COMODO SSL Checker (public documentation)

API URL: http(s)://secure.comodo.com/sslchecker
Example webpage: http(s)://secure.comodo.com/utilities/sslchecker.html

Version History

1.0 Original version.

The request parameters should be URL-encoded and GETed or POSTed to the URL quoted above. They are assumed to be encoded in UTF-8 and the response parameters will be encoded in UTF-8.

1. Request Parameters

Parameter	Description
`url`	A URL, Domain Name or IP Address. If no "protocol://" prefix is specified, "https://" is assumed. If no port number is specified, ":443" is assumed.
`response_format`	Format of the response data: • **0** (the default) = URL-encoded parameters in the Response Body. • **1** = HTTP 302 Redirect, with URL-encoded parameters in the Query String. • **2** = Dynamically-generated JavaScript.
`redirect_url`	A URL to redirect to (only relevant when `response_format=1`).
`caller_name`	A friendly name (or a description) to identify who or what is calling this API.

2. Response Parameters

Parameter	Description
`error_code`	One of the following integers: **0** = OK **-1** = "Chunked" encoding is unsupported **-2** = Unknown Content-Type **-3** = Unsupported Content-Type **-4** = Domain not found **-5** = Invalid Protocol/Port **-6** = Domain has no addresses **-7** = Permanent nameserver error **-8** = Temporary nameserver error **-9** = Unexpected error **-10** = Timed out while attempting to connect **-11** = Invalid Domain or URL (e.g. the supplied `url` is an empty string) **-12** = Unable to establish an SSL connection **-13** = No Site Certificate was returned **-14** = This protocol does not use SSL/TLS **-15** = Permission denied
`error_message`	A string describing the error (see description above for `error_code`).
`server_url`	The URL that was contacted.
`server_domain_isIDN`	**Y** = This is an Internationalized Domain Name. **N** = This is not an Internationalized Domain Name.
`server_domain_utf8`	The UTF-8 representation of the IDN. This parameter will only be present if `server_domain_isIDN=Y`.
`server_domain_ace`	The ASCII representation (with "xn--" bits) of the IDN. This parameter will only be present if `server_domain_isIDN=Y`.
`server_ip`	The IP Address at which the SSL Server was contacted.
`server_port`	The Port at which SSL Server was contacted.
`server_software`	A string describing the server software being used on the SSL Server. When the protocol is HTTPS, this is the value of the "Server:" HTTP response header, obtained by sending a "HEAD /robots.txt" request to the SSL Server. If the server software cannot be determined, the value of this parameter will be an empty string.
`cert_notBefore`	The "Not Before" date/time from the site certificate, expressed as number of seconds since the Unix "Epoch" (00:00:00 UTC on Jan 1st 1970). Note: It is recommended to use `cert_validity_notBefore` instead, because `cert_notBefore` cannot handle dates that are not in the range Jan 1st 1970 00:00:00 -> Jan 19th 2038 03:14:07 UTC.
`cert_notAfter`	The "Not After" date/time from the site certificate, expressed as number of seconds since the Unix "Epoch" (00:00:00 UTC on Jan 1st 1970). Note: It is recommended to use `cert_validity_notAfter` instead, because `cert_notAfter` cannot handle dates that

