Alex Warden
COSC583
Project 2
10/23/2025

A. Website key properties summary.
    1. utk.instructure.com : Overall Rating - A+
    - Subject: cluster95.canvas-user-content.com
      Common name: cluster95.canvas-user-content.com
      Alternative names: cluster95.canvas-user-content.com *.instructure.com instructure.com canvaslms.com *.canvaslms.com *.cluster95.canvas-user-content.com
    - Validity period: Mon, 02 Jun 2025 00:00:00 UTC - Wed, 01 Jul 2026 23:59:59 UTC (expires in 8 months and 6 days)
    - Type of cryptographic key: RSA 2048 bits (e 65537)
    - Certificate chain: cluster95.canvas-user-content.com > Amazon RSA 2048 M03 > Amazon Root CA 1
    - Authentication algorithm: SHA256withRSA
    - Symmetric algorithm: AES or CHACHA20, 128 or 256 bit, GCM
    - Hashing algorithm: SHA-2
    - Cryptographic guarantees: Confidentiality, Integrity, Forward Secrecy
    - Uses Amazon Trust Services for certificate management, which is why we had the issues last week.
    - Only allows for TLS 1.3 and 1.2
    - Uses HSTS to help prevent man in the middle attacks.

    2. www.amazon.com : Overall Rating - B
    - Subject: www.amazon.com
      Common name: www.amazon.com
      Alternative names: amazon.com amzn.com uedata.amazon.com us.amazon.com www.amazon.com www.amzn.com corporate.amazon.com buybox.amazon.com iphone.amazon.com yp.amazon.com home.amazon.com origin-www.amazon.com
    - Validity period: Fri, 24 Oct 2025 00:00:00 UTC - Tue, 20 Oct 2026 23:59:59 UTC (expires in 11 months and 25 days)
    - Type of cryptographic key: RSA 2048 bits (e 65537)
    - Certificate chain: www.amazon.com > DigiCert Global CA G2 > DigiCert Global Root G2
    - Authentication algorithm: SHA256withRSA
    - Symmetric algorithm: AES or CHACHA20, 128 or 256 bit, GCM
    - Hashing algorithm: SHA-2

- Cryptographic guarantees: Confidentiality, Integrity, Forward Secrecy
- Supports TLS 1.1 and 1.0, which hurt it's grade.
- Also uses HSTS.
- Has a large list of alternative names (list shortened some here for brevity sake).

3. www.youtube.com : Overall Rating - B

- Subject: *.google.com
  Common name: *.google.com
  Alternative names: googletraveladservices-cn.com
  *.googletraveladservices-cn.com googletagservices-cn.com
  *.googletagservices-cn.com googletagmanager-cn.com
- Validity period:Wed, 01 Oct 2025 14:32:25 UTC - Wed, 24 Dec 2025 14:32:24 UTC (expires in 1 month and 29 days)
- Type of cryptographic key: EC 256 bits
- Certificate chain: *.google.com > WE2 > GTS Root R4
- Authentication algorithm: SHA256withECDSA
- Symmetric algorithm: AES or CHACHA20, 128 or 256 bit, GCM
- Hashing algorithm: SHA-2
- Cryptographic guarantees: Confidentiality, Integrity, Forward Secrecy
- Uses EC 256 bits unlike the other website.
- Supports TLS 1.1 and 1.0 which are outdated.
- Another huge list of alternative names.

4. www.reddit.com : Overall Rating - A+

- Subject: *.reddit.com
  Common name: *.reddit.com
  Alternative names: *.reddit.com reddit.com
- Validity period: Sat, 12 Jul 2025 00:00:00 UTC - Wed, 07 Jan 2026 23:59:59 UTC (expires in 2 months and 13 days)
- Type of cryptographic key: RSA 2048 bits (e 65537)
- Certificate chain: *.reddit.com > DigiCert Global G2 TLS RSA SHA256 2020 CA1 > DigiCert Global Root G2
- Authentication algorithm: SHA256withRSA
- Symmetric algorithm: AES or CHACHA20, 128 or 256 bit, GCM
- Hashing algorithm: SHA-2
- Cryptographic guarantees: Confidentiality, Integrity, Forward Secrecy
- Only allows for TLS 1.3 and 1.2, which is surprising given the previous two results.
- Has a much shorter alternative names list, again surprising to me.

