Kommunikation im Unternehmen

Vier Gruppen

Unternehmensleitung

Unternehmensleitung

IT-Administration

IT-Administration

Kunden

Kunden

BenutzerInnen

BenutzerInnen

Wer

Alle

Sicherheit ist ein Prozess

Alle

– Marc Coleman

Was passiert, wenn wir in die Fortbildung unserer MitarbeiterInnen investieren und sie verlassen die Firma?

– Marc Coleman

Was passiert wenn wir das nicht tun und sie bleiben?

– Marc Coleman

Alle

Gute Sicherheit ist benutzbar

Sicher

Sicher

Was bedeutet „sicher“?

Bedrohungslage?

Fehler in Software

Konkurrenz

Wirtschaftsspionage

Vorratsdatenspeicherung

Dezentrale Sicherungskopien

Zeit

Sicherer

Sicherer

Infrastruktur Lösungen

Altlasten loswerden

FAX

‘43

1843

2014


FAX

Windows XP

~~Windows XP~~

Updates

Kommunikation


Klartext

~~Unverschlüsselt~~

Status Quo

Testen

Webserver

http://

https://

Webserver testen

https://ssllabs.com/ssltest

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Domain name: Submit

Do not show the results on the boards

Recently Seen

metronets.com	Err
slack.com	
owncloud.jonaskim.de	
wasserwacht-magdeburg.de	A-
pescaboutique.com	C
openmailbox.org	A
d2p-dev.novartis.com	Err
pop.openmailbox.org	A
client.investia.ca	F
smtp.openmailbox.org	A

Recent Best-Rated

londoners.ro	A+
openmailbox.org	A
pop.openmailbox.org	A
smtp.openmailbox.org	A
scottlinux.com	A-
sal.investpoint.automatedfin ...	A-
vlietlandziekenhuis.nl	B
votesmart.org	B
pescaboutique.com	C
office.com	C

Recent Worst-Rated

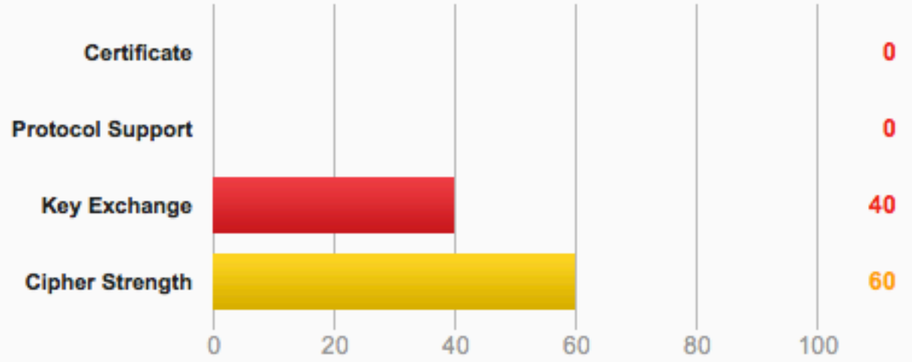
client.investia.ca	F
outlook.com	F
webmin.studiotwo.com	Trust
myhr.ahg.com.au	F
portal.lrgh.org	F
guestful.com	F
poulp.net	Trust
mysql.triedtoswiminlava.net	Trust
my.sph.harvard.edu	F
api.2dehands.com	F

Summary

Overall Rating

F

If trust issues are ignored: F



Documentation: SSL/TLS Deployment Best Practices, SSL Server Rating Guide, and OpenSSL Cookbook.

This server's certificate is not trusted. Grade set to F.

This server supports SSL 2, which is obsolete and insecure. Grade set to F.

This server is vulnerable to MITM attacks because it supports insecure renegotiation. Grade set to F.

This server does not mitigate the CRIME attack. Grade capped to B.

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to B.

