

**TUGAS KEAMANAN JARINGAN KOMPUTER
TRAINING EKSPLOITASI KEAMANAN**



NAMA : Yayang Prayoga
NIM : 09011181320006
KELAS : SK8A

**SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA**

Eksplorasi Keamanan

Keamanan jaringan menjadi semakin penting dengan semakin banyaknya waktu yang dihabiskan orang untuk berhubungan. Mengganggu keamanan jaringan sering lebih mudah daripada fisik atau lokal, dan lebih umum. Celah-celah keamanan jaringan sering digunakan untuk menjebol suatu sistem dibawah ini beberapa Eksplorasi yang dilakukan untuk masuk dalam keamanan suatu sistem.

Anatomi Suatu Serangan Hacking

1. Footprinting

Mencari rincian informasi terhadap sistem-sistem untuk dijadikan sasaran, mencakup pencarian informasi dengan search engine, whois, dan DNS zone transfer. hacker baru mencari-cari sistem mana yang dapat disusupi. Footprinting merupakan kegiatan pencarian data berupa:

- Menentukan ruang lingkup (scope) aktivitas atau serangan
- Network enumeration
- Interogasi DNS
- Mengintai jaringan

Semua kegiatan ini dapat dilakukan dengan tools dan informasi yang tersedia bebas di Internet. Kegiatan footprinting ini diibaratkan mencari informasi yang tersedia umum melalui buku telepon. Tools yang tersedia untuk ini di antaranya :

- Teleport Pro: Dalam menentukan ruang lingkup, hacker dapat men-download keseluruhan situs-situs web yang potensial dijadikan sasaran untuk dipelajari alamat, nomor telepon,contact person,dan lain seagainya.
- Whois for 95/9/NT: Mencari informasi mengenai pendaftaran domain yang digunakan suatu organisasi. Di sini ada bahaya laten pencurian domain (domain hijack).
- NSLookup: Mencari hubungan antara domain name dengan IP address.
- Traceroute 0.2: Memetakan topologi jaringan, baik yang menuju sasaran maupun konfigurasi internet jaringan sasaran.

2. Scanning

Scanning terhadap sasaran tertentu dicari pintu masuk yang paling mungkin. Digunakan ping sweep dan portscan.

3. Enumeration

Telaah intensif terhadap sasaran, yang mencari user account absah, network resource and share, dan aplikasi untuk mendapatkan mana yang proteksinya lemah. enumerasi sudah bersifat sangat intrusif terhadap suatu sistem. Di sini penyusup mencari account name yang absah, password, serta share resources yang ada. Pada tahap ini, khusus untuk sistem-sistem Windows, terdapat port 139 (NetBIOS session service) yang terbuka untuk resource sharing antar-pemakai dalam jaringan. Anda mungkin berpikir bahwa hard disk yang di-share itu hanya dapat dilihat oleh pemakai dalam LAN saja. Kenyataannya tidak demikian. NetBIOS session service dapat dilihat oleh siapa pun yang terhubung ke Internet di seluruh dunia! Tools seperti Legion, SMBScanner, atau SharesFinder membuat akses ke komputer orang menjadi begitu mudah (karena pemiliknya lengah membuka resource share tanpa password).

4. Gaining Access

Mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses sasaran. Melalui mengintip dan merampas password, menebak password, serta melakukan buffer overflow. gaining access adalah mencoba mendapatkan akses ke dalam suatu sistem sebagai user biasa. Ini adalah kelanjutan dari kegiatan enumerasi, sehingga biasanya di sini penyerang sudah mempunyai paling tidak user account yang absah, dan tinggal mencari passwordnya saja. Bila resource share-nya diproteksi dengan password, maka password ini dapat saja ditebak (karena banyak yang menggunakan password sederhana dalam melindungi komputernya). Menebaknya dapat secara otomatis melalui dictionary attack (mencobakan kata-kata dari kamus sebagai password) atau brute-force attack (mencobakan kombinasi semua karakter sebagai password). Dari sini penyerang mungkin akan berhasil memperoleh logon sebagai user yang absah.

