

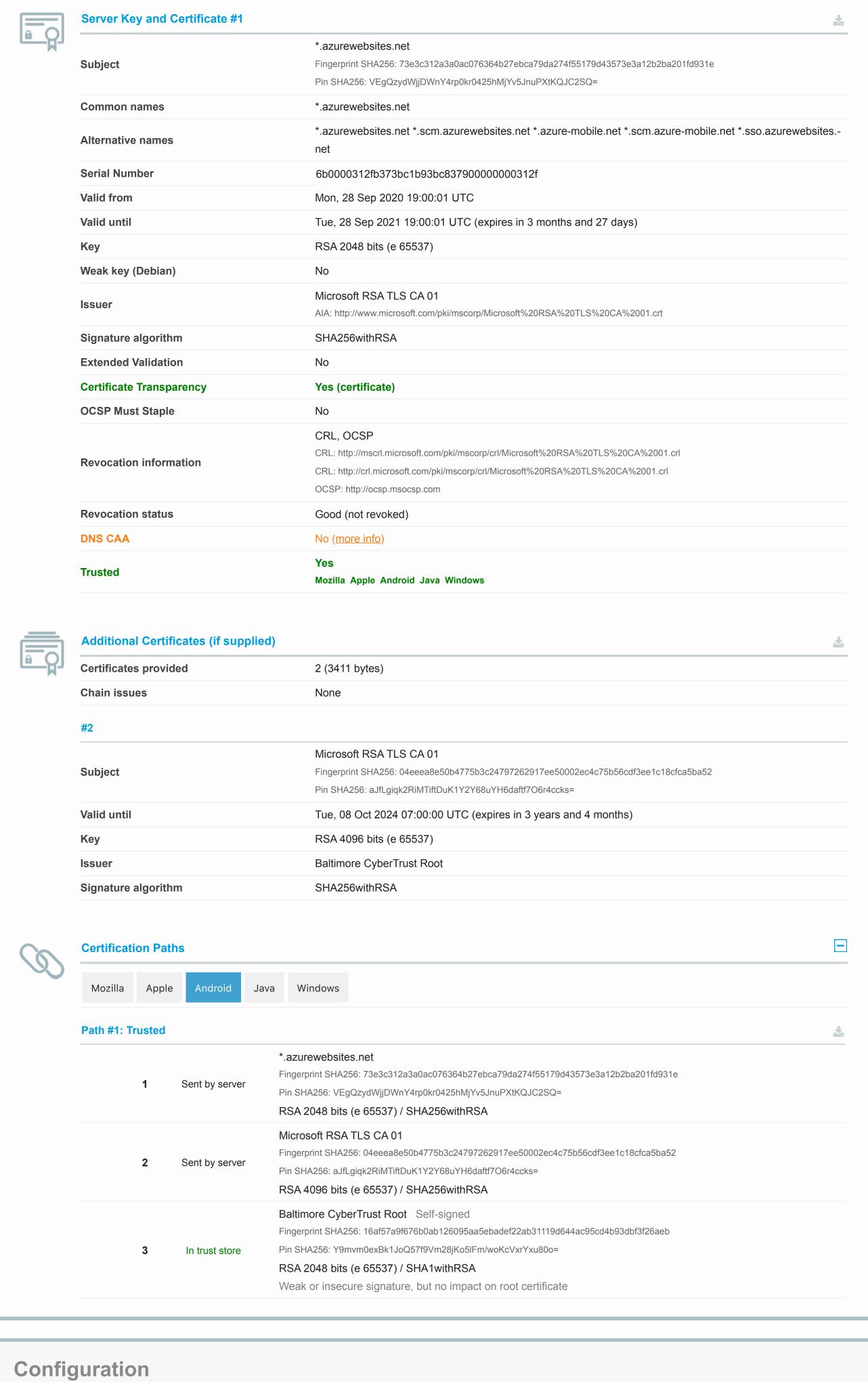
You are here: Home > Projects > SSL Server Test > mastermind-be.azurewebsites.net

SSL Report: mastermind-be.azurewebsites.net (20.50.2.23)

Assessed on: Tue, 01 Jun 2021 15:08:01 UTC | HIDDEN | Clear cache

Certificate #1: RSA 2048 bits (SHA256withRSA)





		RSA 4096 b	its (e 65537) /	DuK1Y2Y68uYH6daftf7O6r4ccks= / SHA256withRSA ot Self-signed f676b0ab126095aa5ebadef22ab31119d644ac95cd4b93dbf3f26aeb		
	3 In trust sto	re Pin SHA256: \\ RSA 2048 b	/9mvm0exBk1Jc its (e 65537) /	pQ57f9Vm28jKo5lFm/woKcVxrYxu80o= / SHA1withRSA re, but no impact on root certificate		
Config	guration					
	TLS 1.3				No Ye:	
	TLS 1.1 TLS 1.0				No No	
	SSL 3 SSL 2				No No	
	Cipher Suites					
	# TLS 1.2 (suites in server-pro	eferred order)			Е	
				CDH secp256r1 (eq. 3072 bits RSA) FS CDH secp256r1 (eq. 3072 bits RSA) FS	250 128	
	TLS_ECDHE_RSA_WITH_AES	S_128_CBC_SHA256	(0×c027) EC	CDH secp256r1 (eq. 3072 bits RSA) FS WEAK CDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128	
	TLS_ECDHE_RSA_WITH_AES	6_128_CBC_SHA (0x	c013) ECDH	secp256r1 (eq. 3072 bits RSA) FS WEAK secp256r1 (eq. 3072 bits RSA) FS WEAK	250 128	
	TLS_RSA_WITH_AES_256_GC TLS_RSA_WITH_AES_128_GC TLS_RSA_WITH_AES_256_CE	CM_SHA256 (0x9c)	WEAK		250 128 250	
	TLS_RSA_WITH_AES_256_CE	3C_SHA256 (0x3c)	WEAK		120	
	TLS_RSA_WITH_AES_128_CE				12	
	Handshake Simulation Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS		
	Android 5.0.0 Android 6.0	RSA 2048 (SHA256) RSA 2048 (SHA256)		TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS		
	Android 7.0 Android 8.0	RSA 2048 (SHA256) RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS		
	Android 8.1 Android 9.0	RSA 2048 (SHA256) RSA 2048 (SHA256)		TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS		
	BingPreview Jan 2015 Chrome 49 / XP SP3	RSA 2048 (SHA256) RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS		
	Chrome 69 / Win 7 R Chrome 70 / Win 10	RSA 2048 (SHA256) RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS		
	Chrome 80 / Win 10 R Firefox 31.3.0 ESR / Win 7 Firefox 47 / Win 7 R	RSA 2048 (SHA256) RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS		
	Firefox 47 / Win 7 R Firefox 49 / XP SP3 Firefox 62 / Win 7 R	RSA 2048 (SHA256) RSA 2048 (SHA256) RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS		
