PROJECT 10
Skipfish dan WebGoat

Latar Belakang

Banyak website memiliki celah keamanana *SQL injection* dan serangan lain. Skipfish merupakan *free vulnerability scanner* dari Google yang bisa menemukan celah keamanan.

Kebutuhan

- BackTrack Linux 5 real atau virtual machine
- Target yang discan – gunakan komputer Windows yang menjalankan WebGoat (project 8 & 9), seting agar WebGoat bisa menerima request dari alamat IP eksternal.

Menjalankan WebGoat

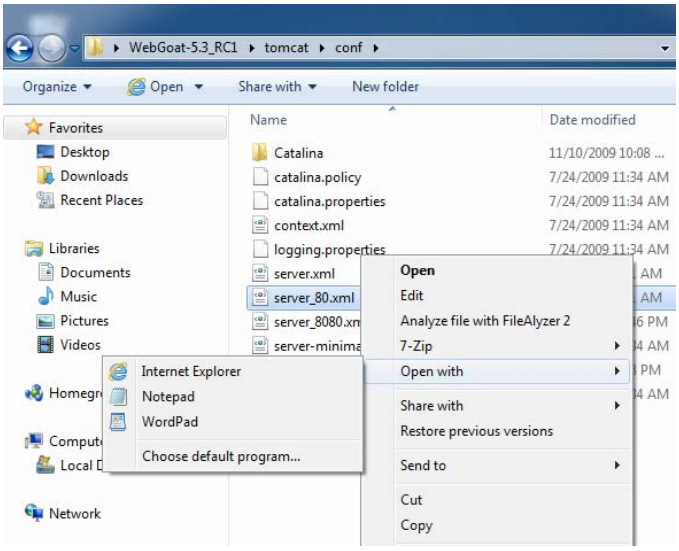
1. Sebaiknya menyelesaikan project 8,9,10 bersamaan, dikarenakan project tersebut berkelanjutan. (Akan tetapi jika project 10 Buka lagi folder WebGoat WebGoat-5.4_RC1 hasil project 8.)

Setting WebGoat untuk bisa menerima akses dari semua Alamat

Secara default, WebGoat hanya menerima akses (listens only) pada localhost. Dengan konfigurasi berikut maka WebGoat bisa diakses oleh semua alamat di jaringan, sehingga komputer Linux bisa melakukan scan.

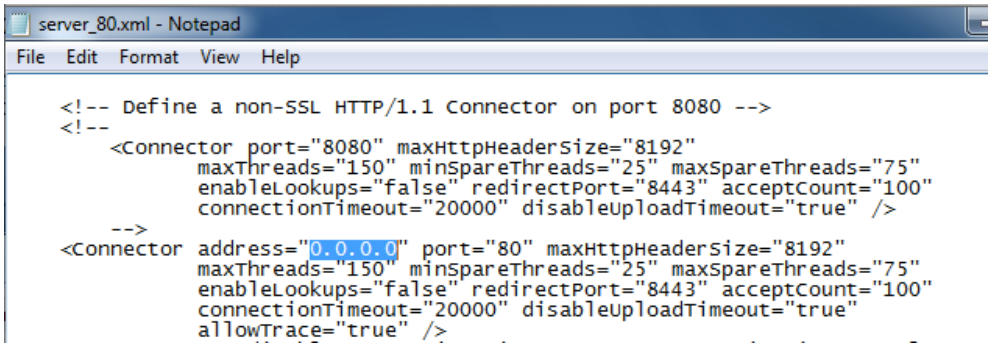
Perhatian: Eksplorasi hanya pada komputer WebGoat untuk serangan di jaringan! Hanya dijalankan pada komputer yang akan diuji yang diizinkan, atau pada jaringan tertutup.

