NAMA : DWI KURNIA PUTRA

NIM : 09011181320019

MK : KEAMANAN JARINGAN KOMPUTER

EKSPLOITASI KEAMANAN

Eksploitasi dapat juga didefiniskan sebagai dalam beberapa hal, mengambil keuntungan dari celah keamanan dalam system untuk pencarian atau penghargaan dari beberapa tujuan. Seluruh eksploitasi celah keamanan merupakan serangan namun tidak seluruh serangan dapat mengeksploitasi celah keamanan. Seorang cracker dapat menggunakan suatu exploit untuk memperoleh akses ke suatu system computer.

Anatomi Suatu Serangan Hacking

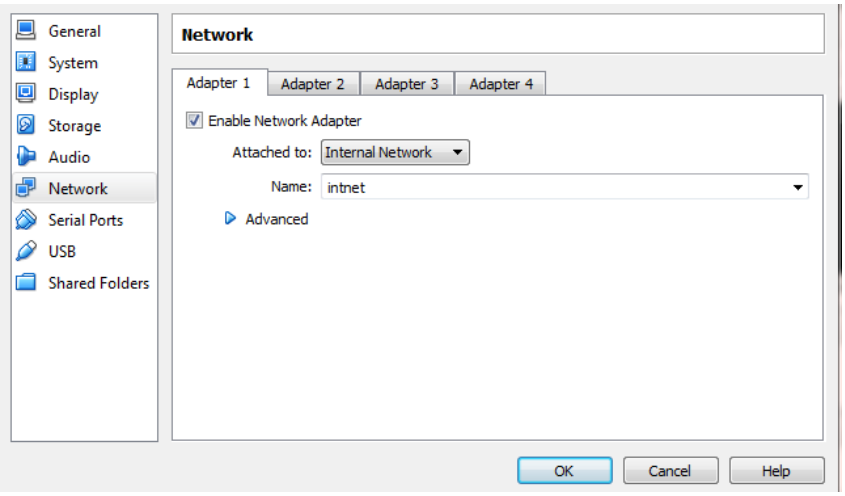
1. Footprinting
   Mencari informasi terhadapa system-sistem untuk dijadikan sasaran, mencakup pencarian informasi dengan search engine, whois, dan DNS zone transfer.
2. Scanning
   Terhadap sasaran tertentu dicari pintu masuk yang paling memungkinkan dan mencari informasi IP menggunakan beberapa software.
3. Enumeration
   Intensif terhadap sasaran yang mencari user account abash, network resource and share, dan aplikasi untuk mendapatkan mana yang proteksinya lemah.
4. Gaining Acces
   Mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses sasaran. Meliputi mengintip dan merampas password, menebak password serta melakukan buffer overflow.
5. Escalating Privilege
   Bila baru mendapatkan user password ditahap sebelumnya, ditahap ini diusahakan mendapat privilese admin jaringan dengan password cracking atau exploit sejenis getadmin, sechole, atau lc_message.
6. Piltering
   Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke trusted system. Mencakup evaluasi trust dan pencarian cleartext password di registry, config file dan user data.
7. Covering Tracks
   Setelah control penuh terhadap system diperoleh, maka menutup jejak menjadi prioritas meliputi membersihkan network log dan penggunaan hide tool seperti macam-macam rootkit dan file streaming.
8. Creating Backdoors

Diciptakan pada berbagai bagian dari system untuk memudahkan masuk kembali ke system ini dengan cara membentuk account palsu, menjadwalkan batch job, mengubah startup file, menanamkan servis pengendali jarak jauh serta monitoring tool, dan menggantikan aplikasi dengan Trojan.

