# **CTF Challenge: Investigating Website Security - Using Crt.sh**



# **1. Introduction**

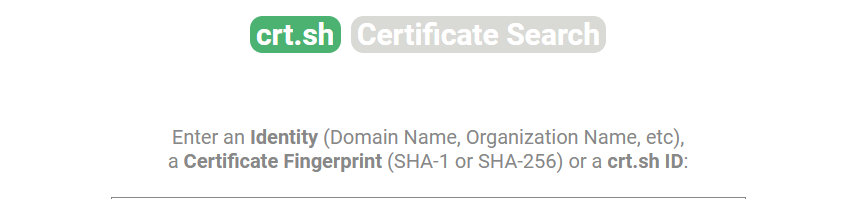


Crt.sh is a certificate transparency log monitoring tool that provides information about issued SSL certificates for domains. This challenge will introduce you to using Crt.sh to gather information about SSL certificates associated with a specific domain.

# **2. Tools and Requirements**

Access to the internet and search for Crt.sh

# **3. Scenario**



You are a cybersecurity analyst working for a company that has recently acquired a new domain. Your task is to investigate if any SSL certificates have been issued for this domain using Crt.sh. You need to determine if any certificates exist and identify one relevant detail associated with one of the certificates.

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

1. Go to Crt.sh: [**https://crt.sh/**](https://crt.sh/)

2. Search: Enter the domain [**www.ingskill.com**](http://www.ingskill.com) in the search bar and start the search.

3. Click on  **ID Number** **13269794235** and solve the CTF.

# **5. Let’s Begin the Challenge**

**Question**

**Flag 1: Have any certificates been issued for the domain?**

*Answer: 22*

**Flag 2: Open the ID Number** **13269794235 and find what signature Algorithm has been seen there?**

*Answer: sha256WithRSAEncryption*

**Flag 3: What is the Public key bit?**

*Answer: 256 bit*

**Flag 4: What is the organization name?**

*Answer: Let’s Encrypt*

**Hint**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated