SSL Report: goes-app.cbp.dhs.gov (216.81.87.21)

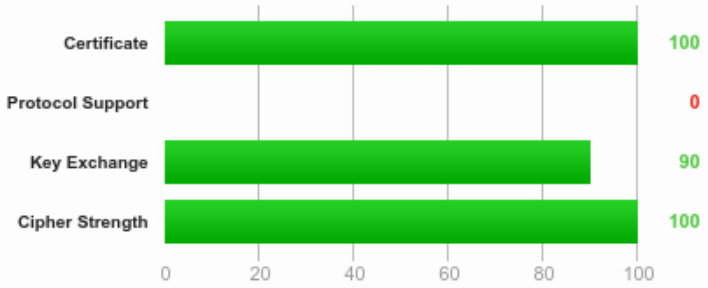
Assessed on: Thu, 17 Sep 2015 07:14:15 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



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

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

Intermediate certificate has a weak signature. When renewing, ensure you upgrade to an all-SHA2 chain. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

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

SSL Report: esta.cbp.dhs.gov (216.81.87.20)

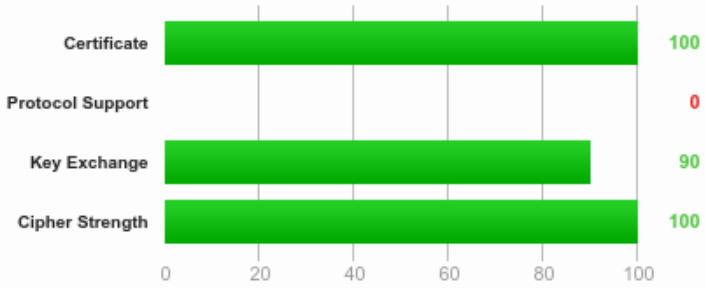
Assessed on: Thu, 17 Sep 2015 07:14:25 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



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

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

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

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

SSL Report: ace.cbp.dhs.gov (216.81.83.93)

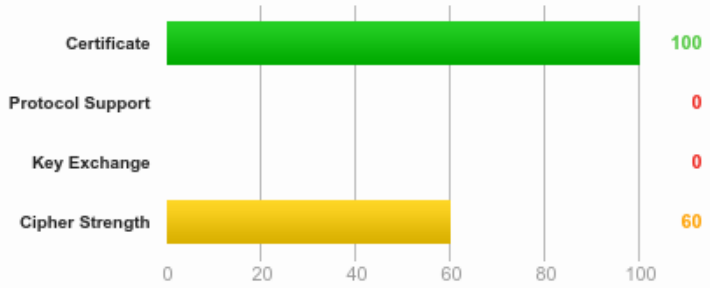
Assessed on: Thu, 17 Sep 2015 07:15:49 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



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

This server supports 512-bit export suites and might be vulnerable to the FREAK attack. Grade set to F. MORE INFO »

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

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

This server accepts the RC4 cipher, which is weak. Grade capped to B. MORE INFO »

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

https://www.ssllabs.com/ssltest/analyze.html?d=eapisws.cbp.dhs.gov

QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > eapisws.cbp.dhs.gov

SSL Report: eapisws.cbp.dhs.gov (216.81.87.19)

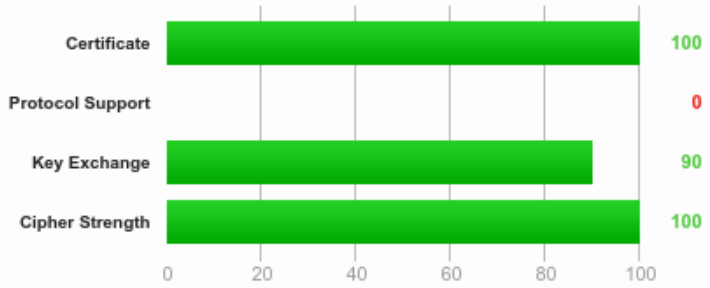
Assessed on: Thu, 17 Sep 2015 07:15:52 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



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

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

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

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

https://www.ssllabs.com/ssltest/analyze.html?d=payment.cbp.dhs.gov

QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > payment.cbp.dhs.gov

SSL Report: payment.cbp.dhs.gov (216.81.87.22)

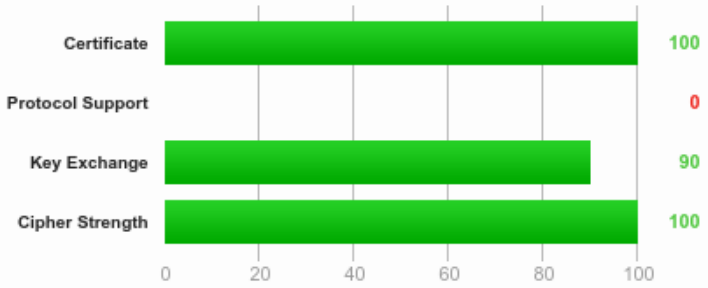
Assessed on: Thu, 17 Sep 2015 07:16:54 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