	Firefox 73 / Win 10 R Googlebot Feb 2018	RSA 2048 (SHA256) RSA 2048 (SHA256)		TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS		
	<u>IE 11 / Win 7</u> R <u>IE 11 / Win 8.1</u> R	RSA 2048 (SHA256) RSA 2048 (SHA256)		TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS		
	IE 11 / Win Phone 8.1 R IE 11 / Win Phone 8.1 Update F	RSA 2048 (SHA256) R RSA 2048 (SHA256)		TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS		
	<u>IE 11 / Win 10</u> R <u>Edge 15 / Win 10</u> R <u>Edge 16 / Win 10</u> R	RSA 2048 (SHA256) RSA 2048 (SHA256) RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS ECDHE RSA WITH AES 256 GCM SHA384 ECDH secp256r1 FS		
	Edge 18 / Win 10 R Edge 13 / Win Phone 10 R	RSA 2048 (SHA256) RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS		
	Java 8u161 Java 11.0.3	RSA 2048 (SHA256) RSA 2048 (SHA256)		TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS		
	<u>Java 12.0.1</u> <u>OpenSSL 1.0.1I</u> R	RSA 2048 (SHA256) RSA 2048 (SHA256)		TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS		
	OpenSSL 1.0.2s R OpenSSL 1.1.0k R	RSA 2048 (SHA256) RSA 2048 (SHA256)		TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS		
	<u>OpenSSL 1.1.1c</u> R <u>Safari 6 / iOS 6.0.1</u>	RSA 2048 (SHA256) RSA 2048 (SHA256)		TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS		
	<u>Safari 7 / iOS 7.1</u> R <u>Safari 7 / OS X 10.9</u> R	RSA 2048 (SHA256) RSA 2048 (SHA256)		TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS		
	<u>Safari 8 / iOS 8.4</u> R <u>Safari 8 / OS X 10.10</u> R <u>Safari 9 / iOS 9</u> R	RSA 2048 (SHA256) RSA 2048 (SHA256) RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS		
	Safari 9 / OS X 10.11 R Safari 10 / iOS 10 R	RSA 2048 (SHA256) RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS		
	Safari 10 / OS X 10.12 R Safari 12.1.2 / MacOS 10.14.6 Beta R	RSA 2048 (SHA256) RSA 2048 (SHA256)		TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS		
	Safari 12.1.1 / iOS 12.3.1 R Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256) RSA 2048 (SHA256)		TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS		
	Yahoo Slurp Jan 2015 YandexBot Jan 2015	RSA 2048 (SHA256) RSA 2048 (SHA256)		TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS		