There is no support for secure renegotiation. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Protocols

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3	Yes
SSL 2 **INSECURE**	Yes

Cipher Suites (sorted by strength; the server has no preference)

SSL_CK_RC4_128_EXPORT40_WITH_MD5 (0x20080) **INSECURE**	40
SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5 (0x40080) **INSECURE**	40
TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x3) **WEAK**	40
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x6) **WEAK**	40
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x8) **WEAK**	40
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0x14) DH 512 bits (p: 64, g: 1, Ys: 64) FS **WEAK**	40
SSL_CK_DES_64_CBC_WITH_MD5 (0x60040) **INSECURE**	56
TLS_RSA_WITH_DES_CBC_SHA (0x9) **WEAK**	56
TLS_DHE_RSA_WITH_DES_CBC_SHA (0x15) DH 1024 bits (p: 128, g: 1, Ys: 128) FS **WEAK**	56
SSL_CK_RC4_128_WITH_MD5 (0x10080) **INSECURE**	128
SSL_CK_RC2_128_CBC_WITH_MD5 (0x30080) **INSECURE**	128
TLS_RSA_WITH_RC4_128_MD5 (0x4)	128
TLS_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
SSL_CK_DES_192_EDE3_CBC_WITH_MD5 (0x700c0) **INSECURE**	112
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112

SSL Report:

Assessed on: Mon Feb 24 15:25:04 UTC 2014 | Clear cache

Scan Another >>

	Server	Domain(s)	Test time	Grade
1	Ready		Mon Feb 24 15:17:27 UTC 2014 **Duration:** 32.521 sec	F
2	Ready		Mon Feb 24 15:17:59 UTC 2014 **Duration:** 31.150 sec	F
3	Ready		Mon Feb 24 15:18:30 UTC 2014 **Duration:** 26.849 sec	F
4	Ready		Mon Feb 24 15:18:57 UTC 2014 **Duration:** 27.329 sec	F
5	Ready		Mon Feb 24 15:19:25 UTC 2014 **Duration:** 29.477 sec	F

SSL Report: wko.at

Assessed on: Mon Feb 24 15:03:14 UTC 2014 | **HIDDEN** | Clear cache

Scan Another >>

	Server	Domain(s)	Test time	Grade
1	194.107.236.209 www.wko.at Ready	wko.at	Mon Feb 24 15:01:34 UTC 2014 **Duration:** 46.971 sec	B
2	194.107.236.210 Ready	www.wko.at	Mon Feb 24 15:02:21 UTC 2014 **Duration:** 52.849 sec	A-

Warning: Inconsistent server configuration

SSL Report v1.7.19

SSL Report: wko.at (194.107.236.210)

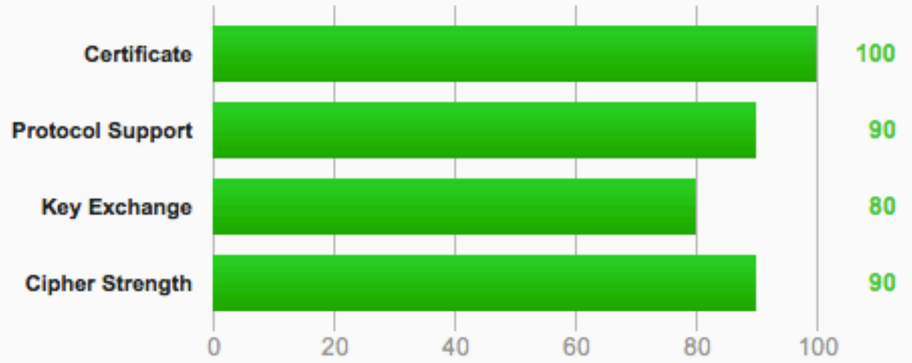
Assessed on: Mon Feb 24 15:03:14 UTC 2014 | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

A-



Documentation: SSL/TLS Deployment Best Practices, SSL Server Rating Guide, and OpenSSL Cookbook.

