SSL Report: www.uminho.pt (193.137.9.114)

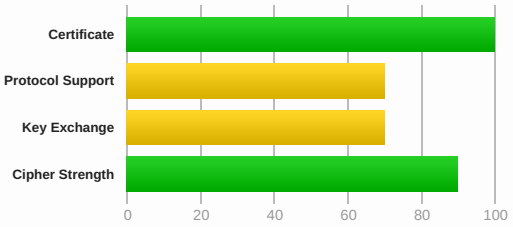
Assessed on: Mon, 02 May 2022 19:29:55 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

B



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

There is no support for secure renegotiation. MORE INFO »

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

Certificate #1: RSA 4096 bits (SHA384withRSA)

Server Key and Certificate #1

Subject	*.uminho.pt Fingerprint SHA256: 578b42546de0527ba75c7f0f4ebde43203a7678dbda527c18faad8da7da42029 Pin SHA256: rYd3l++9If1JPSocBFgUcBWPwqlJWoaMjS5PcncKqW4=
Common names	*.uminho.pt
Alternative names	*.uminho.pt uminho.pt
Serial Number	00848e761ea5f856e935ff5ac56c458d96
Valid from	Thu, 01 Jul 2021 00:00:00 UTC
Valid until	Fri, 01 Jul 2022 23:59:59 UTC (expires in 1 month and 29 days)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	GEANT OV RSA CA 4 AIA: http://GEANT.crt.sectigo.com/GEANTOVRSACA4.crt
Signature algorithm	SHA384withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://GEANT.crl.sectigo.com/GEANTOVRSACA4.crl OCSP: http://GEANT.ocsp.sectigo.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	3 (5419 bytes)
Chain issues	Incorrect order, Contains anchor

#2

Subject	USERTrust RSA Certification Authority In trust store Fingerprint SHA256: e793c9b02fd8aa13e21c31228accb08119643b749c898964b1746d46c3d4cbd2 Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4=

Additional Certificates (if supplied)

Valid until	Mon, 18 Jan 2038 23:59:59 UTC (expires in 15 years and 8 months)
Key	RSA 4096 bits (e 65537)
Issuer	USERTrust RSA Certification Authority Self-signed
Signature algorithm	SHA384withRSA

#3

Subject	GEANT OV RSA CA 4 Fingerprint SHA256: 37834fa5ea40fbf7b61196955962e1ca0558872435e4206653d3f620dd8e988e Pin SHA256: j0qRK9S0oUba9b4ttZdKp42Q4T2J8S4FFKPNG5FTFVA=
Valid until	Sun, 01 May 2033 23:59:59 UTC (expires in 10 years and 11 months)
Key	RSA 4096 bits (e 65537)
Issuer	USERTrust RSA Certification Authority
Signature algorithm	SHA384withRSA

Certification Paths

Click here to expand

Certificate #2: RSA 4096 bits (SHA384withRSA)

Server Key and Certificate #1

Subject	*.uminho.pt Fingerprint SHA256: 578b42546de0527ba75c7f0f4ebde43203a7678dbda527c18faad8da7da42029 Pin SHA256: rYd3I++9If1JPSocBFgUcBWPwqlJWoaMjS5PcncKqW4=
Common names	*.uminho.pt
Alternative names	*.uminho.pt uminho.pt
Serial Number	00848e761ea5f856e935ff5ac56c458d96
Valid from	Thu, 01 Jul 2021 00:00:00 UTC
Valid until	Fri, 01 Jul 2022 23:59:59 UTC (expires in 1 month and 29 days)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	GEANT OV RSA CA 4 AIA: http://GEANT.crt.sectigo.com/GEANTOVRSACA4.crt
Signature algorithm	SHA384withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://GEANT.crl.sectigo.com/GEANTOVRSACA4.crl OCSP: http://GEANT.ocsp.sectigo.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	**Yes** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	3 (5419 bytes)
Chain issues	**Contains anchor**

#2

Subject	GEANT OV RSA CA 4 Fingerprint SHA256: 37834fa5ea40fbf7b61196955962e1ca0558872435e4206653d3f620dd8e988e Pin SHA256: j0qRK9S0oUba9b4ttZdKp42Q4T2J8S4FFKPNG5FTFVA=
Valid until	Sun, 01 May 2033 23:59:59 UTC (expires in 10 years and 11 months)
Key	RSA 4096 bits (e 65537)
Issuer	USERTrust RSA Certification Authority
Signature algorithm	SHA384withRSA

#3

Subject	USERTrust RSA Certification Authority In trust store Fingerprint SHA256: e793c9b02fd8aa13e21c31228accb08119643b749c898964b1746d46c3d4cbd2 Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4ITdO/nEW/Td4=

Additional Certificates (if supplied)

