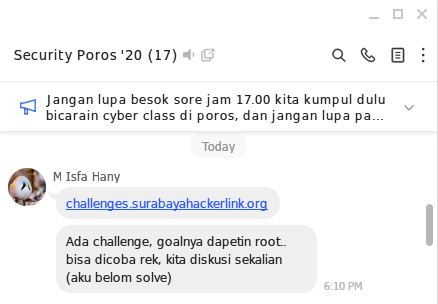
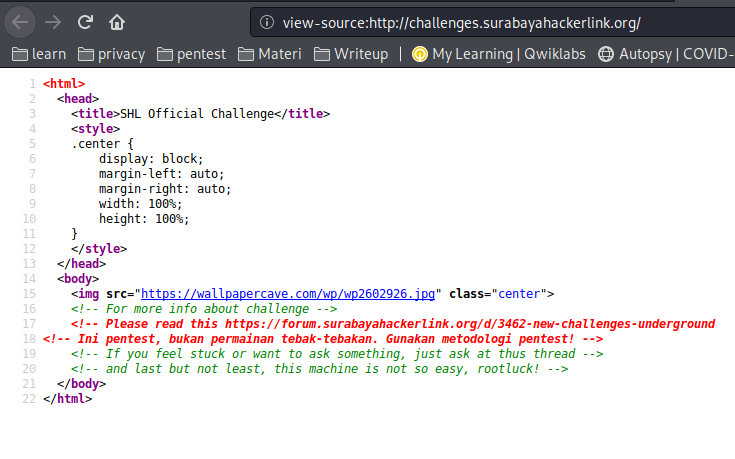
**Write-Up Challenge SHL - Underground**

**By wuvel**

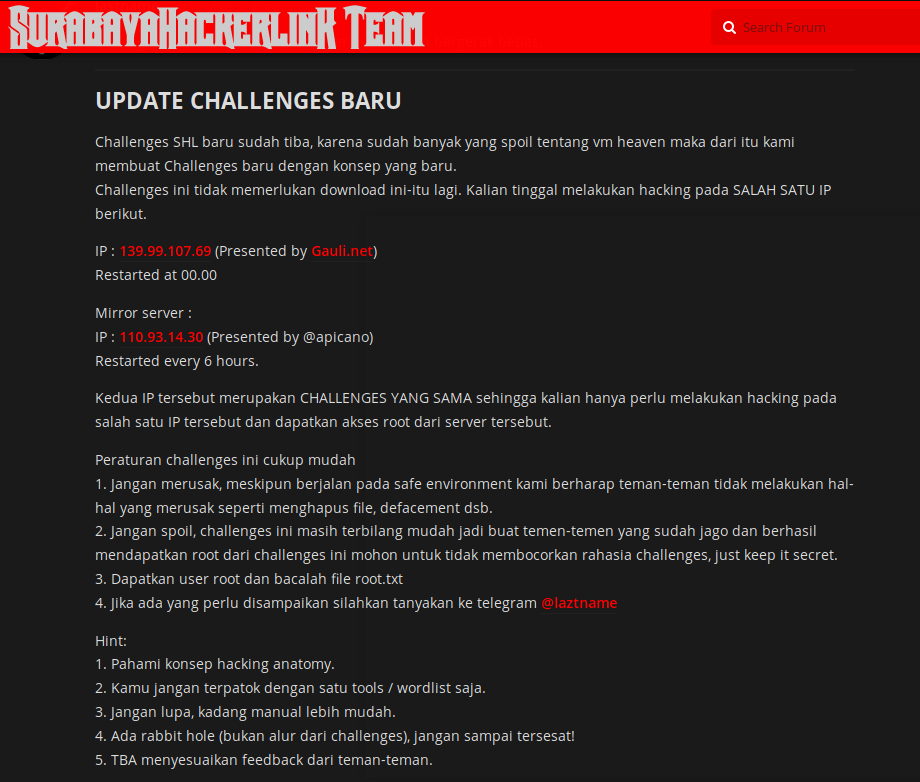
Jadi waktu itu lagi buka line dan kating grup security ngeshare challenge dari SHL (surabaya hacker link) yang goal-nya buat dapetin user root. Karena lagi gabut jadi saya nyoba langsung challenge-nya dengan ngebuka URL tersebut (http://challenges.surabayahackerlink.org/).



