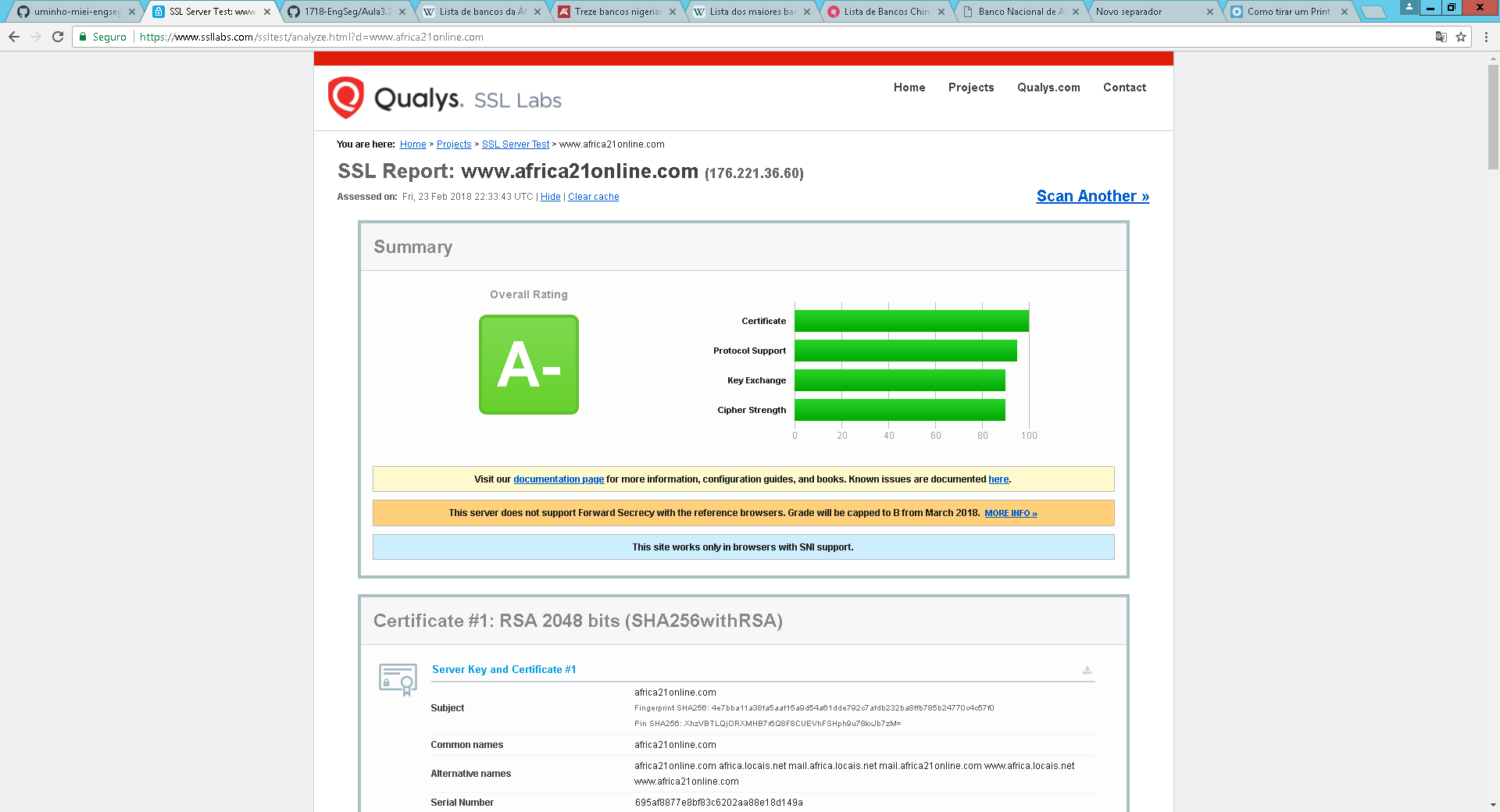
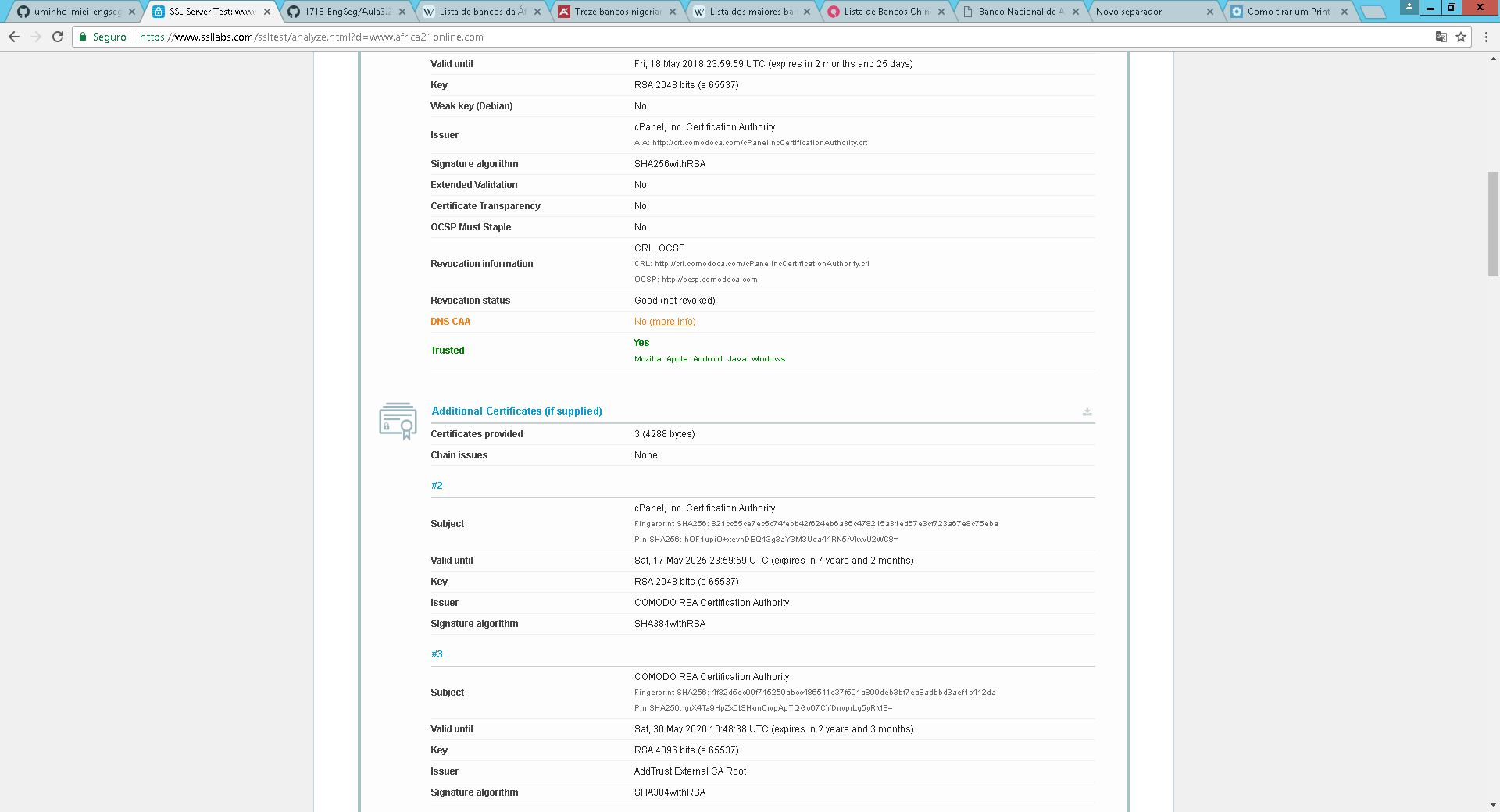
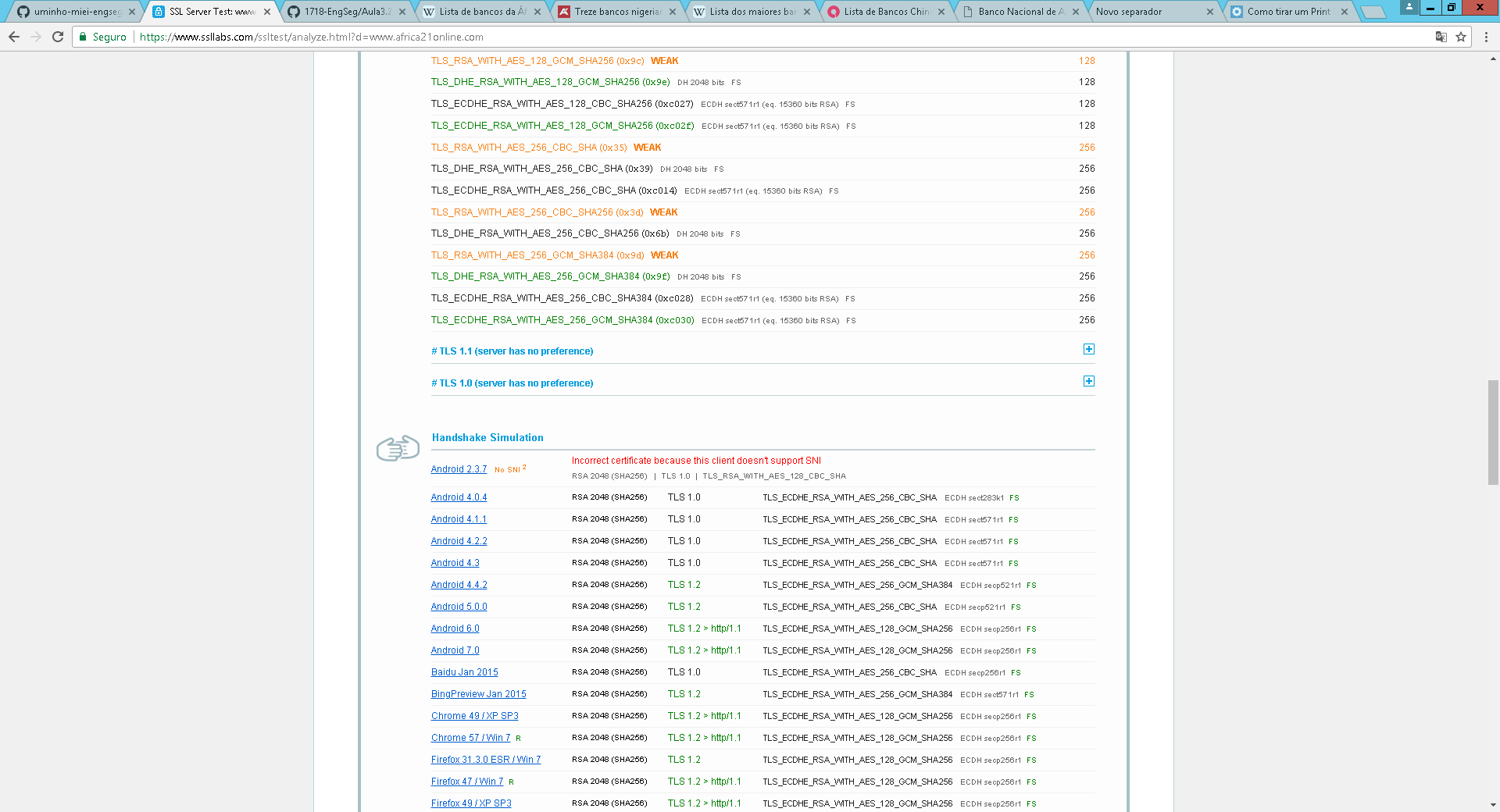
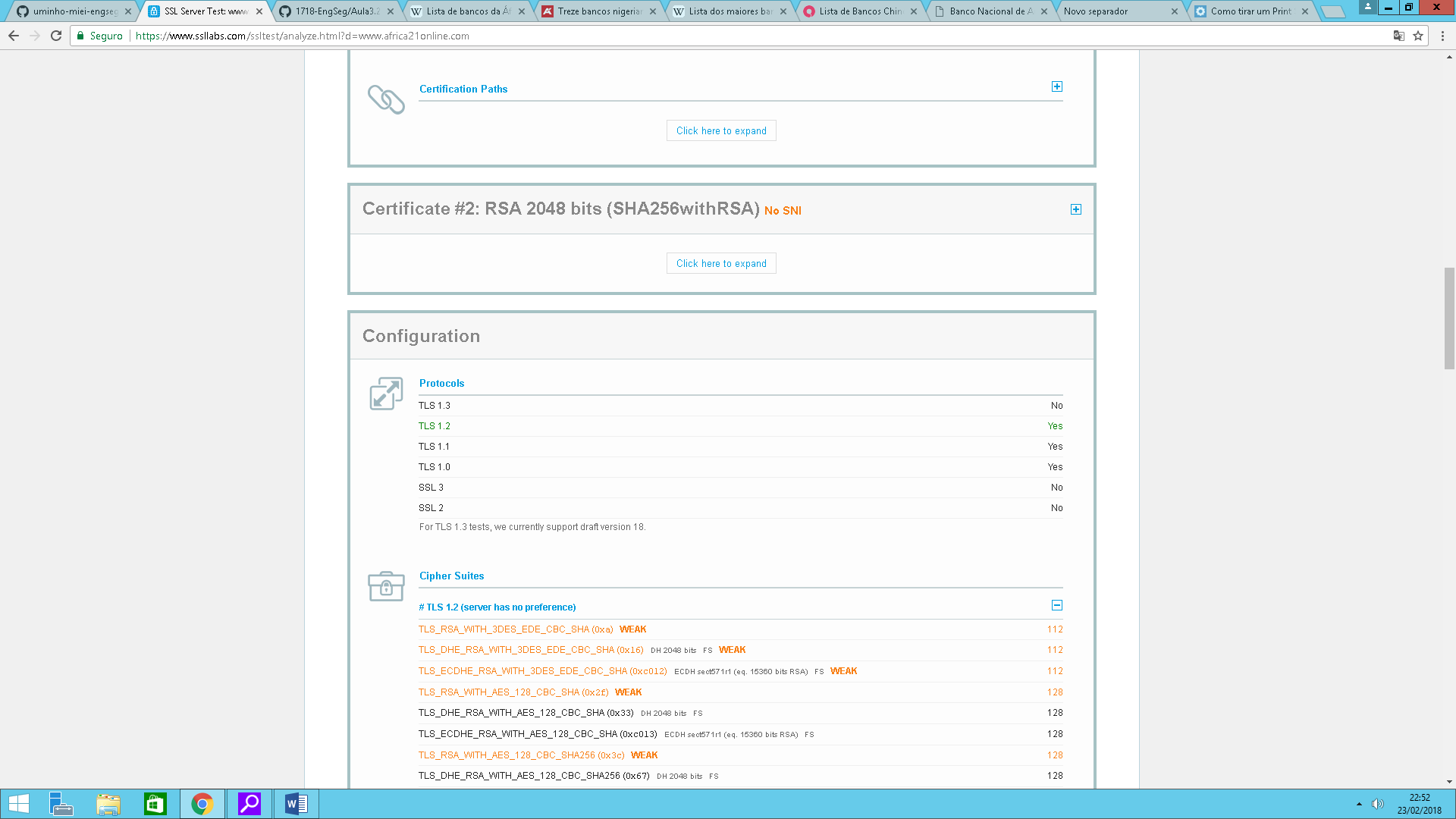
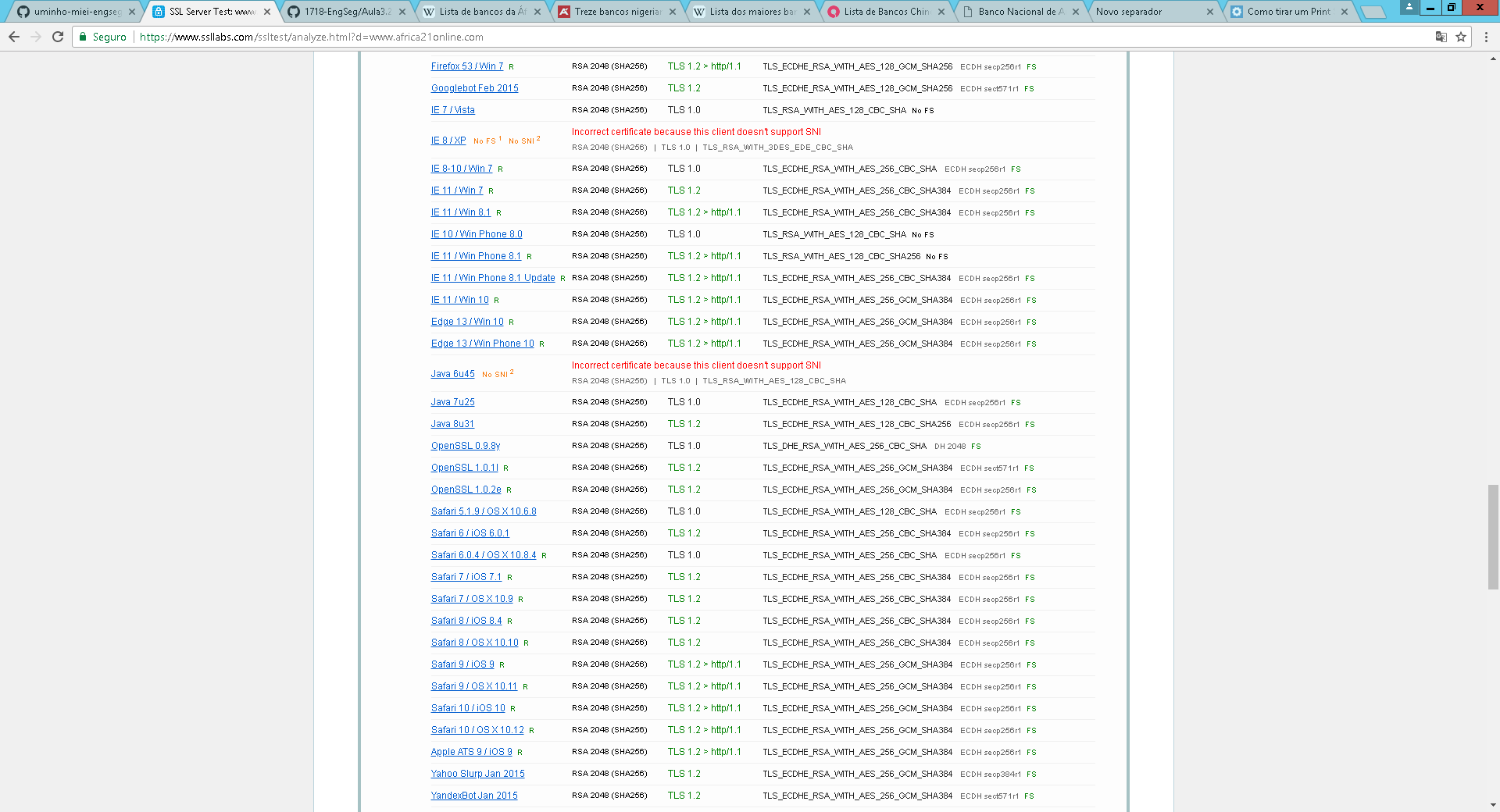
**BANCO DA REPÚBLICA NIGERIANA**

