**Melakukan Scanning Network**

**Dan Scanning System**



***Robbi Anggara Pranata(09031181520011)***

**UNIVERSITAS SRIWIJAYA**

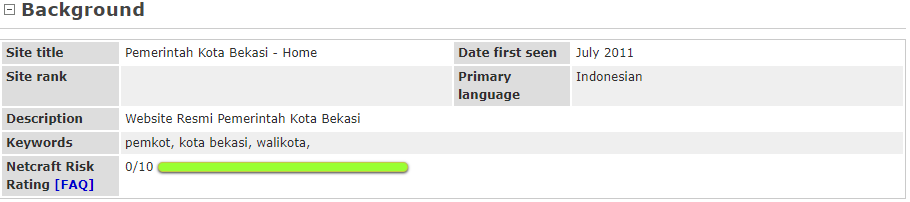
**PALEMBANG**

**2017**

**Melakukan Scanning Network**

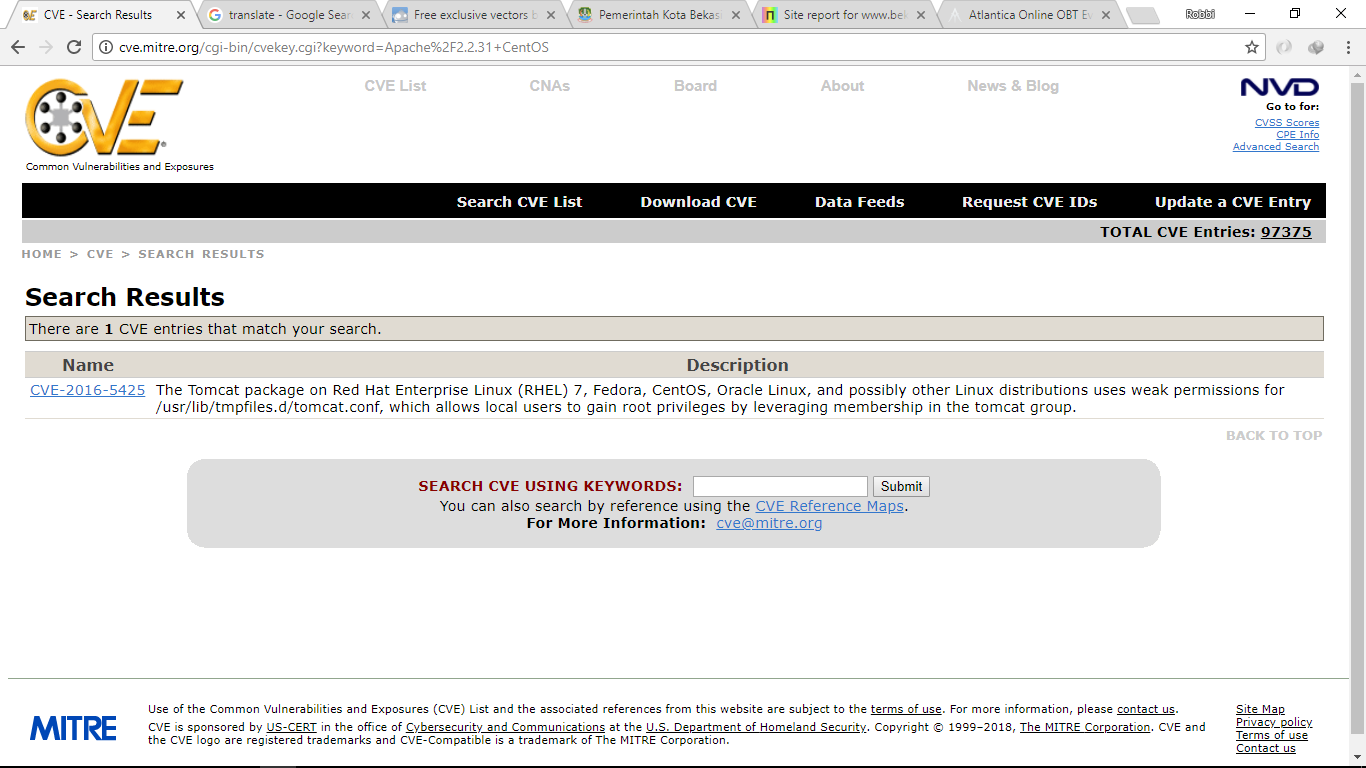
**Dan Scanning System Pada Website Kota Bekasi**

