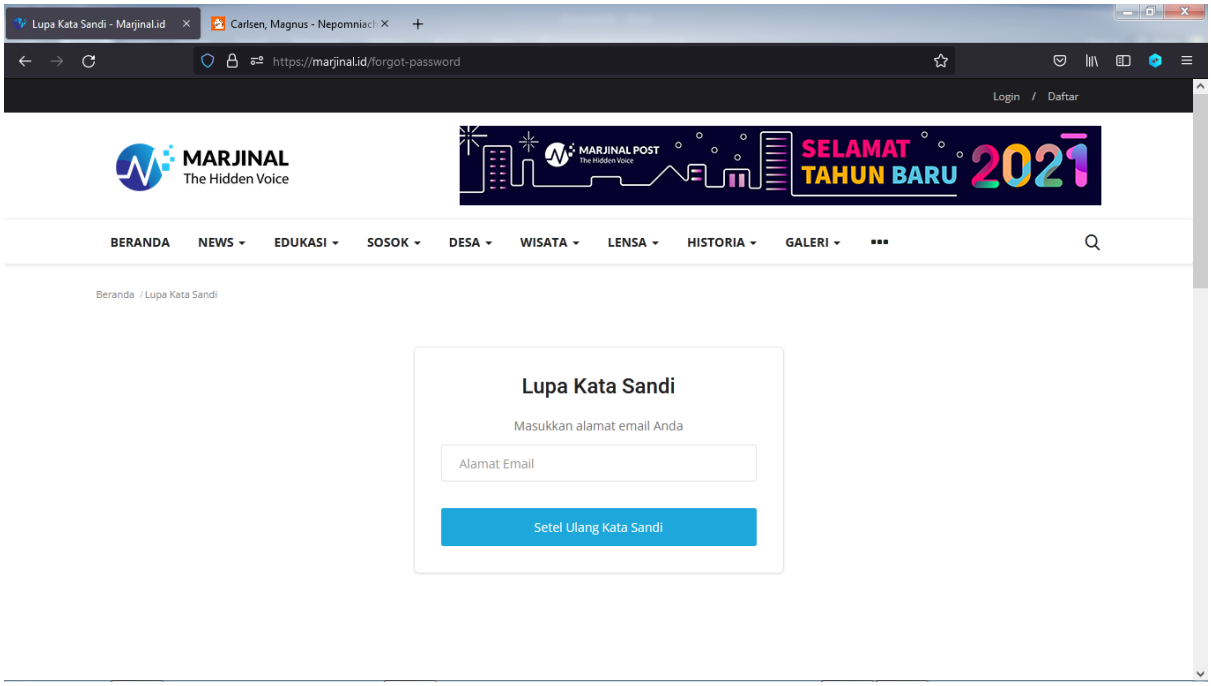
IDOR on Change Password to Account Takeover – marjinal.id

Bug Reporter : Muhammad Bayu Juhri
Bug Severity : Critical
Bug Reference :

1. https://www.linuxsec.org/2018/01/memahami-dan-menemukan-kerentanan.html
2. https://pentestmag.com/i-d-o-r-to-account-takeover/
3. https://rohit443.medium.com/idor-on-password-change-to-full-account-takeover-4d96b9f7f9f0

