

# Claro Web Scan Report

## certificados

### TLS 1.2

CVE ID	Description	CVSS Score	Severity
CVE-2013-0169	The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the "Lucky Thirteen" issue.	2.6	Low
CVE-2021-42017	A vulnerability has been identified in RUGGEDCOM i800 (All versions < V4.3.8), RUGGEDCOM i801 (All versions < V4.3.8), RUGGEDCOM i802 (All versions < V4.3.8), RUGGEDCOM i803 (All versions < V4.3.8), RUGGEDCOM M2100 (All versions < V4.3.8), RUGGEDCOM M2100F (All versions), RUGGEDCOM M2200 (All versions < V4.3.8), RUGGEDCOM M2200F (All versions), RUGGEDCOM M969 (All versions < V4.3.8), RUGGEDCOM M969F (All versions), RUGGEDCOM RMC30 (All versions < V4.3.8), RUGGEDCOM RMC8388 V4.X (All versions < V4.3.8), RUGGEDCOM RMC8388 V5.X (All versions < V5.6.0), RUGGEDCOM RP110 (All versions < V4.3.8), RUGGEDCOM RS1600 (All versions < V4.3.8), RUGGEDCOM RS1600F (All versions < V4.3.8), RUGGEDCOM RS1600T (All versions < V4.3.8), RUGGEDCOM RS400 (All versions < V4.3.8), RUGGEDCOM RS400F (All versions), RUGGEDCOM RS401 (All versions < V4.3.8), RUGGEDCOM RS416 (All versions < V4.3.8), RUGGEDCOM RS416F (All versions), RUGGEDCOM RS416P (All versions < V4.3.8), RUGGEDCOM RS416PF (All versions), RUGGEDCOM RS416Pv2 (All versions < V5.6.0), RUGGEDCOM RS416v2 (All versions < V5.6.0), RUGGEDCOM RS8000 (All versions < V4.3.8), RUGGEDCOM RS8000A (All versions < V4.3.8), RUGGEDCOM RS8000H (All versions < V4.3.8), RUGGEDCOM RS8000T (All versions < V4.3.8), RUGGEDCOM RS900 (All versions < V4.3.8), RUGGEDCOM RS900 (32M) V4.X (All versions < V4.3.8), RUGGEDCOM RS900 (32M) V5.X (All versions < V5.6.0), RUGGEDCOM RS900F (All versions), RUGGEDCOM RS900G (All versions < V4.3.8), RUGGEDCOM RS900G (32M) V4.X (All versions < V4.3.8), RUGGEDCOM RS900G (32M) V5.X (All versions < V5.6.0), RUGGEDCOM RS900GF (All versions), RUGGEDCOM RS900GP (All versions < V4.3.8), RUGGEDCOM RS900GPF (All versions), RUGGEDCOM RS900L (All versions < V4.3.8), RUGGEDCOM RS900M-GETS-C01 (All versions < V4.3.8), RUGGEDCOM RS900M-GETS-XX (All versions < V4.3.8), RUGGEDCOM RS900M-STND-C01 (All versions < V4.3.8), RUGGEDCOM RS900M-STND-XX (All versions < V4.3.8), RUGGEDCOM RS900W (All versions < V4.3.8), RUGGEDCOM RS910 (All versions < V4.3.8), RUGGEDCOM RS910L (All versions < V4.3.8), RUGGEDCOM RS910W (All versions < V4.3.8), RUGGEDCOM RS920L (All versions < V4.3.8), RUGGEDCOM RS920W (All versions < V4.3.8), RUGGEDCOM RS930L (All versions < V4.3.8), RUGGEDCOM RS930W (All versions < V4.3.8), RUGGEDCOM RS940G (All versions < V4.3.8), RUGGEDCOM RS940GF (All versions), RUGGEDCOM RS969 (All versions < V4.3.8), RUGGEDCOM RSG2100 (All versions < V4.3.8), RUGGEDCOM RSG2100 (32M) V4.X (All versions < V4.3.8), RUGGEDCOM RSG2100 (32M) V5.X (All versions < V5.6.0), RUGGEDCOM RSG2100F (All versions), RUGGEDCOM RSG2100P (All versions < V4.3.8), RUGGEDCOM RSG2100PF (All versions), RUGGEDCOM RSG2200 (All versions < V4.3.8), RUGGEDCOM RSG2200F (All versions), RUGGEDCOM RSG2288 V4.X (All versions < V4.3.8), RUGGEDCOM RSG2288 V5.X (All versions < V5.6.0), RUGGEDCOM RSG2300 V4.X (All versions < V4.3.8), RUGGEDCOM RSG2300 V5.X (All versions < V5.6.0), RUGGEDCOM RSG2300F (All versions), RUGGEDCOM RSG2300P V4.X (All versions < V4.3.8), RUGGEDCOM