5. Escalating Privilege

Bila baru mendapatkan user password di tahap sebelumnya, di tahap ini diusahakan mendapat privilese admin jaringan dengan password cracking atau exploit sejenis getadmin, sechole, atau lc_messages. Escalating Privilege mengasumsikan bahwa penyerang sudah mendapatkan logon access pada sistem sebagai user biasa. Penyerang kini berusaha naik kelas menjadi admin (pada sistem Windows) atau menjadi root (pada sistem Unix/Linux). Teknik yang digunakan sudah tidak lagi dictionary attack atau brute-force attack yang memakan waktu itu, melainkan mencuri password file yang tersimpan dalam sistem dan memanfaatkan kelemahan sistem. Pada sistem Windows 9x/ME password disimpan dalam file .PWL sedangkan pada Windows NT/2000 dalam file .SAM.

6. Pilfering

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 Track

Begitu kontrol penuh terhadap sistem diperoleh, maka menutup jejak menjadi prioritas. Meliputi membersihkan network log dan penggunaan hide tool seperti macam-macam rootkit dan file streaming. Penyerang sudah berada dan menguasai suatu sistem dan kini berusaha untuk mencari informasi lanjutan (pilfering), menutupi jejak penyusupannya (covering tracks), dan menyiapkan pintu belakang (creating backdoor) agar lain kali dapat dengan mudah masuk lagi ke dalam sistem. Adanya Trojan pada suatu sistem berarti suatu sistem dapat dengan mudah dimasuki penyerang tanpa harus bersusah payah melalui tahapan-tahapan di atas, hanya karena kecerobohan pemakai komputer itu sendiri.

8. Creating Backdoors

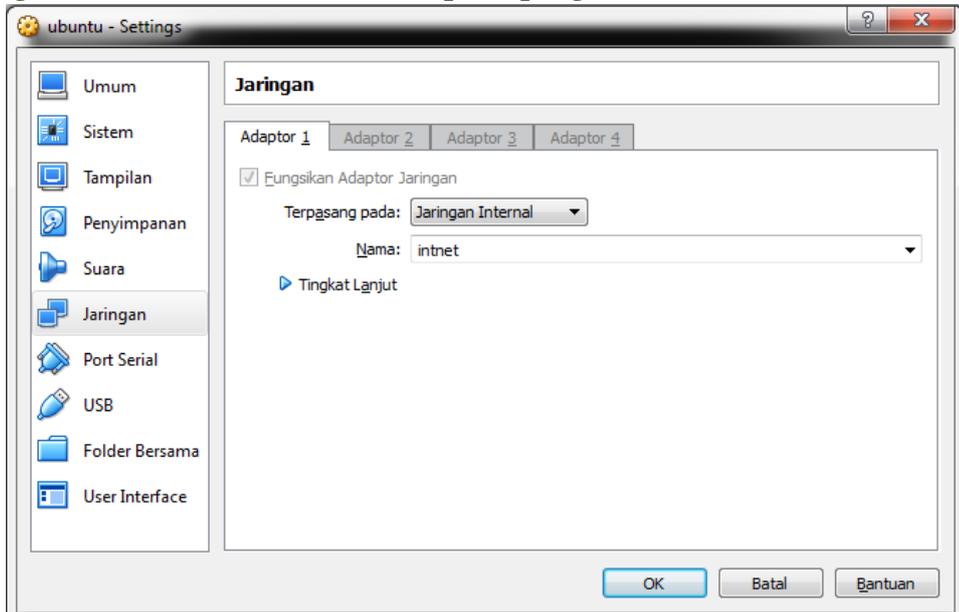
Pintu belakang diciptakan pada berbagai bagian dari sistem untuk memudahkan masuk kembali ke sistem ini dengan cara membentuk user account palsu, menjadwalkan batch job, mengubah startup file, menanamkan servis pengendali jarak jauh serta monitoring tool, dan menggantikan aplikasi dengan trojan.

