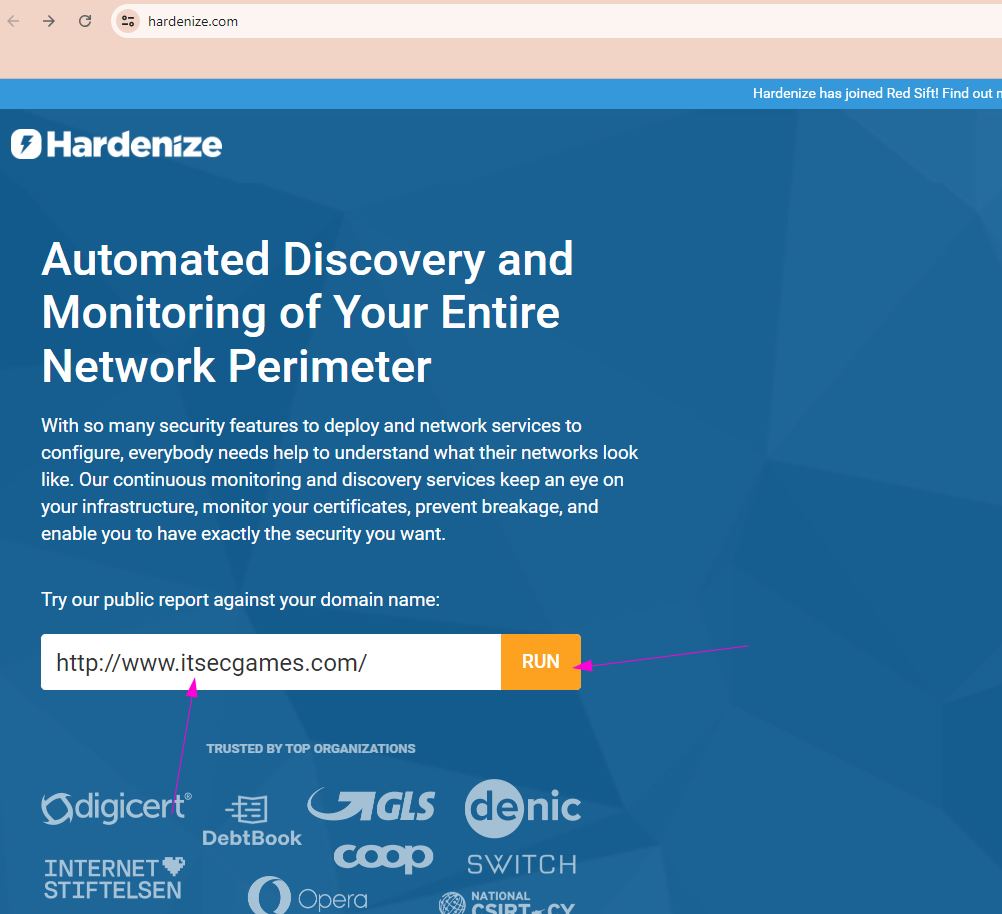
**Flag 3: Has the email certificate been passed?**