RSG2300P V5.X (All versions < V5.6.0), RUGGEDCOM RSG2300PF (All versions), RUGGEDCOM RSG2488 V4.X (All versions < V4.3.8), RUGGEDCOM RSG2488 V5.X (All versions < V5.6.0), RUGGEDCOM RSG2488F (All versions), RUGGEDCOM RSG907R (All versions < V5.6.0), RUGGEDCOM RSG908C (All versions < V5.6.0), RUGGEDCOM RSG909R (All versions < V5.6.0), RUGGEDCOM RSG910C (All versions < V5.6.0), RUGGEDCOM RSG920P V4.X (All versions < V4.3.8), RUGGEDCOM RSG920P V5.X (All versions < V5.6.0), RUGGEDCOM RSL910 (All versions < V5.6.0), RUGGEDCOM RST2228 (All versions < V5.6.0), RUGGEDCOM RST2228P (All versions < V5.6.0), RUGGEDCOM RST916C (All versions < V5.6.0), RUGGEDCOM RST916P (All versions < V5.6.0). A new variant of the POODLE attack has left a third-party component vulnerable due to the implementation flaws of the CBC encryption mode in TLS 1.0 to 1.2. If an attacker were to exploit this, they could act as a man-in-the-middle and eavesdrop on encrypted communications.	4.3	Medium
CVE-2022-41724	Large handshake records may cause panics in crypto/tls. Both clients and servers may send large TLS handshake records which cause servers and clients, respectively, to panic when attempting to construct responses. This affects all TLS 1.3 clients, TLS 1.2 clients which explicitly enable session resumption (by setting Config.ClientSessionCache to a non-nil value), and TLS 1.3 servers which request client certificates (by setting Config.ClientAuth >= RequestClientCert).	nan	None
CVE-2020-13777	GnuTLS 3.6.x before 3.6.14 uses incorrect cryptography for encrypting a session ticket (a loss of confidentiality in TLS 1.2, and an authentication bypass in TLS 1.3). The earliest affected version is 3.6.4 (2018-09-24) because of an error in a 2018-09-18 commit. Until the first key rotation, the TLS server always uses wrong data in place of an encryption key derived from an application.	5.8	Medium
CVE-2022-38153	An issue was discovered in wolfSSL before 5.5.0 (when --enable-session-ticket is used); however, only version 5.3.0 is exploitable. Man-in-the-middle attackers or a malicious server can crash TLS 1.2 clients during a handshake. If an attacker injects a large ticket (more than 256 bytes) into a NewSessionTicket message in a TLS 1.2 handshake, and the client has a non-empty session cache, the session cache frees a pointer that points to unallocated memory, causing the client to crash with a "free(): invalid pointer" message. NOTE: It is likely that this is also exploitable during TLS 1.3 handshakes between a client and a malicious server. With TLS 1.3, it is not possible to exploit this as a man-in-the-middle.	nan	None
CVE-2022-37177	** DISPUTED ** HireVue Hiring Platform V1.0 suffers from Use of a Broken or Risky Cryptographic Algorithm. NOTE: this is disputed by the vendor for multiple reasons, e.g., it is inconsistent with CVE ID assignment rules for cloud services, and no product with version V1.0 exists. Furthermore, the rail-fence cipher has been removed, and TLS 1.2 is now used for encryption.	nan	None
CVE-2015-4000	The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.	4.3	Medium
	The TLS protocol 1.2 and earlier supports the rsa_fixed_dh, dss_fixed_dh, rsa_fixed_ecdh, and ecdsa_fixed_ecdh		

