CSR Decoder and Certificate Decoder


```
-----BEGIN CERTIFICATE REQUEST-----
MIICmzCCAYMCAQAwVjELMAkGA1UEBgwCVVMxGDAWBgNVBAoMD0FsbGV5T29wIFNv
Y2lhbDEYMBYGA1UECwwPQWxsZXlPb3AgU29jaWFsMRMwEQYDVQQDDAp5ZlFYWmZ6
QWRBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsve8K2VYirLF+M6s
NCBwRi1vRJlDVHzte5yKCTXSmid++Op9i2pPp3UC34w7n7YOHLLvjy6ydHOeuTTd
uIw6cpA46UskRYhS8NY+btchWywtv8Qp4SK+ZFg2b4gZej/4BV1cqt2q8linslL0
zdWQ0+xsgP/5CO092FrpxGsP6GAkANdCrMxQ3+muxa6ZLpsPB9UEiZKH/ZejU5as
KqCO7H4AyXFtB5l/ehfefvkS0ZyV0ezCId59EGBWTSM4HaHY6I/dWn8x5f6WCbYQ
7SULm0qdIDWr8czSfaq84Bfkf8jcZcZ9qy8NnVy7MQGAglXwacDnyU2gUlk3PalD
5sbSFQIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAH0tAmubbEd7TSrYG9sz5Fc3
9MRDaRls9wOsS9ttiVGD8pS3Umycpp5zmPsmpqlB5KqEbhNTIyn8pY1DPMufKKB0
q7SNbV9lw+P0xv7zIpqhteemmMqkFm8BaOl7HyB814Xbx3PzDLAOrYgndqgbslxS
T+xZCw2tyZCi+CE5AQ79C0gh/aT1+Njtgfl9XXsub+yHrmEmKzmgcJwFOmg3+yWA
PKEK7W3flU5k6WODXEjZCNgsVUOEX8Y/X/cq6lugbTAORhw8dPk+9JztNuBjghQD
z56VwDRUwLI8XQ/AMeARBjTUQoYFHPRHlA0FG5ALuF3XKS9+5zWTmZ865qGVtWM=
-----END CERTIFICATE REQUEST-----
```


Or Choose File...

Decode

CSR Summary

CSR Checks

Check	Result
Debian Weak Key	PASSED - Does not use a key on our blacklist - this is good
Key Size	PASSED (2048 bits)
Signature	PASSED - CSR has a valid signature
MD5	PASSED - Not using the MD5 algorithm

CSR Subject

Common Name (CN)	yfQXZfzAdA
Organizational Unit (OU)	AlleyOop Social
Organization (O)	AlleyOop Social
Country (C)	US

CSR Properties

Subject	C=US, O=AlleyOop Social, OU=AlleyOop Social, CN=yfQXZfzAdA
Key Size	2048 bits
Key Algorithm	RSA
Sig. Algorithm	sha256WithRSAEncryption
SHA256 Fingerprint	7B:18:AA:0C:9D:B6:12:A2:DC:33:5D:B9:BF:9B:F3:C9:B7:A1:C6:93:6C:50:E9:A6:AC:1A:11:AE:AE:A9:CB:B6
SHA1 Fingerprint	A3:27:C3:90:91:E4:44:3E:23:E7:D0:FD:F2:76:50:33:B1:5C:5B:A7