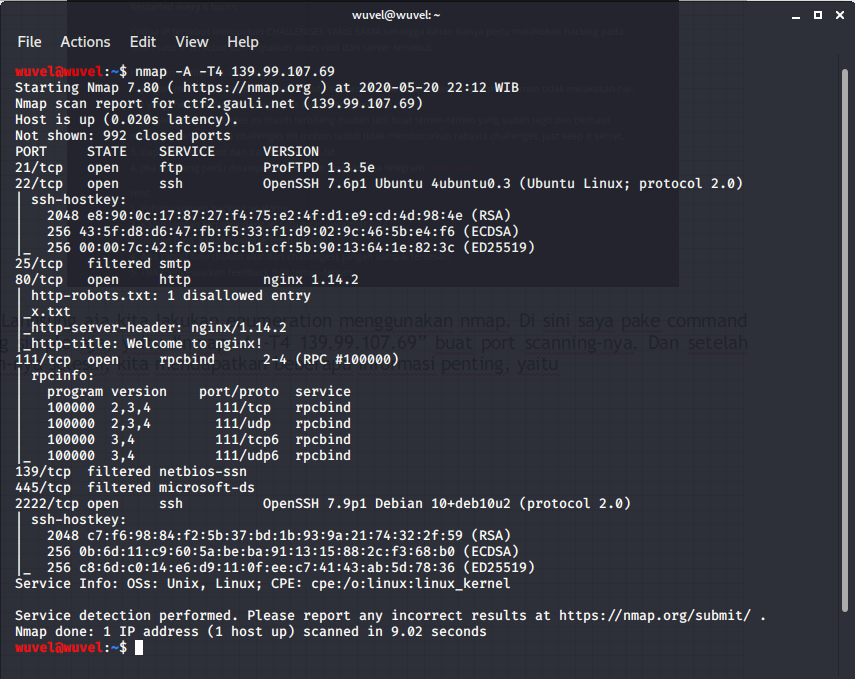
Tampilan pada saat pertama kali ngakses ya cuman gambar rel aja. Langsung aja kita liat source codenya dan kita dapet link buat kita baca (https://forum.surabayahackerlink.org/d/3462-new-challenges-underground).



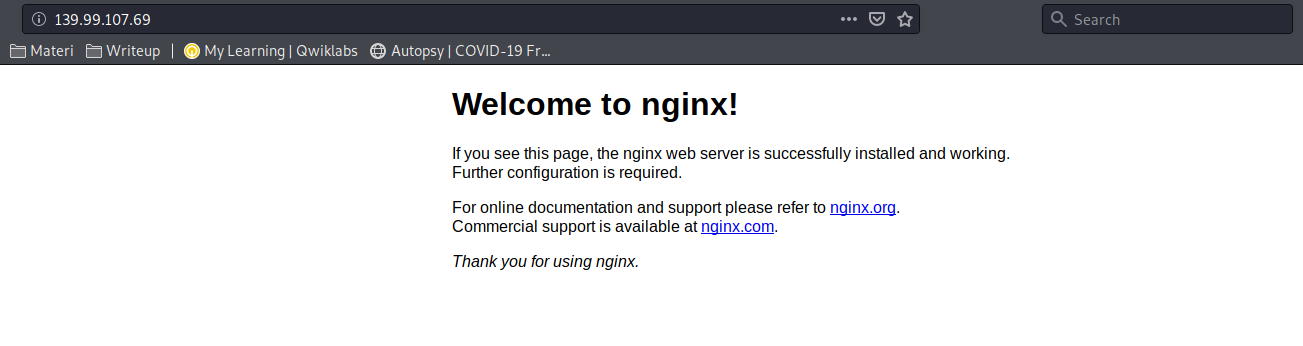
Setelah alamat URL tersebut dibuka, ada panduan seputar challenge baru “underground” ini. Disediakan 2 alamat IP yang dapat kita test langsung. Di sini saya bakal pake alamat IP 139.99.107.69 (Presented by Gauli.net) buat di-test.