	# Not simulated clients (Proto Android 2.3.7 No SNI ²	ocol mismatch) Protocol mismatch	(not simulated		E	
	Android 4.0.4 Android 4.1.1	Protocol mismatch	•			
	Android 4.2.2 Android 4.3	Protocol mismatch	•			
	Baidu Jan 2015 IE 6 / XP No FS 1 No SNI 2	Protocol mismatch	`			
	IE 7 / Vista IE 8 / XP No FS ¹ No SNI ²	Protocol mismatch	`			
	IE 8-10 / Win 7 R IE 10 / Win Phone 8.0	Protocol mismatch	(not simulated			
	<u>Java 6u45</u> No SNI ² <u>Java 7u25</u> <u>OpenSSL 0.9.8y</u>	Protocol mismatch Protocol mismatch Protocol mismatch	(not simulated			
	Safari 5.1.9 / OS X 10.6.8 Safari 6.0.4 / OS X 10.8.4 R	Protocol mismatch	(not simulated			
	(2) No support for virtual SSL ho	osting (SNI). Connects	s to the defaul	when determining support for it. It site if the server uses SNI. etry with a lower protocol version.		
	(R) Denotes a reference browse (All) We use defaults, but some	er or client, with which platforms do not use	we expect be their best prot			
-	Protocol Details	noonou iii manaonano	omaiation, v			
	DROWN	(1) F	or a better u	nd hostname not seen elsewhere with SSLv2 nderstanding of this test, please read this longer explanation		
	Secure Renegotiation	(3) (a kindly provided by the <u>Censys</u> network search engine; original DROWN website only indicative of possible key and certificate reuse; possibly out-of-date and not		
	Secure Client-Initiated Renegotiation No Insecure Client-Initiated Renegotiation No					
	POODLE (SSLv3)			ide (<u>more info</u>) pported (<u>more info</u>)		
	Zombie POODLE	No (more info) TL			
	OpenSSL 0-Length Sleeping POODLE	No (more info) TL	LS 1.2 : 0xc027 LS 1.2 : 0xc027 LS 1.2 : 0xc027		
	Downgrade attack prevention SSL/TLS compression			s support for at least two protocols, excl. SSL2)		
	RC4 Heartbeat (extension)	No No				
	Heartbleed (vulnerability) Ticketbleed (vulnerability)	No (more info)			
	OpenSSL CCS vuln. (CVE-201 OpenSSL Padding Oracle vull (CVE-2016-2107)	n.	more info)			
	ROBOT (vulnerability) Forward Secrecy		more info) (with most b	rowsers) ROBUST (more info)		
	ALPN NPN	No No				
	Session resumption (caching Session resumption (tickets)	No	IDs assigned	I but not accepted)		
	OCSP stapling	Yes				
	Strict Transport Security (HST HSTS Preloading	,	in: Chromo '	Edge Firefox IE		