2. Pada komputer Windows, buka WebGoat folder. Buka folder **Tomcat** folder, dan folder **conf**. Klik kanan file **server_80.xml** dan click **Open With...**, **Notepad**, seperti terlihat pada gambar di samping.
3. Pada Notepad, scroll down untuk mencari tulisan berikut:



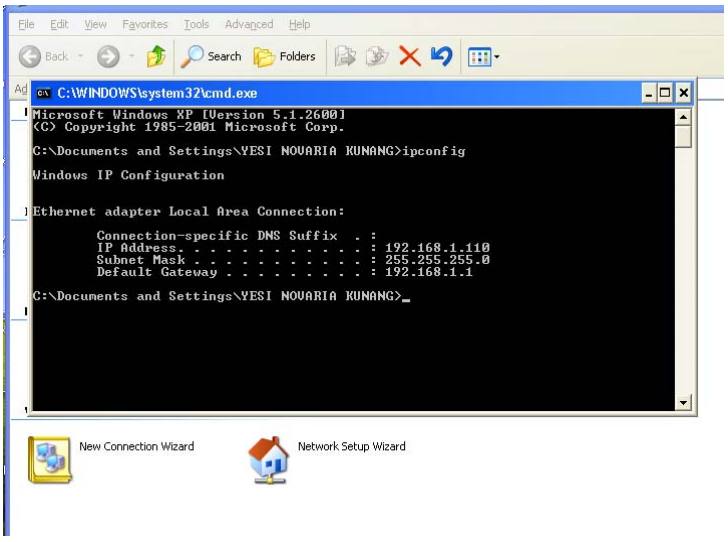
```
<!-- Define a non-SSL HTTP/1.1 Connector on port 8080 -->
<!--
    <Connector port="8080" maxHttpHeaderSize="8192"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
          enableLookups="false" redirectPort="8443" acceptCount="100"
          connectionTimeout="20000" disableUploadTimeout="true" />
    -->
    <Connector address="127.0.0.1" port="80" maxHttpHeaderSize="8192"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
          enableLookups="false" redirectPort="8443" acceptCount="100"
          connectionTimeout="20000" disableUploadTimeout="true"
          allowTrace="true" />
```

4. Rubah alamat dari **127.0.0.1** menjadi **0.0.0.0**, seperti terlihat di bawah ini.



5. Pada Notepad, click **File**, **Save**. Tutup Notepad.
6. Kembali ke folder WebGoat-5.4_RC1 dan double-click file **webgoat.bat** file. Webgoat akan kembali jalan.

Periksa IP Address komputer Windows



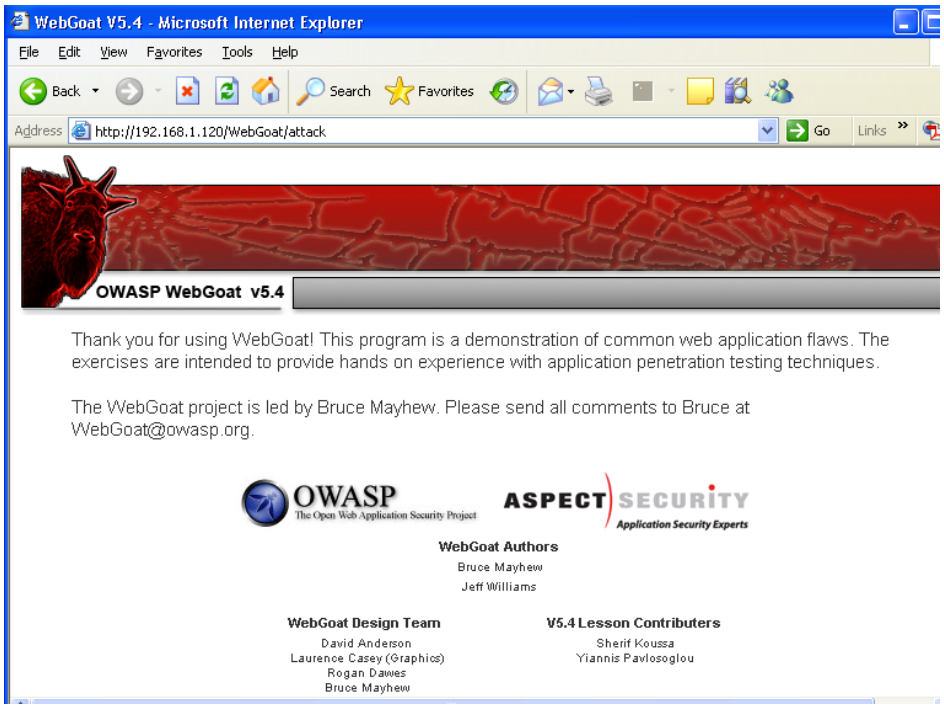
7. Click **Start**, ketikan **CMD**, dan tekan Enter. Pada jendela Command Prompt, ketik **IPCONFIG** dan tekan enter. Lihat IP address untuk komputer "Local Area Connection". Maka akan Nampak IP address 192.168.77.xx (alamat network lab Foresec, jika ada yang mendapatkan IP 10.1.x.x, minta bantuan asisten lab)