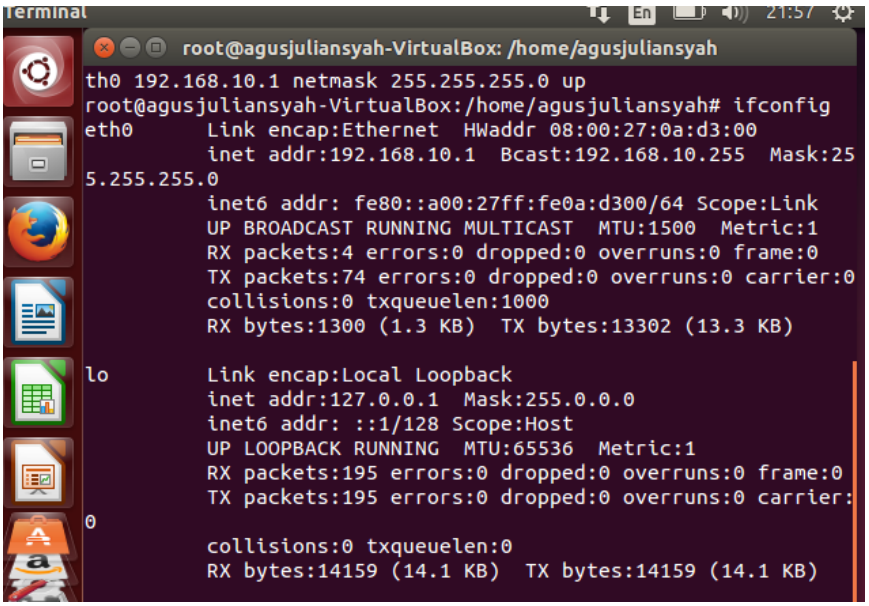
9. Denial of Service

   Bila semua usaha di atas gagal, penyerang dapat melumpuhkan sasaran sebagai usaha terakhir dengan berusaha mencegah pemakai yang sah untuk mengakses sebuah sumber daya tau informasi.