<b>CVE-2015-8960</b>	values for ClientCertificateType but does not directly document the ability to compute the master secret in certain situations with a client secret key and server public key but not a server secret key, which makes it easier for man-in-the-middle attackers to spoof TLS servers by leveraging knowledge of the secret key for an arbitrary installed client X.509 certificate, aka the "Key Compromise Impersonation (KCI)" issue.	<b>6.8</b>	Medium
<b>CVE-2022-39339</b>	user_oidc is an OpenID Connect user backend for Nextcloud. In versions prior to 1.2.1 sensitive information such as the OIDC client credentials and tokens are sent in plain text of HTTP without TLS. Any malicious actor with access to monitor user traffic may have been able to compromise account security. This issue has been addressed in in user_oidc v1.2.1. Users are advised to upgrade. Users unable to upgrade may use https to access Nextcloud. Set an HTTPS discovery URL in the provider settings (in Nextcloud OIDC admin settings).	<b>nan</b>	None
<b>CVE-2020-9491</b>	In Apache NiFi 1.2.0 to 1.11.4, the NiFi UI and API were protected by mandating TLS v1.2, as well as listening connections established by processors like ListenHTTP, HandleHttpRequest, etc. However intracluster communication such as cluster request replication, Site-to-Site, and load balanced queues continued to support TLS v1.0 or v1.1.	<b>5.0</b>	Medium

librerias

PHP 5.2.4

CVE ID	Description	CVSS Score	Severity
<b>CVE-2021-44967</b>	A Remote Code Execution (RCE) vulnerabilty exists in LimeSurvey 5.2.4 via the upload and install plugins function, which could let a remote malicious user upload an arbitrary PHP code file.	<b>9.0</b>	Critical
<b>CVE-2007-4657</b>	Multiple integer overflows in PHP 4 before 4.4.8, and PHP 5 before 5.2.4, allow remote attackers to obtain sensitive information (memory contents) or cause a denial of service (thread crash) via a large len value to the (1) strspn or (2) strcspn function, which triggers an out-of-bounds read. NOTE: this affects different product versions than CVE-2007-3996.	<b>7.5</b>	High
<b>CVE-2007-3998</b>	The wordwrap function in PHP 4 before 4.4.8, and PHP 5 before 5.2.4, does not properly use the breakcharlen variable, which allows remote attackers to cause a denial of service (divide-by-zero error and application crash, or infinite loop) via certain arguments, as demonstrated by a 'chr(0), 0, ""' argument set.	<b>5.0</b>	Medium
<b>CVE-2007-3997</b>	The (1) MySQL and (2) MySQLi extensions in PHP 4 before 4.4.8, and PHP 5 before 5.2.4, allow remote attackers to bypass safe_mode and open_basedir restrictions via MySQL LOCAL INFILE operations, as demonstrated by a query with LOAD DATA LOCAL INFILE.	<b>7.5</b>	High
<b>CVE-2007-4889</b>	The MySQL extension in PHP 5.2.4 and earlier allows remote attackers to bypass safe_mode and open_basedir restrictions via the MySQL (1) LOAD_FILE, (2) INTO DUMPFILE, and (3) INTO OUTFILE functions, a different issue than CVE-2007-3997.	<b>6.8</b>	Medium
<b>CVE-2007-4887</b>	The dl function in PHP 5.2.4 and earlier allows context-dependent attackers to cause a denial of service (application crash) via a long string in the library parameter. NOTE: there are limited usage scenarios under which this would be a vulnerability.	<b>4.3</b>	Medium
<b>CVE-2007-4850</b>	curl/interface.c in the cURL library (aka libcurl) in PHP 5.2.4 and 5.2.5 allows context-dependent attackers to bypass safe_mode and open_basedir restrictions and read arbitrary files via a file:// request containing a \x00 sequence, a different vulnerability than CVE-2006-2563.	<b>5.0</b>	Medium
<b>CVE-2007-4840</b>	PHP 5.2.4 and earlier allows context-dependent attackers to cause a denial of service (application crash) via (1) a long string in the out_charset parameter to the iconv function; or a long string in the charset parameter to the (2) iconv_mime_decode_headers, (3) iconv_mime_decode, or (4) iconv_strlen function. NOTE: this might not be a vulnerability in most web server environments that support multiple threads, unless these issues can be demonstrated for code execution.	<b>5.0</b>	Medium
<b>CVE-2007-4825</b>	Directory traversal vulnerability in PHP 5.2.4 and earlier allows attackers to bypass open_basedir restrictions and possibly execute arbitrary code via a .. (dot dot) in the dl function.	<b>7.5</b>	High
<b>CVE-2007-4784</b>	The setlocale function in PHP before 5.2.4 allows context-dependent attackers to cause a denial of service (application crash) via a long string in the locale parameter. NOTE: this might not be a vulnerability in most web server environments that support multiple threads, unless this issue can be demonstrated for code execution.	<b>5.0</b>	Medium

