UTS CEH Praktikum



Kelompok :

Belinda Permata P. (00000023490)

Michael Sihotang(00000022711)

Michael Roni(00000026087)

Muhammad Farrel Adivia(00000025885)

**Universitas Multimedia Nusantara**

**Tangerang, Indonesia**

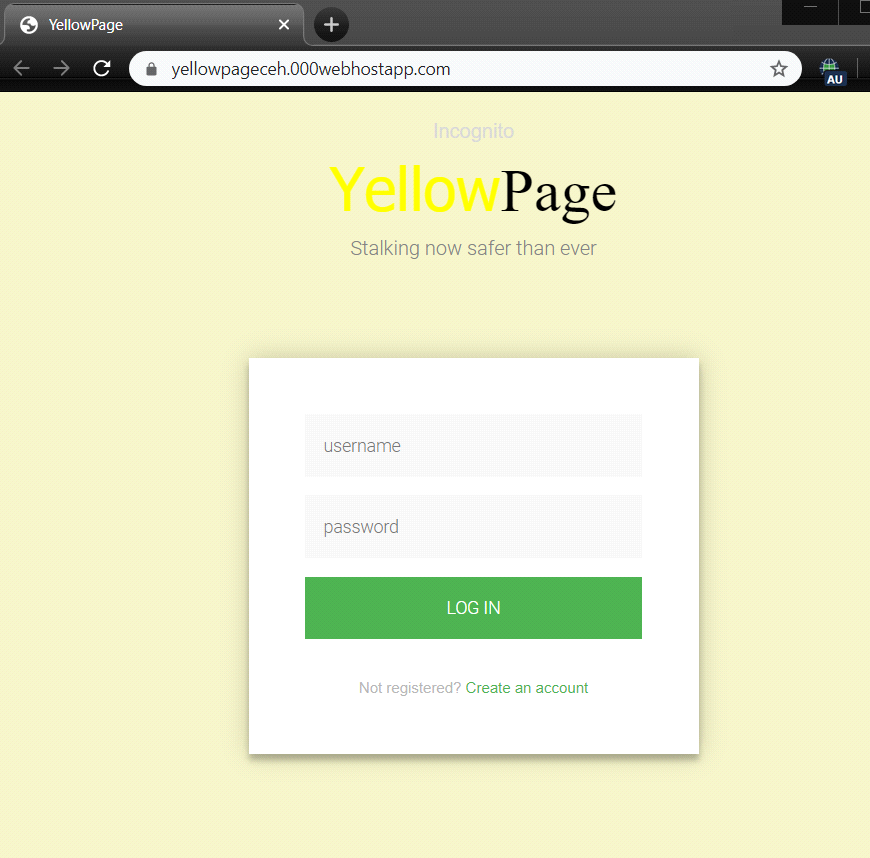
**2020**

# **Parameter Tampering**

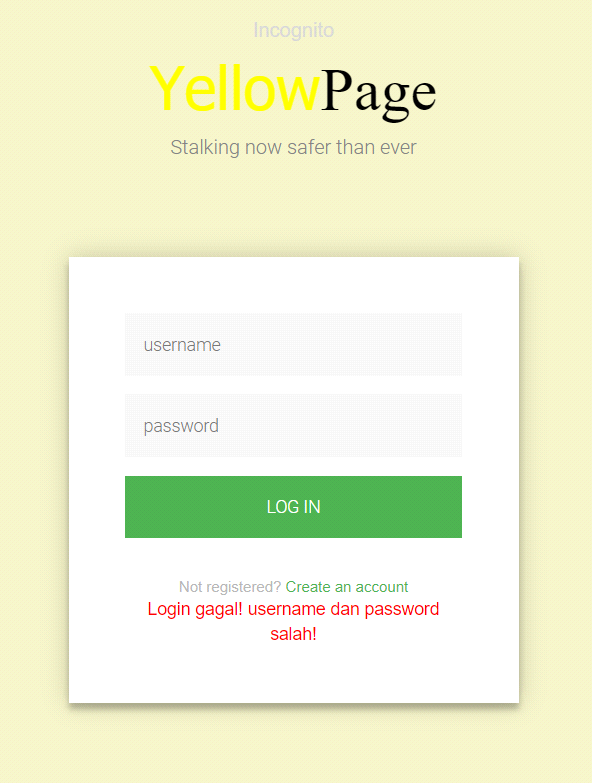
Parameter tampering adalah sebuah attack yang dapat dilakukan kepada web yang melakukan passing parameter dengan metode GET yang membuat valuenya muncul pada url sehingga dapat dimodifikasi dengan mudah.

Berikut adalah contoh cara melakukan parameter tampering pada sebuah website yang vulnerable terhadap attack ini