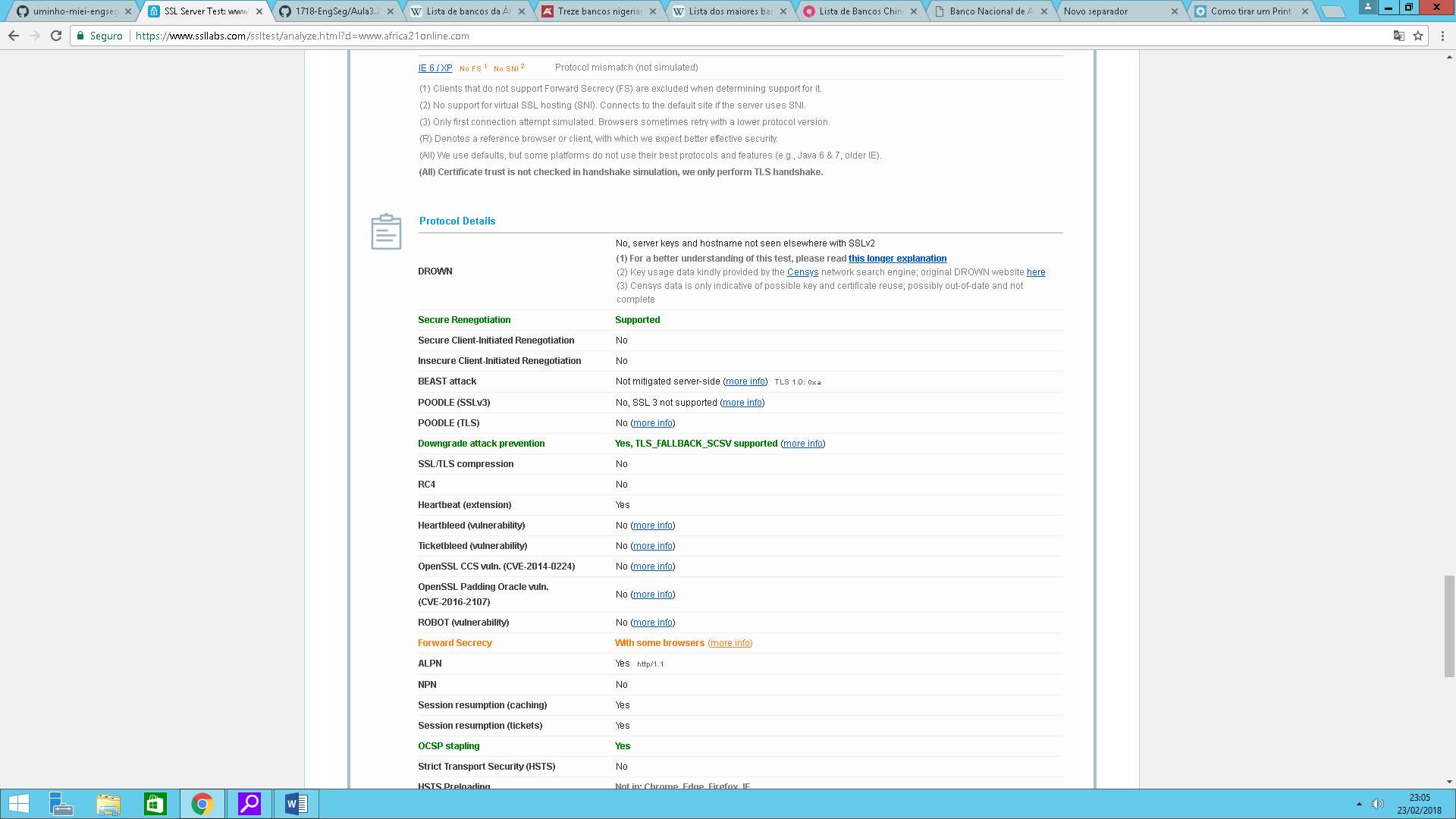


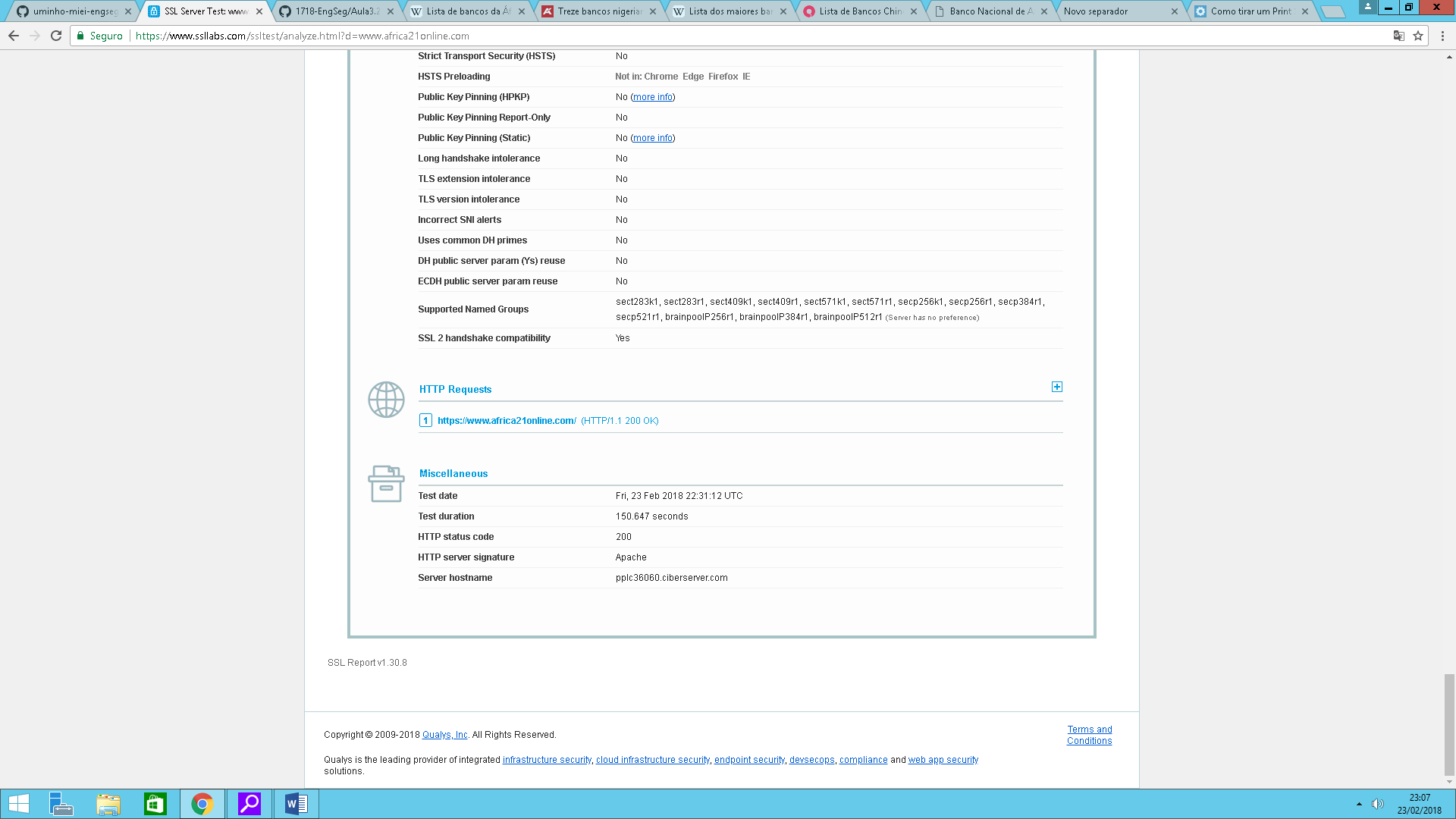




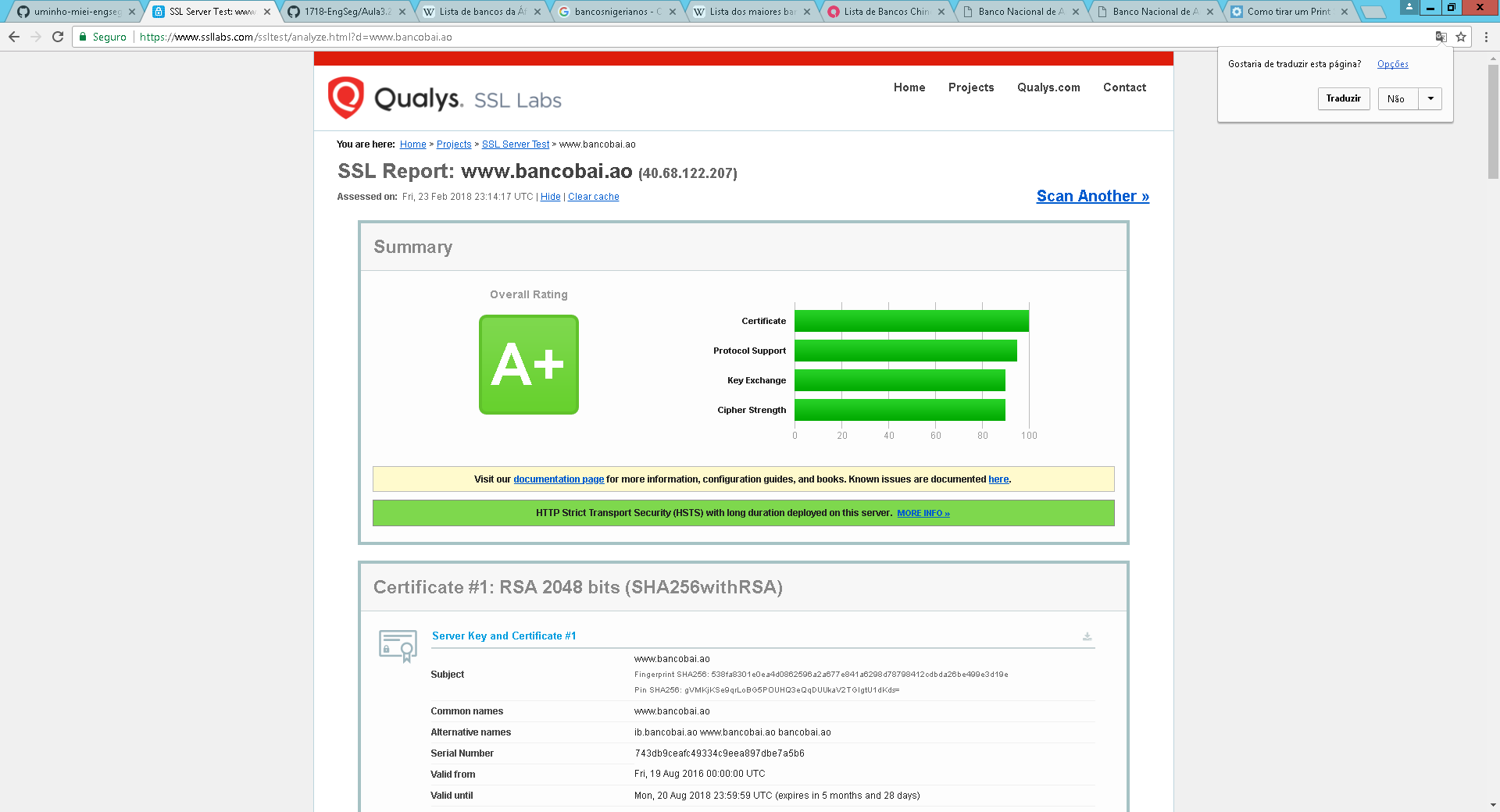


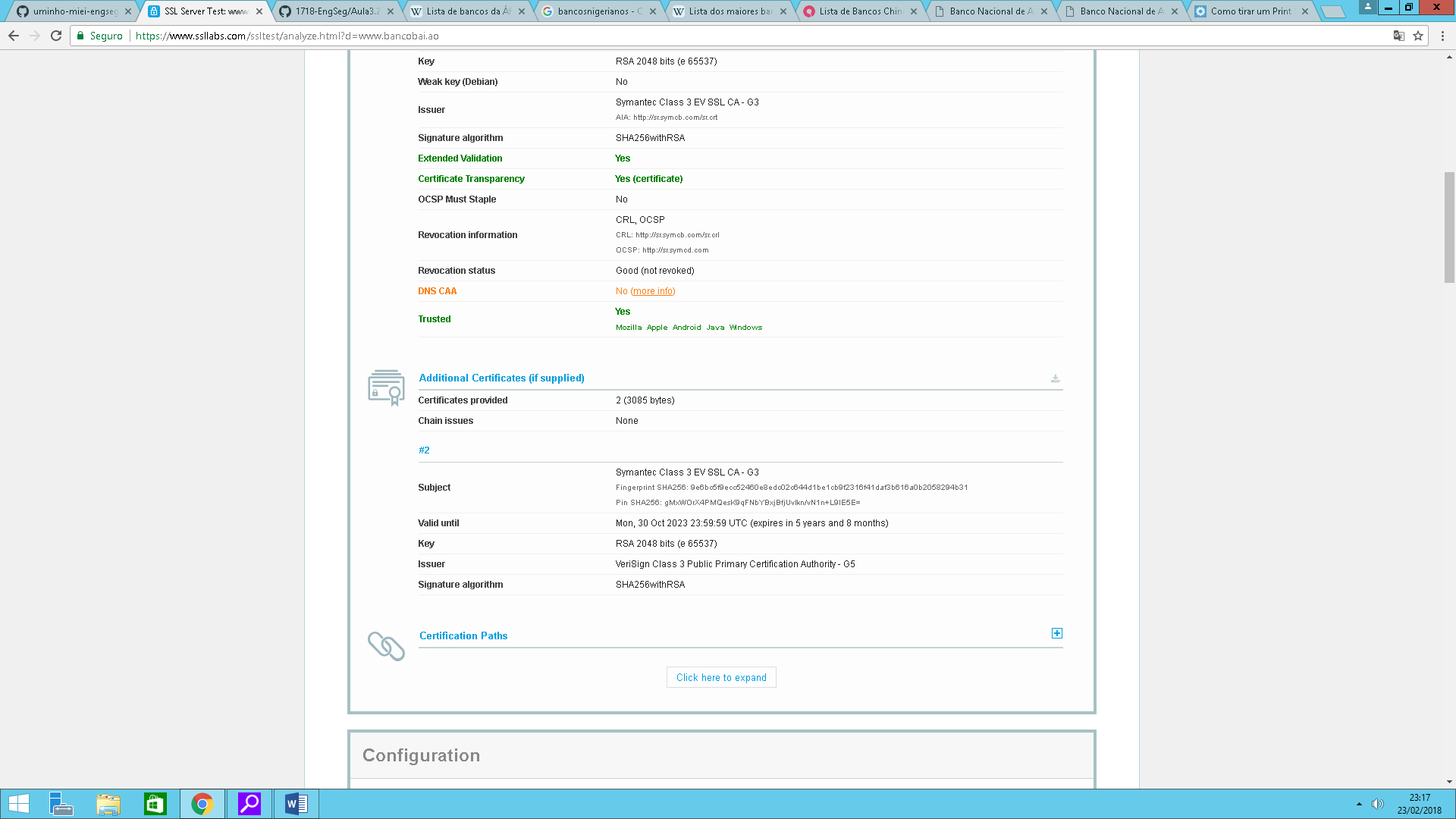