Android 4.1.1 Protocol mismatch (not simulated) Android 4.2.2 Protocol mismatch (not simulated) Android 4.3 Protocol mismatch (not simulated) Baidu_Jan_2015 Protocol mismatch (not simulated) Baidu_Jan_2015 Protocol mismatch (not simulated) IE_BI_XP_No_FS^1_No_SNI^2 Protocol mismatch (not simulated) Java_Gi_JS_No_SNI^2 Protocol mismatch (not simulated) Java_Gi_JS_No_SNI^2 Protocol mismatch (not simulated) Java_Gi_JS_No_SNI_No_SNI^2 Protocol mismatch (not simulated) Safan_FS_NO_SNI_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. (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 No, server keys and hostname not seen elsewhere with SSLv2 (1) For a better understanding of this tost, please read this longer explanation (2) Key usage data kindly provided by the Censys network search engine; original DROWN website here	Android 2.3.7 No SNI ² Android 4.0.4	Protocol mismatch (not simulated) Protocol mismatch (not simulated)
Amuse 2	Android 4.0.4 Android 4.1.1	Protocol mismatch (not simulated) Protocol mismatch (not simulated)
A mail 4		
	Baidu Jan 2015	Protocol mismatch (not simulated)
### Process 1	IE 6 / XP No FS ¹ No SNI ²	Protocol mismatch (not simulated)
Process Pro	IE 7 / Vista	Protocol mismatch (not simulated)
Protect Pro	IE 8 / XP No FS ¹ No SNI ²	Protocol mismatch (not simulated)
Protect	<u>IE 8-10 / Win 7</u> R	Protocol mismatch (not simulated)
Part	IE 10 / Win Phone 8.0	Protocol mismatch (not simulated)
Part	Java 6u45 No SNI ²	Protocol mismatch (not simulated)
Read \$1.0 (D.S.) Line R Protect Prot	<u>Java 7u25</u>	Protocol mismatch (not simulated)
	OpenSSL 0.9.8y	Protocol mismatch (not simulated)
Contact and over support clausers (10 per excluded year) adtentions of account of the Contact and C	Safari 5.1.9 / OS X 10.6.8	Protocol mismatch (not simulated)
Content		
No. serval keys unit froatburine not seem clean-lee with SSS_22	(2) No support for virtual SSL hos (3) Only first connection attempt (R) Denotes a reference browser (All) We use defaults, but some p	sting (SNI). Connects to the default site if the server uses SNI. simulated. Browsers sometimes retry with a lower protocol version. r or client, with which we expect better effective security. platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).