Step01 : Akses <https://yellowpageceh.000webhostapp.com/>



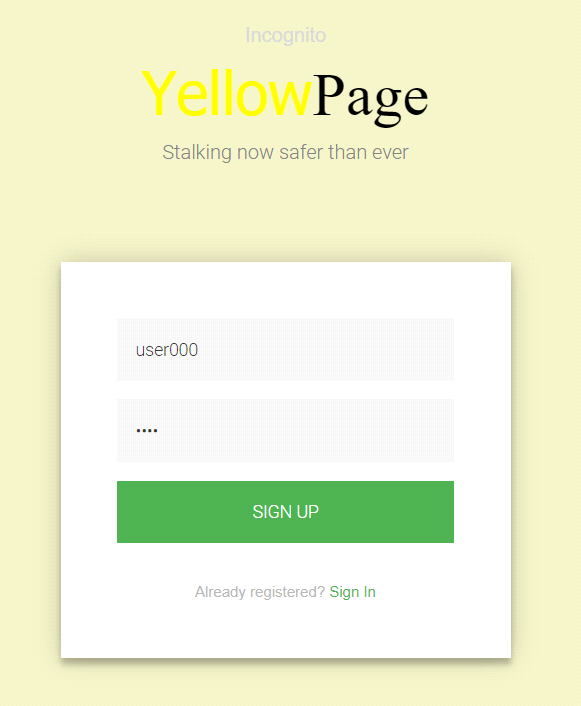
Step02 : Coba login dengan username dan password kosong untuk mengecek security / logika login page



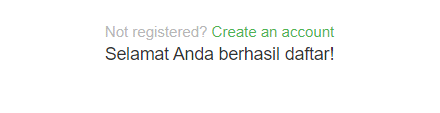
Berdasarkan hasil uji coba diatas, dapat diketahui bahwa kemungkinannya login page memiliki logika login yang membandingkan data input user dengan data yang terhubung / tersimpan pada web. Untuk mengetahuinya lebih lanjut, coba untuk daftar sebagai user.

Step03 : Buat akun baru dengan mengklik "create an account"

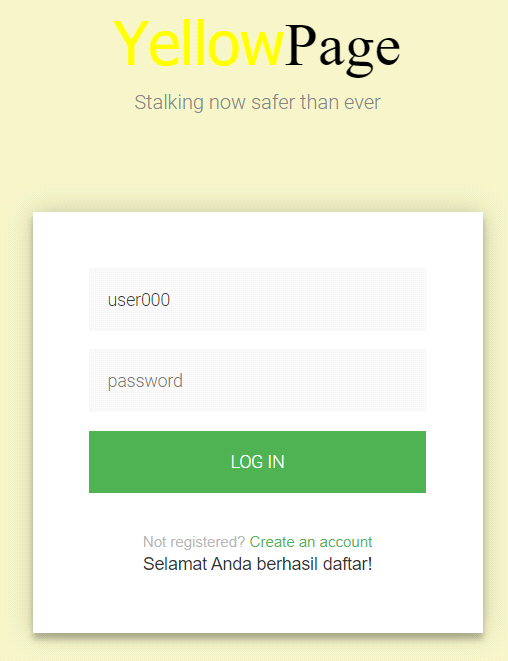
Gunakan "user000" sebagai username dan "1234" sebagai password lalu klik sign up



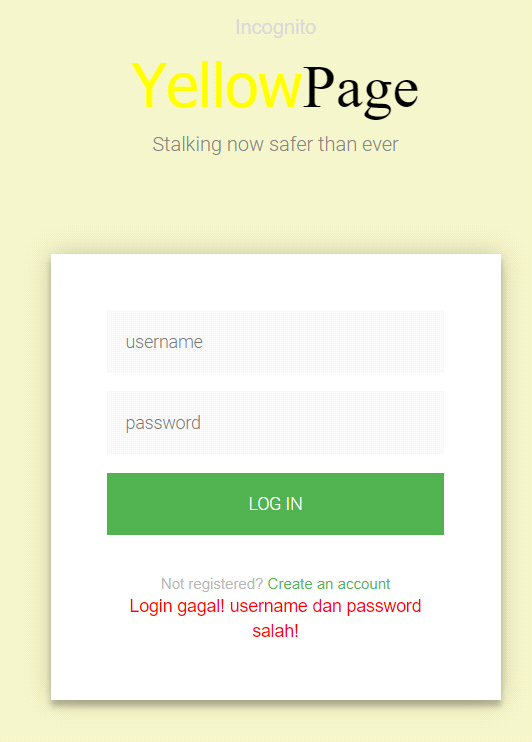
Ketika berhasil, akan muncul message "Selamat Anda berhasil daftar!"



Step04 : Coba login dengan username terisi dan password dibiarkan kosong

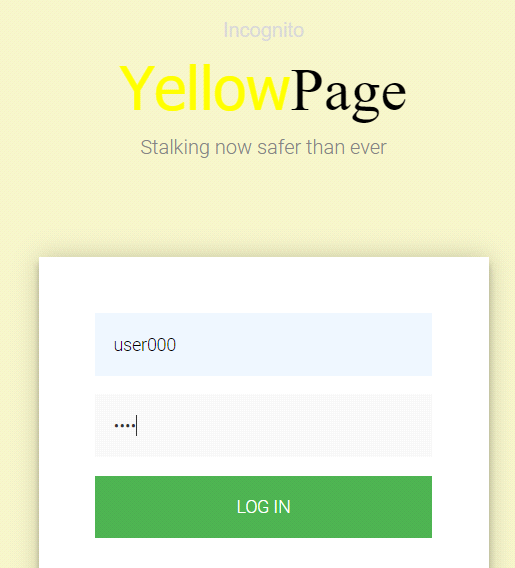


Hasilnya adalah message yang sama seperti jika kedua field dibiarkan kosong



Berdasarkan hasil diatas, dapat disimpulkan bahwa logika login akan membandingkan input user untuk kedua field dan membandingkannya dengan data yang ada. Username dan password harus sesuai dengan data, tidak bisa hanya dengan satu field saja yang terisi.