MD5 Fingeprint	1A:57:FF:99:B9:B4:0B:C7:DC:77:0F:36:1A:06:2A:9F
SANS	

CSR Detailed Information

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=US, O=AlleyOop Social, OU=AlleyOop Social, CN=yfQXZfzAdA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b2:f7:bc:2b:65:58:8a:b2:c5:f8:ce:ac:34:20:
                    70:46:2d:6f:44:99:43:54:7c:ed:7b:9c:8a:09:35:
                    d2:9a:27:7e:f8:ea:7d:8b:6a:4f:a7:75:02:df:8c:
                    3b:9f:b6:0e:1c:b2:ef:8f:2e:b2:74:73:9e:b9:34:
                    dd:b8:8c:3a:72:90:38:e9:4b:24:45:88:52:f0:d6:
                    3e:6e:d7:21:5b:2c:2d:bf:c4:29:e1:22:be:64:58:
                    36:6f:88:19:7a:3f:f8:05:5d:5c:aa:dd:aa:f2:58:
                    a7:b2:52:f4:cd:d5:90:d3:ec:6c:80:ff:f9:08:ed:
                    3d:d8:5a:e9:c4:6b:0f:e8:60:24:00:d7:42:ac:cc:
                    50:df:e9:ae:c5:ae:99:2e:9b:0f:07:d5:04:89:92:
                    87:fd:97:a3:53:96:ac:2a:a0:8e:ec:7e:00:c9:71:
                    6d:07:99:7f:7a:17:de:7e:f9:12:d1:9c:95:d1:ec:
                    c2:21:de:7d:10:60:56:4d:23:38:1d:a1:d8:e8:8f:
                    dd:5a:7f:31:e5:fe:96:09:b6:10:ed:25:0b:9b:4a:
                    9d:20:35:ab:f1:cc:d2:7d:aa:bc:e0:17:e4:7f:c8:
                    dc:65:c6:7d:ab:2f:0d:9d:5c:bb:31:01:80:82:55:
                    f0:69:c0:e7:c9:4d:a0:52:59:37:3d:a9:43:e6:c6:
                    d2:15
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         7d:2d:02:6b:9b:6c:47:7b:4d:2a:d8:1b:db:33:e4:57:37:f4:
         c4:43:69:19:6c:f7:03:ac:4b:db:6d:89:51:83:f2:94:b7:52:
         6c:9c:a6:9e:73:98:fb:26:a6:a9:41:e4:aa:84:6e:13:53:23:
         29:fc:a5:8d:43:3c:cb:9f:28:a0:74:ab:b4:8d:6d:5f:65:c3:
         e3:f4:c6:fe:f3:22:9a:a1:b5:e7:a6:98:ca:a4:16:6f:01:68:
         e9:7b:1f:20:7c:d7:85:db:c7:73:f3:0c:b0:0e:ad:88:27:76:
         a8:1b:b2:5c:52:4f:ec:59:0b:0d:ad:c9:90:a2:f8:21:39:01:
         0e:fd:0b:48:21:fd:a4:f5:f8:d8:ed:81:f9:7d:5d:7b:2e:6f:
         ec:87:ae:61:26:2b:39:a0:70:9c:05:3a:68:37:fb:25:80:3c:
         a1:0a:ed:6d:df:95:4e:64:e9:63:83:5c:48:d9:08:d8:2c:55:
         43:84:5f:c6:3f:5f:f7:2a:ea:5b:a0:6d:30:0e:46:1c:3c:74:
         f9:3e:f4:9c:ed:36:e0:63:82:14:03:cf:9e:95:c0:34:54:c0:
         b2:3c:5d:0f:c0:31:e0:11:06:34:d4:42:86:05:1c:f4:47:94:
         0d:05:1b:90:0b:b8:5d:d7:29:2f:7e:e7:35:93:99:9f:3a:e6:
         a1:95:b5:63
```

CSR ASN.1 Information