### Part "If For a near undestandening of this case, inserance inclination control bis longer preliated sector in control bis longer	Protocol Details	
	DROWN	
Marie		
### PADOLE T. S. P. No. 1951 174 17		
PODOLE [SILS] No. SSI 3 not supprint dywon print) PODOLE (TILS) No. Excels (BIDS) Combine PODOLE No. Excels (BIDS) Combine PODOLE No. Excels (BIDS) Open SEA L+ anight No. Excels (BIDS) Open SEA L+ anight No. Excels (BIDS) Downgrade attack prevention Uniform (Inception) Till 12 c-cs287 Downgrade attack prevention Uniform (Inception) Till 12 c-cs287 No. The Till 12 c-cs287 No. Excels (BIDS) No. No. The Till 12 c-cs287 No. Till 12 c-cs287 No. Excels (BIDS) No. Excels (BIDS) No. No. Excels (BIDS) No. Excels (BIDS) Popen SEA CCS vall., CVC 2014-0223 No. Excels (BIDS) No. Excels (BIDS) ROBOT (vulnerability) No. Excels (BIDS) No. Excels (BIDS) ROBOT (vulnerability) No. (BiDs assigned but not accepted) ROBOT (vulnerability) No. (BiDs assigned but not accepted) Section resumption (caching) No. (BiDs assigned but not accepted) Section resumption (caching) No. Excels (BIDS) Public (Rey Pinaing Report-Only) No. E		
PODDLE TLS		
Zombile PODOLE No (mose leftle) ' 11.5 1.2 16.2327 GOLDENDODLE No (mose leftle) ' 11.5 1.2 16.2327 GOLDENDODLE No (mose leftle) ' 11.5 1.2 16.2327 Sleeping PODOLE No (mose leftle) ' 11.5 1.2 16.2327 Downgrade attack prevention Universities ' 11.5 1.2 16.2327 Downgrade attack prevention No (mose leftle) ' 11.5 1.2 16.2327 RC4 No RC4 No RC4 No (mose leftle) ' 11.5 1.2 16.2321 RC4 No (mose leftle) ' 11.5 1.2 16.2321 RC5 (victionability) No (mose leftle) ' 11.5 1.2 16.2321 OpenSSL Padding ' One I vuln. (VVZ-2014-02.24) No (mose leftle) ' 11.5 1.2 16.2321 OpenSSL COS vuln. (VVZ-2014-02.24) No (mose leftle) ' 11.5 1.2 16.2321 CVZ-2.416-21071 No (mose leftle) ' 11.5 1.2 16.2321 CVZ-2.416-21071 No (mose leftle) ' 11.5 1.2 16.2321 ROBOT (vulnerability) No (mose leftle) ' 11.5 1.2 16.2321 ROBOT (vulnerability) No (mose leftle) ' 11.5 1.2 16.2321 ROBOT (vulnerability) No (mose leftle) ' 11.5 1.2 16.2321 Sabboth resumption (valenting) No (this correction of this correction		
Open SBL Delength No (gozetind) 15 - 22 - 20 - 2072 Open SBL Delength No (gozetind) 15 - 22 - 20 - 2072 SBLTLS compression No (gozetind) Copen SBL CES* with. (CVE-2014-0224) No (gozetind)		
Since princy PCODE No (page size 10 10 10 10 10 10 10 1	GOLDENDOODLE	
Downgrade attack prevention	OpenSSL 0-Length	
SSLTLS compression	Sleeping POODLE	No (more info) TLS 1.2: 0xc027
No.	Downgrade attack prevention	Unknown (requires support for at least two protocols, excl. SSL2)
Heartheat (extension)	SSL/TLS compression	No
Heartbleed (vulnerability) No (more info) Ticketibleed (vulnerability) No (more info) OpenSSL Padding Oracle vuln. No (more info) OpenSSL Padding Oracle vuln. No (more info) No No Session resumption (caching) No (IDs assigned but not accepted) No (CSP stapling) No (IDs assigned but not accepted) No (CSP stapling) No (IDS assigned but not accepted) No (IDS assi	RC4	No
Trebetbleed (vulnerability)	Heartbeat (extension)	No
OpenSSL CCS vuln. (CVE-2014-0224) No (maxe into) OpenSSL Padding Oracle vuln. (CVE-2014-0224) No (maxe into) CVE-2016-2107Y No (maxe into) ROBOT (vuln-marbility) No (maxe into) Forward Secrety Yes (with most browsers) ROBUST (more into) ALPN No NPN No Session resumption (caching) No (IDs assigned but not accepted) Session resumption (tickets) No (IDs assigned but not accepted) Session resumption (tickets) No (IDs assigned but not accepted) Session resumption (tickets) No (IDs assigned but not accepted) Session resumption (tickets) No (IDs assigned but not accepted) Session resumption (tickets) No (IDs assigned but not accepted) Strict