Session 11 – SSL Wei Cui

**Lab Objectives**

* Follow the instructions for Project 6-1 SSL Server and Client Tests
* Write a report including screenshots and written descriptions. Be sure to include a screenshot and description for step 4 (import a screenshot of one of the recent best and one of the recent worst sites).

**Lab Results**

1. Went to [www.ssllabs.com/ssltest/index.html](http://www.ssllabs.com/ssltest/index.html) (Fig 1)
2. Clicked the first website listed under Recent Best-Rate: timco.cloud
3. Fig. 2 shows the best overall rating along with scores for Certificate, Protocol Support, Key Exchange, and Cipher Strength, which make up the cipher suite.
4. Clicked the first website listed under Recent Worst-Rate: www.kuschelkirche.de
5. Fig. 3 shows the worst overall rating along with scores for Certificate, Protocol Support, Key Exchange, and Cipher Strength.
6. The scores in the worst rating and in the best rating are almost the same. Because the worst rating host (www.kuschelkirche.de) is vulnerable to DROWN attack, it receives an F grade.
7. Fig. 4 shows the message explains why the host receives F grade.
8. If a site was to increase its security, it should no longer support TLS 1.0 and SSL 3.0 or below because the current best is TLS 1.2.
9. Clicked Projects and clicked SSL Client Test in Chrome. Repeated the test in IE 11. The reports of the two browsers are more or less the same, but only difference is that Chrome upgrades insecure requests request header whereas IE 11 does not as shown in Fig 5. Thus, I think Chrome a slightly better browser.

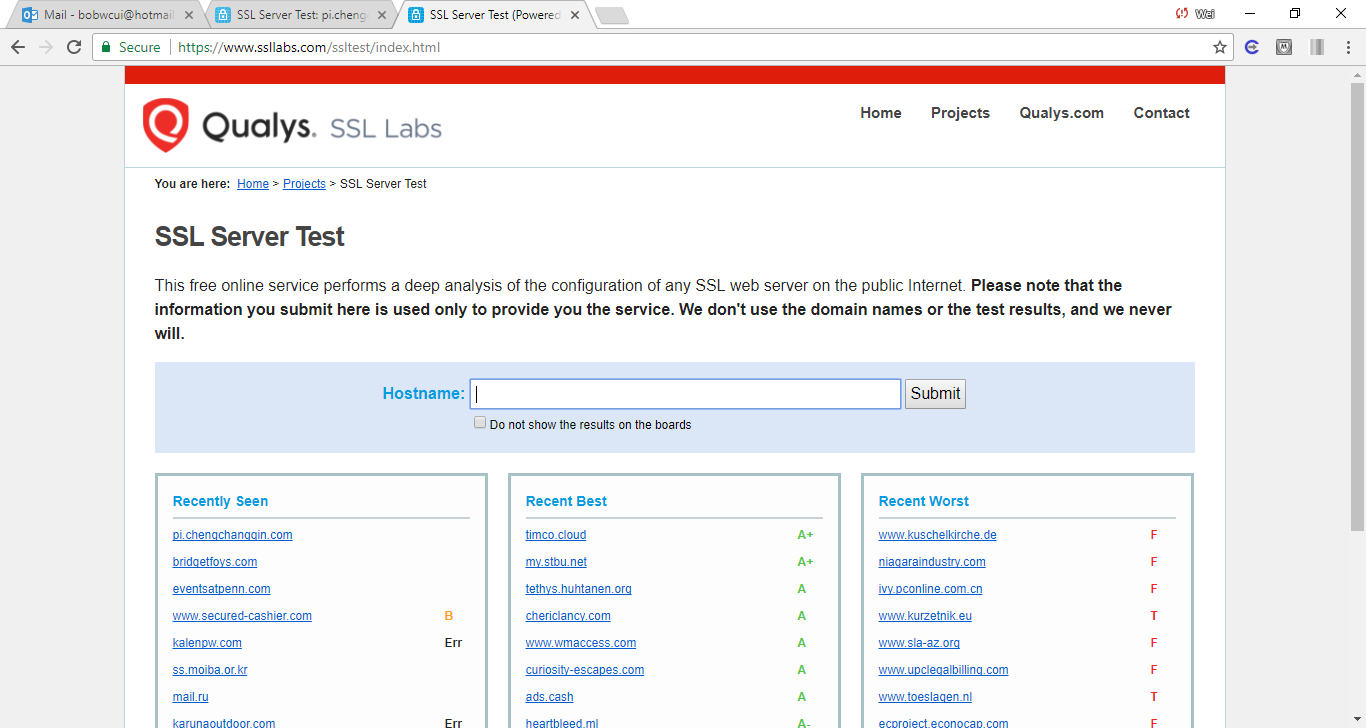


Fig. 1. Qualys SSL Labs official site: https://www.ssllabs.com/ssltest/index.html

