

PROJECT 10

Skipfish dan WebGoat

Latar Belakang

Banyak website memiliki celah keamanan *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

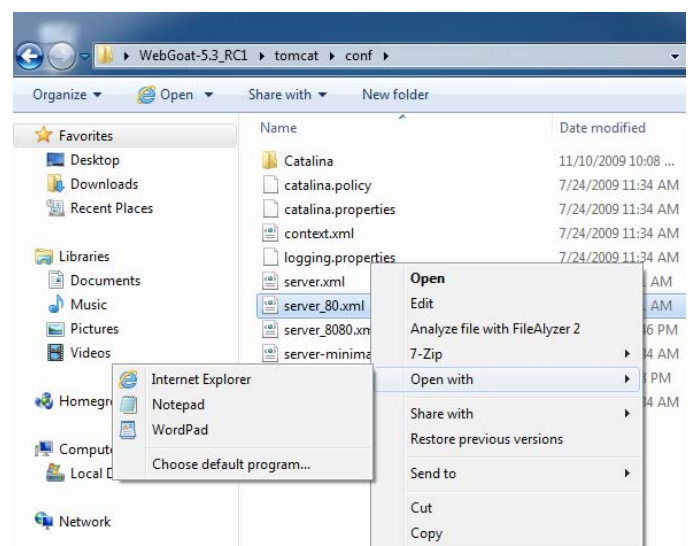
1. Sebaiknya menyelesaikan project 8,9,10 bersamaan, dikarenakan project tersebut berkelanjutan. (Akan tetapi jika project 10 Buka lagi folder WebGoat WebGoat-5.4_RC1 hasil project 8.)

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.

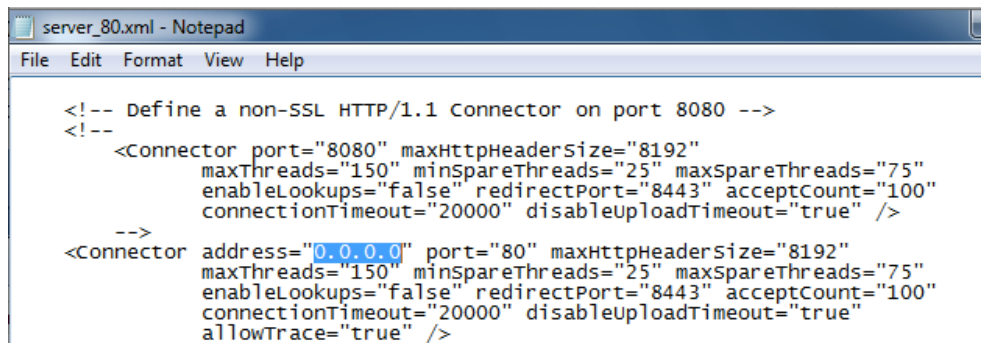
Perhatian: Eksplorasi hanya pada komputer WebGoat untuk serangan di jaringan! Hanya dijalankan pada komputer yang akan diuji yang diizinkan, atau pada jaringan tertutup.