Apache 2.2.8

CVE ID	Description	CVSS Score	Severity
<b>CVE-2022-29405</b>	In Apache Archiva, any registered user can reset password for any users. This is fixed in Archiva 2.2.8	<b>4.0</b>	Medium
<b>CVE-2010-0408</b>	The ap_proxy_ajp_request function in mod_proxy_ajp.c in mod_proxy_ajp in the Apache HTTP Server 2.2.x before 2.2.15 does not properly handle certain situations in which a client sends no request body, which allows remote attackers to cause a denial of service (backend server outage) via a crafted request, related to use of a 500 error code instead of the appropriate 400 error code.	<b>5.0</b>	Medium
<b>CVE-2008-2364</b>	The ap_proxy_http_process_response function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server 2.0.63 and 2.2.8 does not limit the number of forwarded interim responses, which allows remote HTTP servers to cause a denial of service (memory consumption) via a large number of interim responses.	<b>5.0</b>	Medium

mod\_dav 2

CVE ID	Description	CVSS Score	Severity
CVE-2010-1452	The (1) mod_cache and (2) mod_dav modules in the Apache HTTP Server 2.2.x before 2.2.16 allow remote attackers to cause a denial of service (process crash) via a request that lacks a path.	5.0	Medium
CVE-2013-1896	mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI.	4.3	Medium
CVE-2004-0809	The mod_dav module in Apache 2.0.50 and earlier allows remote attackers to cause a denial of service (child process crash) via a certain sequence of LOCK requests for a location that allows WebDAV authoring access.	5.0	Medium
CVE-2013-6438	The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.	5.0	Medium
CVE-2003-0245	Vulnerability in the apr_psprintf function in the Apache Portable Runtime (APR) library for Apache 2.0.37 through 2.0.45 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via long strings, as demonstrated using XML objects to mod_dav, and possibly other vectors.	5.0	Medium
CVE-2002-1593	mod_dav in Apache before 2.0.42 does not properly handle versioning hooks, which may allow remote attackers to kill a child process via a null dereference and cause a denial of service (CPU consumption) in a preforked multi-processing module.	5.0	Medium
CVE-2011-1752	The mod_dav_svn module for the Apache HTTP Server, as distributed in Apache Subversion before 1.6.17, allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a request for a baselined WebDAV resource, as exploited in the wild in May 2011.	5.0	Medium