Step05 : Sekarang login dengan data yang digunakan untuk mendaftar

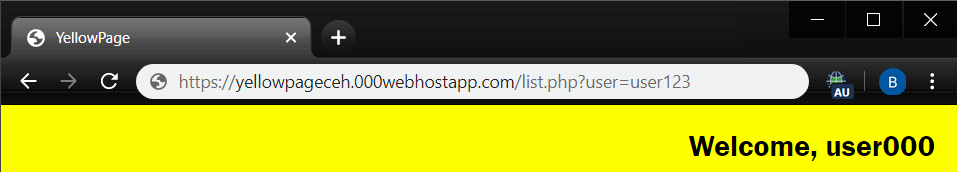


Berikut adalah tampilan halaman awal ketika berhasil login

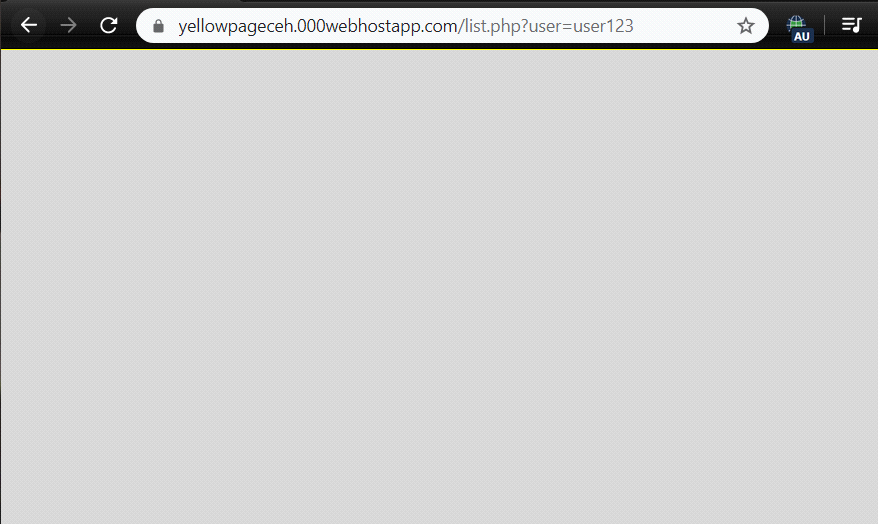


Dapat dilihat pada pojok kanan atas terdapat message Welcome dan username yang digunakan untuk login, lalu pada url terdapat parameter berupa user=user000

Step06 : Coba ubah parameter user pada url secara random, misalnya menjadi "user123"

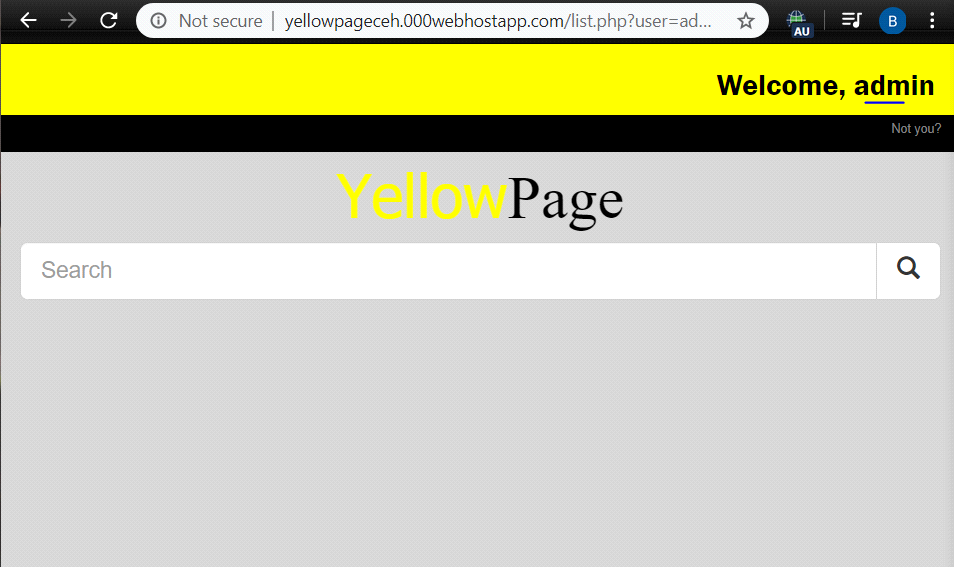


Hasilnya halaman akan menjadi blank dan tidak bisa lagi menggunakan fitur search



Step06: Ubah parameter user dengan nama user yang terdaftar.

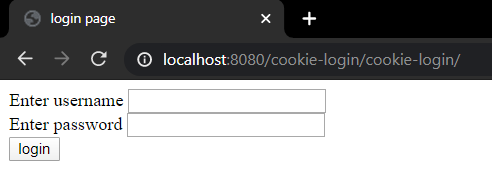
Misalnya "admin"



Hasil diatas menunjukkan bahwa user dengan username "admin" terdaftar dan parameter tampering berhasil dilakukan. Sekarang searching dapat dilakukan dengan menggunakan akun milik admin.

# **2.Cookie Manipulation**

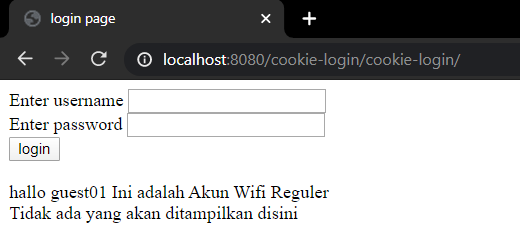
1. Misal ada sebuah page login sebagai berikut



Sebagai pengunjung hotel yang hanya bisa menggunakan wifi reguler (free) kita diminta untuk mendapatkan kode Wifi vip dari sebuah kamar hotel yang berkelas deluxe tanpa memesan sebuah kamar. Diketahui kamar yang telah dipakai pelanggan adalah kamar deluxe 01.

