

Keamanan Jaringan Komputer



Disusun Oleh

Nama : Kusuma Dwi Indriani

NIM : 09011181320017

**JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA**

2017

ACTUAL EXPLOIT

Exploit adalah sebuah kode yang menyerang keamanan komputer secara spesifik. Exploit banyak digunakan untuk penetrasi baik secara legal ataupun ilegal untuk mencari kelemahan (Vulnerability) pada komputer tujuan. Bisa juga dikatakan sebuah perangkat lunak yang menyerang kerapuhan keamanan (security vulnerability) yang spesifik namun tidak selalu bertujuan untuk melancarkan aksi yang tidak diinginkan. Banyak peneliti keamanan komputer menggunakan exploit untuk mendemonstrasikan bahwa suatu sistem memiliki kerapuhan.

Berikut tahapan yang dilakukan pada saat hands di Laboratorium Jaringan Komputer:

1. Melalui virtual box dijalankan dua virtual machine yaitu Damn Vulnerable Linux (DVL) dan os linux. Terdapat dua hal yang perlu dilakukan saat akan menjalankan kedua virtual machine tersebut diantaranya, setting network pada kedua virtual machine ke 'internal network' dan pada general setting operating sistem pilih Linux 2.6.x hal tersebut karna saat memilih operating sistem yang lain tidak akan terjadi booting.
2. Masukkan ip address masing-masing virtual machine dengan ketentuan
 - DVL = 192.168.1.1
 - Linux ubuntu = 192.168.1.5

```

root@mahasiswa:/home/mahasiswa# ifconfig eth0 192.168.1.5 netmask 255.255.255.0
root@mahasiswa:/home/mahasiswa# ifcon
ifcon: command not found
root@mahasiswa:/home/mahasiswa# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1b:fb:a1
          inet addr:192.168.1.5  Bcast:192.168.1.255  Mask:255.
255.255.0
          inet6 addr: fe80::a00:27ff:fe1b:fba1/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:6 errors:0 dropped:0 overruns:0 frame:0
TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1464 (1.4 KB)  TX bytes:12247 (12.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host

```

Gambar 1. Pemberian IP address pada ubuntu

```

bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:B4:D8:C0
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:54 errors:0 dropped:0 overruns:0 frame:0
          TX packets:196 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12444 (12.1 KiB)  TX bytes:15270 (14.9 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:85 errors:0 dropped:0 overruns:0 frame:0
          TX packets:85 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:9520 (9.2 KiB)  TX bytes:9520 (9.2 KiB)

```

Gambar 2. Pemberian IP address pada DVL

- Melakukan proses scanning menggunakan nmap melalui ubuntu (gambar 5) dan melalui DVL (gambar 6)

```

root@mahasiswa:/home/mahasiswa# nmap -sV -p 22 192.168.1.1
Starting Nmap 6.40 ( http://nmap.org ) at 2017-02-23 10:15 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 192.168.1.1
Host is up (0.0012s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.4 (protocol 1.99)
MAC Address: 08:00:27:B4:D8:C0 (Cadmus Computer Systems)

Service detection performed. Please report any incorrect result
s at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
root@mahasiswa:/home/mahasiswa#