*Hasil Scaning network menggunakan bantuan tools pada netcraft.com*



*Hasil Scaning System Web server menggunakan bantuan tools pada* ***cve.mitre.org***

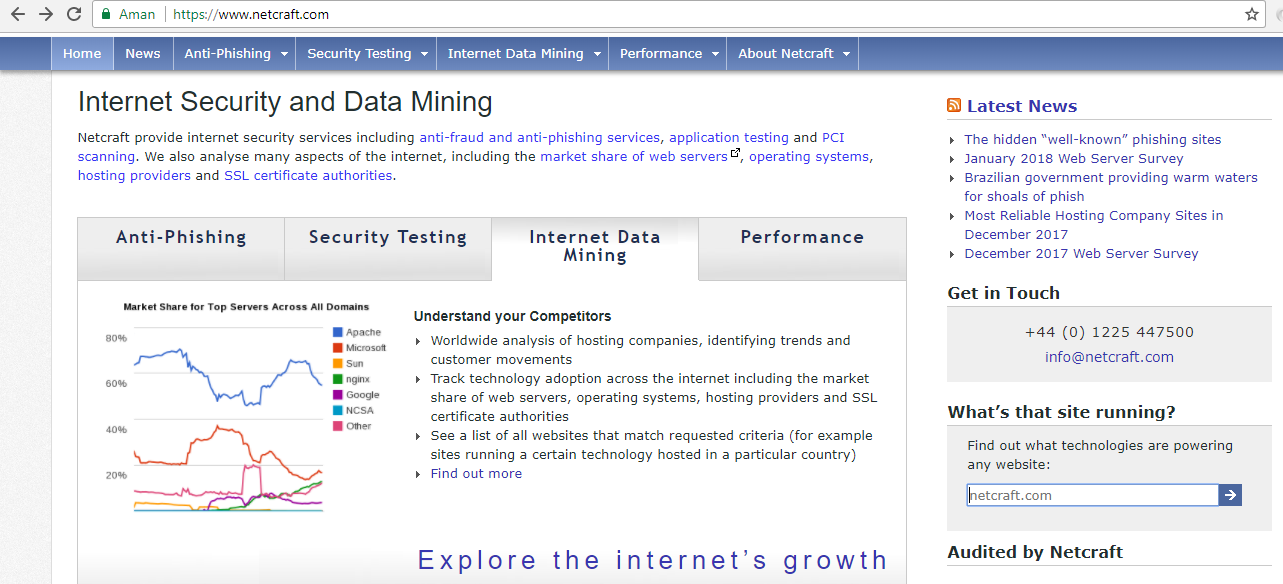
The Tomcat pada Red Hat Enterprise Linux (RHEL) 7, Fedora, CentOS, Oracle Linux, dan mungkin Linux lainnya menggunakan hak akses yang lemah /usr/lib/tmpfiles.d/tomcat.conf, yang memungkinkan pengguna lokal memperoleh hak istimewa root dengan memanfaatkan keanggotaan kelompok tomcat.