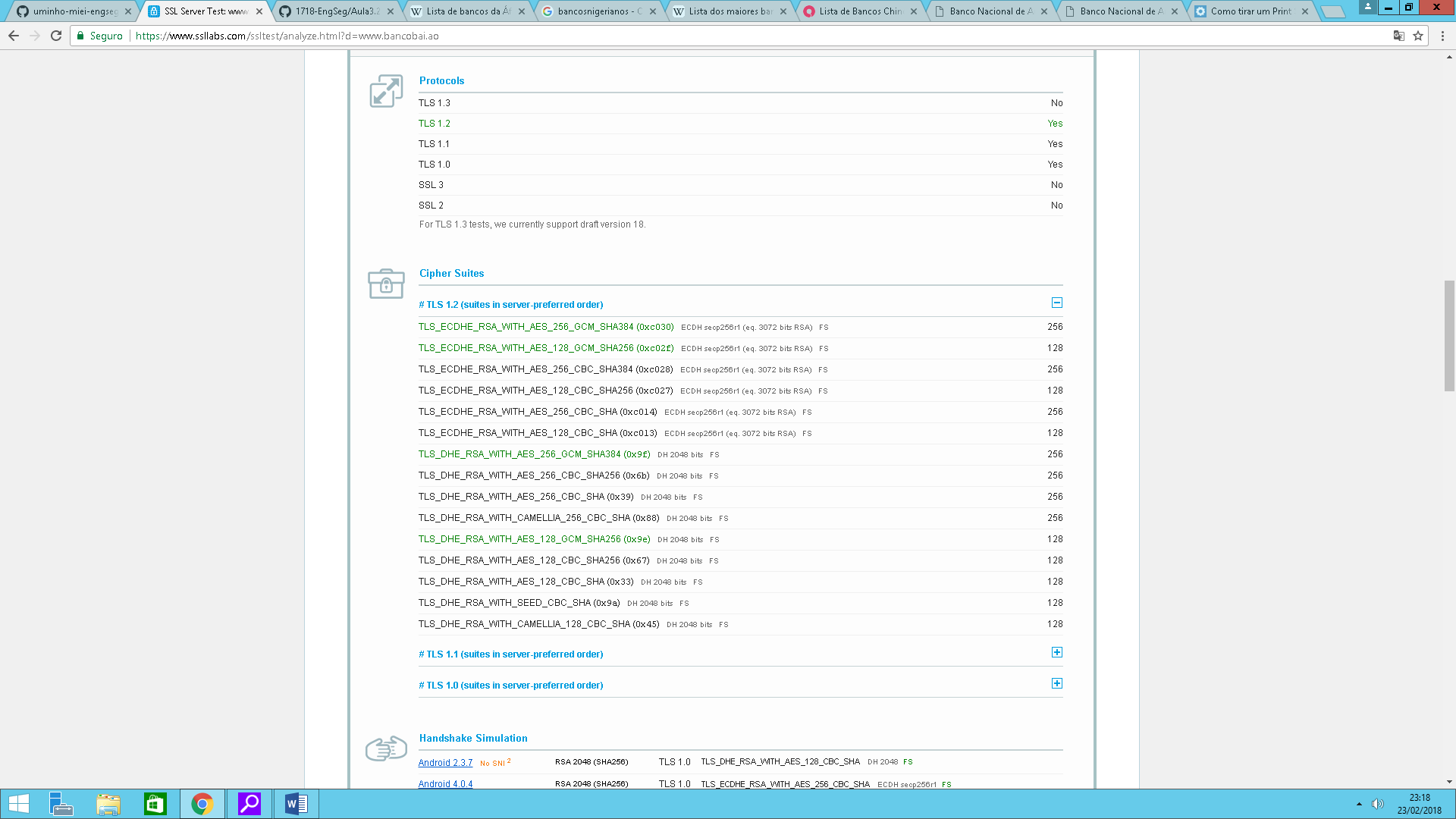


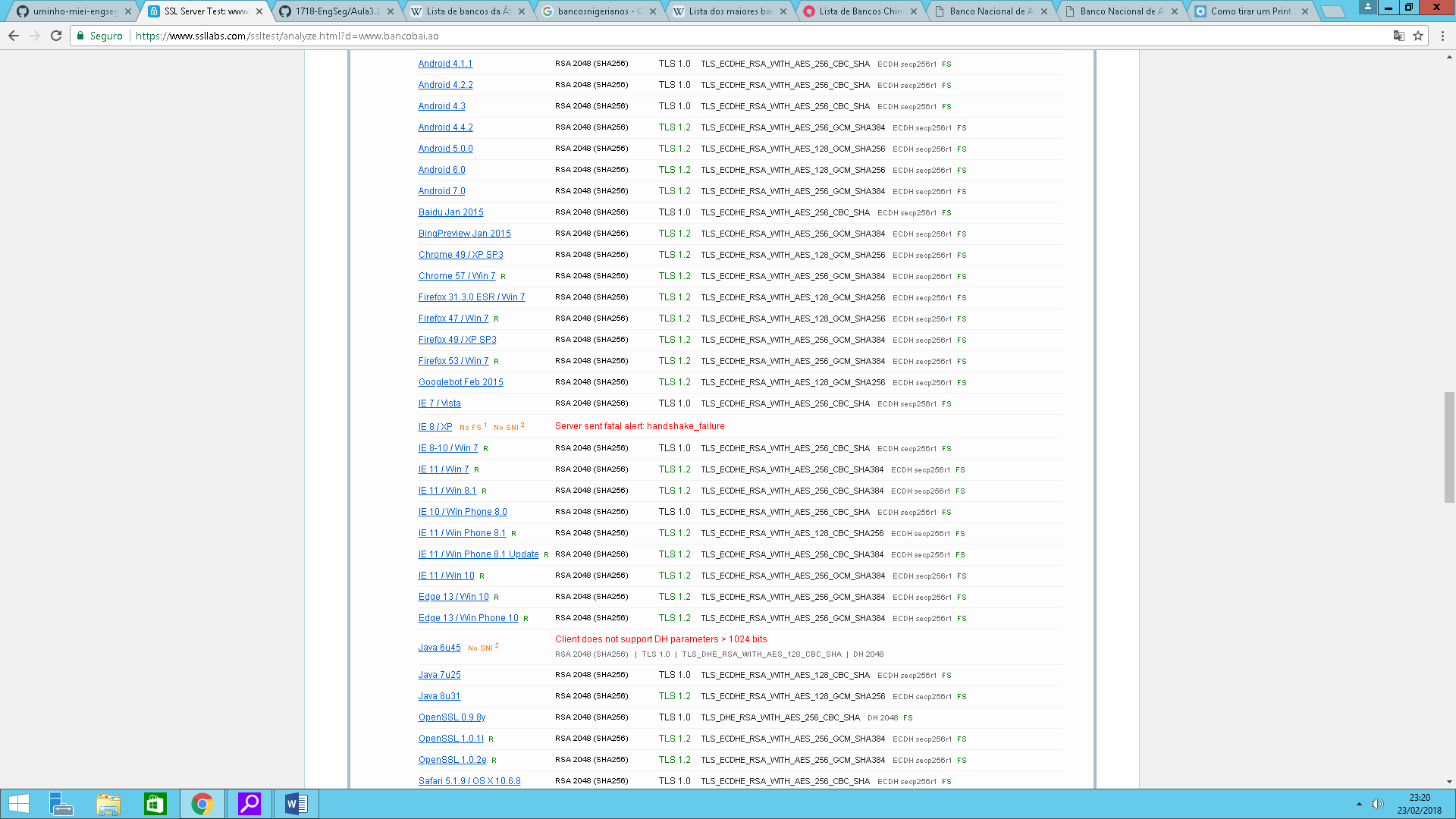


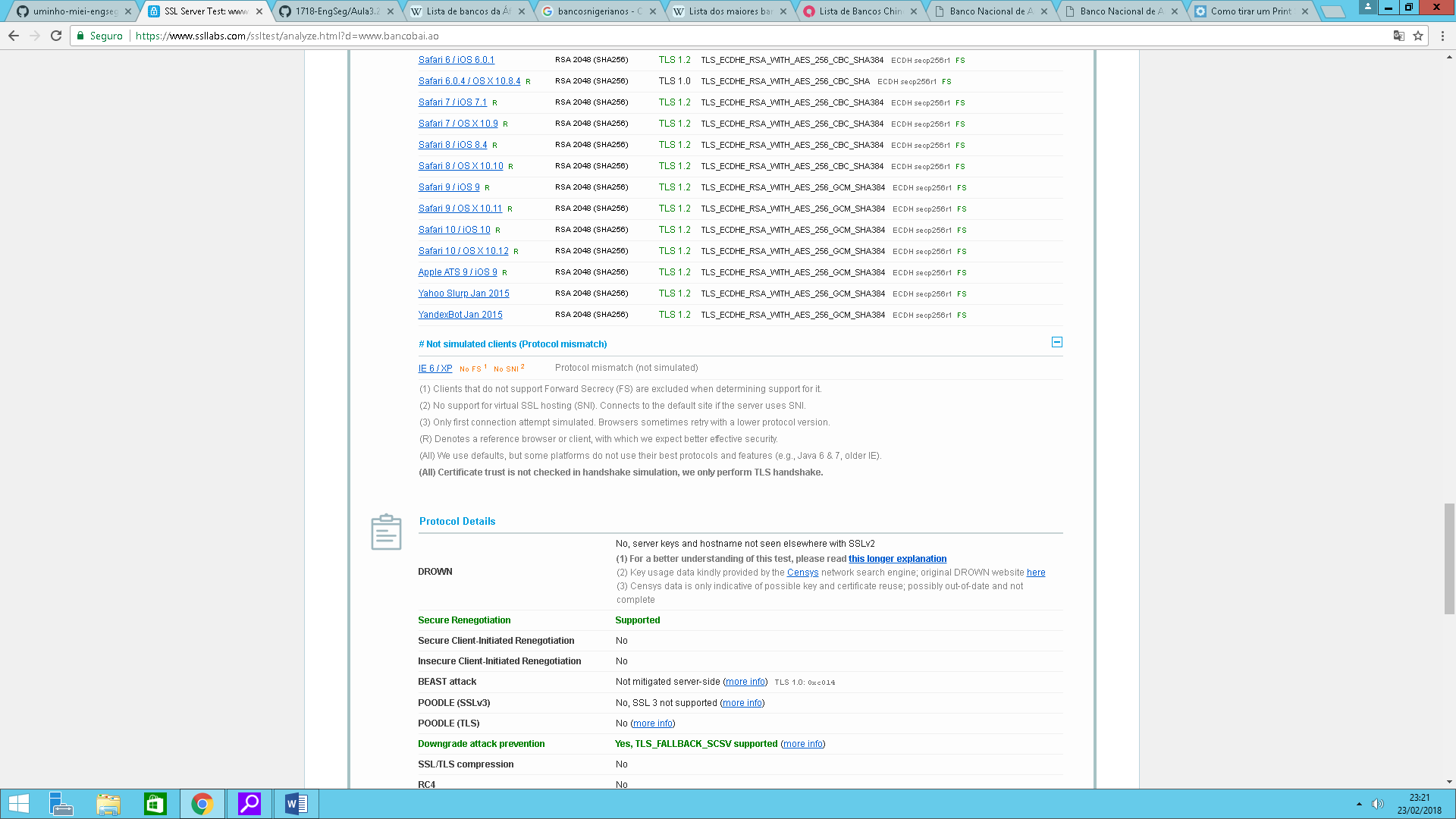
**BANCO AFRICANO DE INVESTIMENTO (BAI)**