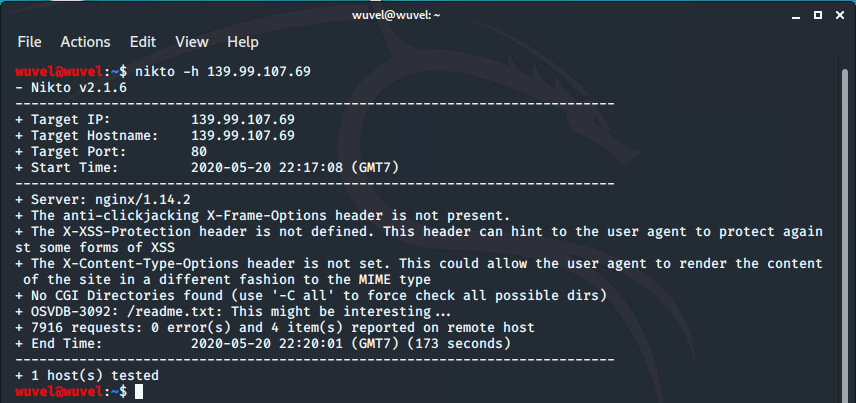
Langsung aja kita lakukan enumeration menggunakan nmap. Di sini saya pake command yang simple aja, yaitu “nmap -A -T4 139.99.107.69” buat port scanning-nya. Dan setelah scan-nya selesai, kita mendapatkan beberapa informasi penting, yaitu port 21 (FTP), 22 (ssh), 80 (http), 111 (rcpbind), dan 2222 (ssh) kebuka.

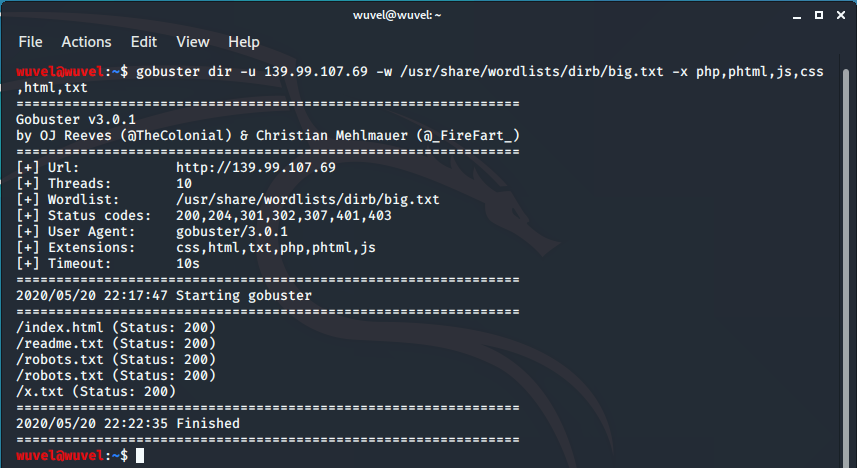


Langsung aja kita cek service httpnya yang ada di port:80.

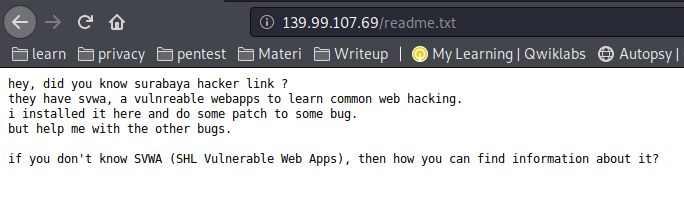


Dan cuman ada tampilan welcome page-nya nginx. Sekarang kita lakukan enumeration lagi untuk nemuin direktori/file-file yang kemungkinan ada di URL ini. Di sini saya bakal pake gobuster dan nikto buat ngelakuin enumeration-nya.