Transport Security (HSTS) No (Insuc into) Public Key Pinning (HPKP) No (Insuc into) No (Insuc into) No (Insuc into) Public Key Pinning (Static) No (Insuc into) Tus Sectession intolerance No (Insuc into) Tus Sectession intolerance No DHE suites not supported Debuggious server param (Ye) ruse No DHE suites not supported <td< td=""><td>Heartbleed (vulnerability)</td><td>No (more info)</td></td<>	Heartbleed (vulnerability)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107) No (more info) ROBOT (vulnerability) No (more info) Forward Secrey Yas (with most browsers) ROBUST (mote info) ALPN No NPN No Session resumption (tacking) No (IDs assigned but not accepted) Session resumption (tacking) No (IDs assigned but not accepted) Session resumption (tacking) No (IDS assigned but not accepted) Session resumption (tacking) No Strict Transport Security (HSTS) No Strict Transport Security (HSTS) No Public Key Pinning (HPKP) No (more info) Public Key Pinning (BRBdit) No (more info) Public Key Pinning (BRBdit) No (more info) Long handshake intolerance No TLS version intolerance No No TLS version intolerance No DLTE suites not supported Bloph public server param (Ye) reuse No PUBL Secret Param (Ye) reuse No PUBL Server param reuse No SSL 2 handshake compatibity No HITTP Requests		
No No No No No No No No No No No No No No No No No No No No No No No No		
No concision No concision		. No (more info)
Para		No (more info)
No No Session resumption (tacking) No (IDs assigned but not accepted) Session resumption (tacking) No Strict Transport Security (HSTS) No HSTS Preloading No (In: Chrome Edge Firefox IE Public Key Pinning (HPKP) No (more info) Public Key Pinning Report-Only No ————————————————————————————————————	Forward Secrecy	
Session resumption (caching) Session resumption (tickets) OCSP stapling Yes 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 Uses common Dt printes No Uses common Dt print	ALPN	No
Sasion resumption (tickets) No OCSP stapling Yes Strict Transport Security (HSTS) Not in: Chrome Edge Firefox IE Not in: Chrome Edge Firefox IE Public Rey Prinning (RPPRP) No (more info) Public Rey Prinning (Static) No (more info) Long handshake Intolerance No TLS extension intolerance No TLS extension intolerance No Interest on Supported Lose common DH primes No, DHE suites not supported SCDH public server param (Ys) reuse No, DHE suites not supported SCDH public server param (Ys) reuse No, DHE suites not supported SSL 2 handshake droups Sec256f1, secp384f1 (server perferred order) SSL 2 handshake droups Sec256f1, secp384f1 (server perferred order) SSL 2 handshake beautrewebsites.set* (HTTP/1.1 200 UK) ***********************************	NPN	No
CCSP stapling Yes Strict Transport Security (HSTS) No HSTS Preloading Not in: Chrome Edge Firefox IE Public Key Plinning (HPKP) No (more info) Public Key Plinning Report-Only No Public Key Plinning (Static) No (more info) Long handshake intolerance No TLS extension intolerance No TLS version intolerance No Incorrect SNI alerts No, DHE suites not supported Uses common DH primes No, DHE suites not supported BCDH public server param (Ys) reuse No, DHE suites not supported ECDH public server param (Ys) reuse No SSL 2 handshake compatibility No HTTP Requester HTTP Requester HTTP Requester Content-Type application/json: charset=ut/6 Date Tue, 01 Jun 2021 15:06:18 GMT Connection dose Miscellaneous Miscellaneous Test date Tue, 01 Jun 2021 15:06:06 UTC Test duration 114:691 seconds	Session resumption (caching)	No (IDs assigned but not accepted)