Hasilnya web server mereka Apache/2.2.31 CentOS memiliki 1 kelemahan yaitu :

**Melakukan scanning network dan scanning system pada Gemscool.com**

***Untuk Scaning network kita menggunakan bantuan netcraft.com kali ini kita akan menscan network dari salah satu perusahaan game ternama PT. KREON yaitu gemscool.com***



Gambar di atas adalah tampilan awal ketika kita membuka netcraft.com, lalu masukan link web yang ingin kita cari tahu networknya, di menu ” *whats thats site running?* ”

Dan berikut adalah informasi yang bisa kita dapatkan dari scaning yang telah kita lakukan :

IP Addres : 203.89.146.41

Netblock Owner : [PT. KREON Corporate / Direct Member IDNIC Menara Jamsostek 16th Floor Jl. Jendral Gatot Subroto No.38 Jakarta, 12930](https://toolbar.netcraft.com/netblock?q=KREON-ID,203.89.146.0,203.89.147.255)

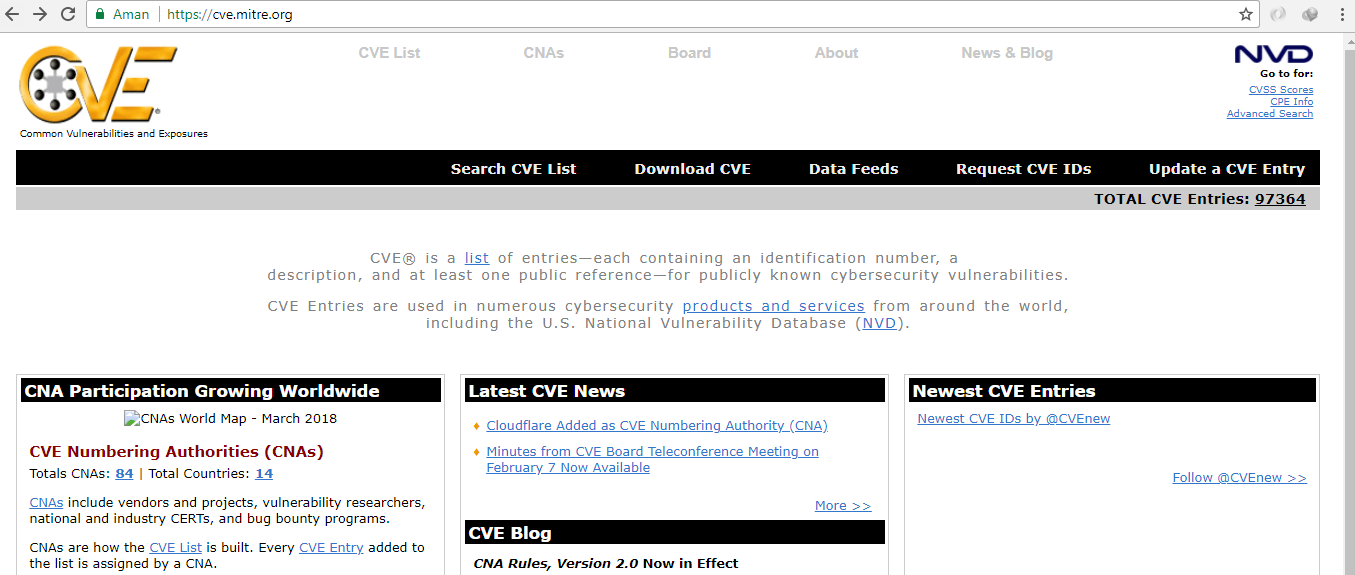
Nameserver : ns1.gemscool.com

DNS Admin : se@kreon.co.id

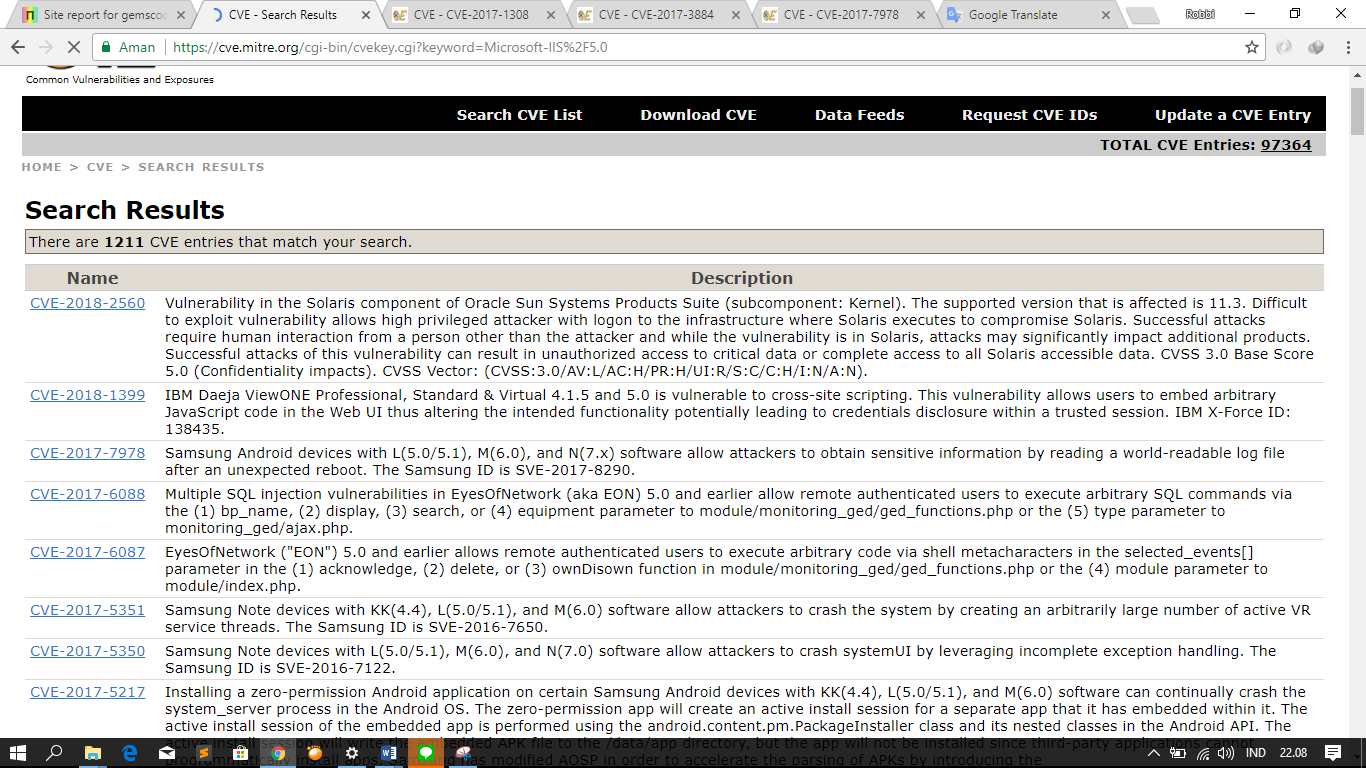
Web Server : Microsoft-IIS/5.0

OS : Linux