## Headers

### Cabeceras

link	vulnerabilidad
https://tienda.claro.com.py	Falta de atributos Secure y http-only
https://tienda.claro.com.py/personas/	
https://tienda.claro.com.py/empresas/	
https://tienda.claro.com.py/personas	
https://tienda.claro.com.py	
https://tienda.claro.com.py/wps/portal/claro/pc/personas/ayuda	Posible Clickjacking
https://tienda.claro.com.py/personas	
https://tienda.claro.com.py/	
https://tienda.claro.com.py/personas/undefined/personas	
https://tienda.claro.com.py/personas/undefined/empresas	
https://tienda.claro.com.py/personas/undefined/personas/portabilidad	
https://tienda.claro.com.py/personas/undefined/personas/planes-pospago-prepago	
https://tienda.claro.com.py/personas/undefined/personas/contenidos	
https://tienda.claro.com.py/personas/undefined/personas/packs-de-internet	
https://tienda.claro.com.py/personas/undefined/personas/roaming	
https://tienda.claro.com.py/personas/undefined/personas/giros-claro	
https://tienda.claro.com.py/personas/undefined/personas/internet	
https://tienda.claro.com.py/personas/undefined/personas/claro-tv	
https://tienda.claro.com.py/personas/undefined/personas/internet/combo-ahorro	
https://tienda.claro.com.py/	
https://tienda.claro.com.py/	
https://tienda.claro.com.py/personas/lugares-medios-pago	
https://tienda.claro.com.py/personas/portabilidad	
https://tienda.claro.com.py/personas/planes-pospago-prepago	