Valid until	Mon, 18 Jan 2038 23:59:59 UTC (expires in 15 years and 8 months)
Key	RSA 4096 bits (e 65537)
Issuer	USERTrust RSA Certification Authority Self-signed
Signature algorithm	SHA384withRSA

Certification Paths

Click here to expand

Configuration

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Cipher Suites

 # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp384r1 (eq. 7680 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp384r1 (eq. 7680 bits RSA) FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp384r1 (eq. 7680 bits RSA) FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp384r1 (eq. 7680 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp384r1 (eq. 7680 bits RSA) FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp384r1 (eq. 7680 bits RSA) FS **WEAK**	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK**	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK**	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK**	256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) **WEAK**	128
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) **WEAK**	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS **WEAK**	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 2048 bits FS **WEAK**	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 2048 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 1024 bits FS **WEAK**	128
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 1024 bits FS **WEAK**	256

 # TLS 1.1 (suites in server-preferred order)

 # TLS 1.0 (suites in server-preferred order)

Handshake Simulation

Android 2.3.7 No SNI [2]	RSA 4096 (SHA384)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Android 4.0.4	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp384r1 FS
Android 4.1.1	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp384r1 FS
Android 4.2.2	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp384r1 FS
Android 4.3	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp384r1 FS
Android 4.4.2	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp384r1 FS
Android 5.0.0	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp384r1 FS
Android 6.0	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp384r1 FS

Handshake Simulation

Android 7.0	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Android 8.0	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Android 8.1	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Android 9.0	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Baidu Jan 2015	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS	
BingPreview Jan 2015	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Chrome 49 / XP SP3	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Chrome 69 / Win 7 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Chrome 70 / Win 10	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Chrome 80 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Firefox 31.3.0 ESR / Win 7	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Firefox 47 / Win 7 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Firefox 49 / XP SP3	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Firefox 62 / Win 7 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Firefox 73 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Googlebot Feb 2018	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
IE 7 / Vista	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS	
IE 8 / XP No FS [1] No SNI [2]	Server sent fatal alert: handshake_failure					
IE 8-10 / Win 7 R	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS	
IE 11 / Win 7 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS	
IE 11 / Win 8.1 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS	
IE 10 / Win Phone 8.0	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS	
IE 11 / Win Phone 8.1 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS	
IE 11 / Win Phone 8.1 Update R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS	
IE 11 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Edge 15 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Edge 16 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Edge 18 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Edge 13 / Win Phone 10 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Java 6u45 No SNI [2]	RSA 4096 (SHA384)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS		
Java 7u25	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS	
Java 8u161	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Java 11.0.3	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Java 12.0.1	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
OpenSSL 0.9.8y	RSA 4096 (SHA384)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS		
OpenSSL 1.0.1l R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
OpenSSL 1.0.2s R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
OpenSSL 1.1.0k R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
OpenSSL 1.1.1c R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Safari 5.1.9 / OS X 10.6.8	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS	
Safari 6 / iOS 6.0.1	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS	
Safari 6.0.4 / OS X 10.8.4 R	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS	
Safari 7 / iOS 7.1 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS	
Safari 7 / OS X 10.9 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS	
Safari 8 / iOS 8.4 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS	
Safari 8 / OS X 10.10 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS	
Safari 9 / iOS 9 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Safari 9 / OS X 10.11 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Safari 10 / iOS 10 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Safari 10 / OS X 10.12 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Safari 12.1.2 / MacOS 10.14.6 Beta R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Safari 12.1.1 / iOS 12.3.1 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Apple ATS 9 / iOS 9 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
Yahoo Slurp Jan 2015	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	
YandexBot Jan 2015	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS	

Not simulated clients (Protocol mismatch)

IE 6 / XP No FS [1] No SNI [2]	Protocol mismatch (not simulated)

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

Handshake Simulation

(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 **(1) For a better understanding of this test, please read this longer explanation** (2) Key usage data kindly provided by the Censys network search engine; original DROWN website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	**Not supported ACTION NEEDED** (more info)
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc013
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0xc013
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc013
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc013
Sleeping POODLE	No (more info) TLS 1.2 : 0xc013
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	**Weak key exchange WEAK**
ALPN	No
NPN	No
Session resumption (caching)	**No (IDs empty)**
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	**Not in: Chrome Edge Firefox IE**
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	**Yes**
ECDH public server param reuse	**Yes**
Supported Named Groups	secp384r1, secp256r1, x25519 (server preferred order)
SSL 2 handshake compatibility	Yes

HTTP Requests

1 **https://www.uminho.pt/** (HTTP/1.1 302 Found)

2 **https://www.uminho.pt/PT** (HTTP/1.1 200 OK)

Miscellaneous

Test date	Mon, 02 May 2022 19:26:19 UTC
Test duration	215.798 seconds
HTTP status code	200
HTTP server signature	Microsoft-IIS/8.5

Miscellaneous

Server hostname	www.uminho.pt

SSL Report v2.1.10