Maka:

2. Coba Login dengan akun reguler/guest

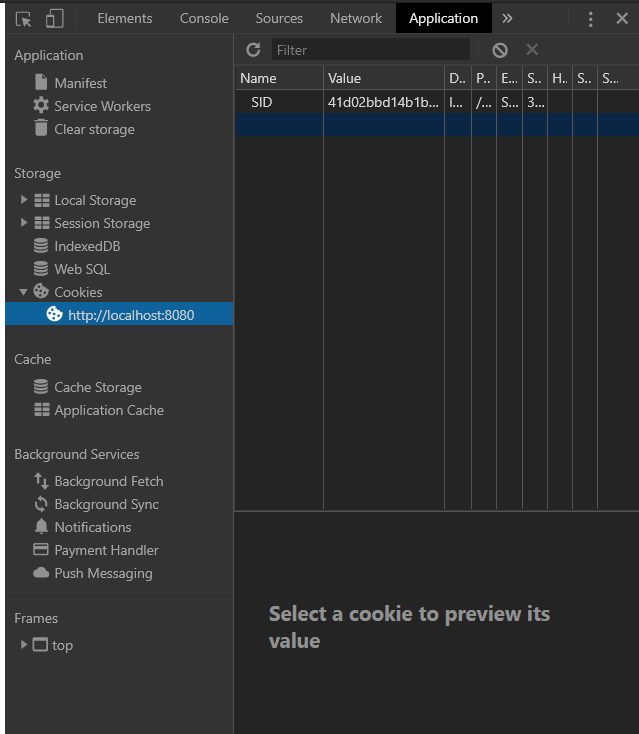


Akan muncul info bahwa kita sedang mengakses atas nama guest01.

3. Lakukan Inspect element

langkah berikutnya klik kanan pada web browser > Inspect Element > pilih tab "Application"

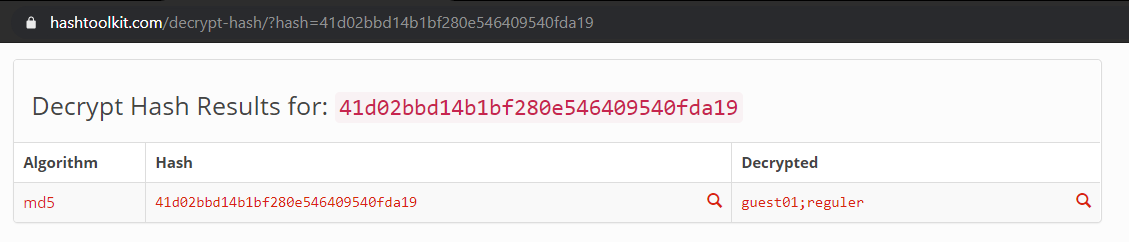
maka akan muncul seperti gambar dibawah:



Setelah masuk Tab "Application" > klik "Cookies" pada bar Storage maka akan muncul sebuah SID dengan kode : 41d02bbd14b1bf280e546409540fda19

4. Lakukan decrypt pada SID tersebut

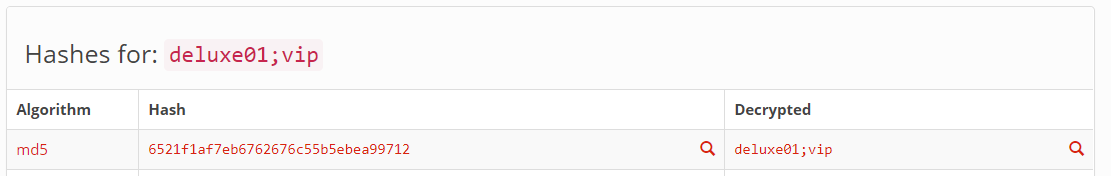
copy SID tersebut lalu masukkan kode tersebut pada situs hashtoolkit.com untuk melakukan decrypt



Ditemukan pola dari cookies page login tersebut berupa guest01;reguler

5. Lakukan encrypt dengan pola yang telah didapatkan

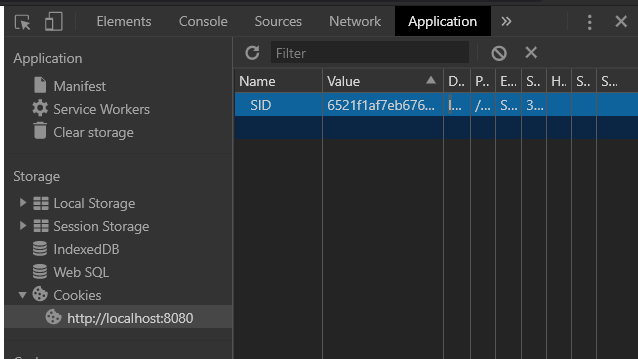
sebagai pengguna reguler pola cookies tersebut adalah guest01;reguler sehingga jika kita ingin menggunakan layanan wifi VIP pada kamar deluxe 01 kita harus merubah hash deluxe01;vip kedalam md5.