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

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

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

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

SSL Report: svrs.cbp.dhs.gov (216.81.83.72)

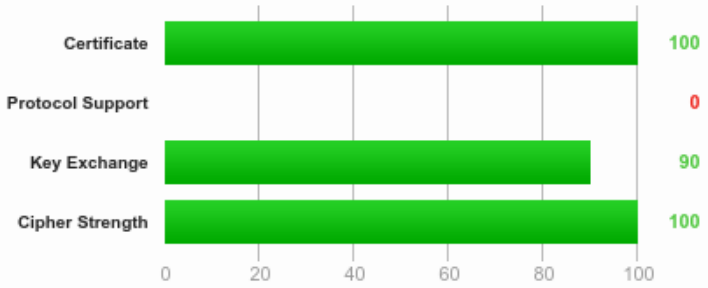
Assessed on: Thu, 17 Sep 2015 07:19:07 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



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

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

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

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

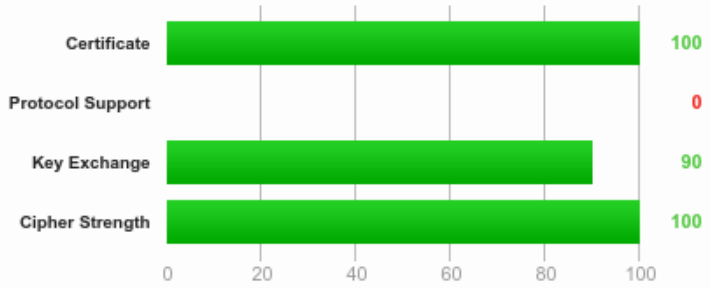
SSL Report: tradeservices.cbp.dhs.gov (216.81.83.86)

Assessed on: Thu, 17 Sep 2015 07:19:21 UTC | Clear cache

Scan Another »

Summary

Overall Rating



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

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

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

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

SSL Report: myaccount.uscis.dhs.gov (216.81.92.53)

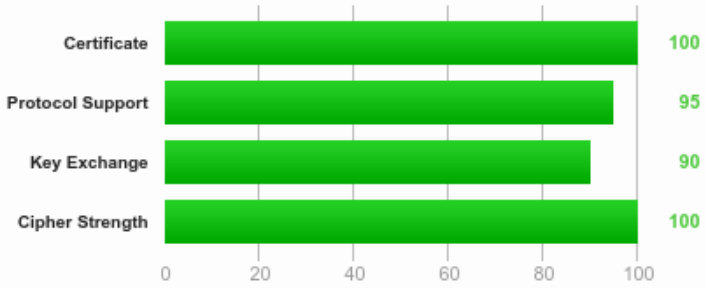
Assessed on: Thu, 17 Sep 2015 07:21:25 UTC | Clear cache

Scan Another »

Summary

Overall Rating

A-



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

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

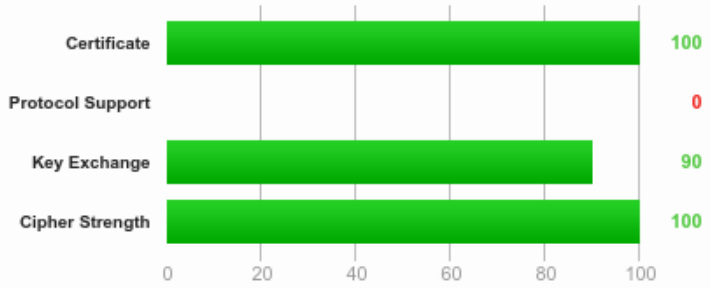
SSL Report: i94.cbp.dhs.gov (216.81.87.24)

Assessed on: Thu, 17 Sep 2015 07:20:47 UTC | Clear cache

Scan Another »

Summary

Overall Rating



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

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

Intermediate certificate has a weak signature. When renewing, ensure you upgrade to an all-SHA2 chain. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

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

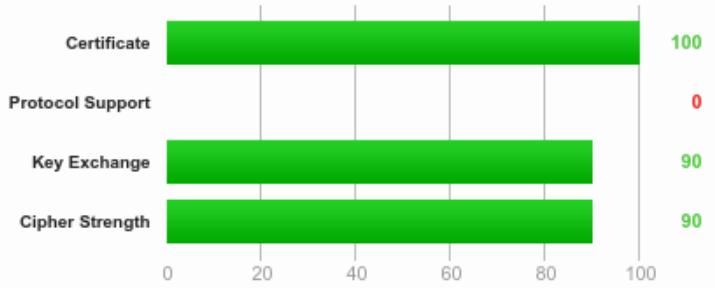
SSL Report: elis.uscis.dhs.gov (216.81.92.62)