Buka Halaman WebGoat dari Browser Windows

8. Pada komputer Windows, buka browser dan arahkan ke

   http://192.168.77.xx/WebGoat/attack
   Gunakan alamat komputer Windows, seharusnya alamatnya 192.168.77.xx. Jika muncul kotak pop-up login --log dengan username **guest** dan password **guest**

9. Maka akan tampil halaman Webgoat seperti berikut.

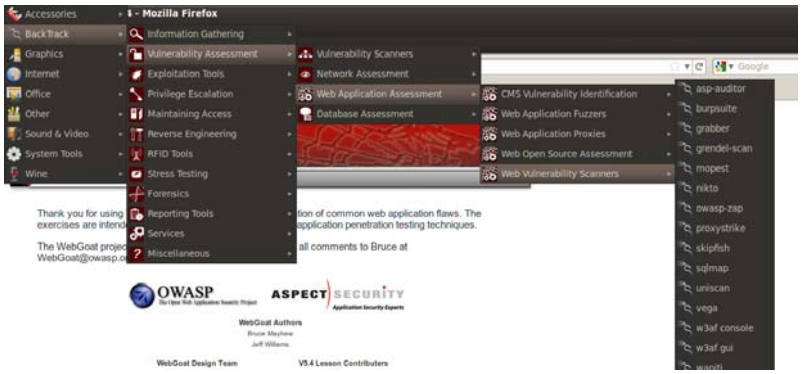


Buka Halaman WebGoat dari Browser Backtrack

10. Pada komputer Linux, buka Web browser dan arahkan ke alamat ip windows

    http://192.168.77.xx/WebGoat/attack
    Gunakan alamat IP komputer windows seperti langkah 8.

11. Maka akan muncul halaman login yang sama, dan halaman Webgoat. Jika tidak muncul, berarti ada masalah. Coba matikan firewall di Windows, pastikan bisa melakukan ping dari komputer windows dan Linux, dan cek juga virtual network settings berada dalam mode bridge. Webgoat harus bisa diakses dari komputer Linux sebelum saudara melakukan scan.