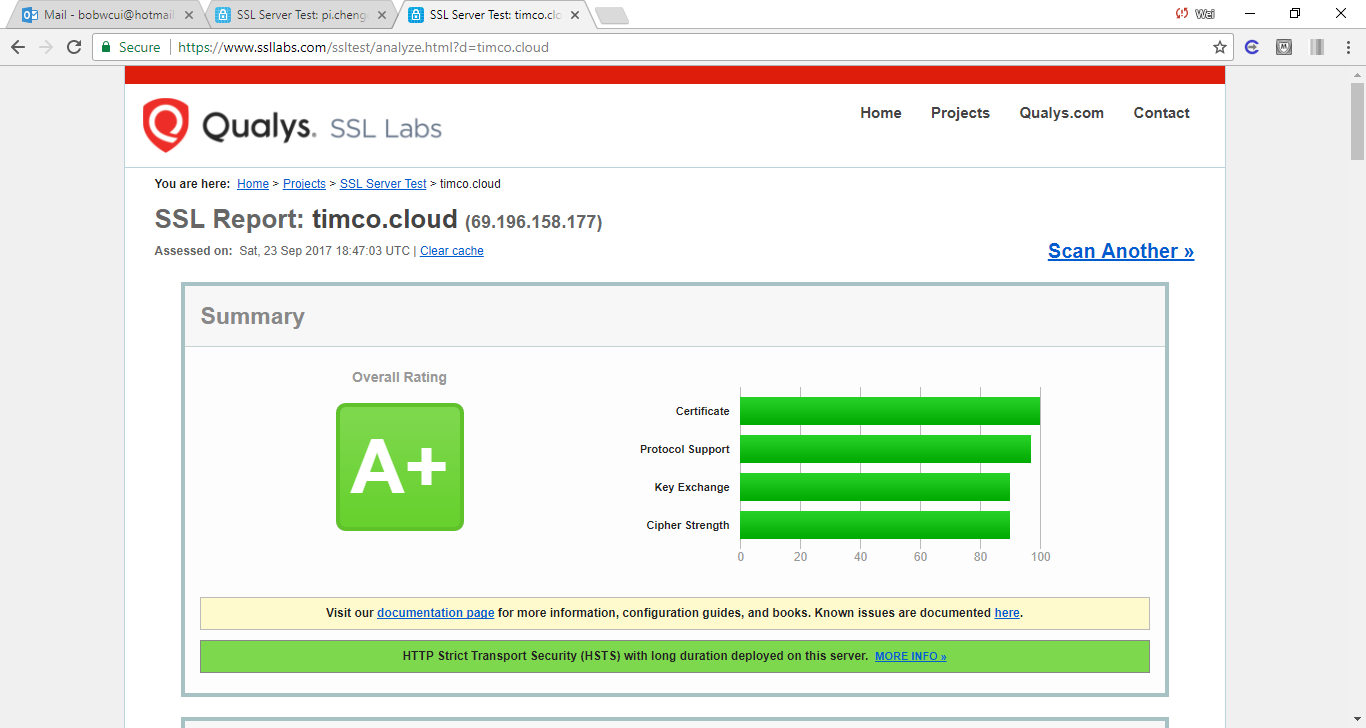


Fig. 2. One of the recent best rating hosts.



Fig. 3. One of the recent worst rating hosts.

