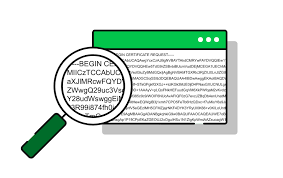
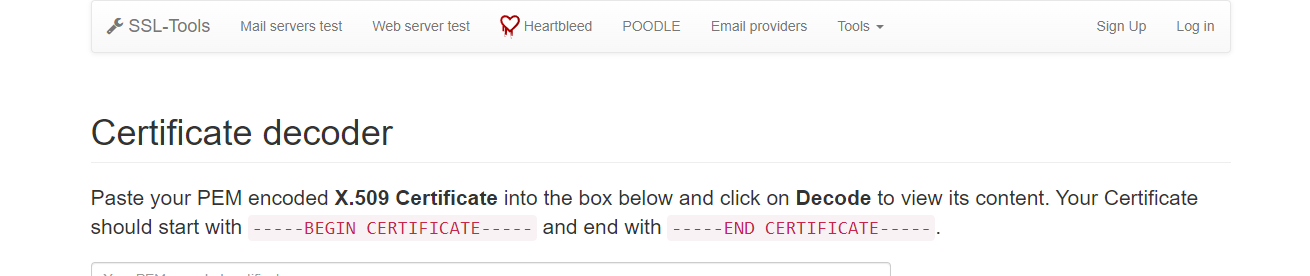
**Certificate Decoder**



**Introduction**



A certificate decoder is a tool used to decode SSL/TLS certificates to reveal their detailed information. This is essential for verifying certificate properties, checking for configuration issues, and ensuring compliance with security standards.

****

**Scenario**

Imagine you are a network administrator responsible for managing the security of your organization's web servers. You receive an SSL certificate and need to verify its details to ensure it meets your security policies before deploying it on your server. Using the certificate decoder tool at <https://ssl-tools.net/certificate-decoder> , you will decode and analyze the certificate.

**Process to Perform**

**Step 1:** Click on this link to access Certificate decoder <https://ssl-tools.net/certificate-decoder> or open any web browser on your PC and type **SSLtools** in the address bar.

**Step 2:** Click on the second link and click on certificate decoder on **X509 Decoder**

**Step 3:** Copy the given encoded certificate below and paste in the given box and click on decode

**Step 4:** Capture the Flag

**Certificate (Copy all From Being certificate to end certificate)**

-----BEGIN CERTIFICATE-----

MIICYzCCAcygAwIBAgIBADANBgkqhkiG9w0BAQUFADAuMQswCQYDVQQGEwJVUzEM

MAoGA1UEChMDSUJNMREwDwYDVQQLEwhMb2NhbCBDQTAeFw05OTEyMjIwNTAwMDBa

Fw0wMDEyMjMwNDU5NTlaMC4xCzAJBgNVBAYTAlVTMQwwCgYDVQQKEwNJQk0xETAP

BgNVBAsTCExvY2FsIENBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD2bZEo

7xGaX2/0GHkrNFZvlxBou9v1Jmt/PDiTMPve8r9FeJAQ0QdvFST/0JPQYD20rH0b

imdDLgNdNynmyRoS2S/IInfpmf69iyc2G0TPyRvmHIiOZbdCd+YBHQi1adkj17ND

cWj6S14tVurFX73zx0sNoMS79q3tuXKrDsxeuwIDAQABo4GQMIGNMEsGCVUdDwGG

+EIBDQQ+EzxHZW5lcmF0ZWQgYnkgdGhlIFNlY3VyZVdheSBTZWN1cml0eSBTZXJ2

ZXIgZm9yIE9TLzM5MCAoUkFDRikwDgYDVR0PAQH/BAQDAgAGMA8GA1UdEwEB/wQF

MAMBAf8wHQYDVR0OBBYEFJ3+ocRyCTJw067dLSwr/nalx6YMMA0GCSqGSIb3DQEB

BQUAA4GBAMaQzt+zaj1GU77yzlr8iiMBXgdQrwsZZWJo5exnAucJAEYQZmOfyLiM

D6oYq+ZnfvM0n8G/Y79q8nhwvuxpYOnRSAXFp6xSkrIOeZtJMY1h00LKp/JX3Ng1

svZ2agE126JHsQ0bhzN5TKsYfbwfTwfjdWAGy6Vf1nYi/rO+ryMO

-----END CERTIFICATE-----

**Question**

Flag 1: What is the version of the certificate?

Answer: 3

Flag Captured

Flag 2: How many bit is the RSA Public key?

Answer: 1024 bit

Flag Captured

Flag 3: What is X509v3 Subject Key Identifier?

Answer: 9D:FE:A1:C4:72:09:32:70:D3:AE:DD:2D:2C:2B:FE:76:A5:C7:A6:0C

Flag Captured

Hint