- Reddit scored significantly better than Amazon and Youtube, which was the opposite of my expectations.

5. discord.com : Overall Rating - A+

- Subject: discord.com
  Common name: discord.com
- Alternative names: discord.com *.discord.com
- Validity period: Mon, 08 Sep 2025 08:33:25 UTC- Sun, 07 Dec 2025 09:33:08 UTC (expires in 1 month and 11 days)
- Type of cryptographic key: EC 256 bits
- Certificate chain: discord.com > WE1 > GTS Root R4
- Authentication algorithm: SHA256withECDSA
- Symmetric algorithm: AES or CHACHA20, 128 or 256 bit, GCM
- Hashing algorithm: SHA-2
- Cryptographic guarantees: Confidentiality, Integrity, Forward Secrecy
- Implements HSTS.
- Safari 6-8 IOS sent Server sent fatal alert: handshake_failure in the handshake simulation
- Is using EC 256 bits, I'm curious the main reasons a company decides one over the other.

6. www.artstation.com : Overall Rating - A-

- Subject: artstation.com
  Common name: artstation.com
- Alternative names: artstation.com *.artstation.com
- Validity period: Sat, 20 Sep 2025 07:32:04 UTC – Fri, 19 Dec 2025 08:28:24 UTC (expires in 1 month and 23 days)
- Type of cryptographic key: RSA 2048 bits (e 65537)
- Certificate chain: artstation.com > WE1 > GTS Root R4
- Authentication algorithm: SHA256withRSA
- Symmetric algorithm: AES or CHACHA20, 128 or 256 bit, GCM
- Hashing algorithm: SHA-2
- Cryptographic guarantees: Confidentiality, Integrity, Forward Secrecy
- Results said Server sent invalid/disabled HSTS policy. No previous websites had an issue with HSTS.
- Scored an A-, was it only because of the HSTS issue?
- Only allows for TLS 1.3 and 1.2, good for them.

7. scryfall.com : Overall Rating - A+

- Subject: scryfall.com
  Common name: scryfall.com
- Alternative names: scryfall.com *.scryfall.com
- Validity period: Fri, 12 Sep 2025 14:08:03 UTC – Thu, 11 Dec 2025 15:06:22 UTC (expires in 1 month and 16 days)
- Type of cryptographic key: RSA 2048 bits (e 65537)
- Certificate chain: scryfall.com > WR1 > GTS Root R1
- Authentication algorithm: SHA256withRSA
- Symmetric algorithm: AES or CHACHA20, 128 or 256 bit, GCM
- Hashing algorithm: SHA-2
- Cryptographic guarantees: Confidentiality, Integrity, Forward Secrecy
- Their score was higher than I was expecting considering they are just a card database.
- There was also a DNS CAA Policy found for this domain.
- According to the SSL report, this site works only in browsers with SNI support.

8. edhrec.com : Overall Rating - A+

- Subject: edhrec.com
  Common name: edhrec.com
- Alternative names: edhrec.com *.edhrecstatic.com *.edhrecstaticjson.com
- Validity period: Sun, 24 Aug 2025 00:00:00 UTC – Tue, 22 Sep 2026 23:59:59 UTC (expires in 10 months and 28 days)
- Type of cryptographic key: RSA 2048 bits (e 65537)
- Certificate chain: edhrec.com > Amazon RSA 2048 M04 > Amazon Root CA 1
- Authentication algorithm: SHA256withRSA
- Symmetric algorithm: AES or CHACHA20, 128 or 256 bit, GCM
- Hashing algorithm: SHA-2
- Cryptographic guarantees: Confidentiality, Integrity, Forward Secrecy
- Also seems to use Amazon in the same way canvas does. I'm curious if this website was also experiencing issues.
- Also has a DNS CAA Policy and only works in browsers with SNI support.
- Handshake simulation IE 11 Windows and Windows Phone 7-8 gave Protocol or cipher suite mismatch.

