

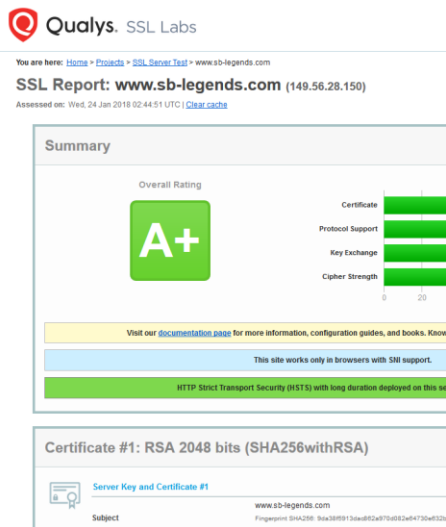
Digital Certificate Lab

IT2700

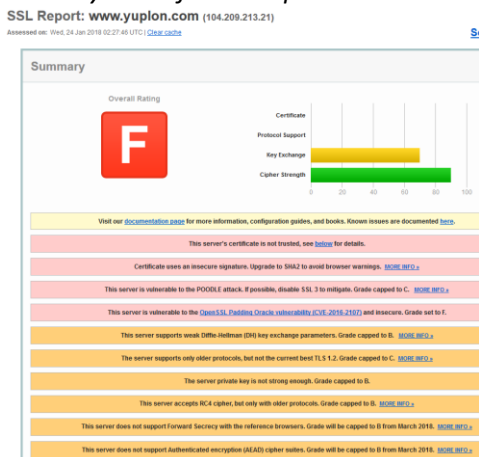
SSL Server and Client Tests

PART 1: Recent Best vs Recent Worst

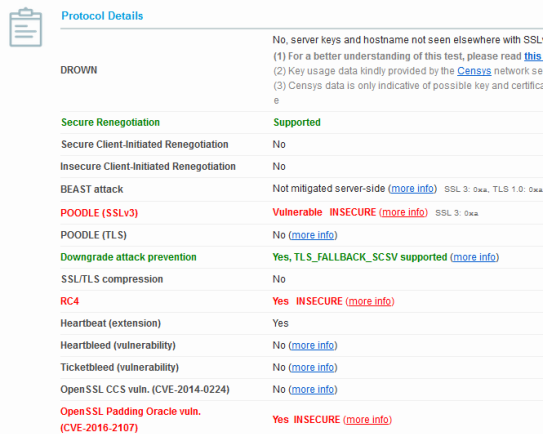
1. Visit <https://www.ssllabs.com/>
2. In the main screen, select **Test your server**
3. Test the certificates of all three websites and answer these questions for each test.
 - a. One from the Recent Best list.
 - b. One from the Recent Worst list.
 - c. A website of your choosing (be sure it has a certificate)
4. Run the report for the web site. Submit a screenshot of the Summary. You should see a screen similar to this:



5. If the site does NOT get an overall rating of A, you will see the reasons listed – See below for an example. (If the site received an A or A+ rating, move to the next question). Read through these reasons. *In your opinion, which three things should be addressed (in order of priority) that this site may do to fix these problems and improve its grade?*



6. Look under one of the Certificate sections. How long is the life of this certificate? Under the certificate section, what kind of asymmetric key is being used?
7. How would the Certificate Revoked if necessary? (look under Revocation information). Is OCSP Stapling required?
8. Looking at the versions of TLS and SSL, what is the most secure protocol supported by this certificate? Are there any insecure protocols listed? If so, list them.
9. Under Protocol Details, are there any vulnerabilities listed (look for listings like POODLE, BEAST attack, etc)? See below for examples:



Protocol Details	
No, server keys and hostname not seen elsewhere with SSL. (1) For a better understanding of this test, please read this . (2) Key usage data kindly provided by the Censys network se (3) Censys data is only indicative of possible key and certificate	
DROWN	
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) SSL 3: Ok, TLS 1.0: Ok
POODLE (SSLV3)	Vulnerable INSECURE (more info) SSL 3: Ok
POODLE (TLS)	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	Yes INSECURE (more info)
Heartbeat (extension)	Yes
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)	Yes INSECURE (more info)

10. Repeat for the other websites.

11. Please answer the following questions:

- a. Briefly describe a POODLE attack.
 - i. Who discovered it?
 - ii. Who is vulnerable to this attack?
 - iii. How can you mitigate the attack?
- b. In your opinion, is it better for the certificate to have a long life (greater than 12 months) or a short life (less than 12 months)?
- c. Browse the article found at <https://www.fir3net.com/Security/Concepts-and-Terminology/certificate-revocation.html>
 - i. List the advantages & disadvantages of CRL versus OCSP.
 - ii. What is OCSP stapling, and how does it help mitigate the weaknesses of OCSP?

Part II: Test your browser

1. From <https://www.ssllabs.com/> test your current browser.
2. **Submit a screenshot of results.** Are there any vulnerabilities to be concerned about?
3. What Protocols are supported?
4. Is OCSP stapling supported by your browser?
5. Repeat the steps and questions but for a different browser. NOTE: You may have to close your previous browser or visit another computer).

Part III: Viewing Digital Certificates

1. Open your browser to www.google.com
2. Click the padlock icon in the browser address bar.
3. Click through whatever screens necessary to view the certificate.
4. Click on the Details tab.
5. Locate the Public Key. Take a screenshot of the public key details.
6. **Submit a screenshot** of the Certification Path. Because web certificates are based on the distributed trust model, there is a path to the root certificate.
7. Compare the expiration date of the root certificate and the expiration date of Google's. Which expires sooner? What effect would it be on Google if the root certificate expired or was revoked (which happened during the Heartbleed fiasco)?

Part IV: Viewing Digital Certificate Revocation Lists

1. From a Windows computer, go to a command prompt.
2. Type **certmgr.msc** and press **Enter**.
3. In the left pane, expand **Trusted Root Certification Authorities**
4. In the left pane, click **Certificates**. These are the CAs approved for your computer.
Submit a screenshot.
 - a. Are there any certificates listed that have expired or been revoked? (finding hint: sort the certs by date) **Submit a screenshot** of the general tab of one of them.
5. In the left pane, expand **Intermediate Certification Authorities**.
6. Click **Certificates** to view the intermediate CAs. **Submit a screenshot** of the Intermediate Certificate list.
7. Click **Certificate Revocation List**.
8. In the right pane, all revoked certificates will display. Select a revoked certificate and double click it to view the details. Why do you think this certificate was revoked?
Submit a screenshot of the revoked certificate you are examining.
9. Return back to the Certificate Manager.
10. In the left pane, expand **Untrusted Certificates**.
11. Click **Certificates**. The certificates that are no longer trusted are listed in the right pane.
12. Double click on one of the untrusted certificates. Read the information. Why do you think it became untrusted? **Submit a screenshot** of the untrusted certificate you are examining.