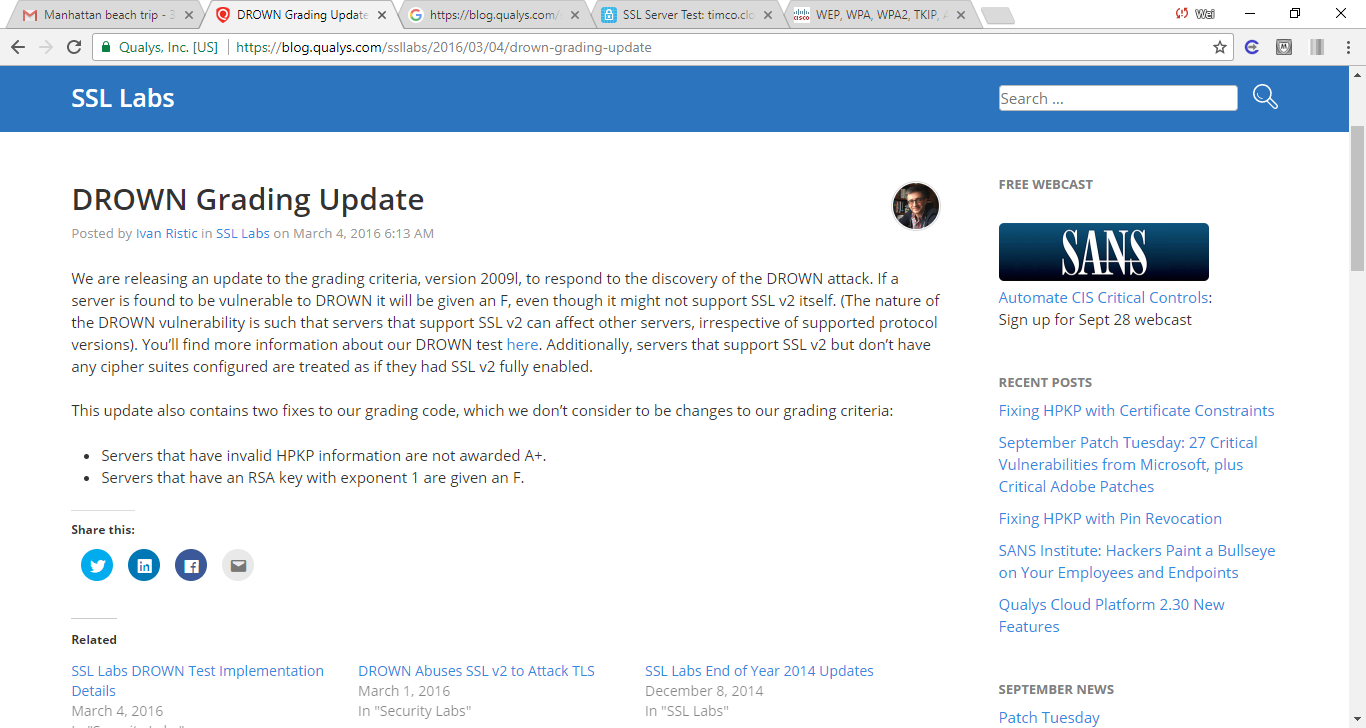


Fig. 4. Detailed rationale that the server found vulnerable to DRWON will receive an F.

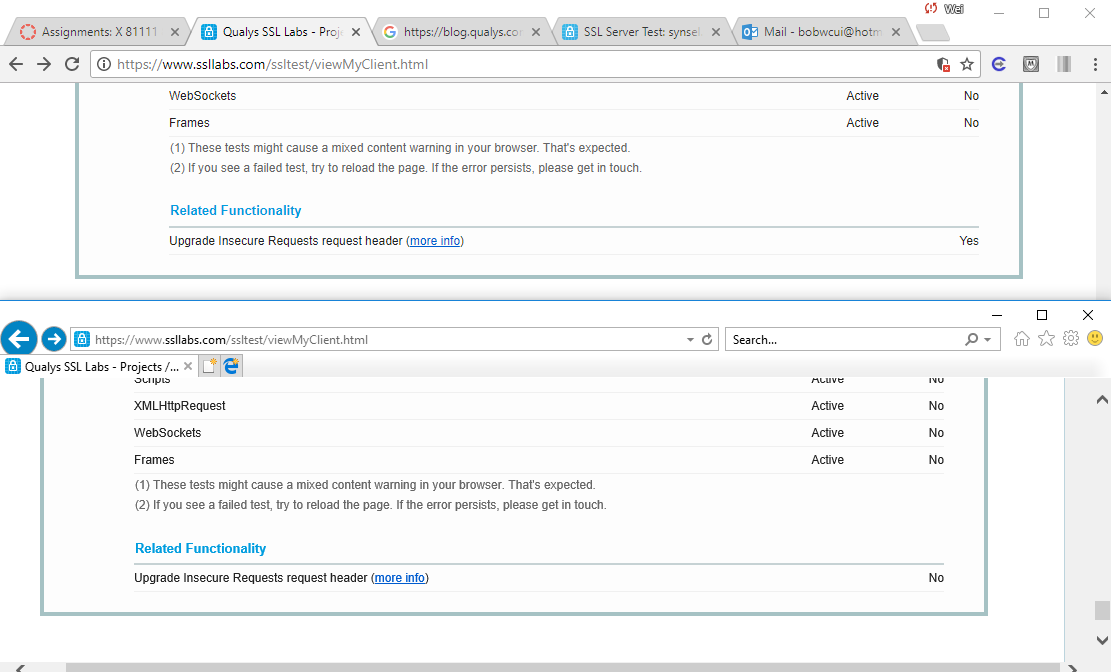


Fig. 5. SSL Client Test: (top) Chrome and (bottom) Internet Explorer 11