DeepViolet

OWASP DeepViolet TLS/SSL JAVA API & Tools

Project Leader Milton Smith Twitter: @deepvioletapi Blog: https://www.securitycurmudgeon.com/

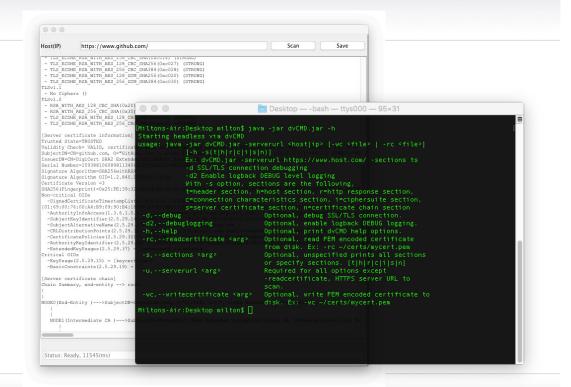
Black Hat EU 2016 London Tools Arsenal

What is DeepViolet?

TLS/SSL scanning API

2 reference cases demonstrating API

Command line tool & desktop application



Why Build DeepViolet?

Why build DeepViolet(DV)? I did not set out to build a tool for the public.

DV was a learning tool for me. Heartbleed was in the popular press, I wanted to learn more about underlying TLS/SSL protocols. When I finished the original code I posted it to my github site.

I was approached several times to add improvements to DV.

Asked others why they liked it. Most common answer is that there are few available choices for libraries that provide TLS/SSL scanning features for applications.

Great tools exist today like OpenSSL, Qualys SSL Server Test, Mozilla Observatory, etc.

Yes, my favorites as well. No intention to compete with any tools.

What Can DeepViolet API/Tools Do?

Identify Weak Server Cipher Suites

Identity Weak Signature Algorithms

Identity Certificates About to Expire

Print X.509 Certificates & Metadata

Print Trust Chains

Print Trust Status, Trusted or Not Trusted

And more...

Getting Started with the API

IDSession session = DVFactory.initializeSession(url);

IDVOnEng eng = DVFactory.getIDVOnEng(session);

// Get certificates, ciphersuites, print some reports...
// Review unit tests in com.mps.deepviolet.test.api to get
started...