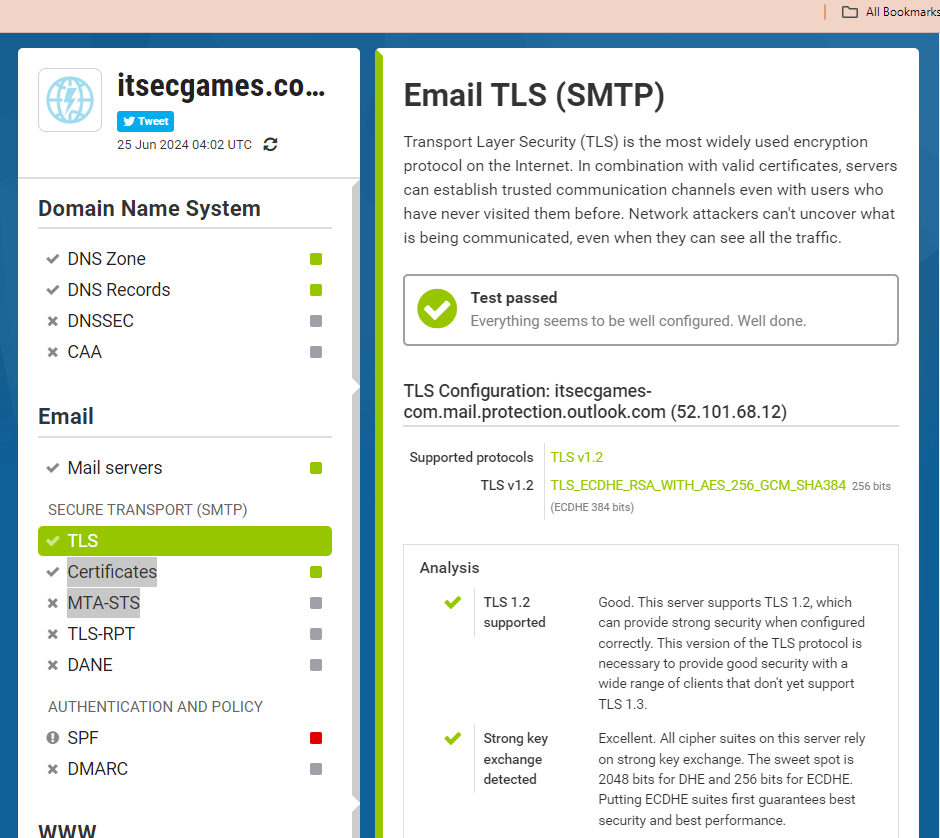
*Answer: Passed*

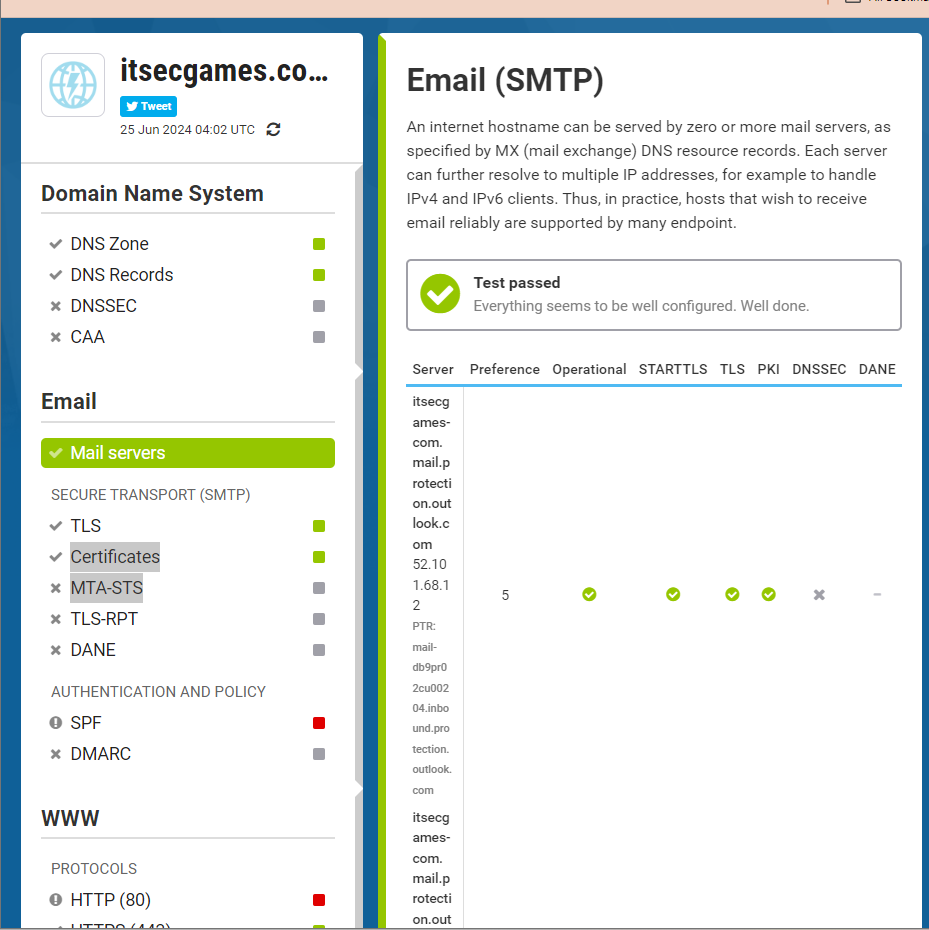
**Flag 4: Has the HTTP (80) Failed the test or Passed?**

*Answer: Failed*

**Hint**







A screenshot of a computer

Description automatically generated