The server does not support Forward Secrecy with the reference browsers. Grade reduced to A-. MORE INFO »

Authentication

SSL Report: bettercrypto.org (78.41.116.68)

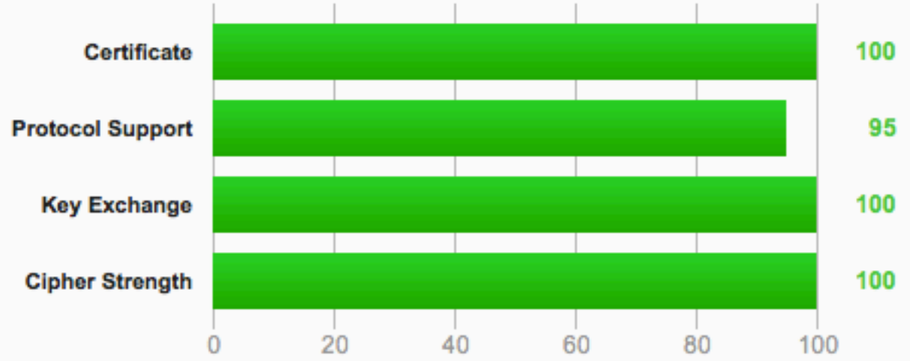
Assessed on: Mon Feb 24 15:13:26 UTC 2014 | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

A+



Documentation: SSL/TLS Deployment Best Practices, SSL Server Rating Guide, and OpenSSL Cookbook.

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »

Authentication

Email

https://starttls.info/

Does your mail server support STARTTLS?

If you care about privacy, it should. Read more in the blog.

Results for: .gv.at

Mail server		Result
mta3.	.gv.at	STARTTLS not supported!
mta2.	.gv.at	STARTTLS not supported!

Click the score for details.

Check another!

Results for: .at

Mail server	Result
mail2. or.at	Error: The server rejected our check
mail1. .or.at	Grade: C (58.0%)

Certificate

- The certificate is not valid for the server's hostname.
- There is a self-signed certificate in the trust chain. It may be a configuration problem.
- There are one or more fatal problems which causes the certificate not to be trusted.

There are validity issues for the certificate. Certificates are seldom verified for SMTP servers, so this doesn't mean that STARTTLS won't be used.

Generally speaking it's a bad practice not to have a valid certificate, and an even worse practice not to verify them. Any attempted encrypted communication is left all but wide open to Man-in-the-Middle attacks.

Protocol

- Supports TLSV1.

Key exchange

- Key size is 2048 bits; that's good.

Cipher

- Weakest accepted cipher: 40.
- Strongest accepted cipher: 56.

Click the score for details.

Check another!

Does your mail server support STARTTLS?

If you care about privacy, it should. Read more in the blog.

Results for: ubermorgen.com

Mail server	Result
ubermorgen.com	Grade: A (93.4%)

Certificate

- No remarks.

Protocol

- Supports SSLV3.
- Supports TLSV1.
- Supports TLSV1.1.
- Supports TLSV1.2.

Key exchange

- Key size is 4096 bits; that's very good.

Cipher

- Weakest accepted cipher: 128.
- Strongest accepted cipher: 256.

Click the score for details.

Check another!

https://starttls.info/stats

Chat

https://xmpp.net/

IM Observatory client report for jabber.at

Test started 2014-02-24 15:25:47 UTC about an hour ago.

Show server to server result | Permalink to this report

Score

jabber.at:5222

Grade: A⁻

Warning: Server allows RC4 when using TLS 1.1 and/or TLS 1.2. Grade capped to A⁻.