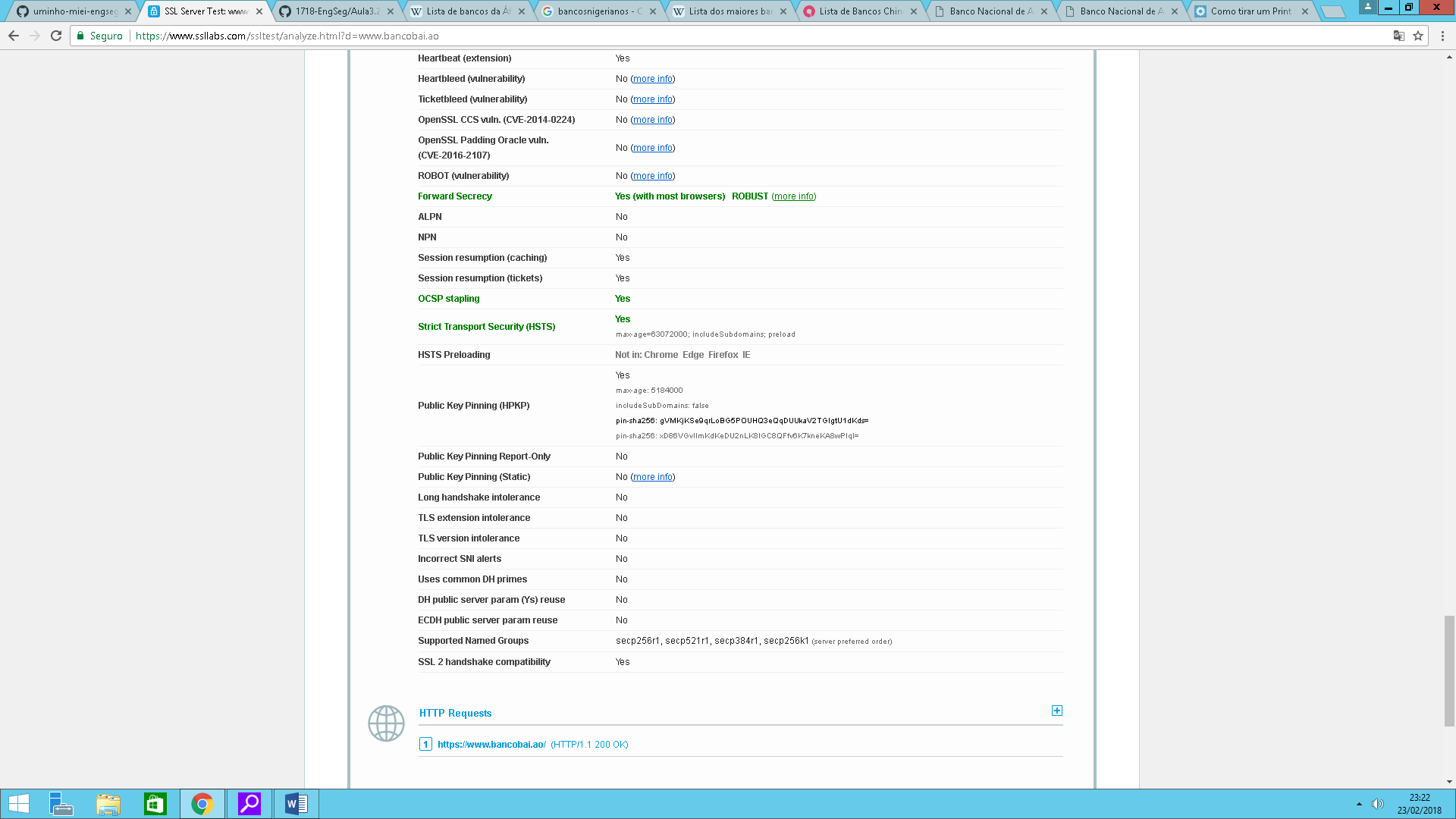


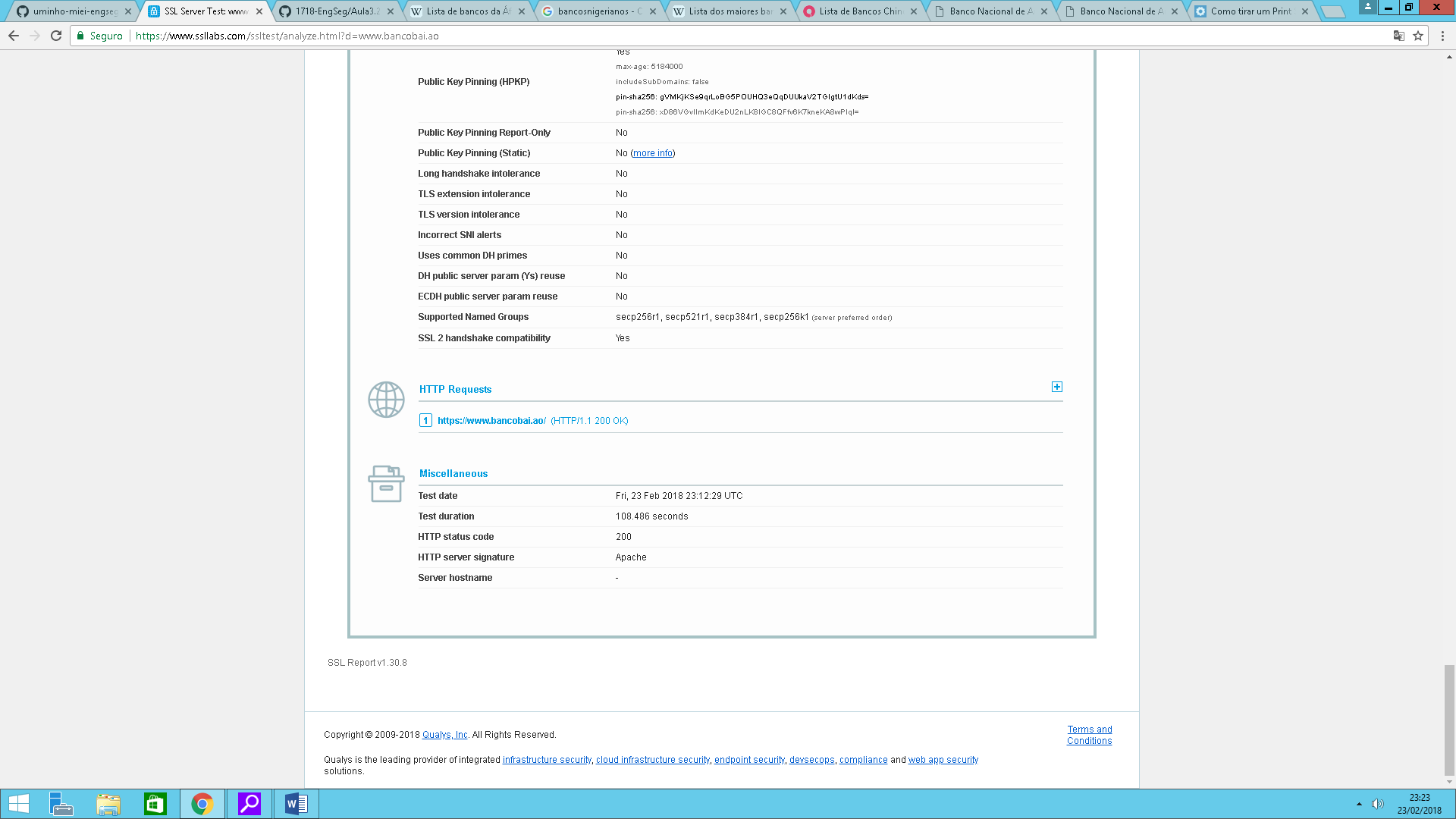




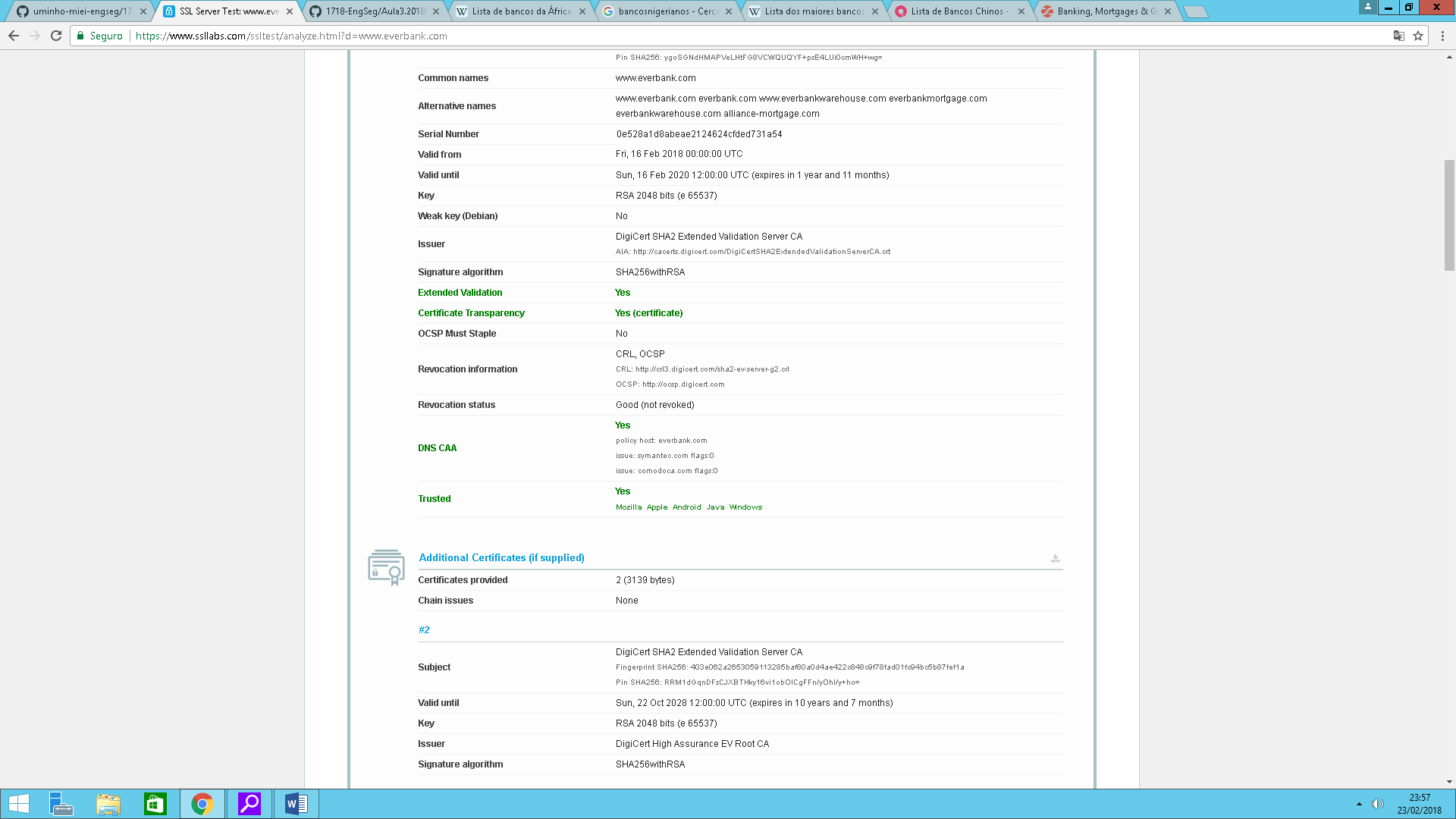
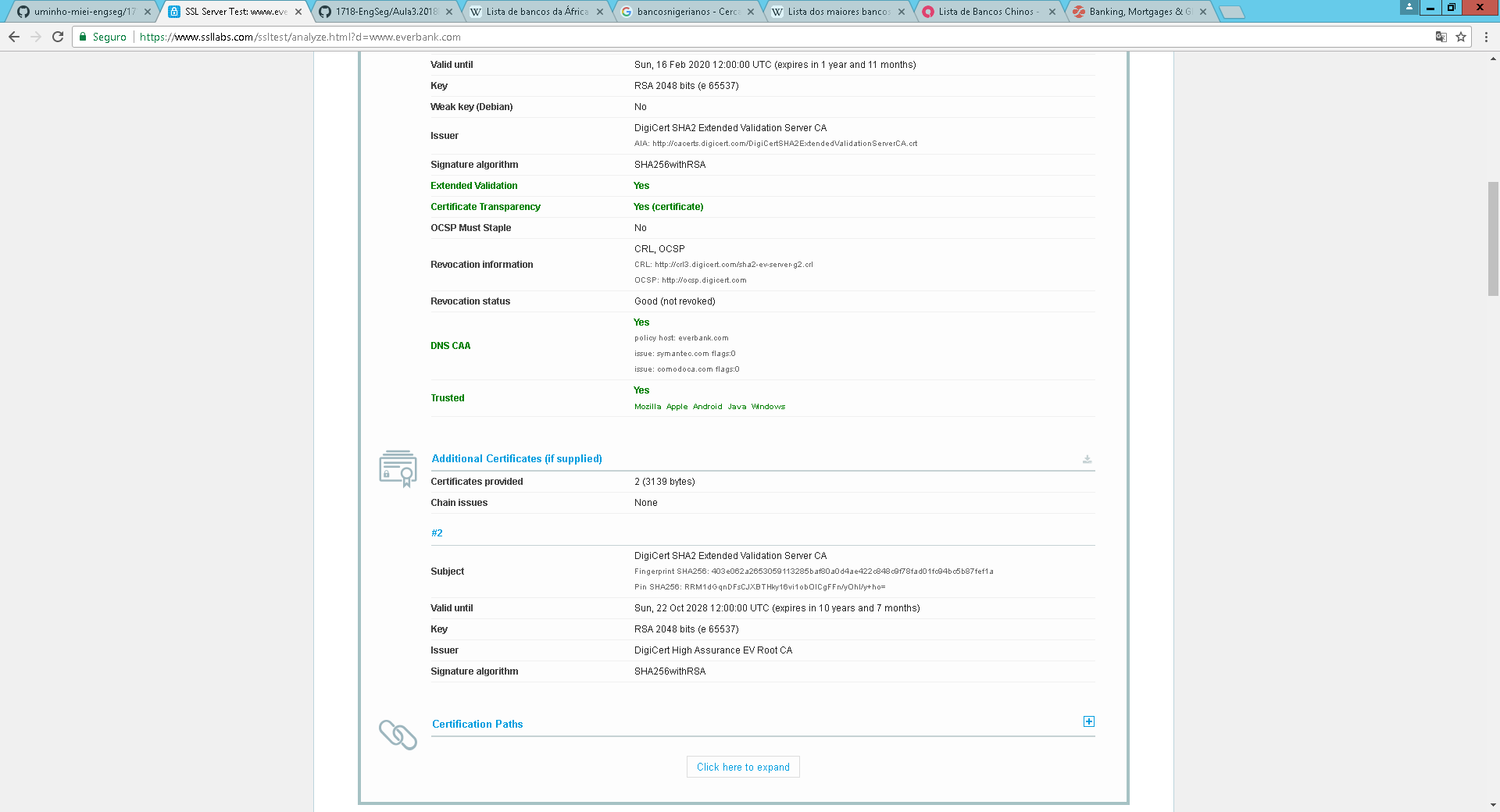