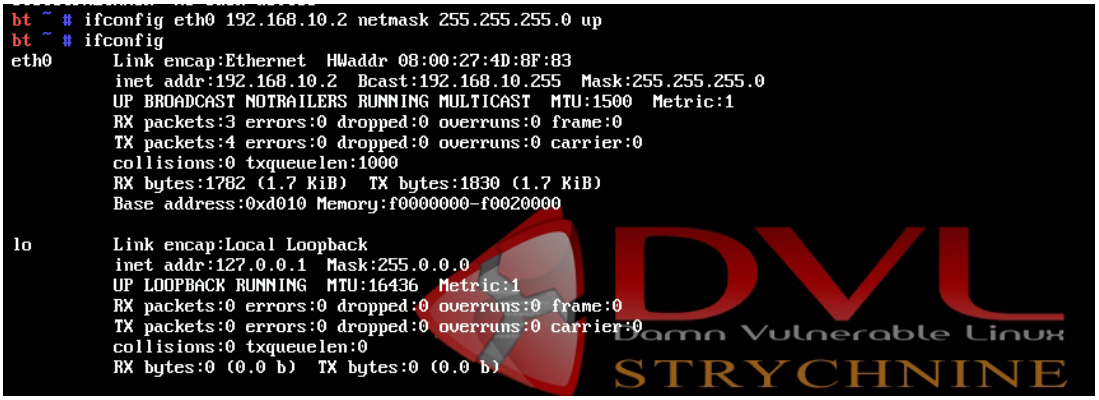
UJI COBA DARI EKSPLOTASI KEAMANAN



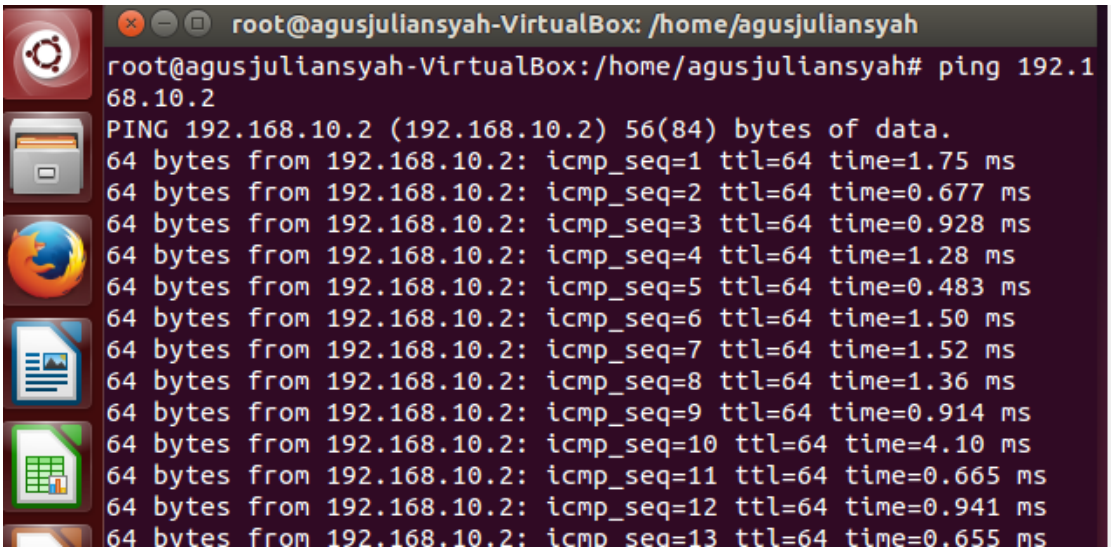
Menggunakan 2 virtualiasi virtual box, yaitu Ubuntu Desktop dngan DVL yang mana sesuai tampilan di atas, mengatur koneksinya menjadi internal network.



Dengan perintah ifconfig pada virtualisasi Ubuntu, sesuai tampilan di atas didapatkan IP yaitu 192.168.10.1 dengan netmask 255.255.255.0

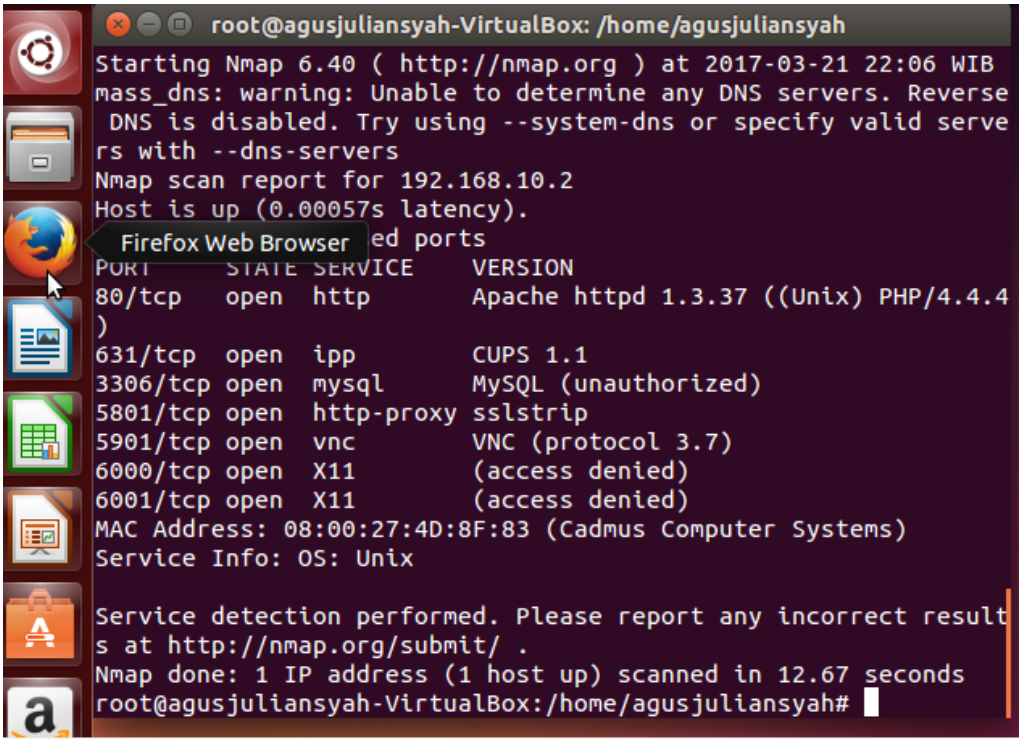


Sedangkan pada virtualisasi DVL, didapatkan IP yaitu 192.168.10.2 dengan netmask 255.255.255.0

