|  |  |  |
| --- | --- | --- |
| **Host:** | **Weak Protocols & Ciphers:** | **Certificate Information:** |
| badssl.com  Port 443 | •TLSv1.2 112 bits ECDHE-RSA-DES-CBC3-SHA •TLSv1.2 112 bits DES-CBC3-SHA •TLSv1.1 112 bits ECDHE-RSA-DES-CBC3-SHA •TLSv1.1 112 bits DES-CBC3-SHA •TLSv1.0 128 bits ECDHE-RSA-AES128-SHA •TLSv1.0 256 bits ECDHE-RSA-AES256-SHA •TLSv1.0 128 bits DHE-RSA-AES128-SHA •TLSv1.0 256 bits DHE-RSA-AES256-SHA •TLSv1.0 112 bits ECDHE-RSA-DES-CBC3-SHA •TLSv1.0 128 bits AES128-SHA •TLSv1.0 256 bits AES256-SHA •TLSv1.0 112 bits DES-CBC3-SHA •TLSv1.0 256 bits DHE-RSA-CAMELLIA256-SHA •TLSv1.0 256 bits CAMELLIA256-SHA •TLSv1.0 128 bits DHE-RSA-CAMELLIA128-SHA | •Subject: \*.badssl.com •Issuer: DigiCert SHA2 Secure Server CA •Signature Algorithm: sha256WithRSAEncryption •Key Strength: 2048 •Expiration: Mar 25 12:00:00 2020 GMT |