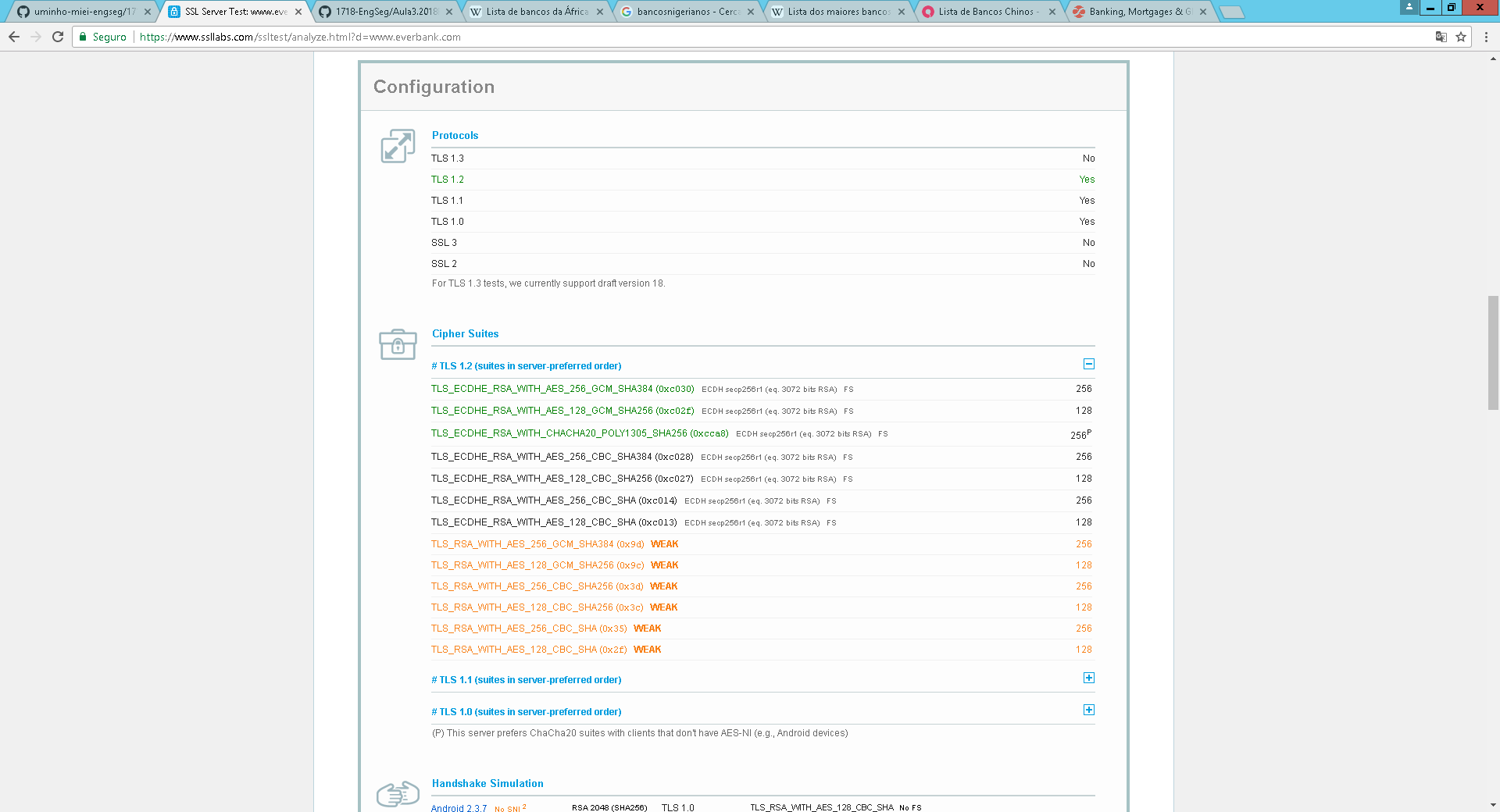


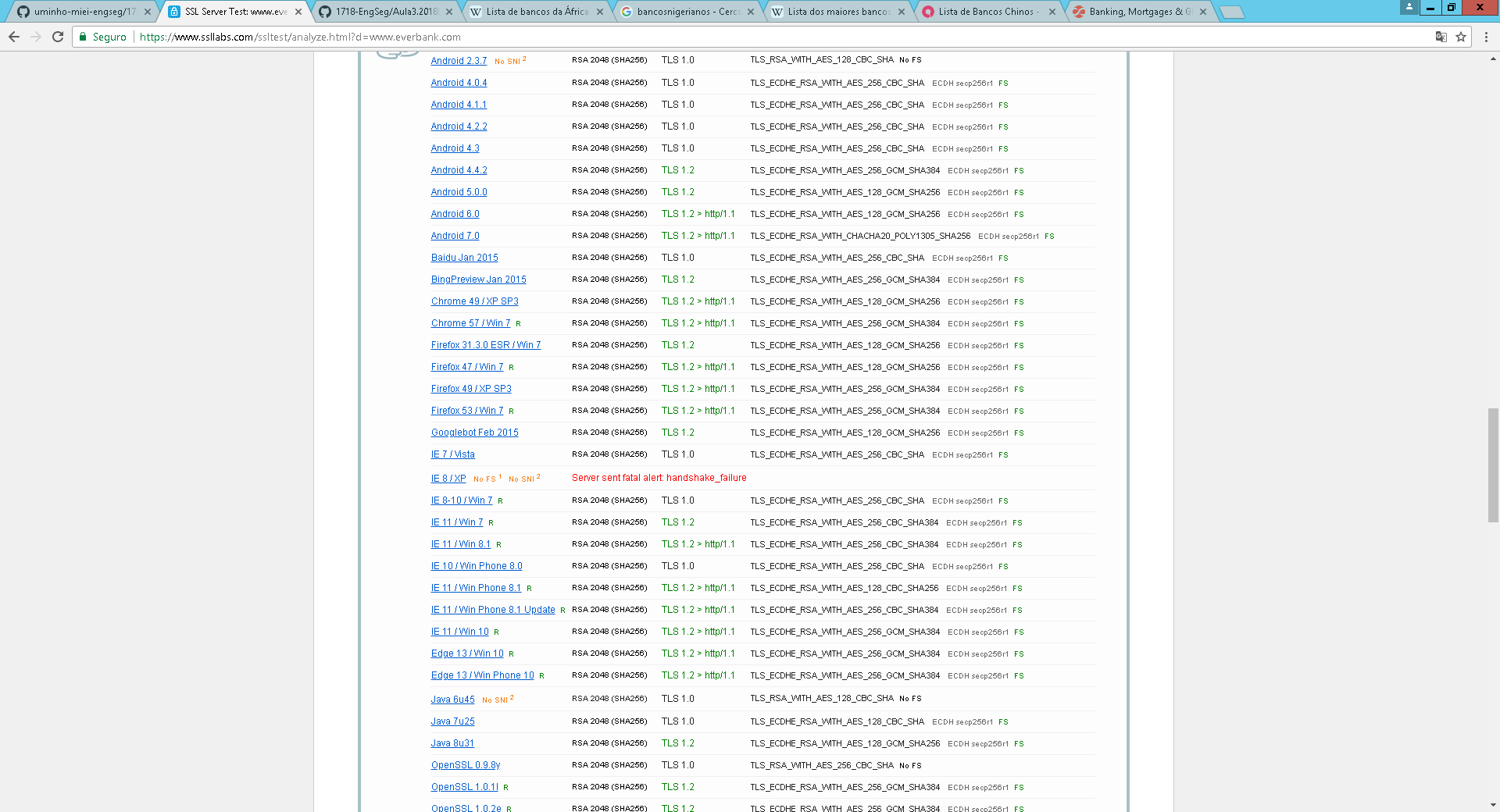


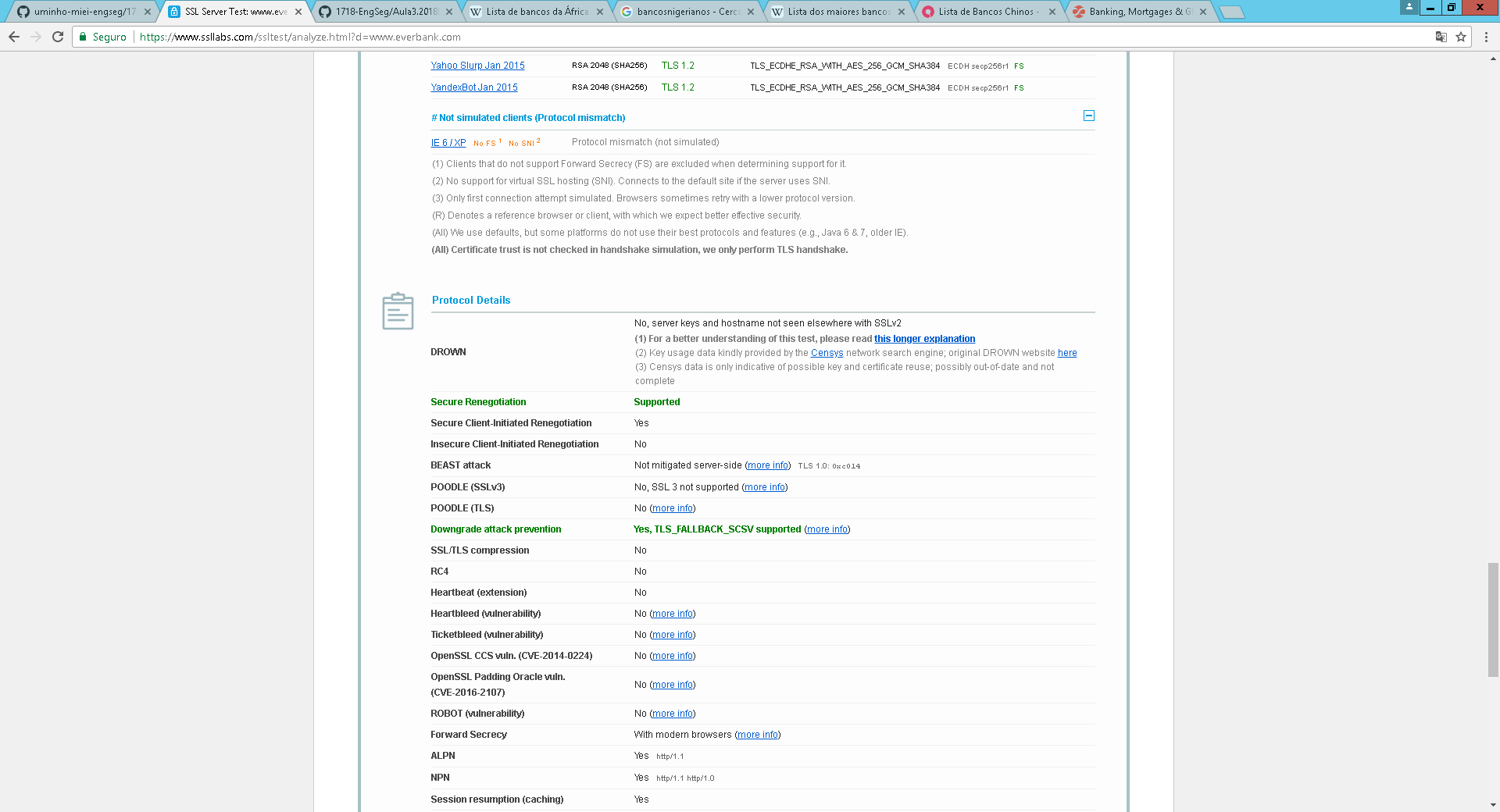


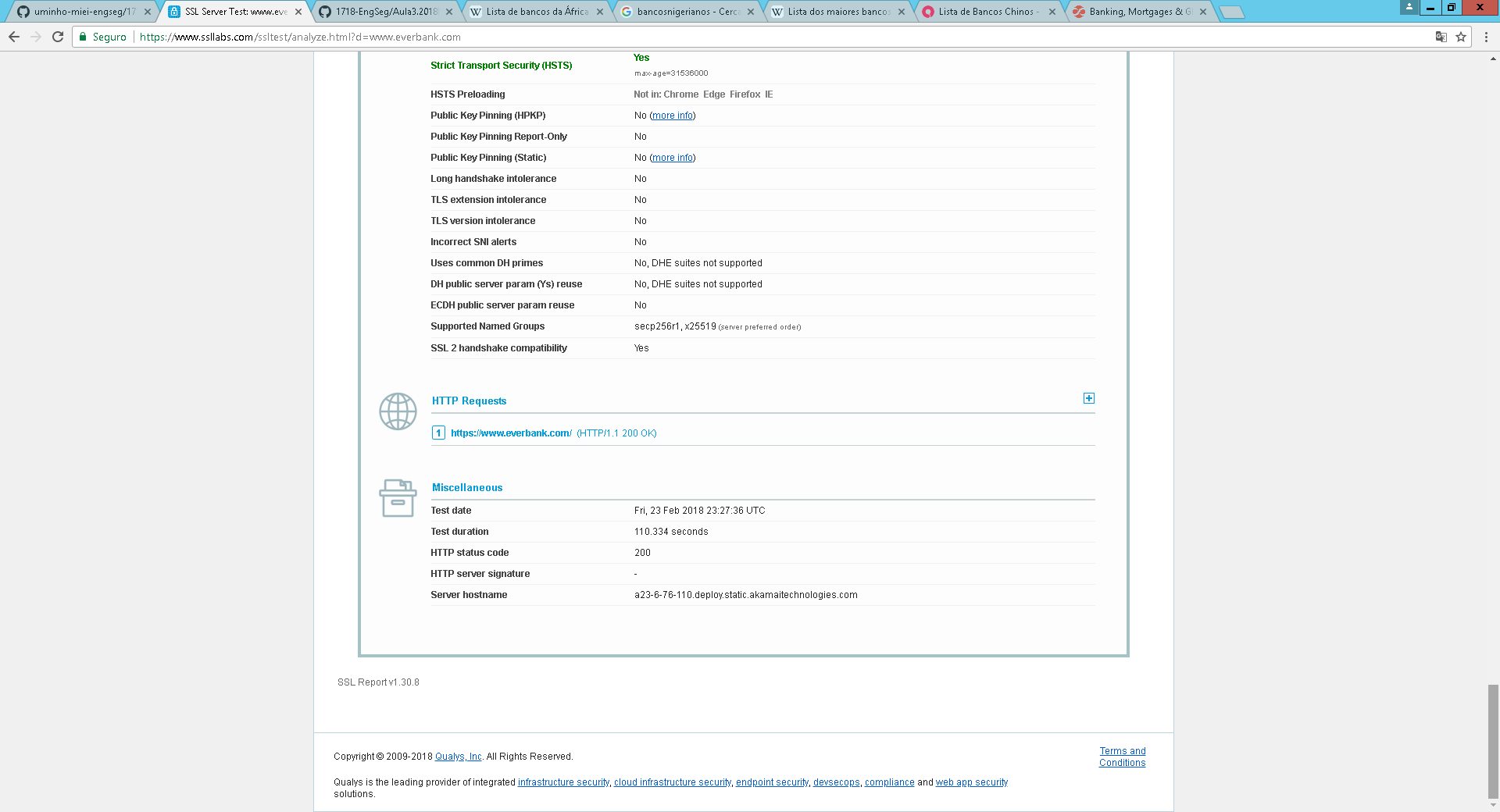
**BANCO DOS ESTADOS UNIDOS DA AMÉRICA**



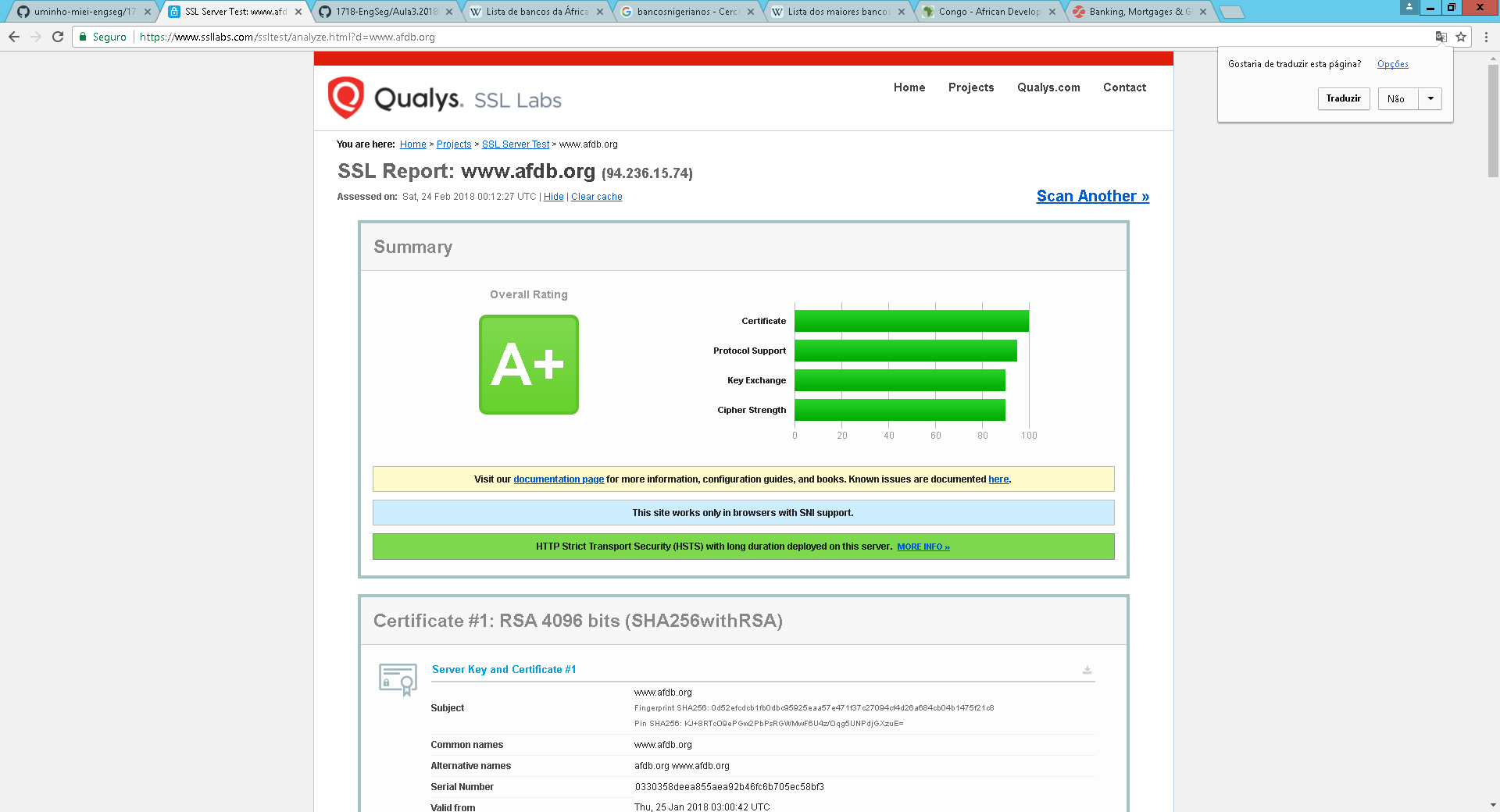


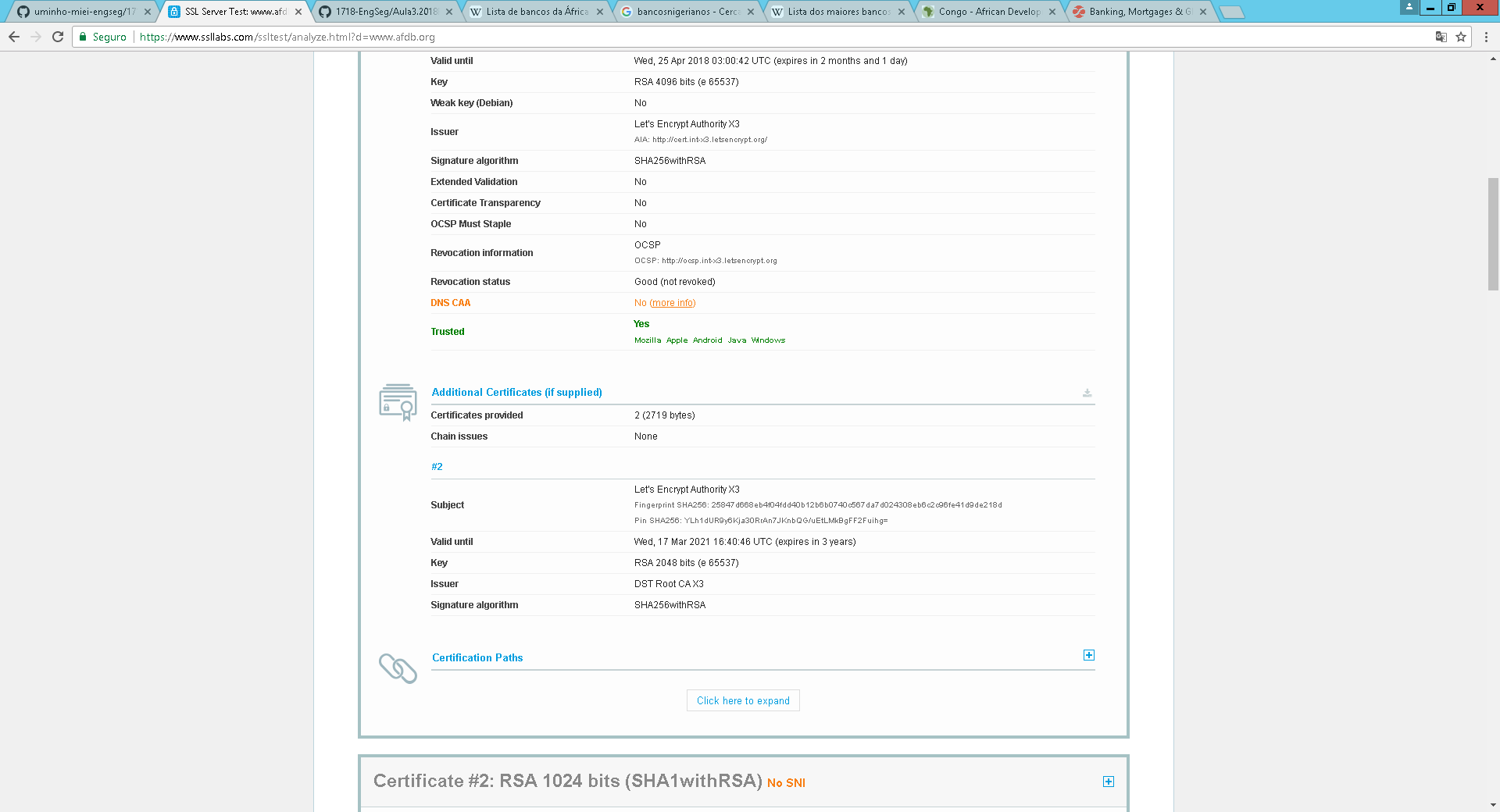


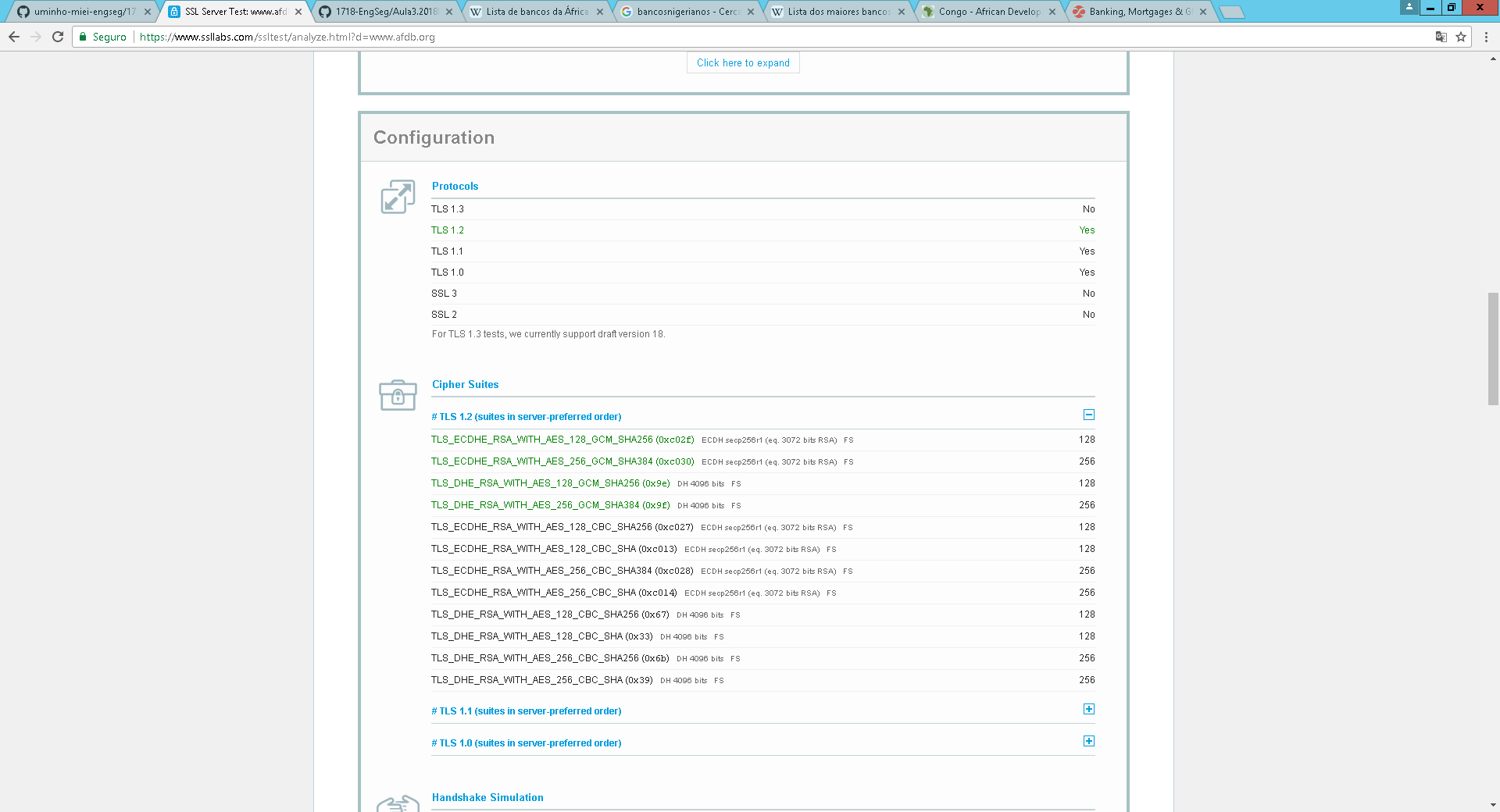


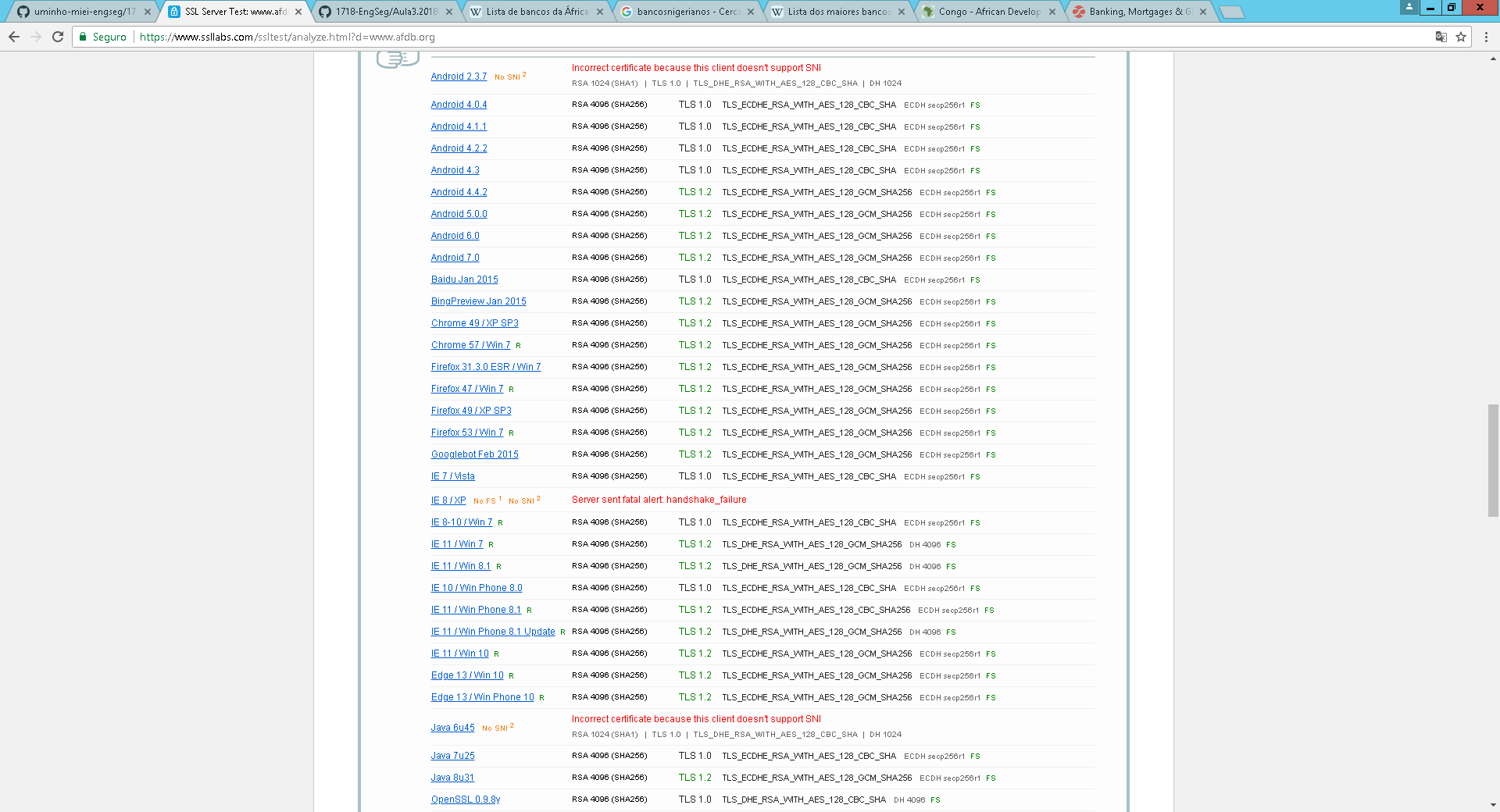


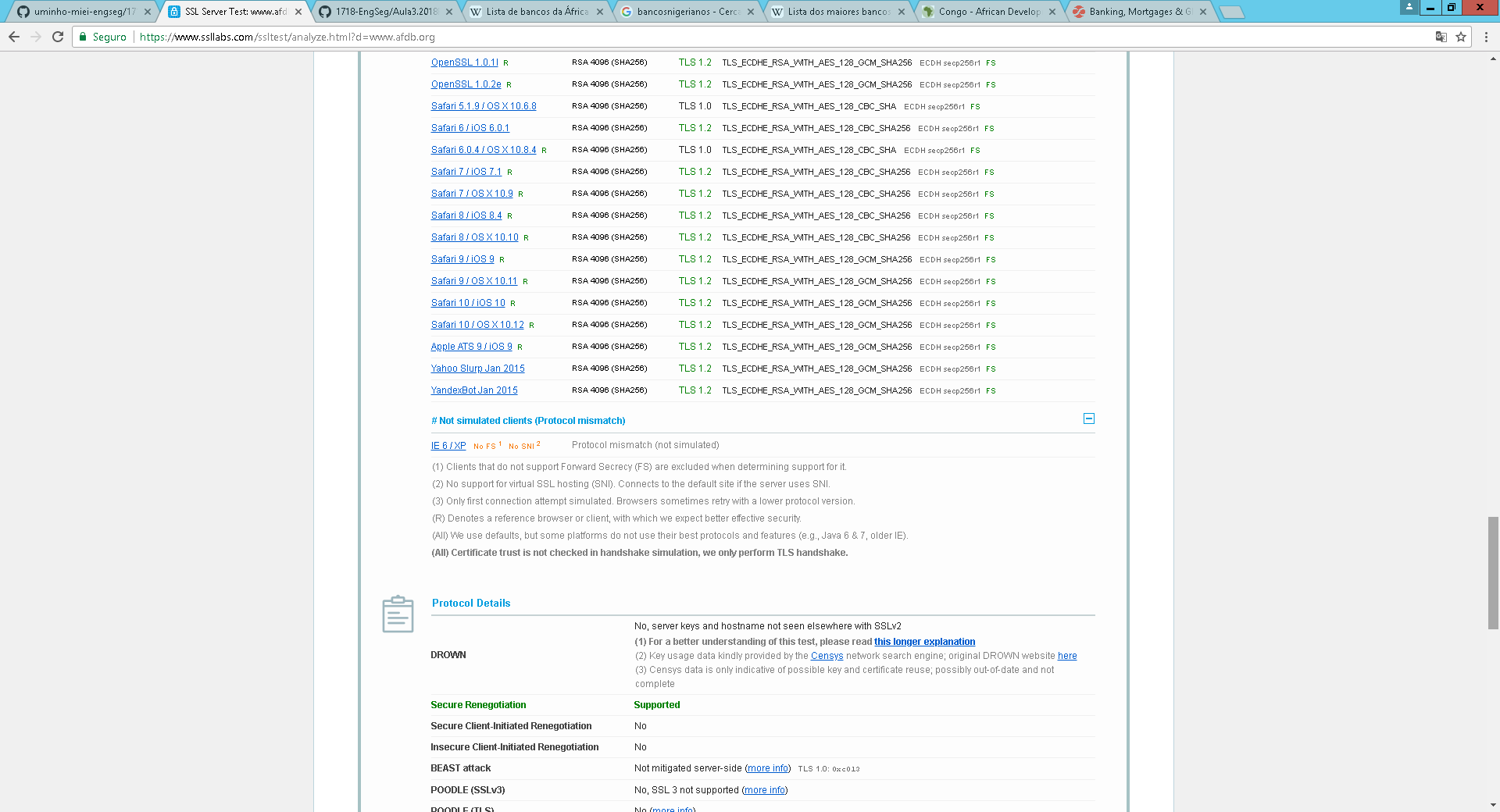
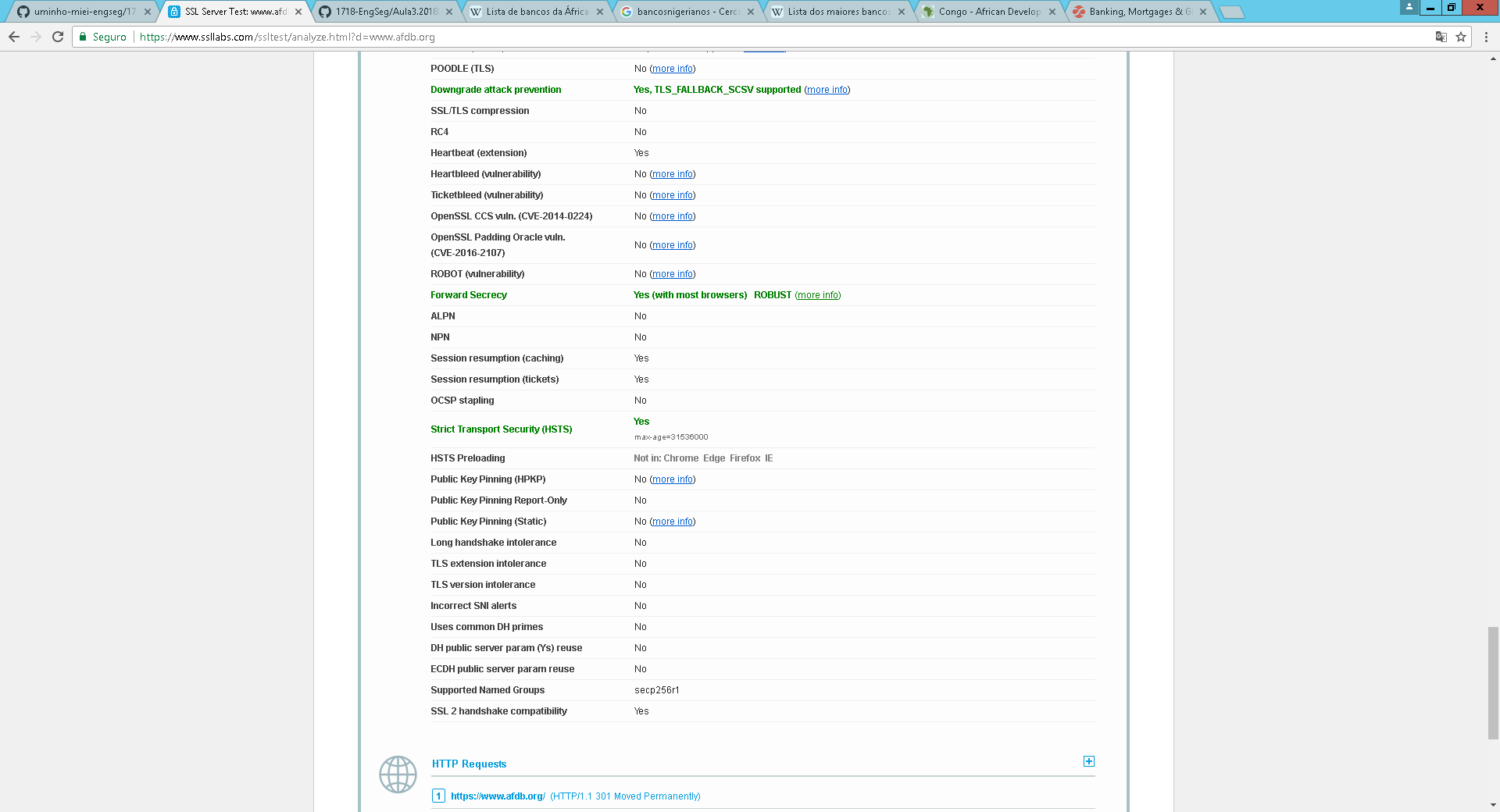
**BANCO DA REPUBLICA DEMOCRÁTICA DO CONGO**

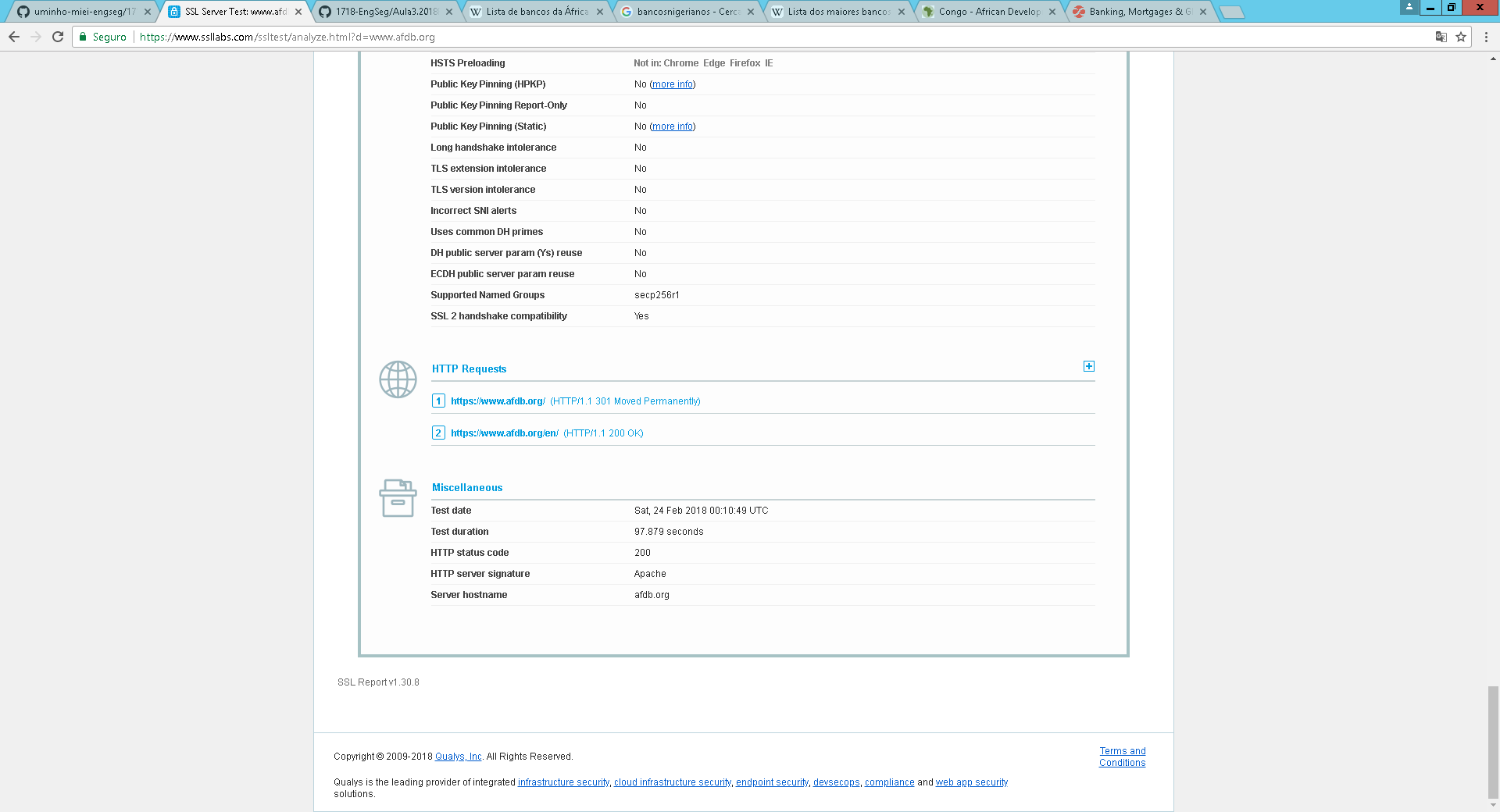












**ii) Comentários**

**- Comentário do Banco Nigeriano:**  
(1) Os clientes que não suportam Privilégio Avançado (FS) são excluídos ao determinar o suporte para isso.

(2) Nenhum suporte para hospedagem SSL virtual (SNI). Conecta-se ao site padrão se o servidor usar o SNI.

(3) Apenas a primeira tentativa de conexão foi simulada. Os navegadores, por vezes, tentam novamente com uma versão de protocolo mais baixa.