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" />
```

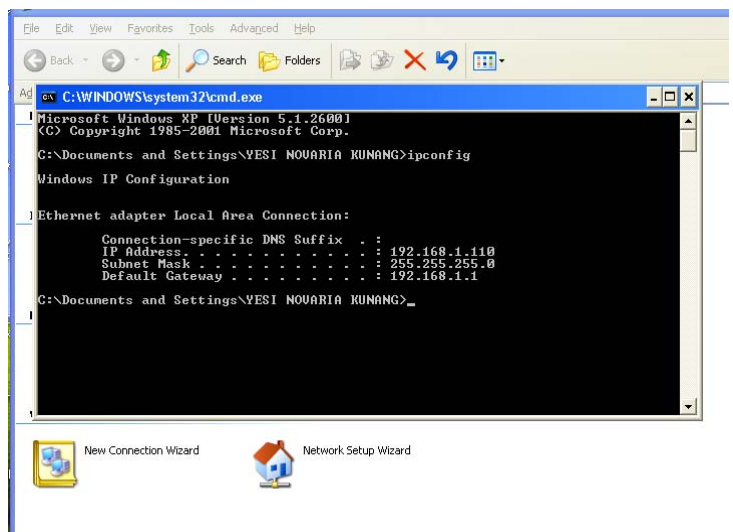
4. Rubah alamat dari **127.0.0.1** menjadi **0.0.0.0**, seperti terlihat di bawah ini.



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**, ketikkan **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)



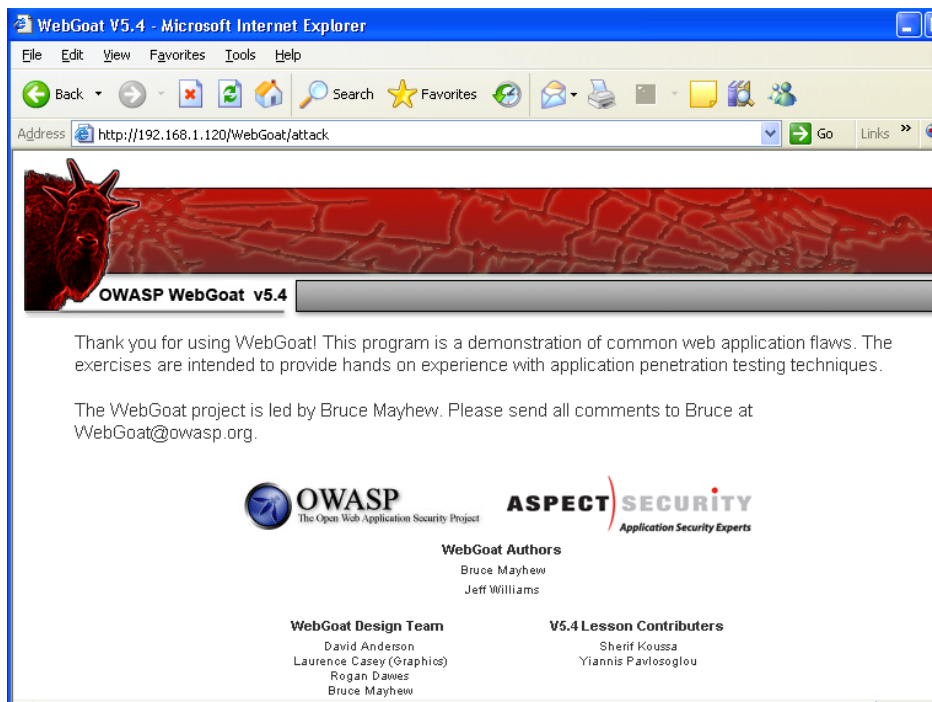
Buka Halaman WebGoat dari Browser Windows

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.



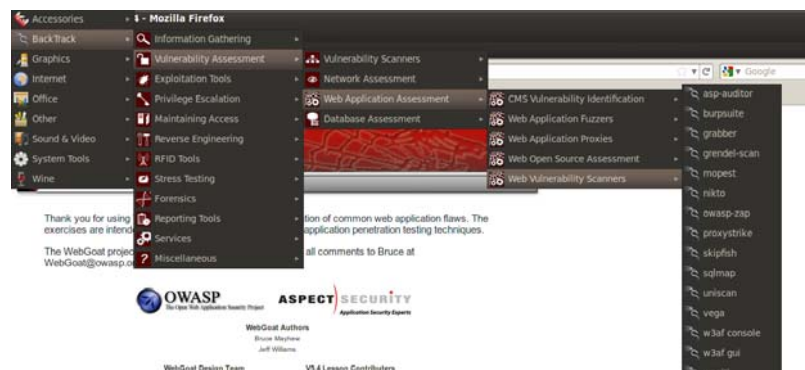
Buka Halaman WebGoat dari Browser Backtrack

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

```

root@bt: /pentest/web/skipfish
File Edit View Terminal Help

Dictionary management options:

-W wordlist      - load an alternative wordlist (skipfish.wl)
-L              - do not auto-learn new keywords for the site
-V              - do not update wordlist based on scan results
-Y              - do not fuzz extensions in directory brute-force
-R age          - purge words hit more than 'age' scans ago
-T name=val     - add new form auto-fill rule
-G max_guess    - maximum number of keyword guesses to keep (256)

Performance settings:

-g max_conn     - max simultaneous TCP connections, global (40)
-m host_conn    - max simultaneous connections, per target IP (10)
-f max_fail     - max number of consecutive HTTP errors (100)
-t req_tmout    - total request response timeout (20 s)
-w rw_tmout     - individual network I/O timeout (10 s)
-i idle_tmout   - timeout on idle HTTP connections (10 s)
-s s_limit      - response size limit (200000 B)
-e             - do not keep binary responses for reporting

Send comments and complaints to <lcamtuf@google.com>.
root@bt: /pentest/web/skipfish#

```

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
```

```

root@bt: /pentest/web/skipfish
File Edit View Terminal Help
root@bt: /pentest/web/skipfish# cp dictionaries/minimal.wl skipfish.wl
root@bt: /pentest/web/skipfish#

```

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"
```

```

root@bt: /pentest/web/skipfish
File Edit View Terminal Help
root@bt: /pentest/web/skipfish# ./skipfish -o /tmp/yesikunang -A guest:guest -m 5 -LVY -X -u "http://192.168.1.120/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:

```

root@bt: /pentest/web/skipfish
File Edit View Terminal Help
Welcome to skipfish. Here are some useful tips:

1) To abort the scan at any time, press Ctrl-C. A partial report will be written
   to the specified location. To view a list of currently scanned URLs, you can
   press space at any time during the scan.

2) Watch the number requests per second shown on the main screen. If this figure
   drops below 100-200, the scan will likely take a very long time.

3) The scanner does not auto-limit the scope of the scan; on complex sites, you
   may need to specify locations to exclude, or limit brute-force steps.

4) There are several new releases of the scanner every month. If you run into
   trouble, check for a newer version first, let the author know next.

More info: http://code.google.com/p/skipfish/wiki/KnownIssues

Press any key to continue (or wait 60 seconds)...

```

Pada saat dijalankan akan tampil seperti ini:

```

root@bt: /pentest/web/skipfish
File Edit View Terminal Help
skipfish version 2.00b by <lsantufegoogle.com>

- 192.168.1.120 -

Scan statistics:

  Scan time : 0:01:09.153
  HTTP requests : 10326 (157.1/s), 17122 kB in, 2879 kB out (289.2 kB/s)
  Compression : 0 kB in, 0 kB out (0.0% gain)
  HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
  TCP handshakes : 135 total (107.0 req/conn)
  TCP faults : 0 failures, 0 timeouts, 1 purged
  External links : 38 skipped
  Reqs pending : 4123

Database statistics:

  Pivots : 33 total, 2 done (6.06%)
  In progress : 18 pending, 8 init, 2 attacks, 3 dict
  Missing nodes : 0 spotted
  Node types : 1 serv, 14 dir, 2 file, 0 pinfo, 15 unkn, 1 par, 0 val
  Issues found : 5 info, 0 warn, 0 low, 0 medium, 0 high impact
  Dict size : 2164 words (0 new), 30 extensions, 0 candidates