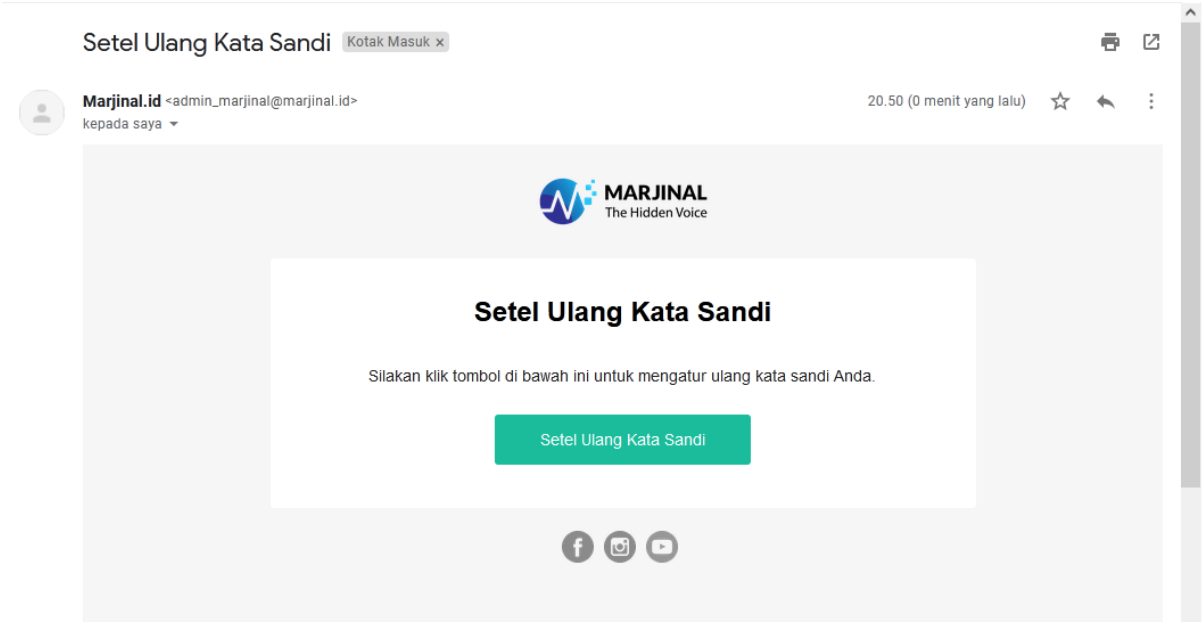
Proof of Concept

Buka situs marjinal.id. Pada menu kanan atas terdapat pilihan untuk Login atau Daftar. Klik Login kemudian pilih Lupa Kata Sandi. Kita akan dialihkan menuju halaman untuk menyetel ulang kata sandi.