md5(deluxe01;vip) = 6521f1af7eb6762676c55b5ebea99712

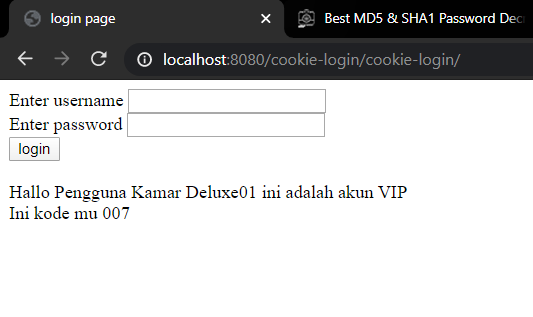
6. Ubah SID dengan hasil hash yang baru

Ubahlah SID yang lama menjadi SID yang baru kita dapat dari hasil md5 deluxe01;vip

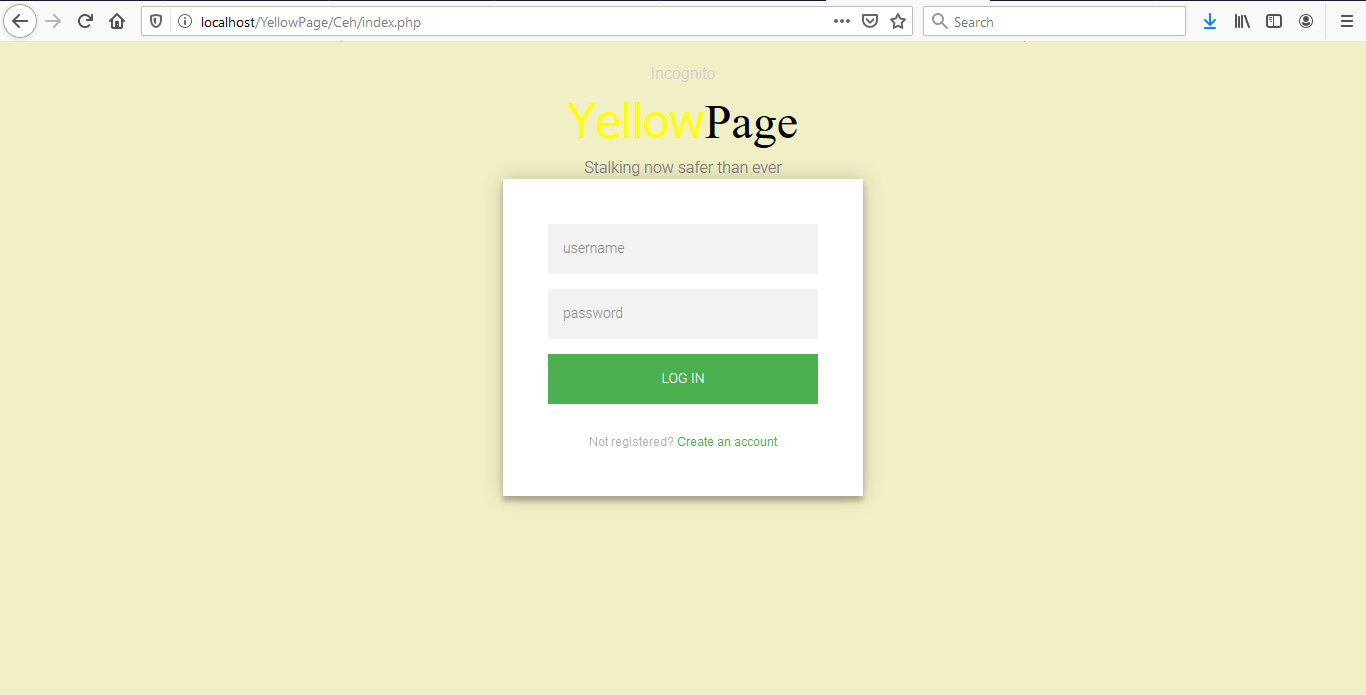


7. Refresh dan lihat apa yang terjadi

selamat anda mendapatkan akses wifi vip

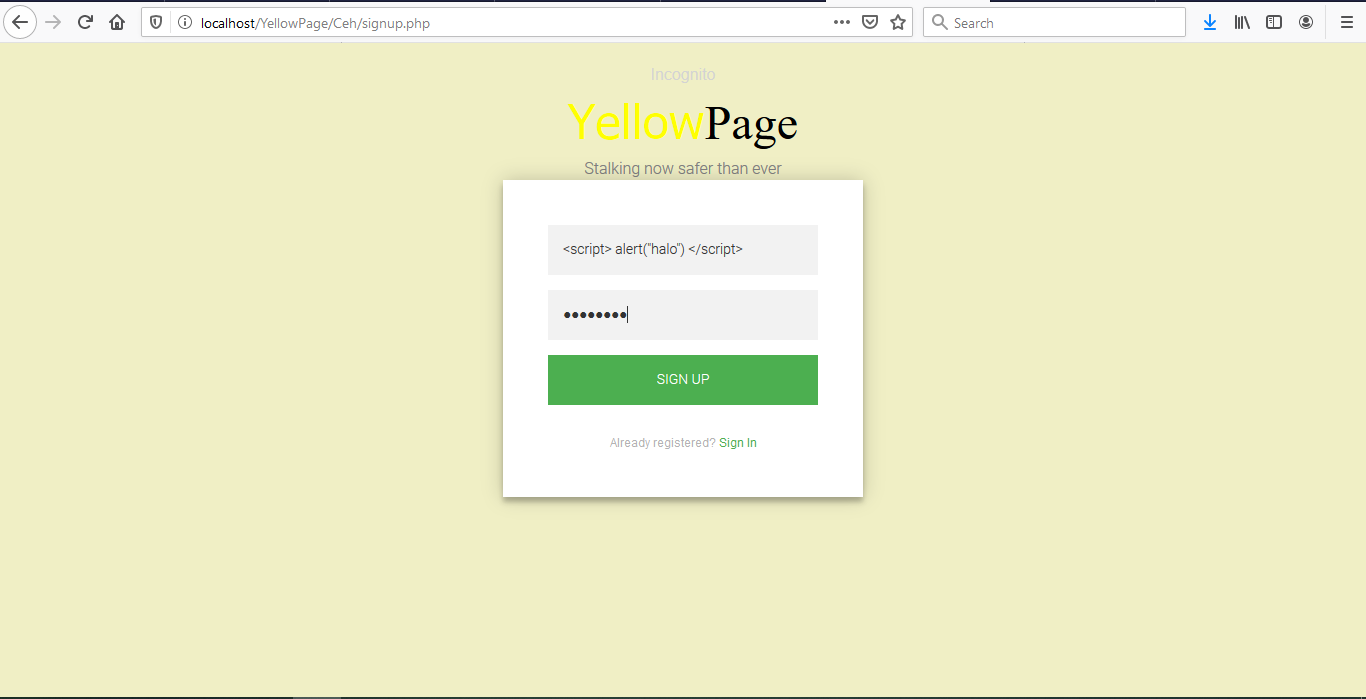


# **3. Cross Site Scripting**

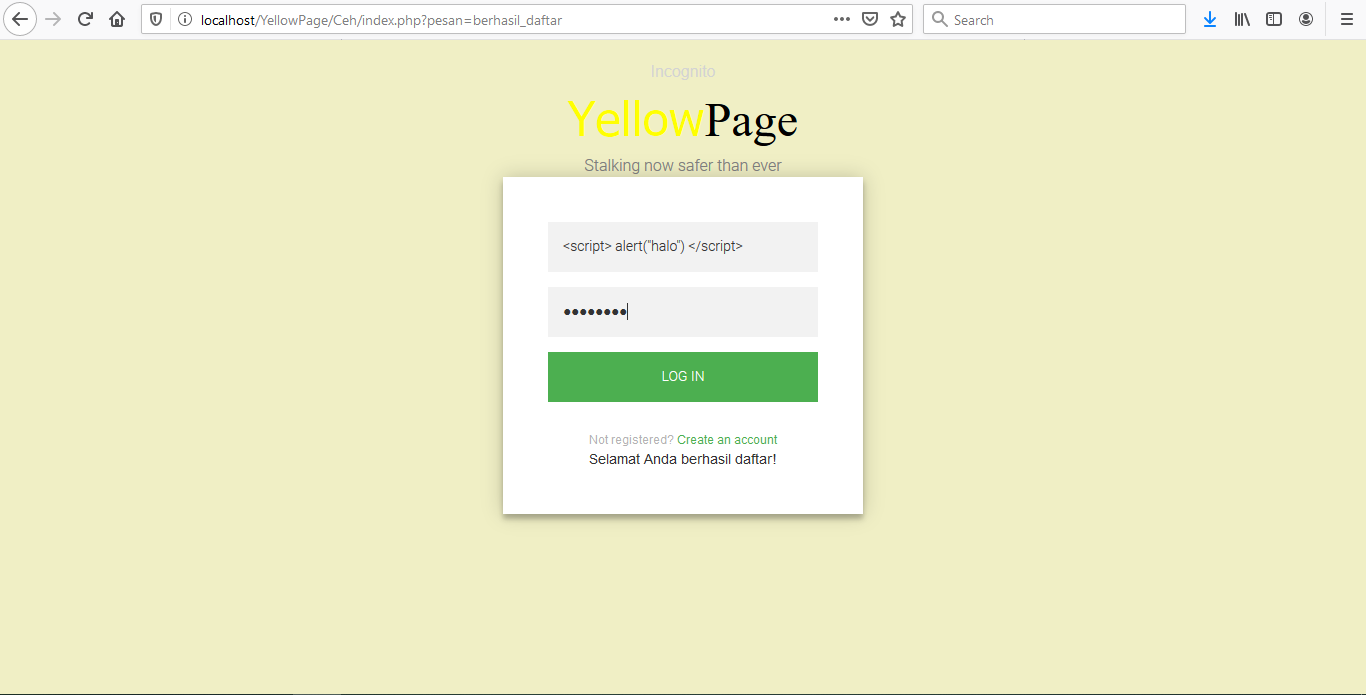


Kita mempunyai akun yang login dengan menggunakan username dan password

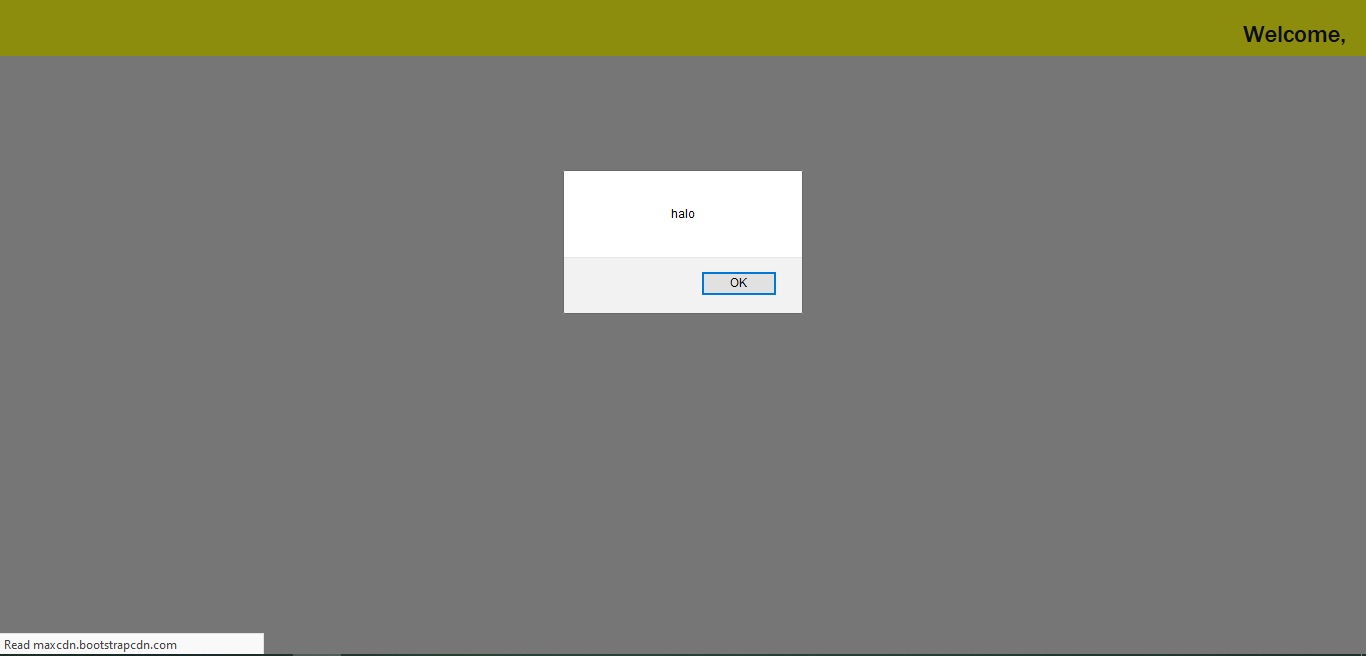