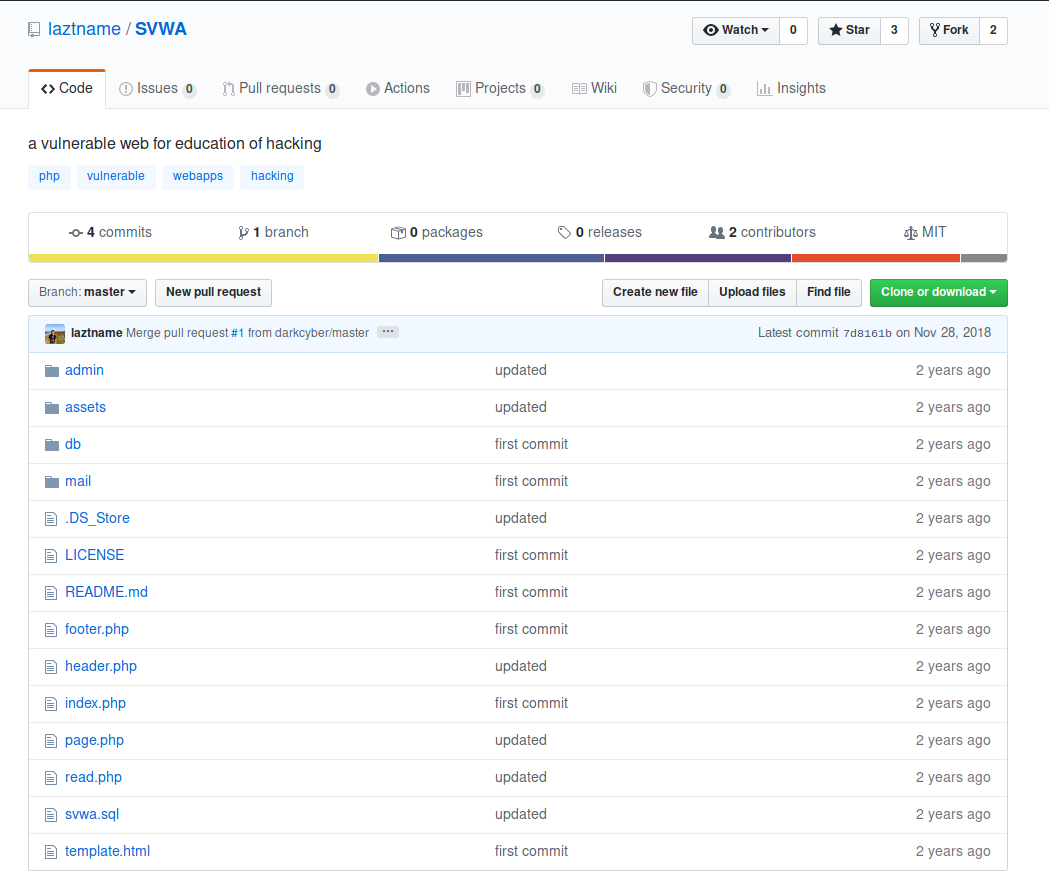




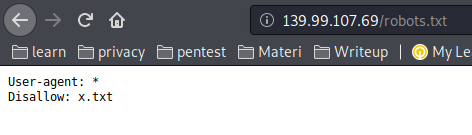
Dari hasil di atas, kita dapet file-file yang menarik. Langsung aja kita cek file readme.txt-nya dulu.

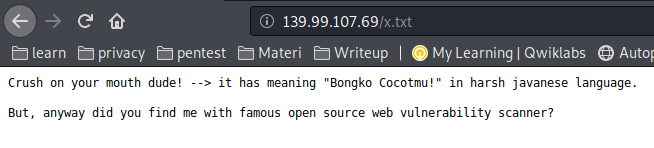


Terdapat tulisan yang intinya itu si pemilik server menginstall projek SVWA (SHL Vulnerable Web Apps) pada host ini. Setelah saya lakukan pencarian pada search engine, saya mendapatkan repository SVWA itu sendiri yang dapat kita lihat semua source codenya (https://github.com/laztname/SVWA).