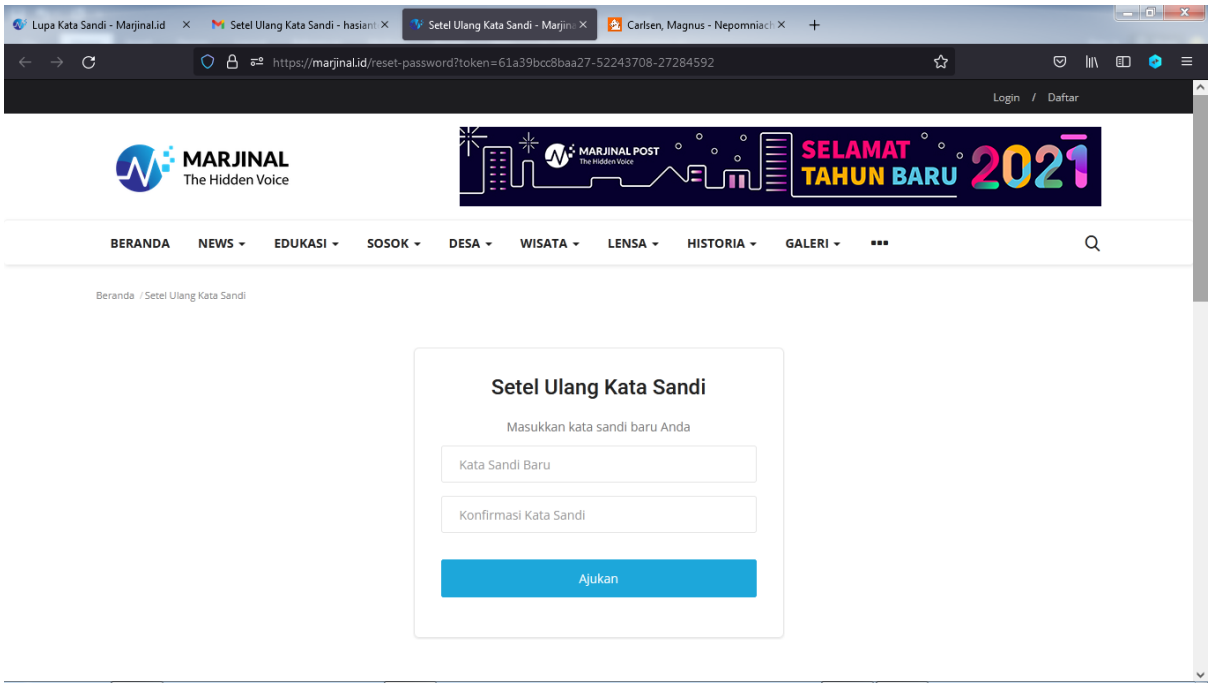
Tampilan halaman reset password

Masukkan email yang sudah didaftarkan kemudian klik tombol Setel Ulang Kata Sandi. Kita akan menerima link untuk mereset kata sandi melalui email.



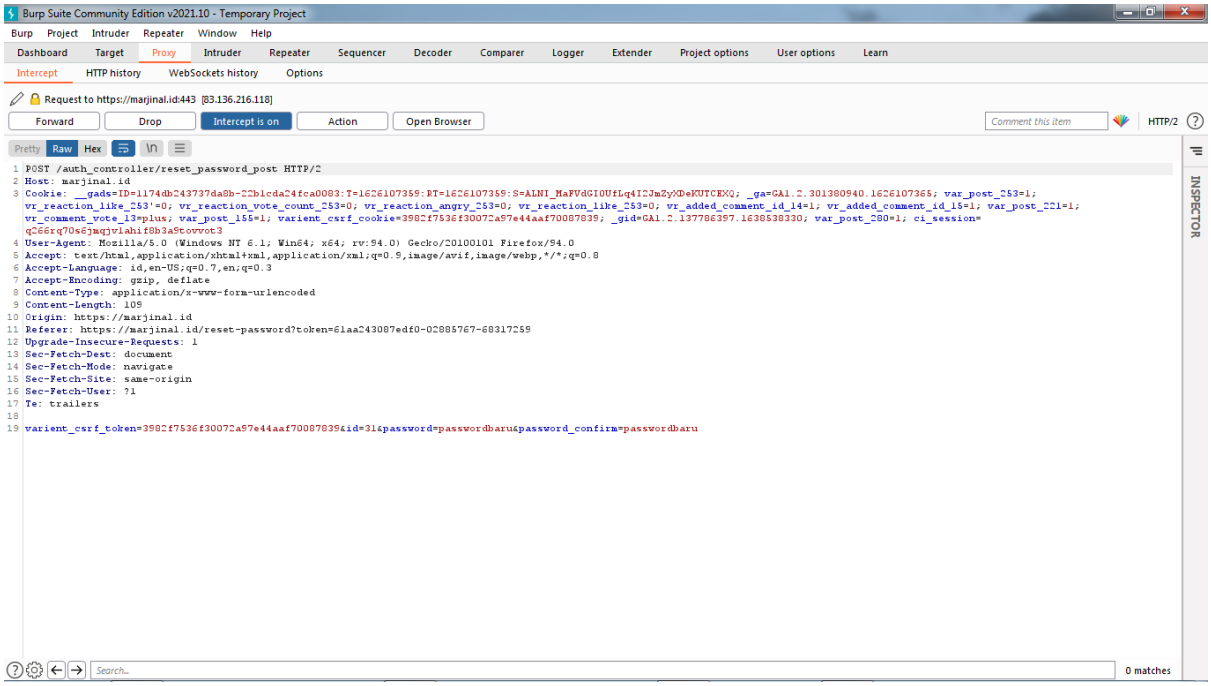
Tampilan pesan untuk reset password

Klik tombol Setel Ulang Kata Sandi yang ada diemail. Kita akan diarahkan menuju halaman untuk memasukkan sandi baru.