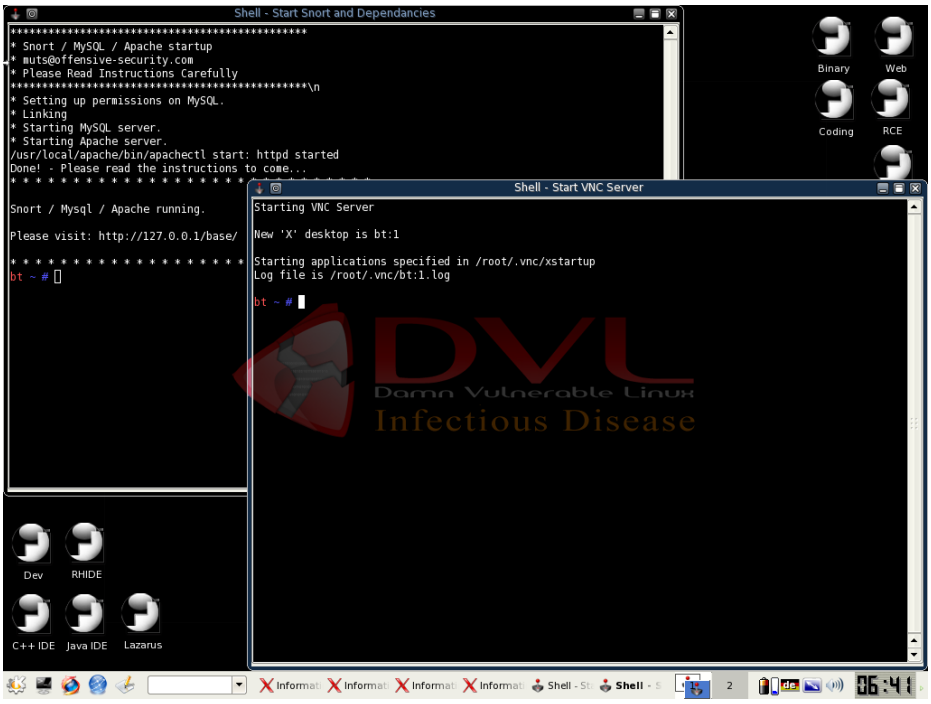


Tes jaringan dari virtualisasi Ubuntu ke DVL dengan perintah ping 192.168.10.2 (IP Virtualisasi DVL)