General

jabber.at:5222


A

Handlungsbedar F

Technisches

Verschlüsselung als Standard

FTP

FTP
Unsicher seit 1971

Transportverschlüsselung

TLS 1.2

TLS 1.1

TLS 1.0

~~*SSLv3*~~

~~*SSLv2*~~

VPN

L2TP

IPSec

OpenVPN

PPTP

Festplatten Verschlüsselung

Passwörter

Zeichenvorrat Länge

Firewalls

Router

WiFi Access Points

Switches

IDS

Dokumentation

Emails

Postkarten

Verschlüsseln

GPG
S/MIME

Sicherheit: ✅ Signiert

Sicherheit: ✅ Signiert

🔒 Verschlüsselt

security@beispiel.at
mit GPG Key


CRYPTO
PARTY


bettercrypto·org

Testseiten

https://ssllabs.com	Web
https://starttls.info	Mail
https://xmpp.net	Chat
https://j.mp/1hPTrIW	XSS

Weitere Information


https://cryptoparty.at


https://bettercrypto.org


https://maclemon.at

Danke

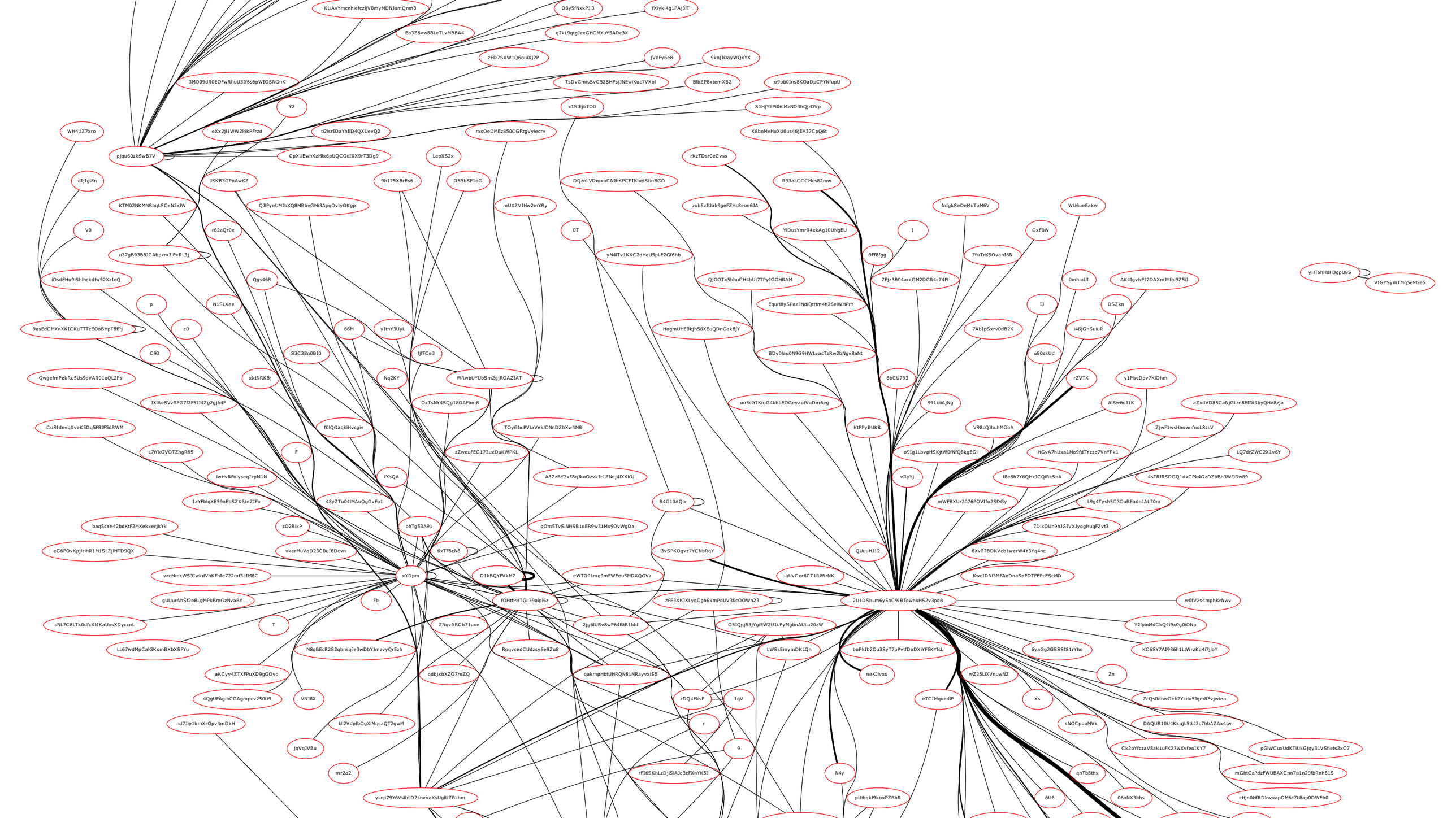
Hashverfahren

bcrypt

SHA256

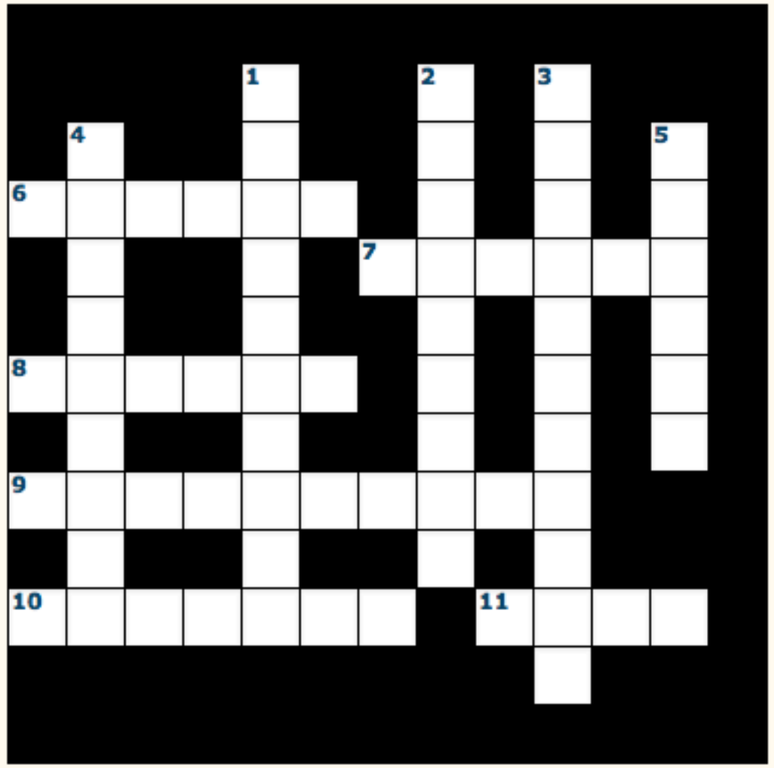
~~*MD5*~~

~~*SHA1*~~


KLiAvYmcnhlefczIjV0myMDNJamQnm3
D8y5fNxkPJi3
fXiyki4g1PAJ3lT
Eo3Z6vw8BLeTLvMBBA4
q2kL9qtgJexGHCMYuY5ADc3X
zED7SXW1Q6ouiXj2P
jVoFy6e8
9knJJDayWQxYX
3MO09dR0EOFwRhuU3If6s6pWIOSNGnK
TsDvGmisSvC52SHPsjJNEwiKuc7VXol
BlbZP8xtemXB2
o9pb0Ins8K0aDpCPYNfupU
Y2
x1SIEjbTO0
S1HjYEPi06IMzND3hQjrDVp
WH4UZ7xro
eXx2jl1WW2l4kPFrzd
ti2isrIDaYhED4QXUevQ2
rxsOeDMEz850CGFzgVylecrv
X8bnMvHuXU0us46jEA37CpQ6t
pJqu60zkSwB7V
CpXUEwhXzMlx6pUQCOcIXX9rT3Dg