```

Pada saat selesai akan tampil seperti ini:

```

root@bt: /pentest/web/skipfish
File Edit View Terminal Help
External links : 103 skipped
Reqs pending : 0

Database statistics:

  Pivots : 95 total, 95 done (100.00%)
  In progress : 0 pending, 0 init, 0 attacks, 0 dict
  Missing nodes : 28 spotted
  Node types : 1 serv, 35 dir, 37 file, 0 pinfo, 11 unkn, 11 par, 0 val
  Issues found : 33 info, 13 warn, 11 low, 2 medium, 0 high impact
  Dict size : 2164 words (0 new), 30 extensions, 0 candidates

[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 95
[+] Looking for duplicate entries: 95
[+] Counting unique nodes: 68
[+] Saving pivot data for third-party tools...
[+] Writing scan description...
[+] Writing crawl tree: 95
[+] Generating summary views...
[+] Report saved to '/tmp/yesikunang/index.html' [0x4144220c].
[+] This was a great day for science!

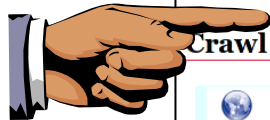
root@bt:/pentest/web/skipfish#

```

Melihat Hasil

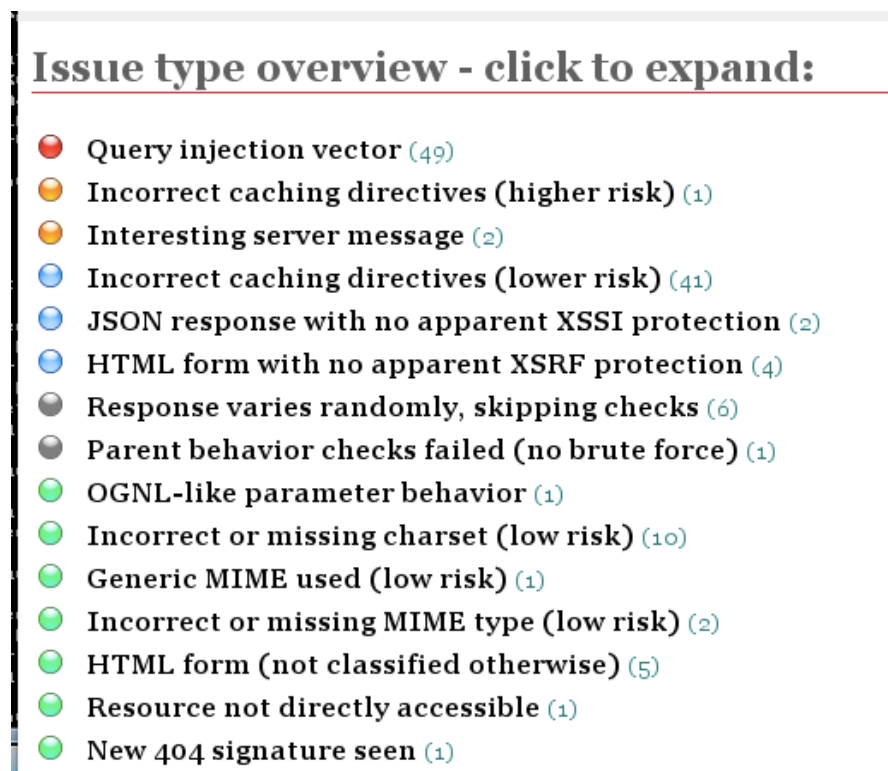
18. Buka jendela Firefox dan masukan URL yang sudah disimpan, yang isinya seperti `/tmp/yesikunang/index.html`
(masukan nama yang tadi masukan sebagai folder)

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:

Issue type overview - click to expand:

● Query injection vector (49)

1. <http://192.168.5.93/> [show trace +]
Memo: response to [different than to](#)
2. http://192.168.5.93/%24CATALINA_HOME/ [show trace +]
Memo: response to [different than to](#)
3. http://192.168.5.93/%24CATALINA_HOME/conf/ [show trace +]
Memo: response to [different than to](#)
4. http://192.168.5.93/%24CATALINA_HOME/webapps/ [show trace +]
Memo: response to [different than to](#)
5. http://192.168.5.93/%24CATALINA_HOME/webapps/ROOT/ [show trace +]
Memo: response to [different than to](#)
6. <http://192.168.5.93/admin/> [show trace +]
Memo: response to [different than to](#)
7. <http://192.168.5.93/jsp-examples/> [show trace +]
Memo: response to [different than to](#)

Last modified 5-11-12