```

Gambar 3. Nmap ke DVL melalui ubuntu

```

bt ~ # nmap -O 192.168.1.5
Starting Nmap 4.20 ( http://insecure.org ) at 2017-02-23 02:59 GMT
Warning: OS detection for 192.168.1.5 will be MUCH less reliable because we did not find at least 1 open a
nd 1 closed TCP port
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP
port
All 1697 scanned ports on 192.168.1.5 are closed
MAC Address: 08:00:27:1B:FB:A1 (Cadmus Computer Systems)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/ .
Nmap finished: 1 IP address (1 host up) scanned in 19.147 seconds
bt ~ #

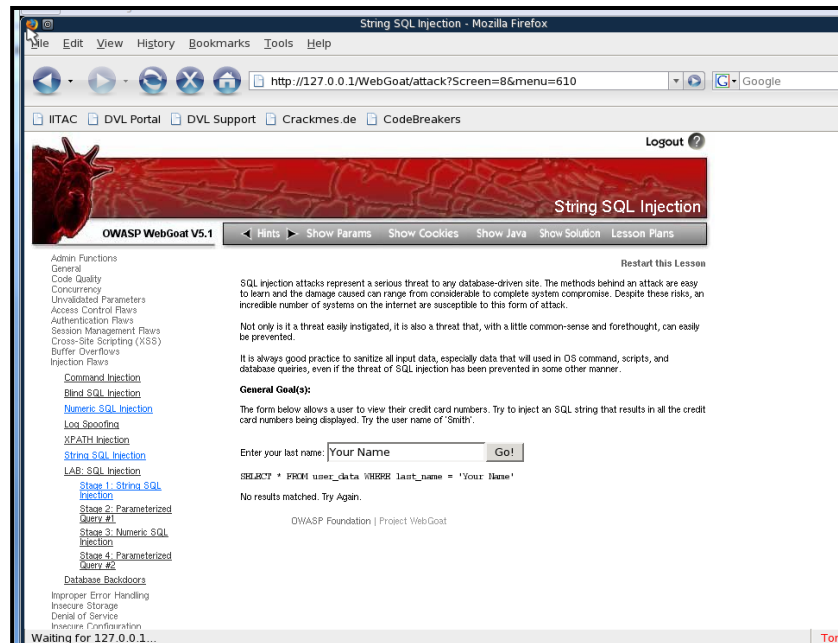
```

Gambar 4. Nmap Ubuntu ke DVL

4. Ada beberapa kesalahan yang dilakukan oleh admin diantaranya :
- Bruteforce : mencoba melakukan input password ke sistem menggunakan tools. Tools tersebut berupa John The Ripper dan Hydra.
 - Salah konfigurasi
 - Salah implementasi : kurang cermat pada saat melakukan proses coding(tidak melakukan filter input).

Cara mengatasi salah implementasi

- Buka DVL
- Buka web browser Mozilla, masukkan url <http://127.0.0.1/WebGoat/attack>
- Masukkan username ; guest dan password;guest
- Saat telah login kemudian pilih String SQL injection ditunjukkan seperti pada gambar 5



Gambar 5. Hasil setelah login pada WebGoat serangan injeksi SQL merupakan ancaman serius ke situs database-driven. Metode balik serangan yang mudah untuk

dipelajari dan kerusakan yang disebabkan dapat berkisar untuk melengkapi sistem.

- Contoh yang dapat dilakukan pada pilihan String SQL injection seperti pada gambar 6 dan gambar 7.

String SQL Injection

OWASP WebGoat V5.1

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
Loop Spoofing
XPath 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

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 noticeable 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:

SQL:?' * 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	0
102	John	Smith	4352209902222	AMEX	0	0

OWASP Foundation | Project WebGoat

Gambar 6. Hasil penggunaan String SQL injection

String SQL Injection

OWASP WebGoat V5.1

Access Control Flaws
Authentication Flaws
Session Management Flaws
Cross-Site Scripting (XSS)
Buffer Overflows
Injection Flaws

Command Injection
Blind SQL Injection
Numeric SQL Injection
Loop Spoofing
XPath 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
AJAX Security
Challenge

increase 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:

SQL:?' * 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	0
101	Joe	Snow	223420065411	MC	0	0
102	John	Smith	243560002222	MC	0	0
102	John	Smith	4352209902222	AMEX	0	0
103	Jane	Plane	123456789	MC	0	0
103	Jane	Plane	333498703333	AMEX	0	0
10312	Jolly	Hersey	176696789	MC	0	0
10312	Jolly	Hersey	33300003333	AMEX	0	0
10323	Grumpy	White	673834489	MC	0	0
10323	Grumpy	White	33413003333	AMEX	0	0
15603	Peter	Sand	123609789	MC	0	0
15603	Peter	Sand	338893453333	AMEX	0	0
15613	Joseph	Something	33843453333	AMEX	0	0

OWASP Foundation | Project WebGoat

*** Congratulations. You have successfully completed this lesson.
* But 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.**

Gambar 7. Hasil penggunaan String SQL injection

5. Bug adalah kesalahan yang terjadi pada komputer baik disebabkan oleh perangkat lunak (software) ataupun perangkat keras (hardware) sehingga mempengaruhi kinerja komputer. Berikut jenis-jenis bug :

- Divide by Zero
- Infinite Loop
- Buffer Overflow
- Deadlock
- Memory Leak
- Access Violation
- Off by One Error