LepXS2x
rKzTDsr0eCvss
dIJIgl8n
JSKB3GPxAwKZ
9h175XBrEs6
O5RbSF1oG
DQzoLVDmxoCNJbKPCPIKhetStinBGO
R93aLCCCMcs82mw
KTM02NKMNSbqLSCeN2xIW
QJlPyeUMIbXQ8MBbvGMi3ApqOvtyOKgp
mUXZVIHw2mYRy
zub5zJUak9geFZHc8eoe6JA
NdgkSeDeMuTuM6V
WU6oeEakw
V0
r62aQr0e
0T
YlDusYmrR4xkAg10UNgEU
I
GxF0W
u37gB93B8JCAbpzm3iExRL3j
yN4lTv1KXC2dHeU5pLE2Gf6hb
9Ff8fgg
IYuTrK9Ovan16N
yHTahHdH3gpU9S
VIGYSymTMq5ePGe5
iOsdEHu9iShlhckdfw52XzIoQ
Qgs468
QJOOTx5bhuGH4bUt7TPyIGGHRAM
7Ejz3B04accGM2DGR4c74FI
0mhiuUI
AK4IgvNEJ2DAXmJYfol9ZSiJ
p
N1SLXee
EquH8ySPaeJNdiQtHm4h26eIWHPrY
IJ
DSZkn
9asEdCMXnXKICKuTTTzEOoBHpT8fPJ
z0
66M
yItnY3UyL
HogmUHE0kjh58XEuQDnGak8jY
7AbIpSxrv0dB2K
i48jGhSuiuR
C93
S3C28n0BI0
lJfFCe3
BDv0lau0N9G9HWLvacTzRw2bNgv8aNt
u80skUd
QwgefmPekRu5Us9pVAR01oQL2Psi
xktNRKBj
Nq2KY
WRwbUYUbSm2gJROAZJAT
8bCU793
rZVTX
y1MscDpv7KlOhm
JXlAeSVzRPG7f2F5JJ4Zg2gjh4F
OxTsNY4SQg18OAFbm8
uo5clYIKmG4khbEOGeyaotVaDm6eg
991kiiAjNg
AlRw6oJ1K
aZxdVD85CaNjGLrn8EfDt3byQHv8zja
CuSIdnvqXveK5Dq5F8IF5dRWM
f0lQOaqkiHvcgiv
TOyGhcPVtaVekICNnDZhXw4M8
KtPPyBUK8
V98LQJhuhMOoA
ZjwF1wsHaownfnoL8zLV
LQ7drZWC2X1v6Y
L7iYkGVOTZhgRfi5
F
zZweuFEG173uxOuKWPKL
o9Ig1LbvpHSKJtW0fNfQ8kgEGI
hGyA7hUxa1Mo9fdTYzzq7VnYPk1
lwHvRFolyseqIzpM1N
fXsQA
A8ZzBY7xF8qJkoOzvkJr1ZNej4IXXKU
vRyYJ
f8e6b7Y6QHxJCQiRcSnA
4sT8JRSDGQ1dxCPk4GzDZbBh3WfJRw89
IaYFbiqXE59nEbSZXRteZIFa
48yZTu04IMAuOgGvFo1