```
  0 667: SEQUENCE {
  4 387:   SEQUENCE {
  8   1:     INTEGER 0
 11  86:     SEQUENCE {
 13  11:       SET {
 15   9:         SEQUENCE {
 17   3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 22   2:           UTF8String 'US'
       :           }
       :         }
 26  24:       SET {
 28  22:         SEQUENCE {
 30   3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 35  15:           UTF8String 'AlleyOop Social'
       :           }
       :         }
 52  24:       SET {
 54  22:         SEQUENCE {
 56   3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 61  15:           UTF8String 'AlleyOop Social'
       :           }
       :         }
 78  19:       SET {
 80  17:         SEQUENCE {
 82   3:           OBJECT IDENTIFIER commonName (2 5 4 3)
 87  10:           UTF8String 'yfQXZfzAdA'
       :           }
       :         }
       :       }
 99 290:     SEQUENCE {
103  13:       SEQUENCE {
105   9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
116   0:         NULL
       :         }
118 271:       BIT STRING
       :         30 82 01 0A 02 82 01 01 00 B2 F7 BC 2B 65 58 8A
       :         B2 C5 F8 CE AC 34 20 70 46 2D 6F 44 99 43 54 7C
       :         ED 7B 9C 8A 09 35 D2 9A 27 7E F8 EA 7D 8B 6A 4F
       :         A7 75 02 DF 8C 3B 9F B6 0E 1C B2 EF 8F 2E B2 74
       :         73 9E B9 34 DD B8 8C 3A 72 90 38 E9 4B 24 45 88
       :         52 F0 D6 3E 6E D7 21 5B 2C 2D BF C4 29 E1 22 BE
       :         64 58 36 6F 88 19 7A 3F F8 05 5D 5C AA DD AA F2
       :         58 A7 B2 52 F4 CD D5 90 D3 EC 6C 80 FF F9 08 ED
       :                 [ Another 142 bytes skipped ]
       :       }
393   0:     [0]
       :       Error: Object has zero length.
       :     }
395  13:   SEQUENCE {
397   9:     OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
408   0:     NULL
       :     }
410 257:   BIT STRING
       :     7D 2D 02 6B 9B 6C 47 7B 4D 2A D8 1B DB 33 E4 57
       :     37 F4 C4 43 69 19 6C F7 03 AC 4B DB 6D 89 51 83
       :     F2 94 B7 52 6C 9C A6 9E 73 98 FB 26 A6 A9 41 E4
       :     AA 84 6E 13 53 23 29 FC A5 8D 43 3C CB 9F 28 A0
       :     74 AB B4 8D 6D 5F 65 C3 E3 F4 C6 FE F3 22 9A A1
       :     B5 E7 A6 98 CA A4 16 6F 01 68 E9 7B 1F 20 7C D7
       :     85 DB C7 73 F3 0C B0 0E AD 88 27 76 A8 1B B2 5C
       :     52 4F EC 59 0B 0D AD C9 90 A2 F8 21 39 01 0E FD
       :             [ Another 128 bytes skipped ]
       :   }
```

CSR Hex Encoded

```
3082029b30820183020100305631 0b300906035504060c025553311830160603
55040a0c0f416c6c65794f6f7020536f6369616c31183016060355040b0c0f41
6c6c65794f6f7020536f6369616c311330110603550403 0c0a796651585a667a
4164413082012230 0d06092a864886f70d01010105000382010f003082010a02
82010100b2f7bc2b65588ab2c5f8ceac342070462d6f449943547ced7b9c8a09
35d29a277ef8ea7d8b6a4fa77502df8c3b9fb60e1cb2ef8f2eb274739eb934dd
b88c3a729038e94b24458852f0d63e6ed7215b2c2dbfc429e122be6458366f88
197a3ff8055d5caaddaaf258a7b252f4cdd590d3ec6c80fff908ed3dd85ae9c4
6b0fe8602400d742accc50dfe9aec5ae992e9b0f07d504899287fd97a35396ac
2aa08eec7e00c9716d07997f7a17de7ef912d19c95d1ecc221de7d1060564d23
381da1d8e88fdd5a7f31e5fe9609b610ed250b9b4a9d2035abf1ccd27daabce0
17e47fc8dc65c67dab2f0d9d5cbb3101808255f069c0e7c94da05259373da943
e6c6d2150203010001a000300d06092a864886f70d01010b050003820101007d
2d026b9b6c477b4d2ad81bdb33e45737f4c44369196cf703ac4bdb6d895183f2
94b7526c9ca69e7398fb26a6a941e4aa846e13532329fca58d433ccb9f28a074
abb48d6d5f65c3e3f4c6fef3229aa1b5e7a698caa4166f0168e97b1f207cd785
dbc773f30cb00ead882776a81bb25c524fec590b0dadc990a2f82139010efd0b
4821fda4f5f8d8ed81f97d5d7b2e6fec87ae61262b39a0709c053a6837fb2580
3ca10aed6ddf954e64e963835c48d908d82c5543845fc63f5ff72aea5ba06d30
0e461c3c74f93ef49ced36e063821403cf9e95c03454c0b23c5d0fc031e01106
34d44286051cf447940d051b900bb85dd7292f7ee73593999f3ae6a195b563
```