9. Denial Of Service

Bila semua usaha di atas gagal, penyerang dapat melumpuhkan sasaran sebagai usaha terakhir. Meliputi SYN flood, teknik-teknik ICMP, Supernuke, land/latierra, teardrop, bonk, newtear, trincoo, smurf, dan lain-lain. Kalau penyerang sudah frustrasi tidak dapat masuk ke dalam sistem yang kuat pertahanannya, maka yang dapat dilakukannya adalah melumpuhkan saja sistem itu dengan menyerangnya menggunakan paket-paket data yang bertubi-tubi sampai sistem itu crash. Denial of service attack sangat sulit dicegah, sebab memakan habis bandwidth yang digunakan untuk suatu situs. Pencegahannya harus melibatkan ISP yang bersangkutan. Para script kiddies yang pengetahuan hacking-nya terbatas justru paling gemar melakukan kegiatan yang sudah digolongkan tindakan kriminal di beberapa negara ini.

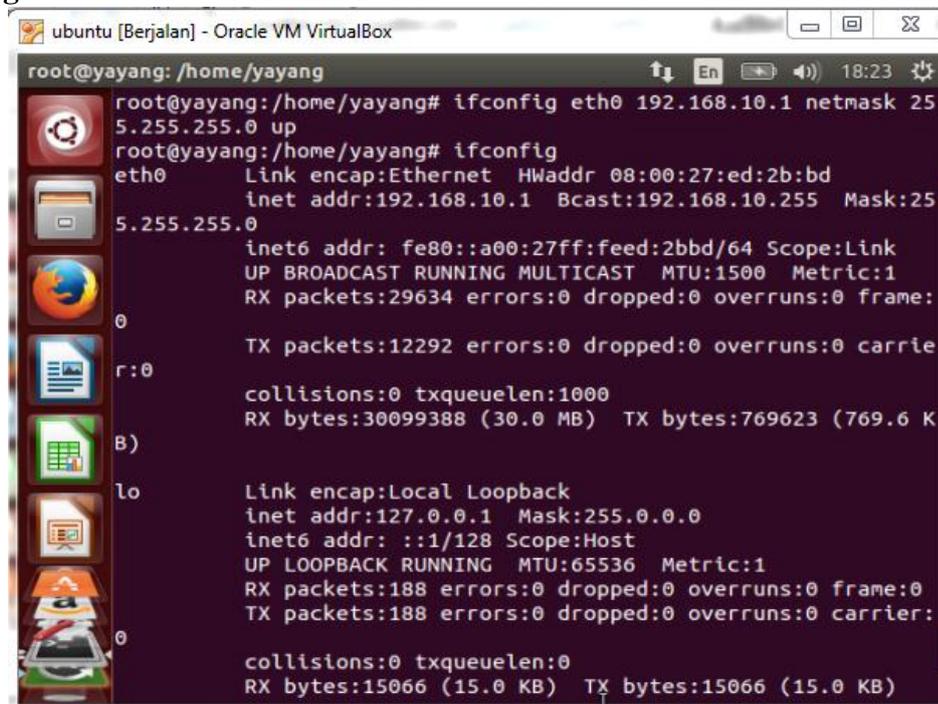
Langkah-langkah dalam melakukan percobaan Eksploitasi

1. Setting network di Ubuntu dan DVL pada pengaturan VirtualBox



Langkah ini hanya untuk menghubungkan Ubuntu dan DVL dalam satu jaringan internal. Namun jika Ubuntu dan DVL diletakkan pada komputer yang berbeda maka langkah ini tidak diperlukan namun harus menggunakan koneksi internet atau bisa menggunakan perantara penghubung seperti router dan sebagainya.

2. Setting IP Address di Ubuntu dan DVL



```
Shell - Konsole
bt ~ # ifconfig eth0 192.168.10.2 netmask 255.255.255.0 up
bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:A1:51:74
          inet addr:192.168.10.2  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feal:5174/64  Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1782 (1.7 KiB)  TX bytes:2298 (2.2 KiB)
          Base address:0xd010  Memory:f0000000-f0020000

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: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)

bt ~ #
```

Langkah ini diperlukan jika dilakukan dalam jaringan internal untuk mengetahui IP Address masing-masing agar mudah dalam melakukan percobaan penyerangan sebagai bahan pembelajaran.