Assessed on: Thu, 17 Sep 2015 07:21:28 UTC | Clear cache

Scan Another »

Summary

Overall Rating



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

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »

This server is vulnerable to the POODLE attack against TLS servers. Patching required. Grade set to F. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

There is no support for secure renegotiation. MORE INFO »

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

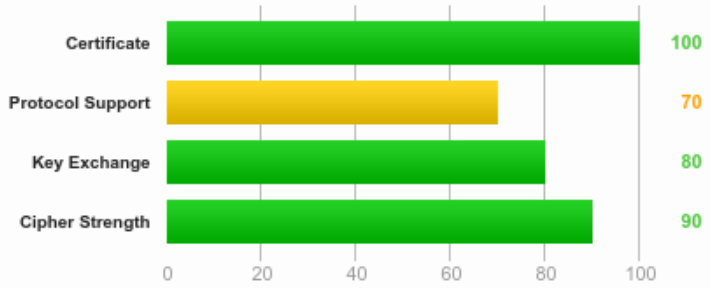
SSL Report: cdp.dhs.gov (207.203.45.66)

Assessed on: Thu, 17 Sep 2015 07:25:10 UTC | Clear cache

Scan Another »

Summary

Overall Rating



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 »

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »

Certificate uses a weak signature. When renewing, ensure you upgrade to SHA2. MORE INFO »

This server accepts the RC4 cipher, which is weak. Grade capped to B. MORE INFO »

SSL Report: csi-rt.cbp.dhs.gov (216.81.83.75)

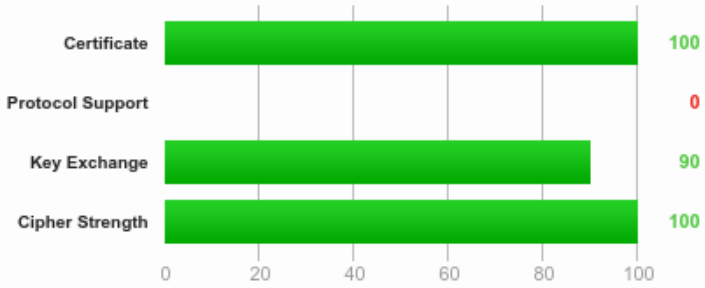
Assessed on: Thu, 17 Sep 2015 07:24:36 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



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

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

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

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

SSL Report: universalenroll.dhs.gov (67.216.165.41)

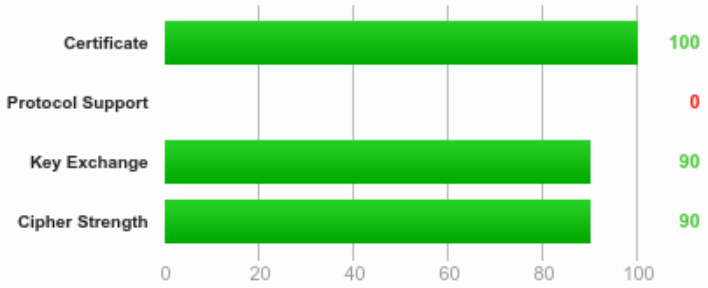
Assessed on: Thu, 17 Sep 2015 07:25:37 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



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

This server is vulnerable to the POODLE attack against TLS servers. Patching required. Grade set to F. MORE INFO »

This server uses SSL 3, which is obsolete and insecure. Grade capped to B. MORE INFO »

Certificate uses a weak signature. When renewing, ensure you upgrade to SHA2. MORE INFO »

This server uses RC4 with modern browsers. Grade capped to C.

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

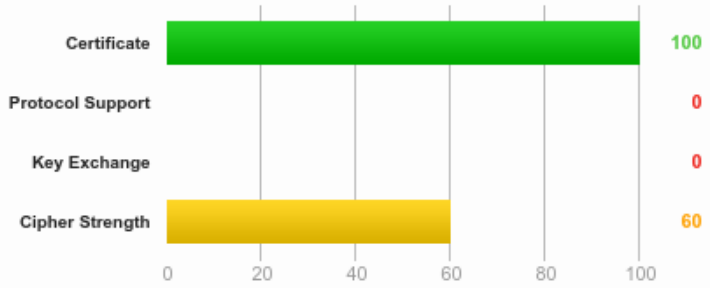
SSL Report: reporting.odp.dhs.gov (216.81.83.130)

Assessed on: Thu, 17 Sep 2015 07:27:54 UTC | Clear cache

Scan Another »