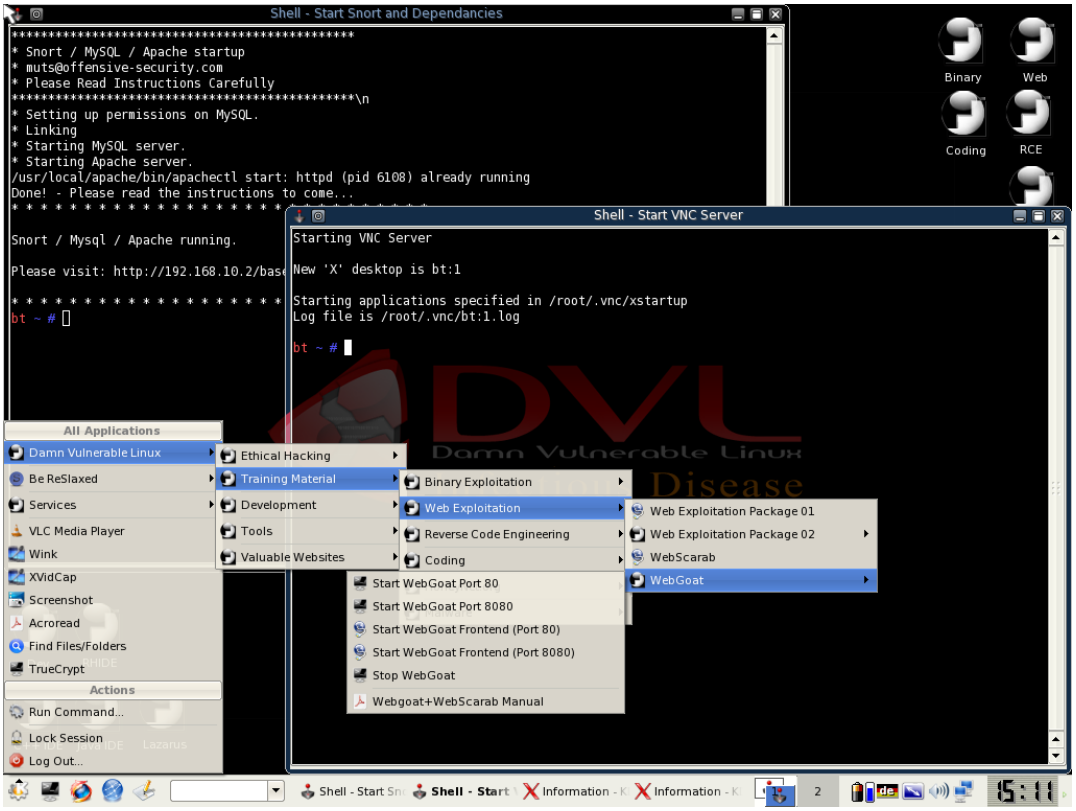
Dan sebaliknya, tes jaringan dari virtualisasi DVL ke Ubuntu dengan perintah ping 192.168.10.1 (IP Virtualisasi Ubuntu). Hasilnya, kedua virtualisasi berkomunikasi dengan baik.



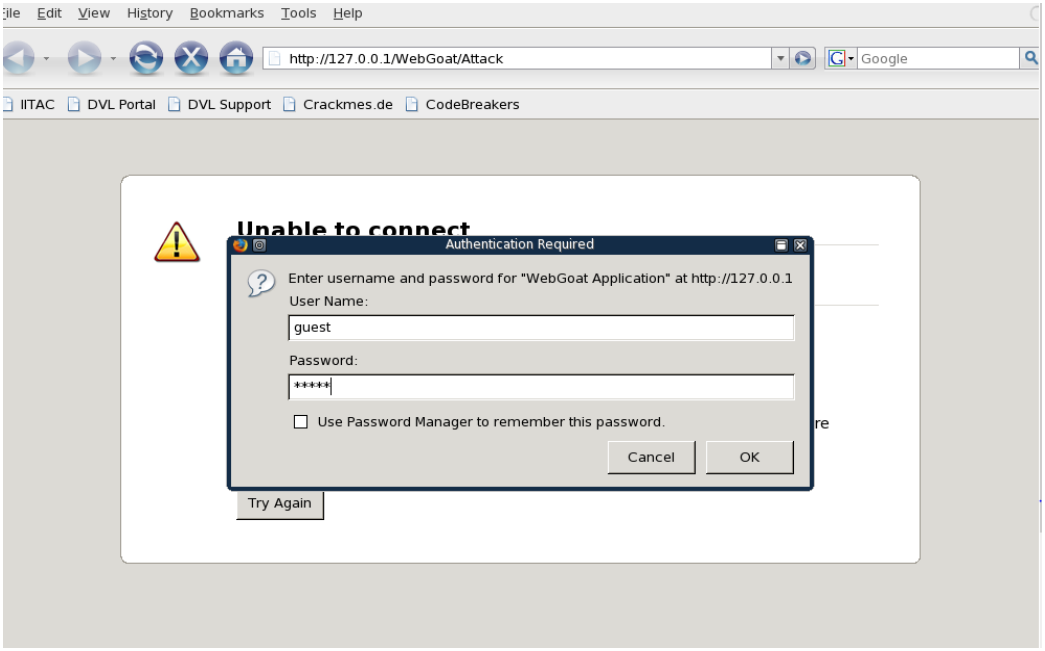
Menggunakan tool nmap untuk mengetahui informasi berupa port yang terbuka, service yang digunakan beserta versionnya pada virtualisasi/jaringan DVL dengan IP 192.168.10.2