<a href="https://tienda.claro.com.py/personas/internet">https://tienda.claro.com.py/personas/internet</a>	
<a href="https://tienda.claro.com.py/personas/internet/combo-ahorro">https://tienda.claro.com.py/personas/internet/combo-ahorro</a>	
<a href="https://tienda.claro.com.py/personas/claro-tv">https://tienda.claro.com.py/personas/claro-tv</a>	
<a href="https://tienda.claro.com.py/personas/packs-de-internet">https://tienda.claro.com.py/personas/packs-de-internet</a>	
<a href="https://tienda.claro.com.py/personas/contenidos">https://tienda.claro.com.py/personas/contenidos</a>	
<a href="https://tienda.claro.com.py/personas/roaming">https://tienda.claro.com.py/personas/roaming</a>	
<a href="https://tienda.claro.com.py/personas/giros-claro">https://tienda.claro.com.py/personas/giros-claro</a>	
<a href="https://tienda.claro.com.py/">https://tienda.claro.com.py/</a>	
<a href="https://tienda.claro.com.py/personas/sucursales">https://tienda.claro.com.py/personas/sucursales</a>	
<a href="https://tienda.claro.com.py/personas/llamar-a-claro">https://tienda.claro.com.py/personas/llamar-a-claro</a>	
<a href="https://tienda.claro.com.py/personas/lugares-medios-pago">https://tienda.claro.com.py/personas/lugares-medios-pago</a>	
<a href="https://tienda.claro.com.py/personas/encuesta/dejanos-tu-opinion">https://tienda.claro.com.py/personas/encuesta/dejanos-tu-opinion</a>	
<a href="https://tienda.claro.com.py/personas/planes-pospago-prepago/cobertura">https://tienda.claro.com.py/personas/planes-pospago-prepago/cobertura</a>	
<a href="https://tienda.claro.com.py/personas/concursos">https://tienda.claro.com.py/personas/concursos</a>	
<a href="https://tienda.claro.com.py/personas/telecentros">https://tienda.claro.com.py/personas/telecentros</a>	
<a href="https://tienda.claro.com.py/">https://tienda.claro.com.py/</a>	
<a href="https://tienda.claro.com.py/personas/legal-y-regulatorio">https://tienda.claro.com.py/personas/legal-y-regulatorio</a>	
<a href="https://tienda.claro.com.py/">https://tienda.claro.com.py/</a>	
<a href="https://tienda.claro.com.py/empresas/undefined/personas">https://tienda.claro.com.py/empresas/undefined/personas</a>	
<a href="https://tienda.claro.com.py/empresas/undefined/empresas">https://tienda.claro.com.py/empresas/undefined/empresas</a>	
<a href="https://tienda.claro.com.py/empresas/undefined/empresas/planes-moviles">https://tienda.claro.com.py/empresas/undefined/empresas/planes-moviles</a>	
<a href="https://tienda.claro.com.py/empresas/undefined/empresas/portabilidad">https://tienda.claro.com.py/empresas/undefined/empresas/portabilidad</a>	
<a href="https://tienda.claro.com.py/empresas/undefined/empresas/roaming">https://tienda.claro.com.py/empresas/undefined/empresas/roaming</a>	
<a href="https://tienda.claro.com.py/empresas/undefined/empresas/internet-dedicado">https://tienda.claro.com.py/empresas/undefined/empresas/internet-dedicado</a>	
<a href="https://tienda.claro.com.py/empresas/undefined/empresas/internet-gpon">https://tienda.claro.com.py/empresas/undefined/empresas/internet-gpon</a>	
<a href="https://tienda.claro.com.py/empresas/undefined/empresas/television-satelital">https://tienda.claro.com.py/empresas/undefined/empresas/television-satelital</a>	
<a href="https://tienda.claro.com.py/empresas/undefined/empresas/iot/gestion-de-actividades">https://tienda.claro.com.py/empresas/undefined/empresas/iot/gestion-de-actividades</a>	
<a href="https://tienda.claro.com.py/empresas/planes-moviles">https://tienda.claro.com.py/empresas/planes-moviles</a>	
<a href="https://tienda.claro.com.py/empresas/roaming">https://tienda.claro.com.py/empresas/roaming</a>	
<a href="https://tienda.claro.com.py/empresas/portabilidad">https://tienda.claro.com.py/empresas/portabilidad</a>	
<a href="https://tienda.claro.com.py/empresas/internet-dedicado">https://tienda.claro.com.py/empresas/internet-dedicado</a>	
<a href="https://tienda.claro.com.py/empresas/internet-gpon">https://tienda.claro.com.py/empresas/internet-gpon</a>	
<a href="https://tienda.claro.com.py/empresas/iot/gestion-de-actividades">https://tienda.claro.com.py/empresas/iot/gestion-de-actividades</a>	
<a href="https://tienda.claro.com.py/empresas/television-satelital">https://tienda.claro.com.py/empresas/television-satelital</a>	
<a href="https://tienda.claro.com.py/empresas/consultas">https://tienda.claro.com.py/empresas/consultas</a>	
<a href="https://tienda.claro.com.py/empresas/sucursales">https://tienda.claro.com.py/empresas/sucursales</a>	
<a href="https://tienda.claro.com.py/empresas/llamar-a-claro">https://tienda.claro.com.py/empresas/llamar-a-claro</a>	
<a href="https://tienda.claro.com.py/empresas/lugares-medios-pago">https://tienda.claro.com.py/empresas/lugares-medios-pago</a>	
<a href="https://tienda.claro.com.py/empresas/planes-moviles/cobertura">https://tienda.claro.com.py/empresas/planes-moviles/cobertura</a>	
<a href="https://tienda.claro.com.py/">https://tienda.claro.com.py/</a>	
<a href="https://tienda.claro.com.py/personas/legal-y-regulatorio">https://tienda.claro.com.py/personas/legal-y-regulatorio</a>	
<a href="https://tienda.claro.com.py/">https://tienda.claro.com.py/</a>	
<a href="https://tienda.claro.com.py/undefined/personas">https://tienda.claro.com.py/undefined/personas</a>	Possible Clickjacking
<a href="https://tienda.claro.com.py/undefined/empresas">https://tienda.claro.com.py/undefined/empresas</a>	Possible Clickjacking