Pertama2 kita buat akun dulu tapi untuk usernamenya kita ganti menggunakan kode yang ingin kita inject



Lalu buat akun tersebut



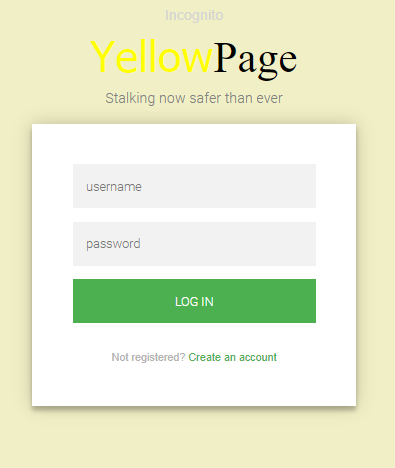
Login dengan akun yang sama



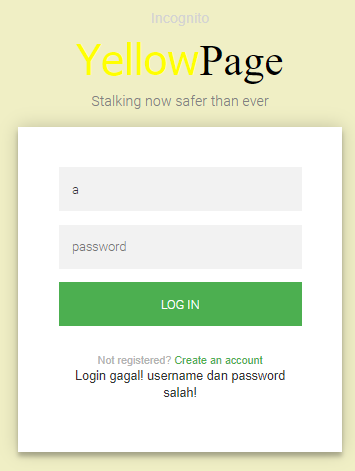
Script akan dijalankan waktu kita login. Di bagian script tadi kita bisa ganti dengan kode2 yang lebih berbahaya tentunya.

# **4. SQL INJECTION**

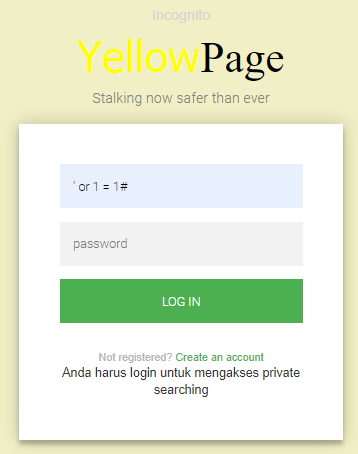
1. Misalkan ada sebuah website Yellowpage yang mengharuskan kita untuk login sebelum membuka isinya seperti berikut. Untuk mengakses yellowpage tersebut bisa mengunjungi link berikut <http://yellowpageceh.000webhostapp.com/>



Jika kita coba asal isi form loginnya, maka hasilnya seperti ini.

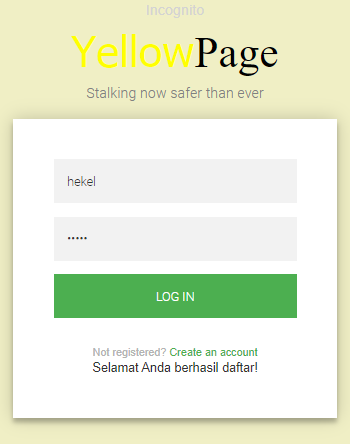


Karena salah, maka selanjutnya adalah melakukan percobaan untuk melakukan sql injection terhadap login tersebut dengan mengisi username dengan ’ or 1 = 1#



Dari hasil tersebut bisa kita lihat bahwa error yang diberikan berbeda dengan error yang salah password. Berarti bisa diketahui bahwa webnya melakukan pengecekkan kembali terhadap username yang ada didalam websitenya.

