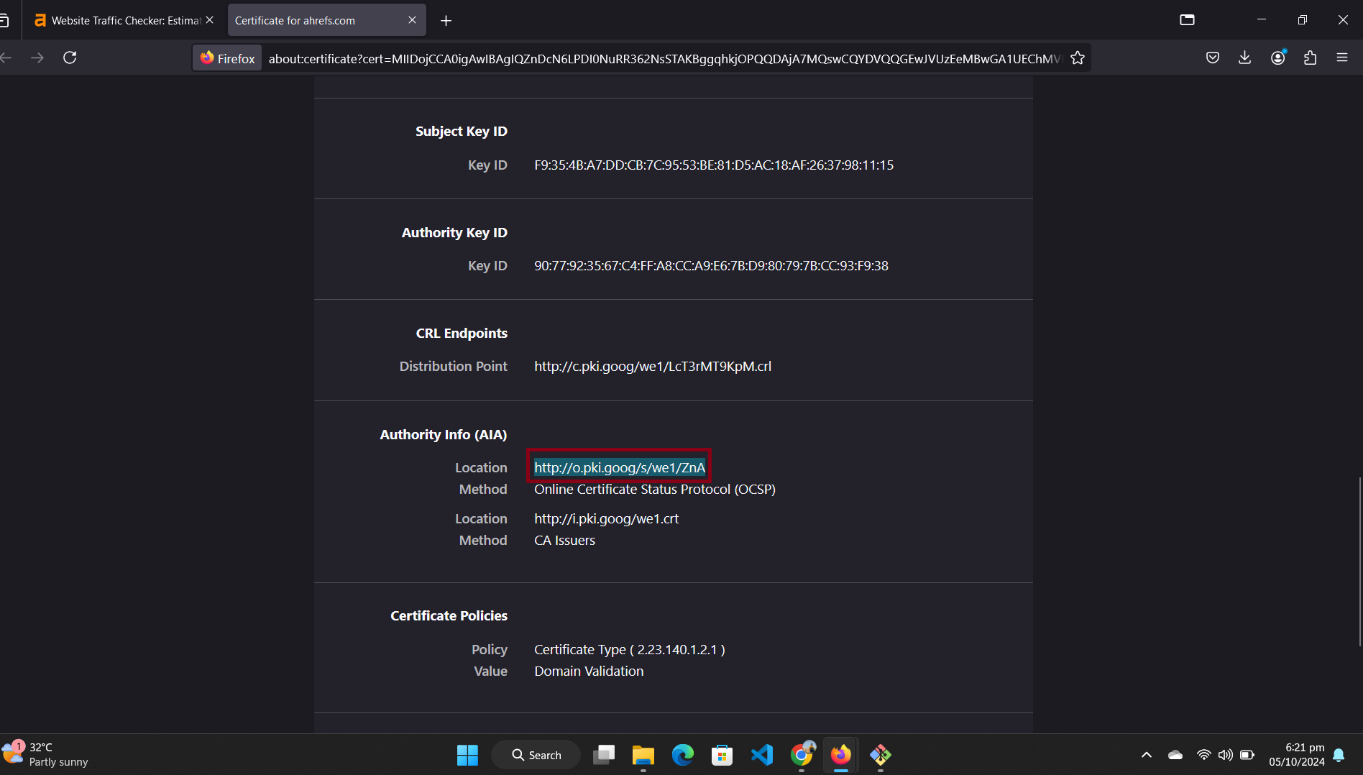
21L-6197

Information Security Assignment 2

**Question 1**

* First download and install the OpenSSL and the Git for windows.
* The open the random website <https://ahrefs.com/traffic-checker> (Website Traffic Checker).
* Follow the steps mentioned in the assignment manual.

Authority Info Link



OCSP query and response.A screenshot of a computer

Description automatically generated

As the steps mentioned in the manual by following those steps achieve the required results.

**Question 2**

Brave, like Chrome, soft-fails when an OCSP responder is down or unreachable. This means that if the browser cannot verify the certificate status (e.g., due to OCSP responder downtime), it allows the site to load as if the certificate were valid.

From a security standpoint, this handling is not ideal. If a revoked certificate is allowed through during an OCSP outage, users may be exposed to potential attacks like man-in-the-middle (MITM). However, this approach ensures that users can still access websites without interruptions caused by temporary network issues.

**Question 3**

To validate that the OCSP response is genuine and not forged, the following mechanisms are involved:

* Digital Signatures: The OCSP response is signed by the OCSP responder using its private key. Brave (like chrome) verifies the signature with the aid of public key in the CA's certificate.
* Timestamping: The response is time-stamped so that there cannot be a replay attack; it does not allow a hacker to reuse a previously sent valid answer to receive an accredited value when revocation checks may not be performed on it.
* OCSP Stapling: OCSP stapling makes use of the cache of the stored certificate response on the server, thus making the possibility for an attacker to manipulate an active OCSP query highly improbable.

**Question 4**

One of the major privacy concerns about the OCSP mechanism is that whenever the user is visiting a site, the browser requests the OCSP responder to check the status of the certificate. This sends communication to third parties, who may include the certificate authority or intermediaries.

OCSP Stapling:

Brave supports OCSP stapling, which is known to be widely admitted to greatly improve privacy. In OCSP stapling. So, in doing so, the server queries the OCSP responder and staples the signed response to its SSL/TLS handshake. Consequently, the browser doesn't need to issue an OCSP query directly; thereby, preserving user privacy.

Certificate status verification and preventing third parties from tracking user behavior can thus be simultaneously ensured by eliminating the need for real-time OCSP queries through stapling.

**Question 5**

As part of the Chromium family, Brave doesn’t rely on real-time OCSP checks for revocation checking. Instead, it employs other methods like CRLSets and OCSP Stapling.

Modern Methods:

CRLSets:

Brave uses CRLSets, which are pre-downloaded lists of revoked certificates distributed by Google. These lists are updated periodically, allowing the browser to check for revocation locally.

Merits: Faster and more reliable than OCSP, as it doesn’t require real-time checks.

Demerits: CRLSets are incomplete and only cover high-risk certificates, potentially missing some revoked certificates.

OCSP Stapling:

Brave supports OCSP stapling, which allows the server to provide the certificate’s revocation status during the SSL/TLS handshake.

Merits: Improves both performance and privacy, as no additional requests to an OCSP server are required.

Demerits: If the server doesn’t implement OCSP stapling properly, the browser may not get the necessary revocation information.

Short-Lived Certificates:

A growing trend is the use of short-lived certificates, which expire quickly (within days or weeks). This reduces the need for revocation checking since compromised certificates will expire naturally in a short timeframe.

Merits: No revocation checks are required, reducing the complexity and overhead.

Demerits: Requires more frequent certificate renewals, which can place a burden on server administrators.