Tampilan halaman memasukkan password baru

Masukkan sandi baru yang kita inginkan, kemudian klik tombol Ajukan. Sebelum mengklik tombol Ajukan, saya menghidupkan Burp Suite untuk menangkap dan mengedit request POST yang dikirim.



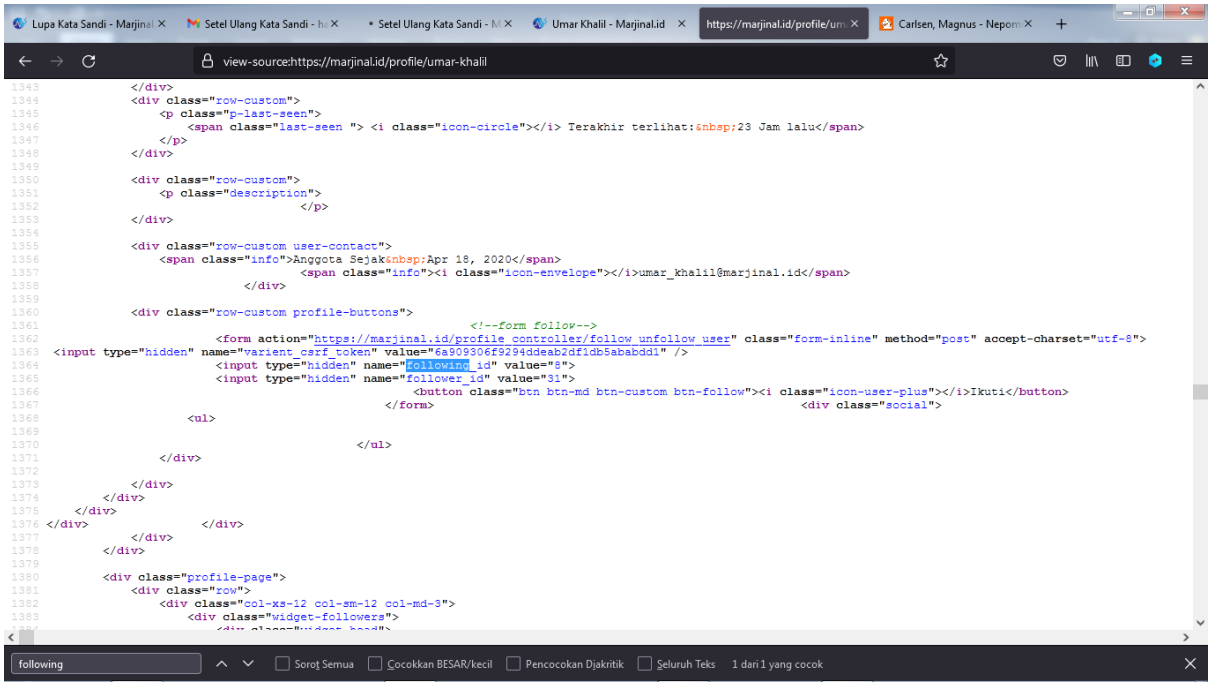
Tampilan Burp Suite menangkap request POST yang dikirim

Dapat dilihat dari gambar di atas, request POST yang dikirim terdiri dari 4 parameter yaitu **varient_csrf_token**, **id**, **password**, dan **password_confirm**. Saya tertarik dengan parameter **id** dimana value dari parameter tersebut diambil dari ID User yang ingin mereset kata sandi. Disini saya mencoba mengubah value dari parameter **id** yang semula 31 (ID User saya) menjadi angka lain (ID User korban).

Sebagai bahan praktik, saya menggunakan akun salah satu penulis yaitu Umar Khalil.