Summary

Overall Rating



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

This server supports 512-bit export suites and might be vulnerable to the FREAK attack. Grade set to F. MORE INFO »

This server is vulnerable to the POODLE attack against TLS servers. Patching required. Grade set to F. MORE INFO »

This server uses SSL 3, which is obsolete and insecure. Grade capped to B. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

This server accepts the RC4 cipher, which is weak. Grade capped to B. MORE INFO »

There is no support for secure renegotiation. MORE INFO »

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

SSL Report: trainingprism.dhs.gov (216.81.94.35)

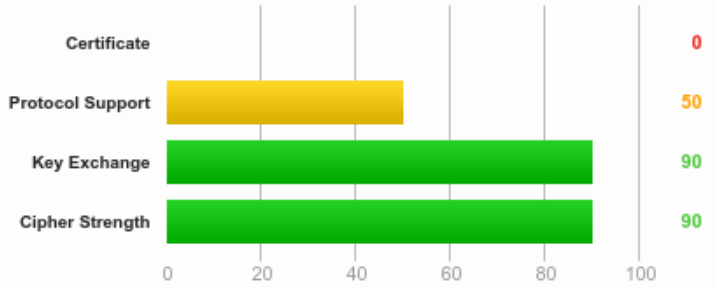
Assessed on: Thu, 17 Sep 2015 07:29:56 UTC | Clear cache

Scan Another »

Summary

Overall Rating

If trust issues are ignored: C



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

This server's certificate is not trusted, see below for details.

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

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

This server's certificate chain is incomplete. Grade capped to B.

SSL Report: ctpat.cbp.dhs.gov (216.81.87.27)

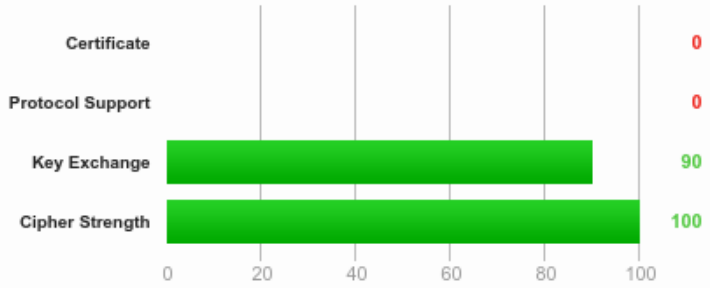
Assessed on: Thu, 17 Sep 2015 07:27:25 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



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

This server's certificate is not trusted, see below for details.

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

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

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

SSL Report: dtops.cbp.dhs.gov (216.81.87.17)

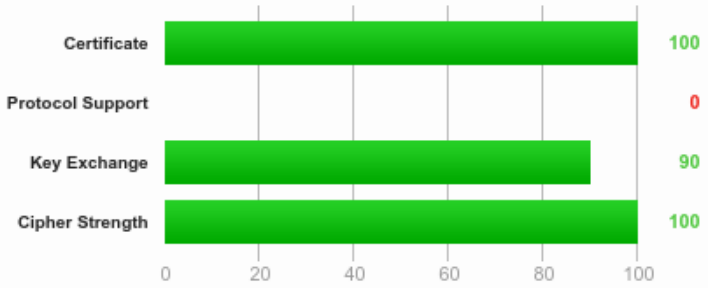
Assessed on: Thu, 17 Sep 2015 07:31:19 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



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

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

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

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

SSL Report: appstore.tsa.dhs.gov (170.225.22.13)

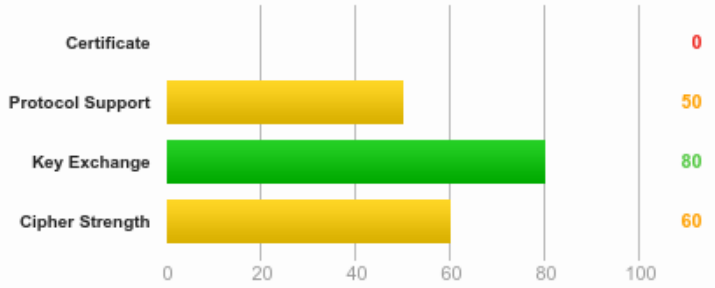
Assessed on: Thu, 17 Sep 2015 07:31:22 UTC | Clear cache

Scan Another »

Summary

Overall Rating

If trust issues are ignored: C



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

This server's certificate is not trusted, see below for details.

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

Intermediate certificate has a weak signature. Upgrade to SHA2 as soon as possible to avoid browser warnings. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

This server accepts the RC4 cipher, which is weak. Grade capped to B. MORE INFO »

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

This server's certificate chain is incomplete. Grade capped to B.

This site works only in browsers with SNI support.