***Selanjutnya kita akan menscan system yang di gunakan oleh web tersebut dengan bantuan tools dari cve.mitre.org***



Lalu kita menggunakan fitur “Search CVE List” lalu masukan web server dari web yg telah kita scan tadi dalam hal ini adalah “Microsoft-IIS/5.0” dan hasilnya akan terdapat **1211** celah yang bisa menjadi kelemahan dari sistem yg mereka gunakan



Berikut saya akan menjelaskan 3 di antaranya :

* IBM Daeja ViewONE Professional, Standard & Virtual 4.1.5.1 and 5.0 bisa membuat system membiarkan perangkat yang tidak dikenali atau penyerang mendownload file yang penting dan seharusnya tidak di bisa mereka akses
* Kerentanan dalam tampilan web dari cisco prime infrastructure dan cisco programmable network manager bisa membuat pengguna yang tidak dikenal dari jauh mengakses data-data sensitive dan bisa meletakan aplikasi pengintai, tanpa harus menggunakan akses admin
* Perangkat Android Samsung dengan perangkat lunak L (5.0 / 5.1), M (6.0), dan N (7.x) memungkinkan penyerang mendapatkan informasi sensitif dengan membaca file log yang dapat dibaca bebas setelah melakukan reboot tertentu . ID Samsung adalah SVE-2017-8290.