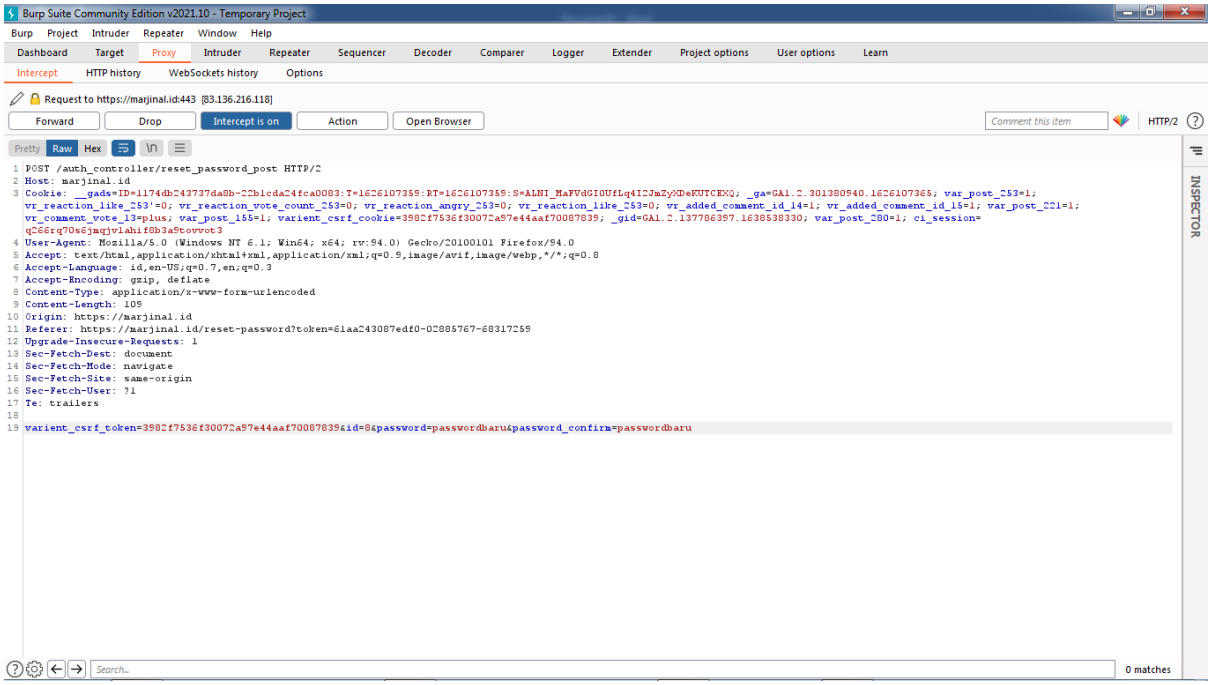
Tampilan akun Umar Khalil

Darimana saya mendapatkan ID User akun Umar Khalil? Caranya Mudah. Klik CTRL+U untuk melihat source website. Kemudian CTRL+F dengan keyword **following_id**.