<a href="https://tienda.claro.com.py/undefined/personas/portabilidad">https://tienda.claro.com.py/undefined/personas/portabilidad</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/personas/planes-pospago-prepago">https://tienda.claro.com.py/undefined/personas/planes-pospago-prepago</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/personas/contenidos">https://tienda.claro.com.py/undefined/personas/contenidos</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/personas/packs-de-internet">https://tienda.claro.com.py/undefined/personas/packs-de-internet</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/personas/roaming">https://tienda.claro.com.py/undefined/personas/roaming</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/personas/giros-claro">https://tienda.claro.com.py/undefined/personas/giros-claro</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/personas/internet">https://tienda.claro.com.py/undefined/personas/internet</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/personas/claro-tv">https://tienda.claro.com.py/undefined/personas/claro-tv</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/personas/internet/combo-ahorro">https://tienda.claro.com.py/undefined/personas/internet/combo-ahorro</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/">https://tienda.claro.com.py/</a>	
<a href="https://tienda.claro.com.py/">https://tienda.claro.com.py/</a>	
<a href="https://tienda.claro.com.py/personas/lugares-medios-pago">https://tienda.claro.com.py/personas/lugares-medios-pago</a>	
<a href="https://tienda.claro.com.py/personas/portabilidad">https://tienda.claro.com.py/personas/portabilidad</a>	
<a href="https://tienda.claro.com.py/personas/planes-pospago-prepago">https://tienda.claro.com.py/personas/planes-pospago-prepago</a>	
<a href="https://tienda.claro.com.py/personas/internet">https://tienda.claro.com.py/personas/internet</a>	
<a href="https://tienda.claro.com.py/personas/internet/combo-ahorro">https://tienda.claro.com.py/personas/internet/combo-ahorro</a>	
<a href="https://tienda.claro.com.py/personas/claro-tv">https://tienda.claro.com.py/personas/claro-tv</a>	
<a href="https://tienda.claro.com.py/personas/packs-de-internet">https://tienda.claro.com.py/personas/packs-de-internet</a>	
<a href="https://tienda.claro.com.py/personas/contenidos">https://tienda.claro.com.py/personas/contenidos</a>	
<a href="https://tienda.claro.com.py/personas/roaming">https://tienda.claro.com.py/personas/roaming</a>	
<a href="https://tienda.claro.com.py/personas/giros-claro">https://tienda.claro.com.py/personas/giros-claro</a>	
<a href="https://tienda.claro.com.py/">https://tienda.claro.com.py/</a>	
<a href="https://tienda.claro.com.py/personas/sucursales">https://tienda.claro.com.py/personas/sucursales</a>	
<a href="https://tienda.claro.com.py/personas/llamar-a-claro">https://tienda.claro.com.py/personas/llamar-a-claro</a>	
<a href="https://tienda.claro.com.py/personas/lugares-medios-pago">https://tienda.claro.com.py/personas/lugares-medios-pago</a>	
<a href="https://tienda.claro.com.py/personas/encuesta/dejanos-tu-opinion">https://tienda.claro.com.py/personas/encuesta/dejanos-tu-opinion</a>	
<a href="https://tienda.claro.com.py/personas/planes-pospago-prepago/cobertura">https://tienda.claro.com.py/personas/planes-pospago-prepago/cobertura</a>	
<a href="https://tienda.claro.com.py/personas/concursos">https://tienda.claro.com.py/personas/concursos</a>	
<a href="https://tienda.claro.com.py/personas/telecentros">https://tienda.claro.com.py/personas/telecentros</a>	
<a href="https://tienda.claro.com.py/">https://tienda.claro.com.py/</a>	
<a href="https://tienda.claro.com.py/personas/legal-y-regulatorio">https://tienda.claro.com.py/personas/legal-y-regulatorio</a>	
<a href="https://tienda.claro.com.py/personas/">https://tienda.claro.com.py/personas/</a>	
<a href="https://tienda.claro.com.py/empresas/">https://tienda.claro.com.py/empresas/</a>	
<a href="https://tienda.claro.com.py/personas">https://tienda.claro.com.py/personas</a>	
<a href="https://tienda.claro.com.py">https://tienda.claro.com.py</a>	
<a href="https://tienda.claro.com.py/wps/portal/claro/pc/personas/ayuda">https://tienda.claro.com.py/wps/portal/claro/pc/personas/ayuda</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/personas">https://tienda.claro.com.py/personas</a>	
<a href="https://tienda.claro.com.py/">https://tienda.claro.com.py/</a>	
<a href="https://tienda.claro.com.py/undefined/personas">https://tienda.claro.com.py/undefined/personas</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/empresas">https://tienda.claro.com.py/undefined/empresas</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/personas/portabilidad">https://tienda.claro.com.py/undefined/personas/portabilidad</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/personas/planes-pospago-prepago">https://tienda.claro.com.py/undefined/personas/planes-pospago-prepago</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/personas/contenidos">https://tienda.claro.com.py/undefined/personas/contenidos</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/personas/packs-de-internet">https://tienda.claro.com.py/undefined/personas/packs-de-internet</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/personas/roaming">https://tienda.claro.com.py/undefined/personas/roaming</a>	Posible Clickjacking