9. charactermodel.gallery : Overall Rating - B

- Subject: charactermodel.gallery
  Common name: charactermodel.gallery
- Alternative names: charactermodel.gallery *.charactermodel.gallery

- Validity period: Wed, 15 Oct 2025 06:20:49 UTC – Tue, 13 Jan 2026 07:18:29 UTC (expires in 2 months and 18 days)
- Type of cryptographic key: EC 256 bits
- Certificate chain: charactermodel.gallery > WE1 > GTS Root R4
- Authentication algorithm: SHA256withECDSA
- Symmetric algorithm: AES or CHACHA20, 128 or 256 bit, GCM
- Hashing algorithm: SHA-2
- Cryptographic guarantees: Confidentiality, Integrity, Forward Secrecy
- Does not seem to support HSTS.
- Only works in browsers with SNI support.
- Even though this is the website I expected to score the lowest, it still got a B

10. ifunny.co : Overall Rating - A-

- Subject: *.ifunny.co
  Common name: *.ifunny.co
- Alternative names: *.ifunny.co, ifunny.co
- Validity period: Fri, 05 Sep 2025 12:57:07 UTC – Wed, 07 Oct 2026 12:57:07 UTC (expires in 11 months and 11 days)
- Type of cryptographic key: RSA 2048 bits (e 65537)
- Certificate chain: *.ifunny.co > Go Daddy Secure Certificate Authority – G2 > Go Daddy Root Certificate Authority – G2
- Authentication algorithm: SHA256withRSA
- Symmetric algorithm: AES or CHACHA20, 128 or 256 bit, GCM
- Hashing algorithm: SHA-2
- Cryptographic guarantees: Confidentiality, Integrity, Forward Secrecy
- Has TLS 1.1 and 1.0 disabled, but does not support 1.3
- Hosted on GoDaddy infrastructure.
- Has one of the longest validity periods besides Amazon.

B. Every site relied on SHA-2 hashing and supported AES or ChaCha20 ciphers in GCM mode. All certificates used either RSA 2048-bit or EC 256-bit keys. The main differences came from key types and protocol support. Some sites like Discord and Scryfall used faster EC keys, while others such as Amazon and Reddit still used RSA. The highest scoring websites disabled older TLS 1.0 and 1.1 protocols and fully supported TLS 1.2 or 1.3, while lower scoring ones kept legacy protocol support. Certificate chains varied between Amazon, DigiCert, Google Trust Services, and GoDaddy, but all followed proper trust hierarchies.

C. How come most certificates are only for a few months or just shy of a year.
   What are the logistical differences between RSA 2048-bit or EC 256-bit?
   Why do some larger companies have so many alternative names, but others don't?
   What are the main benefits of supporting TLS 1.0 and 1.1?

Peer Review done by: Margaret Kelley

While I only briefly looked at the requirements for this report, it is very well organized, clearly formatted, and gives a strong understanding of SSL/TLS security concepts. For each site summary there is a consistent structure (which I really enjoy and makes it easier to read/compare results). I especially liked that you highlighted the different patterns found in each of the topics.

While overall I think this is very well written, many sections repeat the same cryptographic guarantees. Again, I don't know the assignment, but from a reader's POV I think you could summarize those once at the end instead of repeating them for every site (for an assignment, personally I would not do this, but critiquing as a reader I thought I would mention this).

I think this could also benefit from adding little transition sentences or short analytical comments that would make the report read more smoothly. Overall I think it's really good, though! I think you worked very hard on this and it shows.