

Cấu hình Nginx ?? Qualys SSL Labs xếp hạng A

admin Sun, Apr 14, 2019 [Chứng Chỉ Số SSL Certificates](#) 0 1943



Lưu ý: Các tiêu chuẩn đánh giá của Qualys SSL Labs thay đổi theo thời gian, do đó bài viết này cũng sẽ được cập nhật thường xuyên

?? [Qualys SSL Labs](#) xếp hạng A, bạn cần phải cập nhật cấu hình của Nginx theo mã mới sử dụng tiêu chí như thế này. Bạn có thể tham khảo bài viết ?? để biết cách cập nhật cho máy chủ của mình.

1. Cách tắt TLS 1.0, TLS 1.1 và TLS 1.2, vô hiệu hóa SSL 2.0 và SSL 3.0

Bạn cần phải nâng cấp phiên bản OpenSSL lên phiên bản mới nhất không bị vulnerability bằng cách tải và cài đặt TLS 1.2 và TLS 1.2. Ví dụ: các phiên bản 0.9.x và 1.0.0 thì vẫn chưa hỗ trợ TLS 1.2.

Sau khi nâng cấp OpenSSL, bạn cần phải build lại hoặc nâng cấp Nginx lên phiên bản mới nhất. Kể từ phiên bản 1.1.13 trở lên, Nginx đã hỗ trợ TLS 1.1 và TLS 1.2.

?? vô hiệu hóa SSL 2.0, SSL 3.0 và cách tắt TLS 1.0, TLS 1.1 và TLS 1.2, bạn cần chú ý thêm sau:

```
ssl_protocols TLSv1.2 TLSv1.1 TLSv1;
```

2. Poodle and TLS-FALLBACK-SCSV

SSL 3.0 là nguyên nhân quan trọng nhất gây ra lỗi h?ng Poodle. B?ng cách vô hiệu hóa SSL 3.0, b?n ?ã kh?c ph?c l? h?ng Poodle cho máy ch?.

?? vô hiệu hóa l? h?ng "protocol downgrade attack", extension TLS FALLBACK SCSV ph?i ???c kích ho?t trong OpenSSL. Các phiên b?n sau ?ây ?ã bao g?m extension này:

- OpenSSL 1.0.1j ho?c cao h?n
- OpenSSL 1.0.0o ho?c cao h?n
- OpenSSL 0.9.8zc ho?c cao h?n

3. Heartbleed

L? h?ng Heartbleed là m?t l? h?ng khá nghiêm trọng, có th? ?nh h??ng ??n m?i máy ch? s? d?ng th? vi?n OpenSSL. ?? kh?c ph?c l?i này, cách duy nh?t là b?n ph?i ki?m tra phiên b?n OpenSSL ?ang s? d?ng và nâng c?p n?u n?m trong danh sách sau ?ây:

- OpenSSL 1.0.1 ??n 1.0.1f b? ?nh h??ng
- OpenSSL 1.0.1g không b? ?nh h??ng
- OpenSSL 1.0.0 không b? ?nh h??ng
- OpenSSL 0.9.8 không b? ?nh h??ng

4. Cipher suites

Luôn luôn áp d?ng các cipher suites an toàn nh?t và yêu c?u server l?a ch?n ?u tiên theo th? t? mà b?n ?ã thi?t l?p.

```
ssl_prefer_server_ciphers on;  
ssl_ciphers "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM  
EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256  
EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4  
EECDH EDH+aRSA RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK  
!SRP !DSS !RC4";
```

5. Strong DH (Diffie-Hellman)

Ch?y l?nh:

```
openssl dhparam -out /usr/local/ssl/dhparams.pem 2048
```

B? sung dòng sau ?ây vào file c?u hình:

```
ssl_dhparam /usr/local/ssl/dhparams.pem;
```

Online URL: <https://huongdan.maxserver.com/article-42.html>