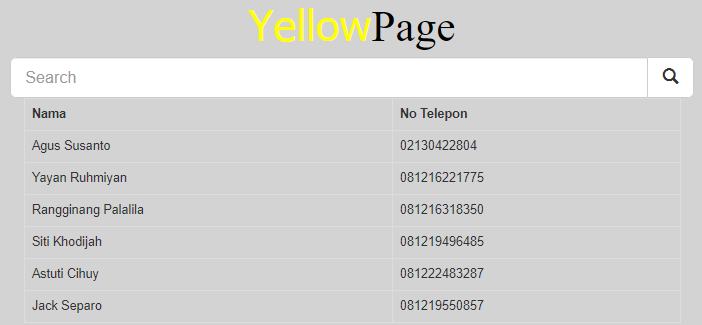
1. Karena tidak bisa menggunakan code tersebut, maka perlu melakukan sign up dan login. Disini kita akan menggunakan username hekel untuk proses signupnya dan dilanjutkan dengan login.



1. Setelah login maka akan ditampilkan tampilan seperti berikut



Tampilan ini berisi form untuk searching yang dapat berguna untuk mencari nomor telepon siapa yang ingin kit cari. Untuk menampilkan semuanya, kita bisa tinggal klik search tanpa mengisi form searchnya.



1. Dari sini bisa diasumsikan website ini menggunakan database untuk menyimpan data-data mereka, karena itu bisa dicoba untuk melakukan sql injection yang mungkin bisa untuk mendapatkan username dan password dari user-user yang pernah mendaftar disini. Yang pertama dilakukan ada melakukan pengecekan apa saja database yang ada di web tersebut dengan menggunakan

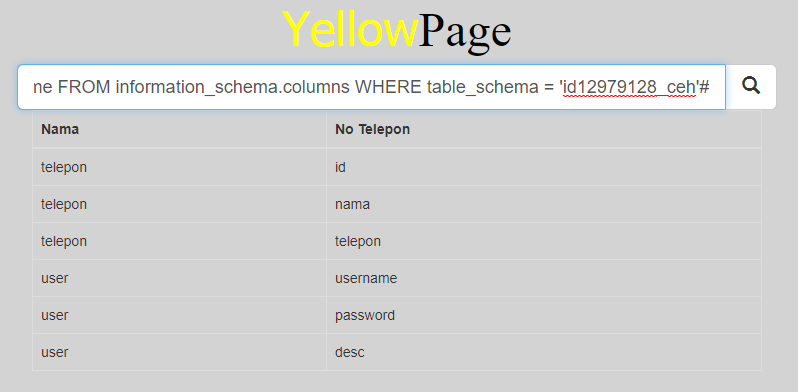
a' UNION SELECT 1,1,schema\_name FROM information\_schema.schemata#

Dari hasilnya dapat kita ketahui bahwa database yang digunakan adalah id12979128\_ceh



1. Setelah mengetahui nama databasenya, yang selanjutnya dilakukan adalah mengetahui isi table dan kolomnya dengan menggunakan

a' UNION SELECT 1,table\_name,column\_name FROM information\_schema.columns WHERE table\_schema = 'id12979128\_ceh'#



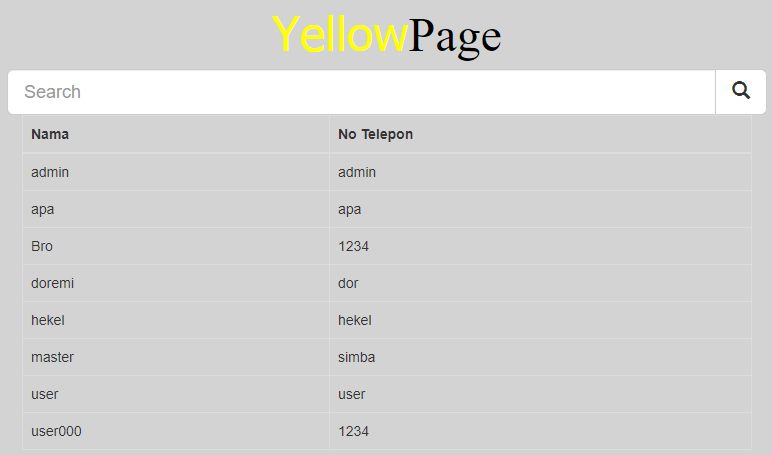
Dari hasil tersebut dapat kita ketahui bahwa isi databasenya adalah sebagai berikut

Telepon : id, nama, telepon

User: username, password, desc

1. Setelah mengetahui bahwa username dan password disimpan pada database id12979128\_ceh dan tabel user, selanjutnya adalah untuk menampilkan isi dari tabel tersebut dengan menggunakan

a' UNION SELECT 1,username,password FROM user#



Dari hasil tersebut bahwa web yellowpage tersebut tidak menggunakan enkripsi untuk menyimpan password-password yang dimiliki oleh user. Karena itu kita dapat langsung mendapat username dan password dari masing-masing user.

1. Selanjutnya adalah melakukan percobaan apakah username dan password yang diperoleh dari sql injection itu benar atau tidak dengan cara mencoba login. Disini kita akan mencoba login dengan username admin dan password admin



Dan benar kita berhasil masuk sebagai admin.