O certificado é seguro, pois usa RSA, com a chave de tamanho 2048 bits (e 65537), algoritmo da assinatura é SHA384withRSA e a validade de utilização do certificado vai até at, 17 May 2025 23:59:59 UTC (expires in 7 years and 2 months). Pois esses pâmetros estão conforme as recomendações da NIST 2016.

**- Comentários do Banco Africano de Investimento-BAI:**

(1) Os clientes que não suportam Privilégio Avançado (FS) são excluídos ao determinar o suporte para isso.

(2) Nenhum suporte para hospedagem SSL virtual (SNI). Conecta-se ao site padrão se o servidor usar o SNI.

(3) Apenas a primeira tentativa de conexão foi simulada. Os navegadores, por vezes, tentam novamente com uma versão de protocolo mais baixa.

O certificado é seguro, pois usa RSA com a chave de tamanho 2048 bits (e 65537), algoritmo da assinatura é SHA256withRSA e a validade de utilização do certificado vai até Wed, 23 Oct 2024 07:33:22 UTC (expires in 6 years and 7 months). Pois esses parâmetros estão conforme as recomendações da NIST 2016.

**- Comentários do Certificado do Banco dos USA:**

1) Os clientes que não suportam Privilégio Avançado (FS) são excluídos ao determinar o suporte para isso.