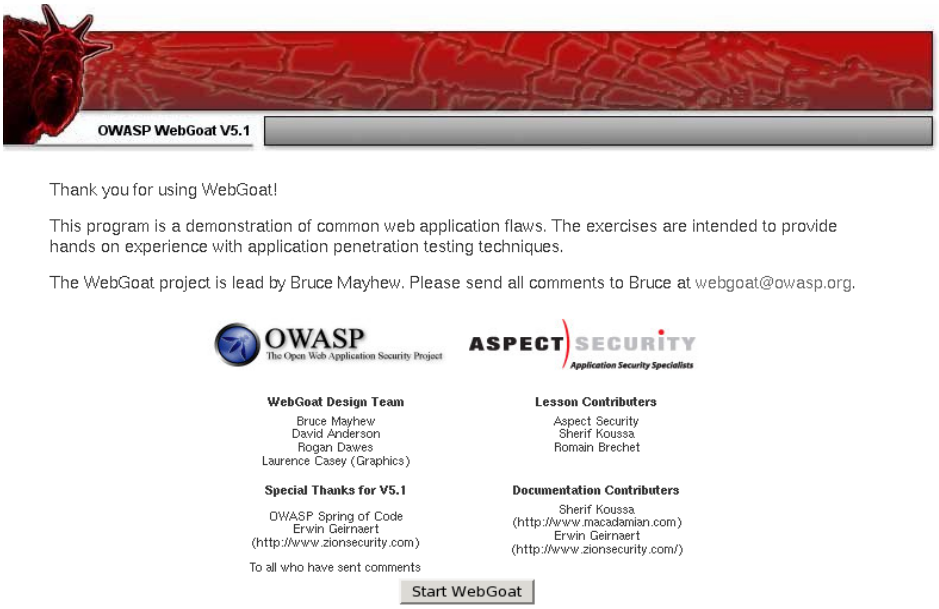
Sedangkan pada virtualisasi DVL, kita mengatur beberapa service yang digunakan sesuai apa yang digunakan dengan cara menstart service tersebut.



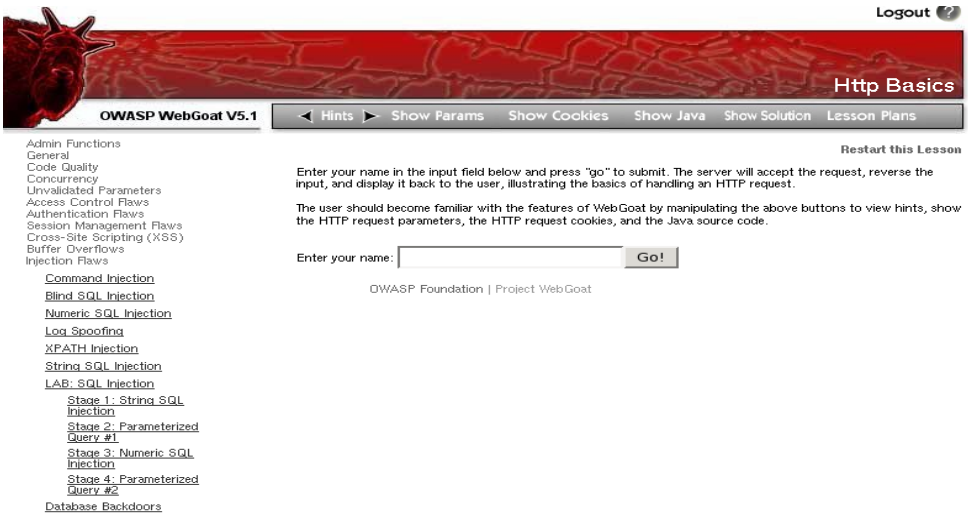
Tampilan di atas merupakan langkah mengatur DAMN VULNEABLE LINUX yang mana berfungsi untuk memulai Webgoat yang ada di DVL. Sesuai gambar di atas, Webgoat yang distart terdapat pada Port 80.