Strict Transport Security (HSTS) Not In: Chrome Edge Firefox IE Public Key Pinning (HPKP) No (more info) Public Key Pinning (BPKP) No (more info) Public Key Pinning (Static) No (more info) Long handshake intolerance No Long handshake intolerance No TLS version intolerance No Incorrect SNI alerts No Uses common DH primes No, DHE suites not supported Bublic server param reuse No, DHE suites not supported ECDH public server param reuse No SUSL 2 handshake compatibility No HTTP Requests Interpretable supported Named Groups SSL 2 handshake compatibility No Interpretable supported Named Groups Interpretable supported Named Groups Interpretable supported Named Groups Interpretable supported Named Groups Interpretable s	Session resumption (tickets)	No
Not in: Chrome Edge Firefox E	OCSP stapling	Yes
Public Key Plinning (HPKP) No (more info) Public Key Plinning (Static) No (more info) Long handshake intolerance No TLS extension intolerance No TLS extension intolerance No Incorrect SNI alerts No Uses common DH primes No. DHE suites not supported DH public server param (Ys) rouse No. DHE suites not supported ECDH public server param reuse No Supported Named Groups secp256r1, secp384r1 (server preferred order) SSL 2 handshake compatibility HTTP Requests In https://mastermind-be.azurrewebsites.net/ (HTTP/1.1 200 OK) HTTP In the supported Named Groups Content-Length 20 Content-Length 20 Content-Length 20 Length 10 colspan="2">Length Miscellaneous Miscellaneous Test date Tue, 01 Jun 2021 15:06:06 UTC Test date Tue, 01 Jun 2021 15:06:06 UTC Test date 114.891 seconds </td <td></td> <td>S) No</td>		S) No
Public Key Plining Report-Only No (moze_info) Public Key Plining (Static) No (moze_info) Long handshake intolerance No TLS extension intolerance No Incorrect SNI alorts No Uses common DH primes No, DHE suites not supported DH public server param (Ys) reuse No, DHE suites not supported ECDH public server param reuse No Supported Named Groups secp256r1, secp384r1 (server preferred order) SSL 2 handshake compatibility No HTTP Requests 1 https://mastermind-be.azurewebsites.net/ (HTTP/1.1 200 OK) A polication/json; charset=uff-8 Date Tue, 01 Jun 2021 15:06:18 GMT Connection close Miscellaneous Miscellaneous Miscellaneous Test date Tue, 01 Jun 2021 15:06:06 UTC Test duration T14.691 seconds HTTP status cols 200 HTTP status cols Language de l'accorde l'accorde l'accorde l'accorde l'accorde l'accorde l'accorde l'accorde l'accor		
Public Key Pinning (Static) Long handshake intolerance No TLS extension Intolerance No TLS version Intolerance No Incorrect SNI alerts No Uses common DH primes No, DHE suites not supported DH public server param (Ys) reuse No, DHE suites not supported ECDH public server param reuse No Supported Named Groups SSL 2 handshake compatibility No HTTP Requests I https://mastermind-be.azurewebsites.net/ (HTTP/1.1.200 UK) Long the time the paramate of the parama		
Long handshake Intolerance No TLS extension intolerance No TLS version intolerace		
TLS extension intolerance No TLS version intolerance No Incorrect SNI alerts No Uses common DH primes No, DHE suites not supported DH public server param (Ys) reuse No, DHE suites not supported ECDH public server param reuse No Supported Named Groups secc256r1, secp384r1 (server preferred order) SSL 2 handshake compatibility No HTTP Requests 1 https://mastermind-be.azurewebsites.net/ (HTTP/1.1 200 CK) 1 content-Length 20 Content-Type application/json: charset=utf-8 Date Tue, 01 Jun 2021 15:06:18 GMT Connection close Miscellaneous Test date Tue, 01 Jun 2021 15:06:08 UTC Test duration 114.681 seconds HTTP status code 200 HTTP status code - 200 HTTP status code - 200 HTTP status code - 200 HTTP server signature - 200		