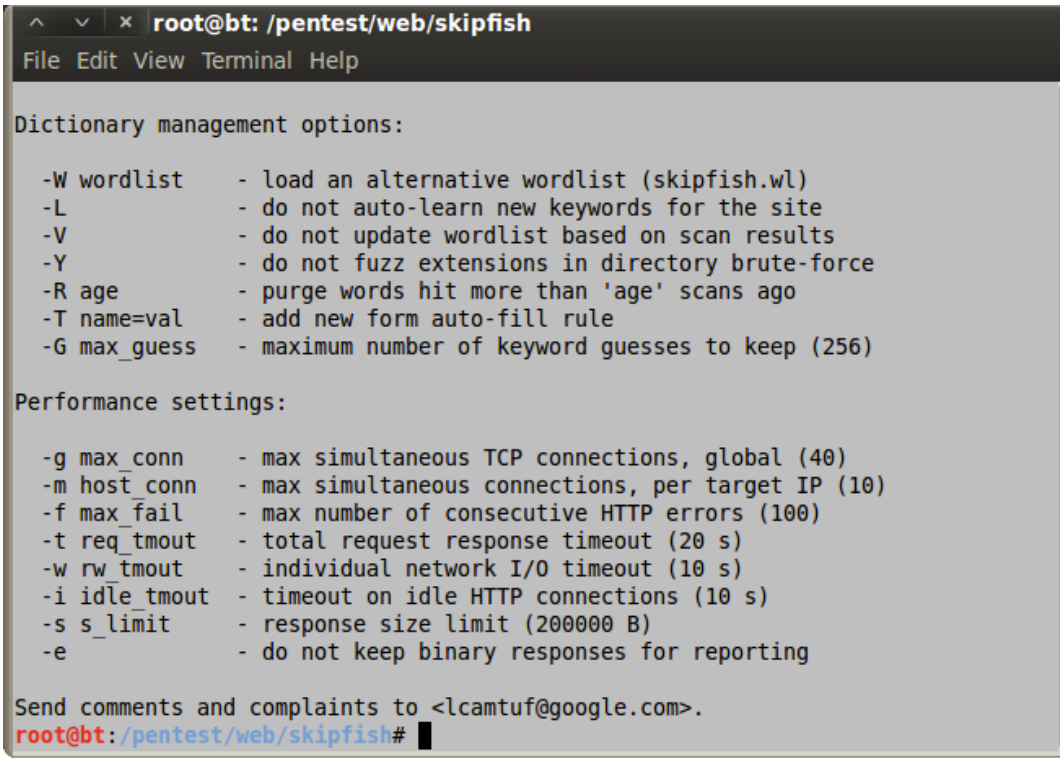


Menjalankan skipfish di Backtrack

12. Buka Backtrack. Pada Backtrack buka :

    Application--Vulnerability Assesment -- Web Application Assesment-- Web Vulnerability Scanners-skipfish

13. Klik pada bagian **'skipfish'**
14. Akan tampak seperti berikut

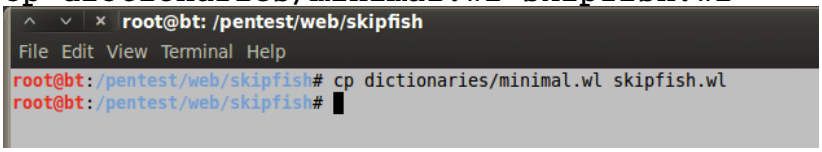


Mengkopi File Dictionary (kamus)

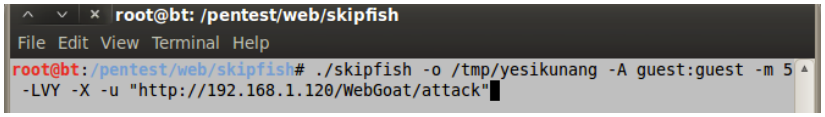
Skipfish menggunakan dictionaries (kamus) untuk mencari celah keamanan file dan object di website. Kita gunakan minimal untuk melakukan scan lebih cepat, tapi celah yang dicari lebih sedikit.

15. Pada jendela terminal, jalankan perintah berikut:

```
cp dictionaries/minimal.wl skipfish.wl
```



Scanning WebGoat



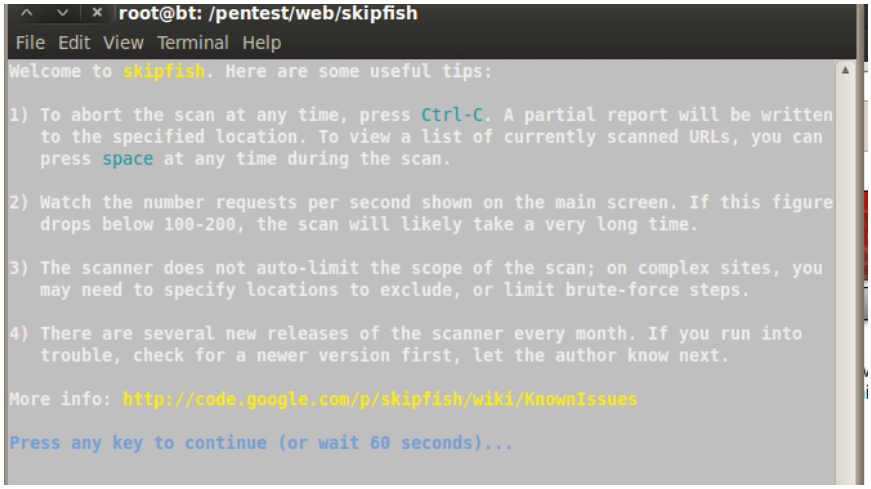
16. Pada jendela Terminal, jalankan perintah berikut:

```
./skipfish -o /tmp/namakamu -A guest:guest -m 5 -LVY -X -u
"http://192.168.5.93/WebGoat/attack"
```