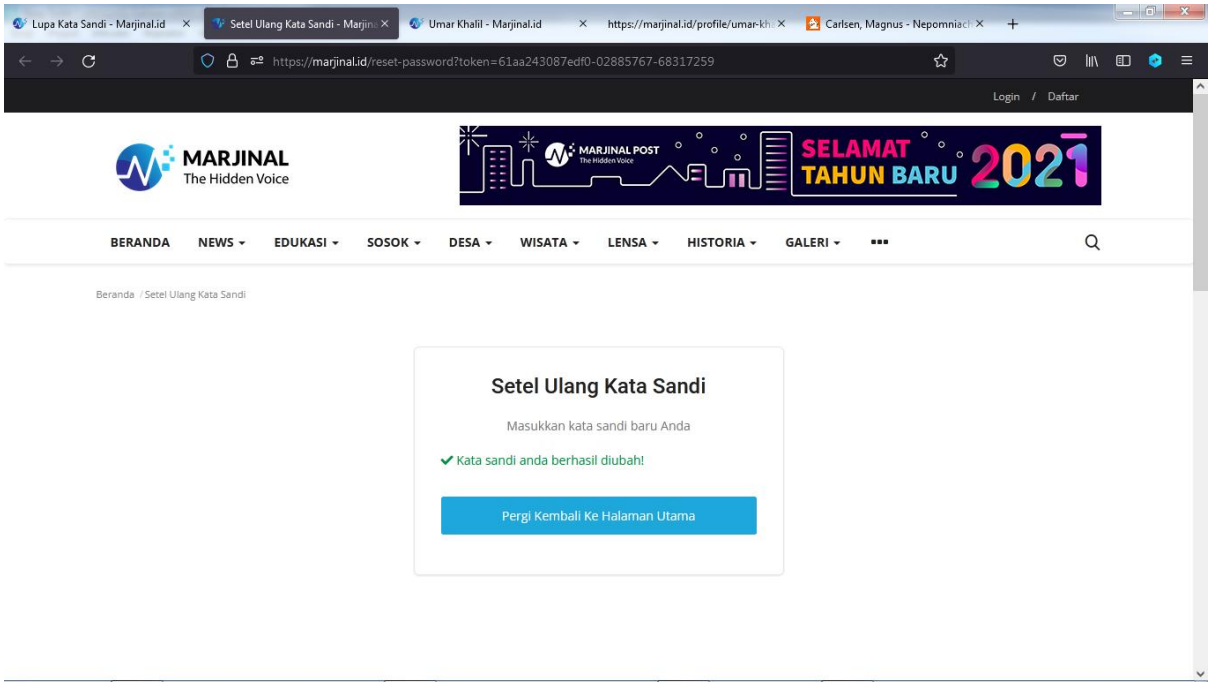
Tampilan view source halaman akun Umar Khalil

Dapat dilihat pada gambar di atas, value dari following_id adalah ID User dari akun Umar Khalil yaitu 8. Karena saya sudah dapat ID User dari akun Umar Khalil, langsung saja saya masukkan di parameter ID pada request POST yang dikirimkan.



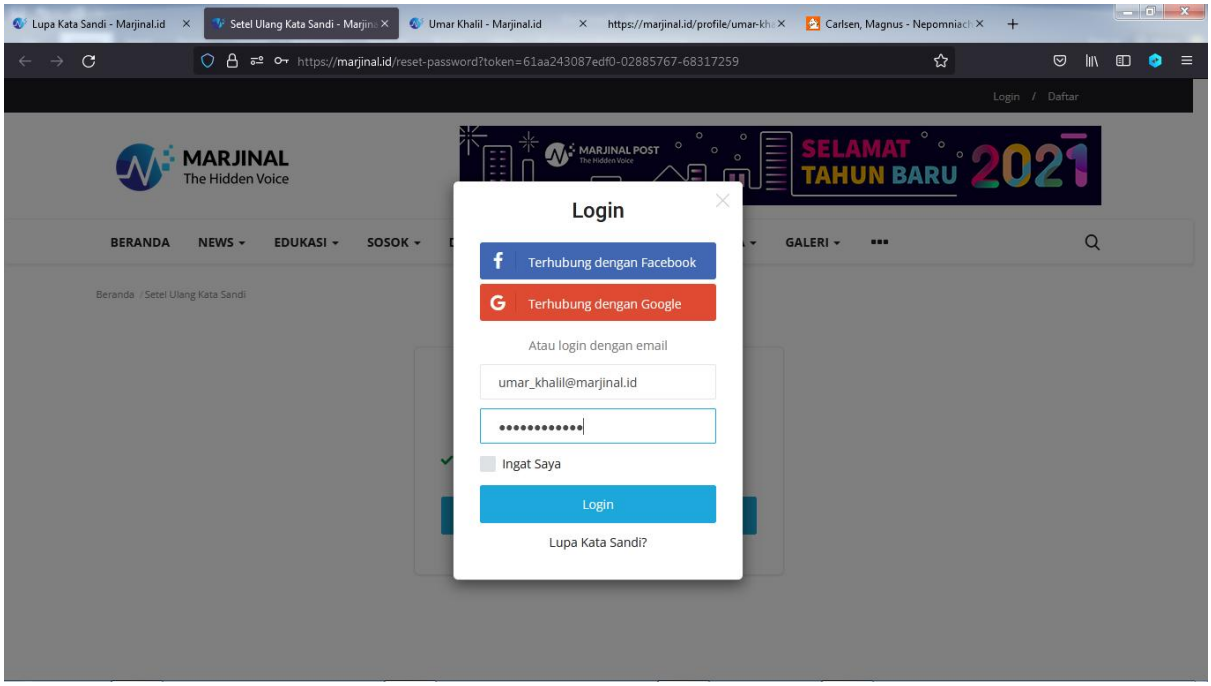
Tampilan ketika mengubah ID User saya menjadi ID User Umar Khalil