<a href="https://tienda.claro.com.py/undefined/personas/giros-claro">https://tienda.claro.com.py/undefined/personas/giros-claro</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/personas/internet">https://tienda.claro.com.py/undefined/personas/internet</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/personas/claro-tv">https://tienda.claro.com.py/undefined/personas/claro-tv</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/undefined/personas/internet/combo-ahorro">https://tienda.claro.com.py/undefined/personas/internet/combo-ahorro</a>	Posible Clickjacking
<a href="https://tienda.claro.com.py/">https://tienda.claro.com.py/</a>	
<a href="https://tienda.claro.com.py/">https://tienda.claro.com.py/</a>	
<a href="https://tienda.claro.com.py/personas/lugares-medios-pago">https://tienda.claro.com.py/personas/lugares-medios-pago</a>	
<a href="https://tienda.claro.com.py/personas/portabilidad">https://tienda.claro.com.py/personas/portabilidad</a>	
<a href="https://tienda.claro.com.py/personas/planes-pospago-prepago">https://tienda.claro.com.py/personas/planes-pospago-prepago</a>	
<a href="https://tienda.claro.com.py/personas/internet">https://tienda.claro.com.py/personas/internet</a>	
<a href="https://tienda.claro.com.py/personas/internet/combo-ahorro">https://tienda.claro.com.py/personas/internet/combo-ahorro</a>	
<a href="https://tienda.claro.com.py/personas/claro-tv">https://tienda.claro.com.py/personas/claro-tv</a>	
<a href="https://tienda.claro.com.py/personas/packs-de-internet">https://tienda.claro.com.py/personas/packs-de-internet</a>	
<a href="https://tienda.claro.com.py/personas/contenidos">https://tienda.claro.com.py/personas/contenidos</a>	
<a href="https://tienda.claro.com.py/personas/roaming">https://tienda.claro.com.py/personas/roaming</a>	
<a href="https://tienda.claro.com.py/personas/giros-claro">https://tienda.claro.com.py/personas/giros-claro</a>	
<a href="https://tienda.claro.com.py/">https://tienda.claro.com.py/</a>	
<a href="https://tienda.claro.com.py/personas/sucursales">https://tienda.claro.com.py/personas/sucursales</a>	
<a href="https://tienda.claro.com.py/personas/llamar-a-claro">https://tienda.claro.com.py/personas/llamar-a-claro</a>	
<a href="https://tienda.claro.com.py/personas/lugares-medios-pago">https://tienda.claro.com.py/personas/lugares-medios-pago</a>	
<a href="https://tienda.claro.com.py/personas/encuesta/dejanos-tu-opinion">https://tienda.claro.com.py/personas/encuesta/dejanos-tu-opinion</a>	
<a href="https://tienda.claro.com.py/personas/planes-pospago-prepago/cobertura">https://tienda.claro.com.py/personas/planes-pospago-prepago/cobertura</a>	
<a href="https://tienda.claro.com.py/personas/concursos">https://tienda.claro.com.py/personas/concursos</a>	
<a href="https://tienda.claro.com.py/personas/telecentros">https://tienda.claro.com.py/personas/telecentros</a>	
<a href="https://tienda.claro.com.py/">https://tienda.claro.com.py/</a>	
<a href="https://tienda.claro.com.py/personas/legal-y-regulatorio">https://tienda.claro.com.py/personas/legal-y-regulatorio</a>	