TLS version intolerance No Incorrect SNI alerts No Uses common DH primes No, DHE suites not supported DH public server param (Ys) reuse No, DHE suites not supported ECDH public server param reuse No Supported Named Groups secp256r1, secp384r1 (server preferred order) SSL 2 handshabe compatibility No HTTP Requests 1 https://mastermind-be.azurewebsites.net/ (HTTP/1.1 200 OK) Content-Length 20 Content-Type application/json; charset=utf-8 Date Tue, 01 Jun 2021 15:06:18 GMT Connection close Miscellaneous Miscellaneous Test date Tue, 01 Jun 2021 15:06:06 UTC Test duration 14.691 seconds HTTP server signature - 200 HTTP status code 200 HTTP server signature		
No		
Uses common DH primes No, DHE suites not supported DH public server param (Ys) reuse No, DHE suites not supported ECDH public server param reuse No Supported Named Groups secp256f1, secp384f1 (server preferred order) SSL 2 handshake compatibility No HTTP Requests 1 https://mastermind-be.azurewebsites.net/ (HTTP/1.1 200 OK) Content-Length 20 Content-Type application/json; charset=utf.8 Date Tue, 01 Jun 2021 15:06:18 GMT Connection close Miscellaneous Test date Tue, 01 Jun 2021 15:06:06 UTC Test duration 114.691 seconds HTTP status code 200 HTTP status code		
DH public server param (Ys) reuse No, DHE suites not supported ECDH public server param reuse No Supported Named Groups secp256r1, secp384r1 (server preferred order) SSL 2 handshake compatibility No HTTP Requests 1 https://mastermind-be.azurewebsites.net/ (HTTP/1.1 200 OK) A public server preferred order) Ontent-Length 20 Content-Length Content-Type application/json; charset=utf-8 Date Tue, 01 Jun 2021 15:06:18 GMT Connection Connection Tue, 01 Jun 2021 15:06:06 UTC Test date Tue, 01 Jun 2021 15:06:06 UTC Test duration HTTP status code 200 HTTP status code 200 HTTP server signature		
Supported Named Groups secp256r1, secp384r1 (server preferred order) SSL 2 handshake compatibility No HTTP Requests 1 https://mastermind-be.azurewebsites.net/ (HTTP/1.1 200 OK) Content-Length 20 Content-Type application/json; charset=utf-8 Date Tue, 01 Jun 2021 15:06:18 GMT Connection close Miscellaneous Miscellaneous Test date Tue, 01 Jun 2021 15:06:06 UTC Test duration 114.691 seconds HTTP status code 200 HTTP status code 200 HTTP status reversignature -		
SSL 2 handshake compatibility No HTTP Requests 1 https://mastermind-be.azurewebsites.net/ (HTTP/1.1 200 OK) 1	ECDH public server param reu	se No
HTTP Requests 1 https://mastermind-be.azurewebsites.net/ (HTTP/1.1 200 OK) 1 Content-Length 20 Content-Type application/json; charset=utf-8 Date Tue, 01 Jun 2021 15:06:18 GMT Connection close Miscellaneous Test date Tue, 01 Jun 2021 15:06:06 UTC Test duration 114.691 seconds HTTP status code 200 HTTP server signature -	Supported Named Groups	secp256r1, secp384r1 (server preferred order)
1	SSL 2 handshake compatibility	, No
Content-Length 20 application/json; charset=utf-8 Date	HTTP Requests	
Content-Length 20 application/json; charset=utf-8 Date	1 https://mastermind-bo.azz	urewebsites.net/ (HTTP/1.1 200 OK)
A pplication/json; charset=utf-8 Date Tue, 01 Jun 2021 15:06:18 GMT Connection close Miscellaneous Test date Tue, 01 Jun 2021 15:06:06 UTC Test duration 114.691 seconds HTTP server signature -		
Date Tue, 01 Jun 2021 15:06:18 GMT		
Miscellaneous Test date Tue, 01 Jun 2021 15:06:06 UTC Test duration 114.691 seconds HTTP status code 200 HTTP server signature -	1	
Test date Tue, 01 Jun 2021 15:06:06 UTC Test duration 114.691 seconds HTTP status code 200 HTTP server signature -	Connection	
Test date Tue, 01 Jun 2021 15:06:06 UTC Test duration 114.691 seconds HTTP status code 200 HTTP server signature -		
Test duration 114.691 seconds HTTP status code 200 HTTP server signature -		Tue 01 lun 2021 15:06:06 LTC
HTTP status code 200 HTTP server signature -		
HTTP server signature -		
		-
	_	-