	are not in the range Jan 1st 1970 00:00:00 -> Jan 19th 2038 03:14:07 UTC.
cert_validity_notBefore	The "Not Before" date/time from the site certificate, expressed as YYYYMMDDhhmmss (e.g. 20070101000000).
cert_validity_notAfter	The "Not After" date/time from the site certificate, expressed as YYYYMMDDhhmmss (e.g. 20071231235959).
cert_key_algorithm	The algorithm for the Public Key from the site certificate: **RSA** = Rivest Shamir Adleman. **DSA** = Digital Signature Algorithm. If the algorithm is unknown, the value of this parameter will be an empty string.
cert_key_size	The size (in bits) of the Public Key from the site certificate.
cert_subject_DN	The full Subject Distinguished Name from the site certificate. Each attribute is separated by a newline character.
cert_subject_CN	The value of the first Subject Common Name attribute (the "CN" field). If no "CN" field is present, the value of this parameter will be an empty string.
cert_subject_OU	The value of the "most relevant" Subject Organizational Unit Name attribute (the "OU" field). The SSL Checker will ignore certain OU fields (common copyright notices, "Domain Control Validated", etc). If no "relevant" OU field is present, the value of this parameter will be an empty string.
cert_subject_O	The value of the Subject Organization Name attribute (the "O" field). If no "O" field is present, the value of this parameter will be an empty string.
cert_subject_streetAddress_1	The value of the first Subject Street Address attribute. If no such field is present, the value of this parameter will be an empty string.
cert_subject_streetAddress_2	The value of the second Subject Street Address attribute. If no more than 1 such field is present, the value of this parameter will be an empty string.
cert_subject_streetAddress_3	The value of the third Subject Street Address attribute. If no more than 2 such fields are present, the value of this parameter will be an empty string.
cert_subject_L	The value of the Subject Locality Name attribute (the "L" field). If no "L" field is present, the value of this parameter will be an empty string.
cert_subject_S	The value of the Subject State or Province Name attribute (the "S" field). If no "S" field is present, the value of this parameter will be an empty string.
cert_subject_postalCode	The value of the Subject Postal Code attribute. If no such field is present, the value of this parameter will be an empty string.
cert_subject_C	The value of the Subject Country Name attribute (the "C" field). If no "C" field is present, the value of this parameter will be an empty string.
cert_isMultiDomain	**Y** = This certificate contains more than 1 domain name. **N** = This certificate contains only 1 domain name.
cert_isWildcard	**Y** = This certificate contains 1 domain name with a Wildcard. **N** = This certificate contains only 1 domain name.
cert_issuer_DN	The full Issuer Distinguished Name from the site certificate. Each attribute is separated by a newline character.
cert_issuer_CN	The value of the Issuer Common Name attribute (the "CN" field). If no "CN" field is present, the value of this parameter will be an empty string.
cert_issuer_O	The value of the Issuer Organization Name attribute (the "O" field). If no "O" field is present, the value of this parameter will be an empty string.
cert_issuer_C	The value of the Issuer Country Name attribute (the "C" field). If no "C" field is present, the value of this parameter will be an empty string.
cert_issuer_brand	The brand name of the Issuer, as defined by the COMODO server-side. If the site certificate cannot be verified by an Issuer CA Certificate that is already known to COMODO, this parameter's value will be an empty string.
cert_policyOID	The Policy OID from the site certificate.
cert_validation	**SS** = Self-signed **NV** = No Validation (i.e. an unvalidated demo/trial certificate from a known commercial CA) **DV** = Domain Validation (aka Low Assurance) **OV** = Organizational Validation (aka High Assurance) **EV** = Extended Validation Note: When `cert_issuer_brand` contains a non-empty string, `cert_validation` can be assumed to accurately report the level of validation that was performed by the Issuing CA before the certificate was issued. When `cert_issuer_brand` is an empty string, `cert_validation` will be mere speculation.

3. Using `response_format=2` (dynamically-generated Javascript)

Each of the parameters described in section 2 will appear as Javascript variable declarations. Note the following points:

- "var g_" will be prepended to each parameter name.
- ";" will appear at the end of each line.
- String values will be surrounded by double-quotes.
- New-line characters within string values (notably `cert_subject_DN` and `cert_issuer_DN`) will be converted to the string "\n", which the Javascript interpreter will then interpret as a newline character.
- " characters within string values will be escaped to \".
- \ characters within string values will be escaped to \\.
- Numeric values (e.g. `cert_notBefore`, `cert_notAfter`, `error_code`) will not be surrounded by double-quotes.
- Boolean values (e.g. `server_domain_isIDN`, `cert_isMultiDomain`) will be converted to proper Javascript boolean types (e.g. var g_server_domain_isIDN = true;).
- The final line of the response will be "sslChecker_callback();". The calling webpage must therefore define a callback function of that name. The callback function will be responsible for doing whatever is required with the variables returned by the SSL Checker.