**http://www.troyhunt.com/2014/04/everything-you-need-to-know-about.html**

The Heartbleed bug memungkinkan pengguna internet untuk membaca memori dari sistem yang dilindungi oleh versi rentan dari perangkat lunak OpenSSL .

**Apa itu OpenSSL dan versi apa yang terpengaruh ?**

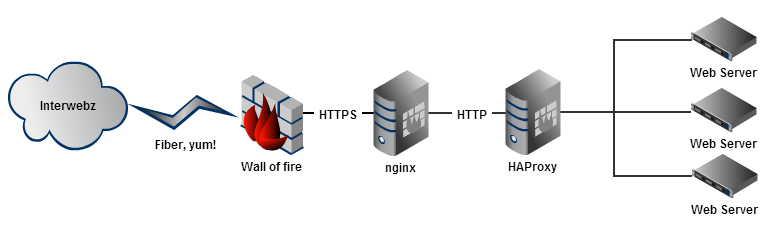
Heartbleed hadir dalam OpenSSL SSL dan TLS ( tetapi cenderung digunakan secara bergantian dan biasanya mengacu pada pelaksanaannya melalui HTTP atau dengan kata lain , HTTPS ) . Itu adalah perangkat lunak open source yang memfasilitasi komunikasi melalui protokol SSL dan bersifat umum.

Open SSL mengimplementasikan sever Apache dan Nginx.

Heartbleed bug diperkenalkan pada Desember 2011 . Bug mempengaruhi OpenSSL versi 1.0.1 yang dirilis pada Maret 2012 melalui ke 1.0.1f .

**Apakah hanya site pada Apache dan Nginx yang terinfeksi ?**

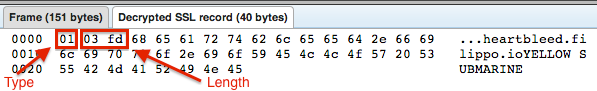
Tidak semua server web tergantung pada open SSL. Contohya IIS , yatitu Schannel Mircrosoft yang tidak terinfeksi bug tersebut tetapi bukan berarti situs di IIS tidak rentan terhadap heartbleed.

Dapat dilihat bahwa IIS (web server) berada pada bagian kanan , seperti gambar dibawah ini :

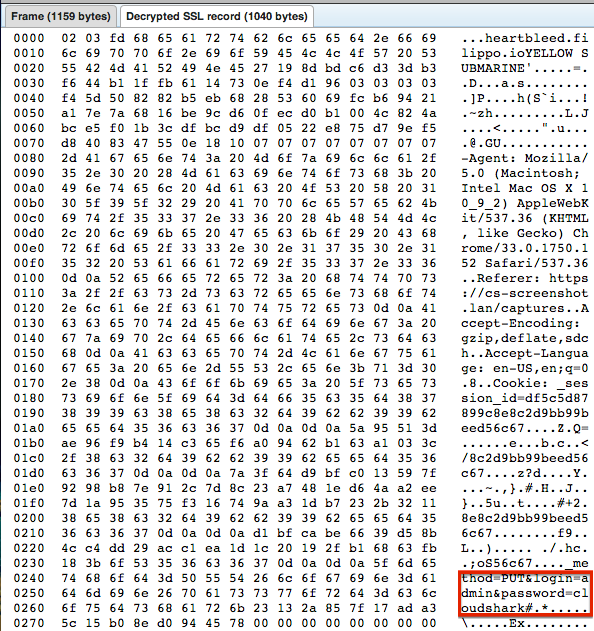
**https://appliance.cloudshark.org/blog/packet-capture-of-heartbleed-in-action/**

Seperti yang diketahui , kerentanan baru ditemukan pada OpenSSL yang dinamakan dengan heartbleed . Serangan ini berpusat pada Heartbeat extension di OpenSSL.

Untuk melihat apakah suatu website terkena heartbleed atau tidak , pertama-tama mengunjungi website “Heartbleed Test” kemudian buka website cloudshark untuk melihat packet capture yang di dapat.

[](https://www.cloudshark.org/captures/f54b25932509)

Pertama-tama lihatlah message enskripsi pada Heartbeat yang kita kirim dimana berisi informasi sensitif, kemudian lihat deskripsi pada SSL yang merekam enskripsi dari message heartbeat. Byte pertama (0x01) menunjukkan jenis pesan pada Heartbeat yaitu request dari Heartbeat. Dua byte berikutnya (0x03fd) menunjukkan panjang Heartbeat message payload.

[](https://www.cloudshark.org/captures/f54b25932509)Kemudian kita akan melihat bagaimana server merespon pesan tersebut. Dalam response server Heartbeat harus mengirim response dari request yang dikirim . Server akan meresponse dengan muatan 1021 byte di dalamnya. Ketika pemeriksaan deskripsi pada SSL sebenarnya server mengirim muatan sesuai dengan request , ditambah dengan header HTTP dari pengguna yang Login termaksud Login dan password yang digunakan untuk sesi login dan ID . Dalam hal ini kita dapat melihat bahwa pengguna (admin) login dengan default cloudshark password.