R4G10AQlx
mWFBXUr2076POVIfo2SDGy
L9g4Tysh5C3CuREadnLAL70m
baq5cYH42bdKtF2MXekxerjkYk
zO2RikP
bhTg53A91
qOm5TvSiNHSB1oER9w31Mx9OvWgDa
7DlkOUn9hJGIVXJyogHuqFZvt3
eG6POvKpJlzihR1M1SLZJlHTD9QX
vkerMuVaD23C0uI6Dcvn
6xTF8cN8
3vSPKOqvz7YCNbRqY
QUuuHJ12
6Xv22BDKVcb1werW4Y3Yq4nc
vzcMmcWS3lwkdVhKfhIe722mf3LIM8C
xYDpm
D1kBQYFVkM7
eWTO0Lmq9mFWEeu5MDXQGVz
aUvCxr6CT1RlWrNK
KwcIDNI3MFAeDnaSoEDTFEPcEScMD
gUUurAhSf2oBLgMPkBmGzNvaBY
Fb
fOHttPHTGll79aipi6z
zFE3XKJXLyqCgb6xmPdUV30cOOWh23
2U1DShLm6y5bC9IBTowhkHS2v3pdB
w0fV2s4mphKrNwv
cNL7C8LTk0dfcXl4KaUosXDyccnL
T
ZNqvARCh71uve
2Jg6lURv8wP64BtRIJdd
O5JQpj53JYgiEW2U1cPyMgbnAULu20zW
Y2lpinMdCkQ4i9x0g0iONp
LL67wdMpCaIGKxmBXbXSFYu
N8qBEcR2S2qbnsqJe3wDbYJmzvyQrEzh
RpqvcedCUdzsy6e9Zu8
LWSsEmymDKLQn
boPkIb2Ou3SyT7pPvfDoDXiYFEKYfsL
6yaGg2GSSSfS1rYho
KC6SY7AI936h1LtWrzKq4i7JloY
aKCyy4ZTXFPuXD9gOOvo
qdbjxhXZO7reZQ
qakmpHbtUHRQN81NRayvxIS5
neKJlvxs
wZ25LIXVnuwNZ
Zn
4QgUFAgibCGAgmpcv250U9
VNJ8X
zDQ4EksF
1qV
eTCIMquedlP
Xs
ZcQs0dhwOeb2Ycdv5Jqm8Evjwteo
nd7Jip1kmXrOpv4mDkH
Ul2VdpfbOgXiMqsaQT2qwM
sNOCpooMVk
DAQUB10U4KkujL5tLJ2c7hbAZAx4tw
jqVqJVBu
r
Ck2oYfczaV8ak1uFK27wXvfeoIKY7
pGlWCuxUdkTiUkGjqy31VShets2xC7
9
mr2a2
rFI6SKhLzDJlSlAJe3cFXnYK5J
N4y
qnTb8thx
mGhtCzPdzFWUBAXCnn7p1n29fbRnh81S
yLcp79Y6VslbLD7snvxaXsUglUZBLhm
pUihqkf9koxPZBbR
6U6
06nNX3bhs
cHjn0NfRDInvxapOM6c7L8ap0DWEh0