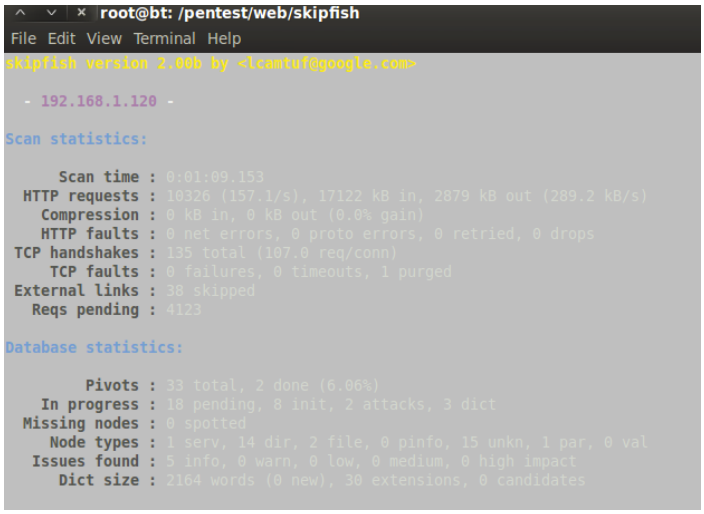
Ganti alamat IP address dengan alamat komputer WebGoat target (Windows).
Ganti namakamu dengan nama kalian (jangan gunakan spasi)

catatan: setiap kali menjalankan Skipfish, gunakan nama directory baru sebagai output (-o). Jika menjalankannya kembali, bisa gunakan /tmp/namakamu2, dll.

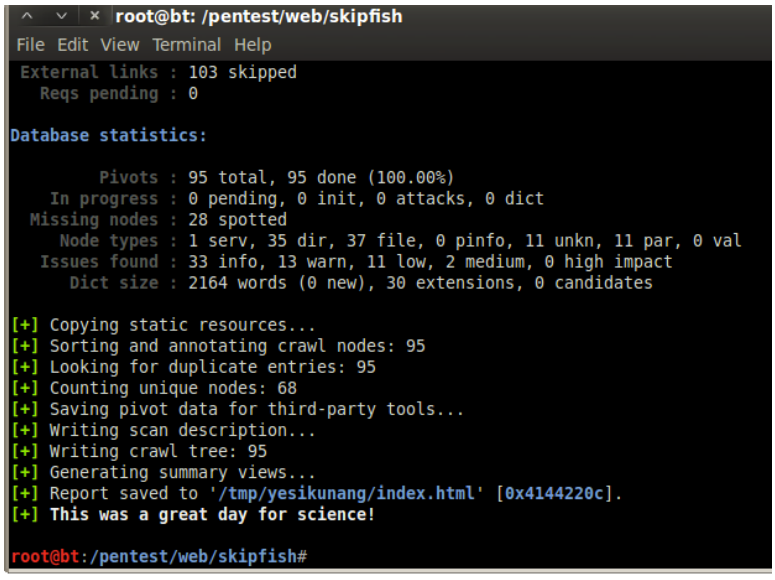
17. Pada saat Skipfish dijalankan, akan tampil gambar berikut:



Pada saat dijalankan akan tampil seperti ini:



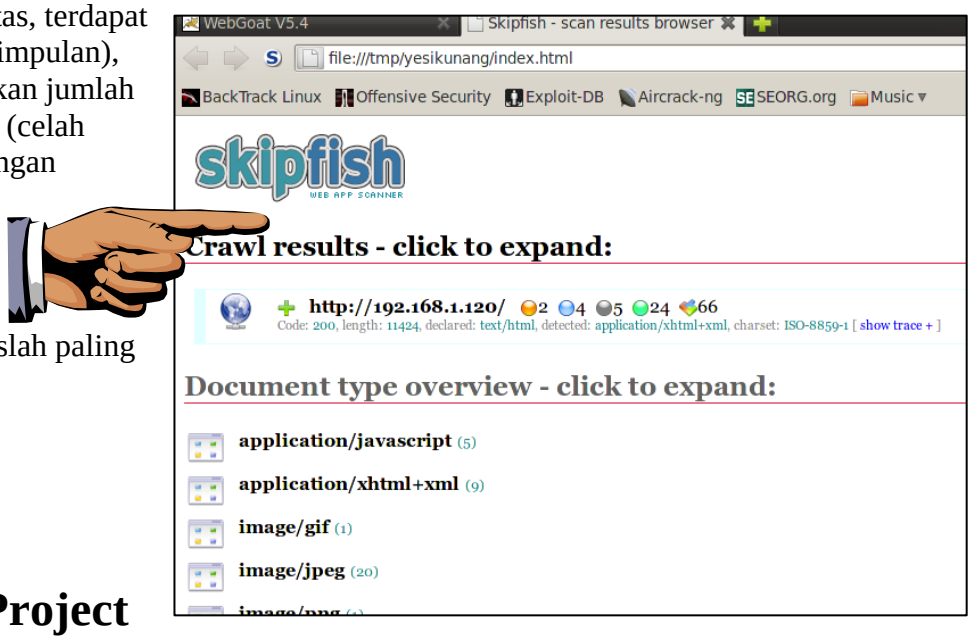
Pada saat selesai akan tampil seperti ini:



Melihat Hasil

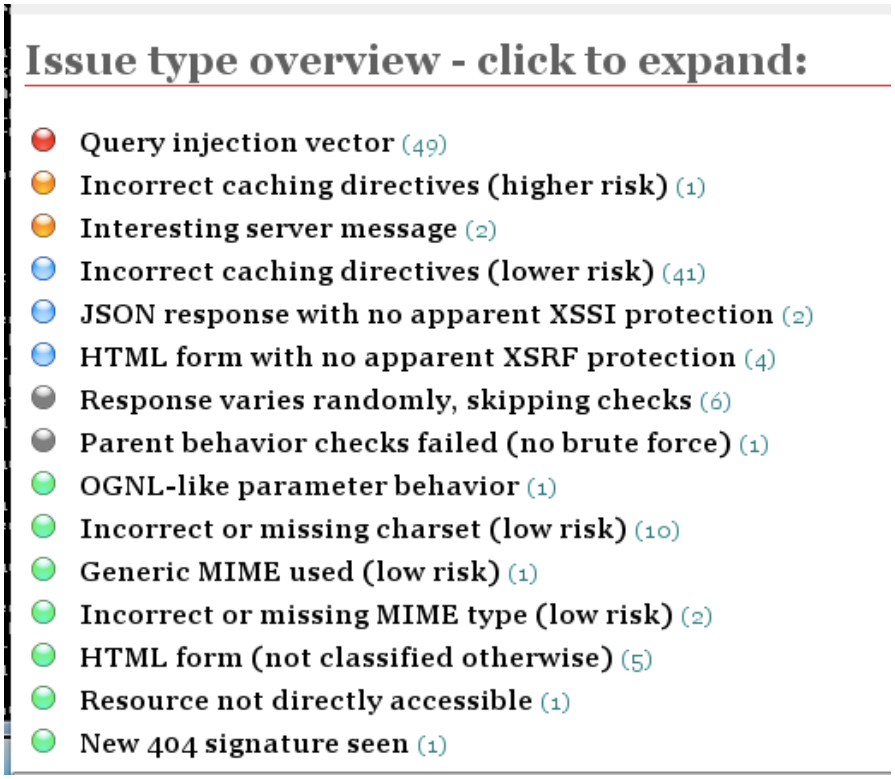
18. Buka jendela Firefox dan masukan URL yang sudah disimpan, yang isinya seperti **`/tmp/yesikunang/index.html`**
    (masukan nama yang tadi masukan sebagai folder)

19. Pada bagian atas, terdapat summary (kesimpulan), memeperlihatkan jumlah vulnerabilities (celah keamanan) dengan bulatan berwarna. Bulatan merah menunjukan aslah paling berbahaya:



Kumpulkan Project

20. Pastikan hasil skipfish tampil dengan header yang menunjukan nama kalian. Simpan screen shot dengan nama file **NamaKamu_Proj 10**.
21. “Kumpul melalui elearning".
22. Gulung ke bawah untuk melihat lebih detail:



Click bagian merah untuk eksplorasinya , akan terlihat URL yang diuji, dan jenis tes yang dilakukan:

Last modified 5-11-12