3. Lakukan proses PING dari Ubuntu ke DVL dan sebaliknya

```
ubuntu [Berjalan] - Oracle VM VirtualBox
root@yayang: /home/yayang
root@yayang: /home/yayang# 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=9.34 ms
64 bytes from 192.168.10.2: icmp_seq=2 ttl=64 time=2.15 ms
64 bytes from 192.168.10.2: icmp_seq=3 ttl=64 time=2.16 ms
64 bytes from 192.168.10.2: icmp_seq=4 ttl=64 time=26.8 ms
64 bytes from 192.168.10.2: icmp_seq=5 ttl=64 time=1.05 ms
64 bytes from 192.168.10.2: icmp_seq=6 ttl=64 time=2.73 ms
64 bytes from 192.168.10.2: icmp_seq=7 ttl=64 time=2.76 ms
64 bytes from 192.168.10.2: icmp_seq=8 ttl=64 time=2.93 ms
^C
--- 192.168.10.2 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7018ms
rtt min/avg/max/mdev = 1.055/6.248/26.836/8.134 ms
root@yayang: /home/yayang#
```

```
Shell - Konsole
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=1.65 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=2.91 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=1.39 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=1.41 ms
64 bytes from 192.168.10.1: icmp_seq=5 ttl=64 time=1.51 ms
64 bytes from 192.168.10.1: icmp_seq=6 ttl=64 time=0.926 ms
64 bytes from 192.168.10.1: icmp_seq=7 ttl=64 time=1.50 ms

--- 192.168.10.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6003ms
rtt min/avg/max/mdev = 0.926/1.617/2.915/0.571 ms
bt ~ #
```

Langkah ini diperlukan untuk memeriksa apakah kedua sistem telah terhubung atau belum.

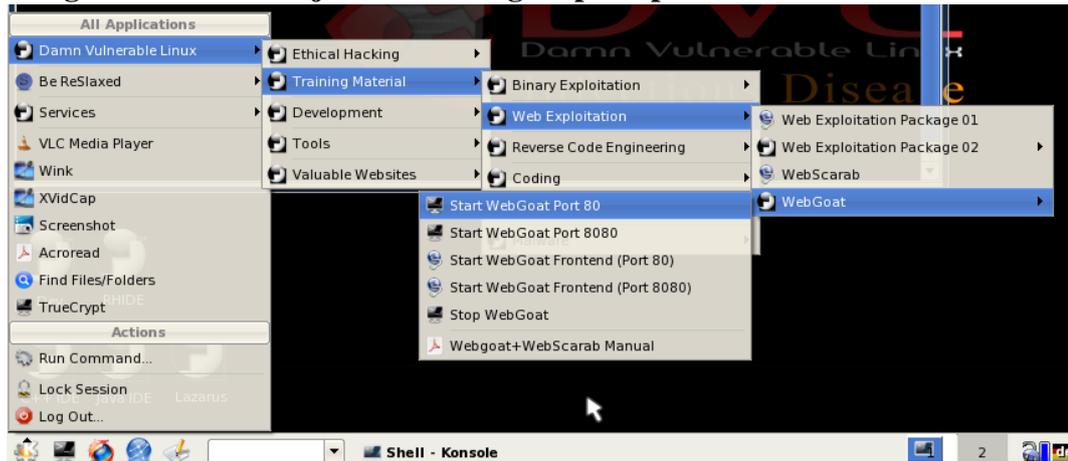
4. Scanning dengan menggunakan nmap dari Ubuntu

```
ubuntu [Berjalan] - Oracle VM VirtualBox
root@yayang: /home/yayang
root@yayang: /home/yayang# nmap -sV 192.168.10.2
Starting Nmap 6.40 ( http://nmap.org ) at 2017-03-22 18:35 WIB
Nmap scan report for 192.168.10.2
Host is up (0.0054s latency).
Not shown: 993 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:A1:51:74 (Cadmus Computer Systems)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.20 seconds
root@yayang: /home/yayang#
```