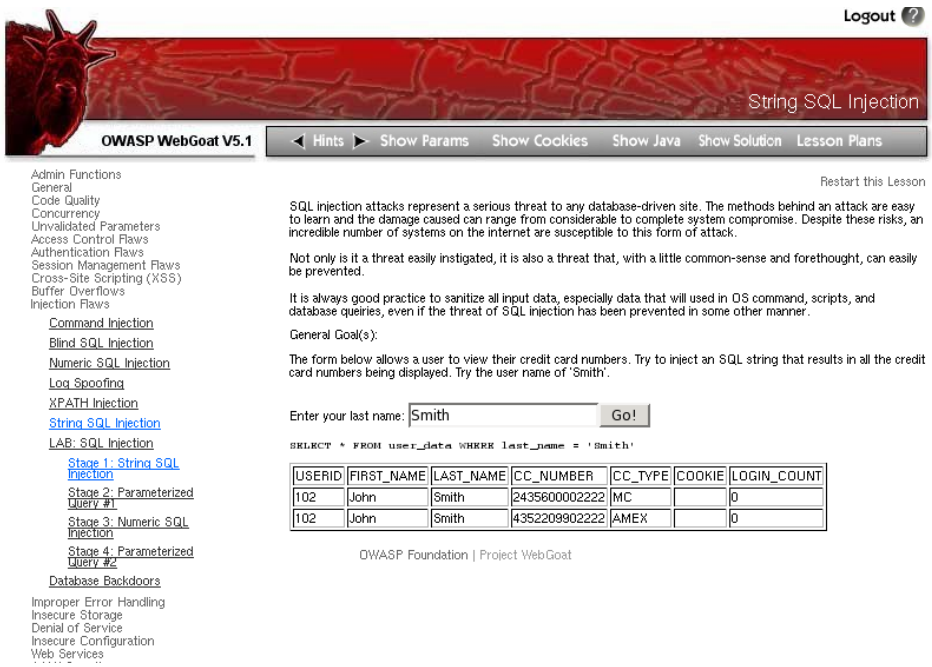


Setelah Webgoat distart, maka akan muncul pada browser dengan interface seperti pada tampilan di atas.



Setelah memasukkan username dan password pada Webgoat Application, maka akan muncul OWASP dan ASPECT SECURITY seperti pada tampilan di atas. OWASP atau Open Web Application Security Project merupakan sebuah non profit komuniti yang bertujuan untuk mengembangkan metodologi, program, dokumentasi dan sebagainya yang berhubungan dengan keamanan web application sedangkan ASPECT SECURITY sama halnya dengan OWASP yang berbasis keaman web application.





Memulai Webgoat seperti tampilan di atas, yang digunakan untuk aplikasi web dan mengubungkannya untuk mencoba serangan hacking.

* **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

Berikut merupakan hasil dari exploitasi menggunakan Webgoat berbasis OWASP, dimana tampilan tersebut merupakan injeksi SQL untuk mencuri nomor kartu kredit palsu.

KESIMPULAN

Salah satu tool yang digunakan dalam exploitasi keamanan yaitu webgoat, sesuai dengan ujicoba yang dilakukan pada bagian di atas. WebGoat sendiri dirancang oleh OWASP untuk mengajarkan pelajaran keamanan apliaski web untuk menunjukkan pemahaman tentang masalah keamanan dengan memanfaatkan kerentanan dalam aplikasi nyata WebGoat.