Jika sudah, klik Forward untuk mengirimkan request.

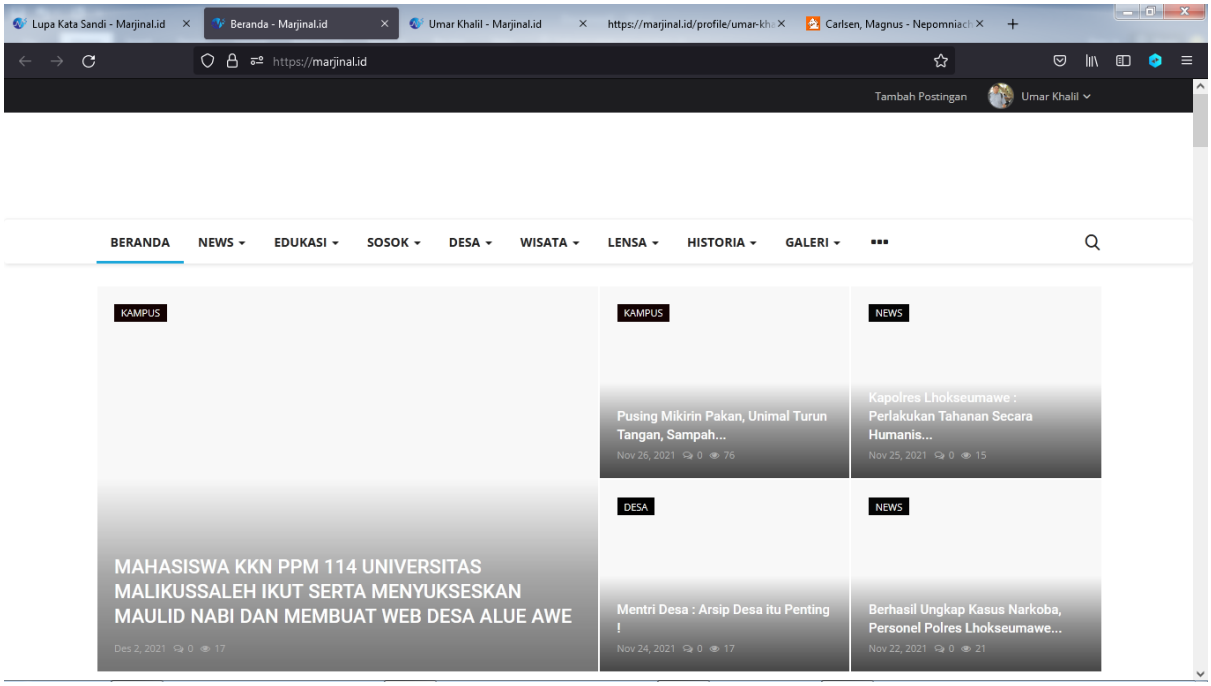


Tampilan notif berhasil reset password

Terlihat pada halaman website, terdapat notif sukses menandakan kata sandi dari akun Umar Khalil berhasil diubah. Untuk membuktikannya, saya mencoba login ke akun tersebut.



Tampilan modal login



Tampilan halaman depan setelah berhasil login

BOOM. Terlihat pada bagian kanan atas terdapat tulisan Umar Khalil yang menandakan saya berhasil login pada akun tersebut.