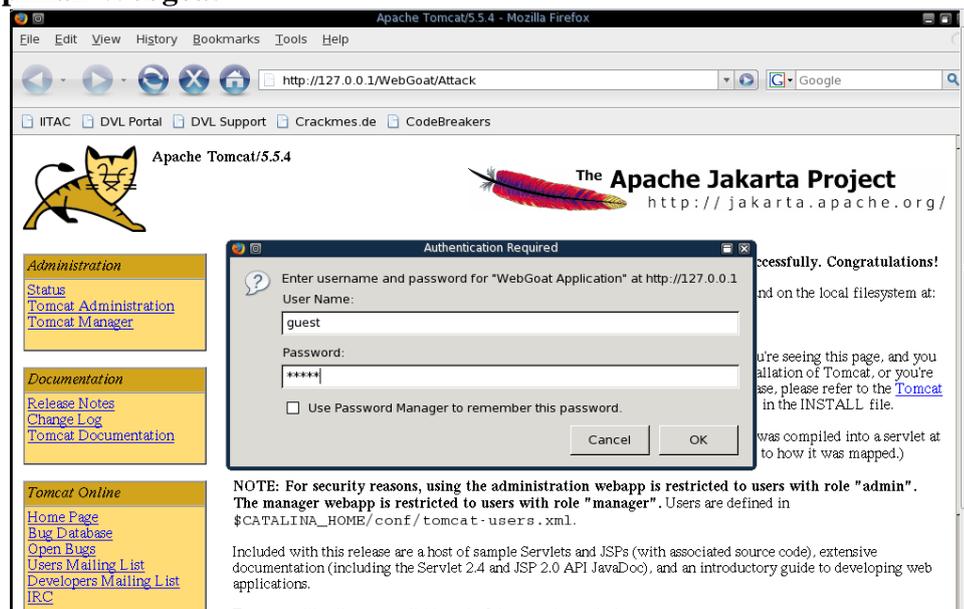
Langkah ini dilakukan untuk memeriksa service apa saja yang terbuka pada DVL. Dalam hal ini service yang aktif adalah http, ipp, mysql, http-proxy, vnc dan x11. Pada tab version adalah versi yang digunakan oleh service tersebut dan dapat digunakan untuk mengetahui kelemahan dari service tersebut dengan bantuan website seperti <https://cve.mitre.org> atau website lainnya.

5. Setting DVL untuk menjalankan Webgoat pada port 80



Langkah ini untuk menjalankan salah satu service yang ada pada DVL untuk melakukan percobaan Exploitasi yaitu WebGoat yang di setting agar berjalan di port 80. Web Goat sendiri adalah sebuah project open source yang digunakan sebagai media pembelajaran web hacking.

6. Tampilkan Webgoat



Setelah melakukan setting web goat pada port 80, selanjutnya kita akses webgoat tersebut dengan cara input `http://127.0.0.1/WebGoat/Attack` pada address bar di web browser. IP address 127.0.0.1 adalah IP address lokal. Setelah kita akses alamat tersebut maka akan tampil form login untuk masuk ke dalam webgoat.

7. Tampilkan hasil webgoat yaitu OWASP dan ASPECT SECURITY



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



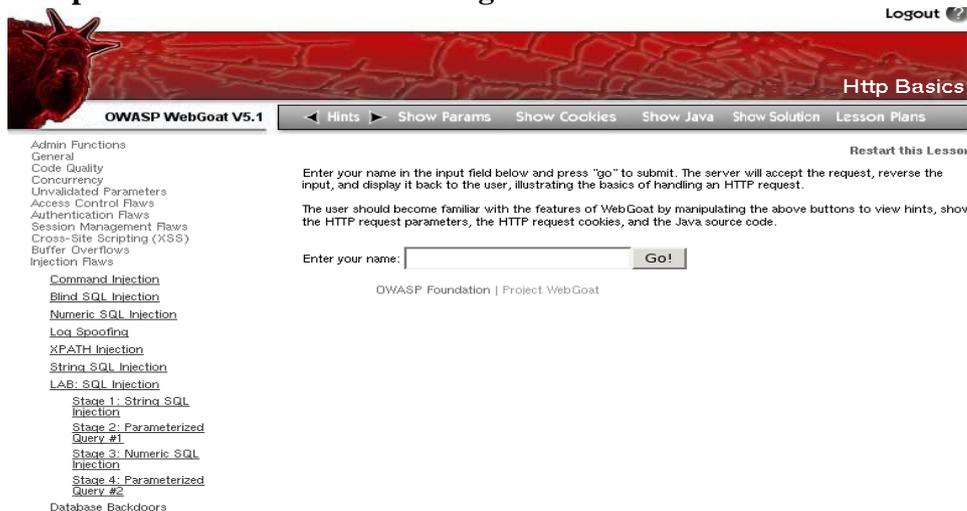
ASPECT SECURITY
Application Security Specialists