(2) Nenhum suporte para hospedagem SSL virtual (SNI). Conecta-se ao site padrão se o servidor usar o SNI.

(3) Apenas a primeira tentativa de conexão foi simulada. Os navegadores, por vezes, tentam novamente com uma versão de protocolo mais baixa.

O certificado é seguro, pois usa o RSA com chaves de tamanho 4096 bits (e 65537), algoritmo da assinatura é SHA256withRSA e a validade de utilização do certificado é até Wed, 17 Mar 2021 16:40:46 UTC (expires in 3 years). Pois esses parâmetros estão conforme as recomendações da NIST 2016.

**- Comentários do Certificado do Banco Congolês: African Developmrnt Bank Group:**

(1) Os clientes que não suportam Privilégio Avançado (FS) são excluídos ao determinar o suporte para isso.

(2) Nenhum suporte para hospedagem SSL virtual (SNI). Conecta-se ao site padrão se o servidor usar o SNI.

(3) Apenas a primeira tentativa de conexão foi simulada. Os navegadores, por vezes, tentam novamente com uma versão de protocolo mais baixa.

O certificado é seguro, pois usa o RSA com chaves de tamanho 4096 bits (e 65537), algoritmo da assinatura é SHA256withRSA e a validade de utilização do certificado é até Wed, 17 Mar 2021 16:40:46 UTC (expires in 3 years). Pois esses parâmetros estão conforme as recomendações da NIST 2016.

**iii)** É natural, pois a Ticketbleed é uma vulnerabilidade divulgada recentemente em alguns balanceadores de carga F5.

Esses problemas permitem que os invasores recuperem até 31 bytes de memória de processo, isto significa que, que ao sofrermos um ataque por meio desta vulnerabilidade, poderia incluir dados confidenciais (por exemplo, chaves privadas). É de natureza semelhante ao Heartbleed (uma vulnerabilidade no OpenSSL a partir de 2014), mas menos grave porque muito menos dados podem ser extraídos. Por isso deve-se adoptar mecanismos de defesa que permitam evitar ataques provocados por esrta vulnerabilidades.

Portanto, (R) Indica um navegador de referência ou cliente, com o qual esperamos uma segurança efetiva melhor. (Todos) Utilizamos padrões, mas algumas plataformas não usam seus melhores protocolos e recursos (por exemplo, Java 6 e 7, IE mais antigo). (Todos) A confiança do certificado não é verificada na simulação de handshake, nós só executamos handshake TLS.