DeepViolet Desktop Application

- TLS ECDHE - TLS ECDHE - TLS ECDHE - TLS ECDHE TLSv1.1 - No Ciphers TLSv1.0	RAM_RIIR_RED_IJ9_CBC_SRA(UACU14) (SIRONB) RSA_RIIR_RED_128_CBC_SRA(UACU14) (SIRONG) RSA_RIIR_RED_256_CBC_SRA(UACU25) (SIRONG) RSA_RIIR_RED_256_CBC_SRA(UACU25) (SIRONG) RSA_RIIR_RED_256_CBC_SRA(UASU46)(SIRONG)	
- TLS_ECDHE - TLS_ECDHE - TLS_ECDHE TLSv1.1 - No Ciphers TLSv1.0	RSA WITH AES 256 CBC SHA384 (0xc028) (STRONG) RSA WITH AES 128 GCM SHA256 (0xc02f) (STRONG)	
- TLS ECDHE - TLS ECDHE TLSv1.1 - No Ciphers TLSv1.0	RSA_WITH_AES_128_GCM_SHA256(0xc02f) (STRONG)	
- TLS_ECDHE FLSv1.1 - No Ciphers FLSv1.0		
FLSv1.1 - No Ciphers FLSv1.0	RSA_WITH_AES_256_GCM_SHA384 (0xc030) (STRONG)	
- No Ciphers FLSv1.0		
FLSv1.0		
	0	
	ES 128 CBC SHA(0x2f) (STRONG)	
	ES 256 CBC SHA(0x35) (STRONG)	
	RSA WITH AES 128 CBC SHA(0xc013) (STRONG)	
	RSA_WITH_AES_256_CBC_SHA(0xc014) (STRONG)	
	ficate information]	
[Server cert1 Trusted State		
	k= VALID, certificate valid between Wed Mar 09 16:00:00	PST 2016 and Thu May 17 05:00:00 PDT 2018
SubjectDN=CN=	github.com, O="GitHub, Inc.", L=San Francisco, ST=Calif	ornia, C=US, OID.2.5.4.17=94107, STREET="88
	DigiCert SHA2 Extended Validation Server CA, OU=www.digi	
Serial Number	=15938810608981134066197160231674485287	
	orithm=SHA256withRSA	
	orithm OID=1.2.840.113549.1.1.11	
Certificate V		anne sense sense an sense someres anatorio
SHA256(Finger Non-critical	print)=0x25:FE:39:32:D9:63:8C:8A:FC:A1:9A:29:87:D8:3E:4	C11D:98:DB:/1:E4:1A:48:03:98:EA:22:6A:BD:88
	ificateTimestampList(1.3.6.1.4.1.11129.2.4.2) =	
	00:A4:B9:09:90:B4:18:58:14:87:BB:13:A2:CC:67:70:0A:3C:3	5 • 98 • 04 • F9 • 1B • DF • B8 • F3 • 77 • CD • 0F • C8 • 0D • DC • 10
	nfoAccess(1.3.6.1.5.5.7.1.1) = [ocsp=http://ocsp.digice	
	<pre>(Identifier(2.5.29.14) = [88:5C:48:67:19:CC:A0:76:59:2D:</pre>	
	ernativeName(2.5.29.17) = [github.com www.github.com	
-CRLDistrib	utionPoints(2.5.29.31) = [http://crl3.digicert.com/sha2	-ev-server-gl.crl http://crl4.digicert.co
	ePolicies(2.5.29.32) = [2.16.840.1.114412.2.1=qualifier	
	<pre>LeyIdentifier(2.5.29.35) = [3D:D3:50:A5:D6:A0:AD:EE:F3:4</pre>	A:60:0A:65:D3:21:D4:F8:F8:D6:0F]
	yUsages(2.5.29.37) = [serverauth clientauth]	
Critical OIDs		
	<pre>:.5.29.15) = [keycertsign] :raints(2.5.29.19) = []</pre>	
-BasicConst	raints(2.5.29.19) = []	
	ficate chain]	
Chain Summary	r, end-entity> root	
t.		
	ity)>SubjectDN=CN=github.com, O="GitHub, Inc.", L=S	The second
NODEO (EIIG-EIIC	ity />adbjectbw-cw-githdb.com, o- dithdb, inc. , b-a	an Francisco, SI-california, C-05, OID.2.5.
NODE1 (Inte	ermediate CA)>SubjectDN=CN=DigiCert SHA2 Extended Va	lidation Server CA, OU=www.digicert.com, O=
1		
_		

- 1) Provide a URL and Click
- 2) Report is generated
- 3) Save report to disk

Easy as that. Adapt as needed.

DeepViolet Command Tool

1) Try a command line like this, java -jar dvCMD.jar -serverurl https://www.google.com/ -s hrcisn

2) Report is generated

3) Redirect output to file or pipe to grep to search certificate metadata

Easy as that. Adapt as needed.

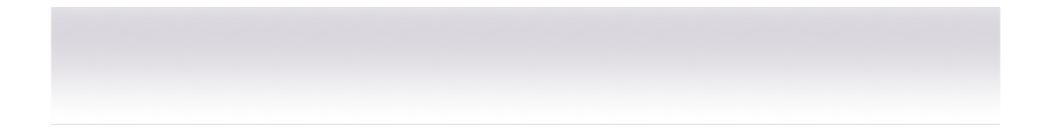
Additional References

OWASP Project Site: https://www.owasp.org/index.php/OWASP_DeepViolet_TLS/SSL_Scanner

GitHub Site: https://github.com/spoofzu/DeepViolet

Download: <u>https://github.com/spoofzu/DeepViolet/releases</u>

Follow Online: twitter, @deepvioletapi



;0)