<p>WebGoat Design Team</p> <p>Bruce Mayhew David Anderson Rogan Dawes Laurence Casey (Graphics)</p> <p>Special Thanks for V5.1</p> <p>OWASP Spring of Code Erwin Geirnaert (http://www.zionsecurity.com/)</p> <p>To all who have sent comments</p>	<p>Lesson Contributors</p> <p>Aspect Security Sherif Koussa Romain Brechet</p> <p>Documentation Contributors</p> <p>Sherif Koussa (http://www.macadamian.com/) Erwin Geirnaert (http://www.zionsecurity.com/)</p>
---	---

[Start WebGoat](#)

Setelah berhasil login maka akan muncul OWASP dan ASPECT SECURITY. Hal ini dikarenakan DVL menggunakan WebGoat versi lama dan di sarankan untuk mengupdatenya, banyak perbaikan bug dan beberapa update.

8. Tampilkan installasi OWASP webgoat VS.1



Logout

Http Basics

Restart this Lesson

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.

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.

Enter your name: [Go!](#)

OWASP Foundation | Project WebGoat

Setelah kita klik "Start Webgoat" kita harus menginput last name untuk menginstall WebGoat. Hal ini dikarenakan WebGoat adalah sebuah aplikasi web yang dikelola oleh OWASP dan dirancang sebagai media pelajaran keamanan aplikasi web. WebGoat memiliki lebih dari satu pelajaran tentang hacking, petunjuk hacking, dan solusi untuk terhindar dari hacking.

9. Tampilkan hasil instalasi OWASP webgoat VS.1 dengan last name 'smith'

OWASP WebGoat V5.1

String SQL Injection

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

Salah satu contoh instalasi ketika kita input last name "smith" maka akan muncul data table yang berisi USER_DATA, FIRST_NAME, LAST_NAME, CC_NUMBER, CC TYPE, COOKIE dan LOGIN_COUNT. Data yang dipatikan dengan input last name "smith" pada OWASP wegoat VS.1 memiliki 2 data saja, itu berarti terdapat 2 kali instalasi dengan last name "smith".

10. Tampilkan hasil instalasi OWASP webgoat VS.1 dengan last name "test' or 1=1"

*** 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

Berbeda hasilnya jika kita input last name "test' or 1=1 .." maka akan tampil banyak data.

ANALISA

Eksplorasi keamanan jaringan adalah sebuah cara untuk melakukan serangan terhadap target dengan melemahkan keamanan pada server target untuk mencuri data-data yang ada di dalam server tersebut. Salah satu contohnya adalah penyerangan terhadap website untuk mencuri data ataupun melumpuhkan website tersebut dengan SQL Injections.

Dalam kasus ini percobaan untuk melakukan serangan tersebut dapat dilakukan dengan menggunakan DVLP sebagai media penyerangan. Di dalam DVLP terdapat sebuah aplikasi open source yang dapat digunakan untuk bahan pembelajaran dalam hacking. Aplikasi tersebut salah satunya adalah WebGoat.

WebGoat adalah aplikasi open source untuk media pembelajaran hacking yang dikembangkan oleh OWASP. Webgoat sendiri adalah sebuah web dengan keamanan yang sangat rendah sehingga dapat dengan mudah diserang.