A crossword based on the Adobe password leak.
Inspired by xkcd #1286: Encryptic

Password popularity: 1-100 | 101-200 | 201-300 | 301-400 | 401-500 | 501-600 | 601-700 | 701-800 | 801-900 | 901-1000



Reveal | Check | Hide

Across

6: zk8NJgAOqc4=

dog; cat; pet; dark; dogs name; Dog; my dog; black dog; dog name; dog's name; darkness; black cat; sonic; black; kitty; horse; Cat; pets name; sombra; puppy; cats name; old dog; shade; first dog; pet name; doggy; hedgehog; cat's name; bike; my cat; nickname; Pet; me; light; favorite pet; usual; sha; doggie; pet's name; first pet; animal; sh; shad; s; car; first cat; Dog's name; chien; favorite dog; ombre

7: WIMTLimQ5b4=

8: FTeB5SkrOZM=

9: WqflwJFYW3+PszVFZo1Ggg==

10: yxzNxPlsFno=

11: L3uQHNDF6Mw=

Down

1: 2aZl4Ouarwm52NYYl936YQ==

adobe; adobex2; adobe2; adobe twice; twice; adobetwice; adobe2x; site; ??????; name; software; 2x; company; 2xadobe; programa; adobe x 2; program; adobe x2; ???; ad; adobe*2; ????; Adobe; double; namename; 2adobe; ?????; x2; a; name twice; photoshop; company name; adobe adobe; adobe?; ado; aa; company twice; 2; marca; website; none; adobe 2x; product; company name twice; adobeX2; this; logiciel; ??; ???????; what is this

2: L8qbAD3jl3jSPm/keox4fA==

3: 7Z6uMyq9bpxe1EB7HijrBQ==

4: vp6d18mfGL+5n2auThm2+Q==

5: dA8D8QYD55E=