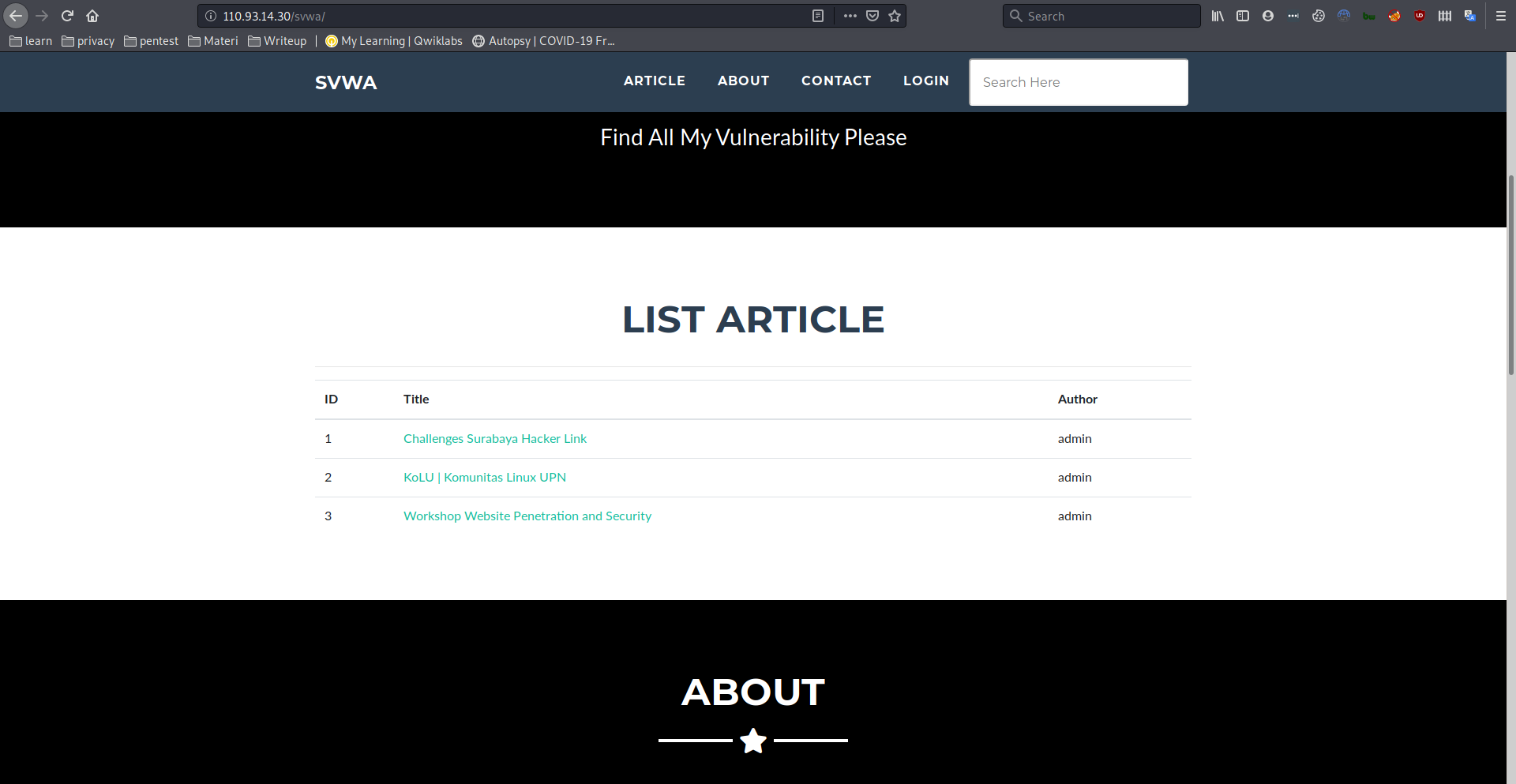


Sebelum lanjut ke svwa, kita cek dulu file menarik lainnya (robots.txt dan x.txt).





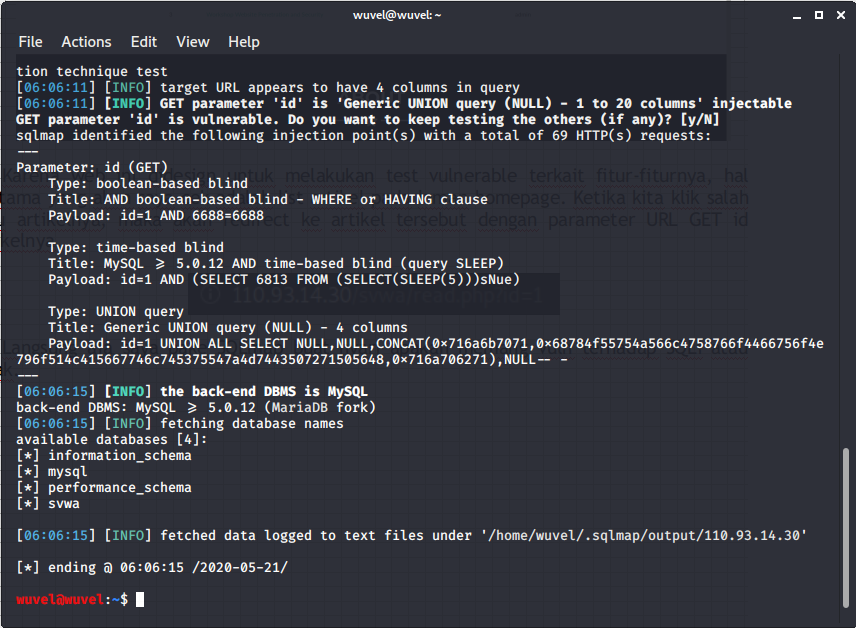
Terdapat file robots yang men-disallow file x.txt untuk dicrawl. Dan isi dari file x.txt itu sendiri adalah tulisan yang intinya bahwa apakah kita menemukan file ini melalui “open source” web vulnerability scanner. Karena tidak ada apa-apa, saya melanjutkan ke direktori svwa tadi yang sudah terinstall di host ini.



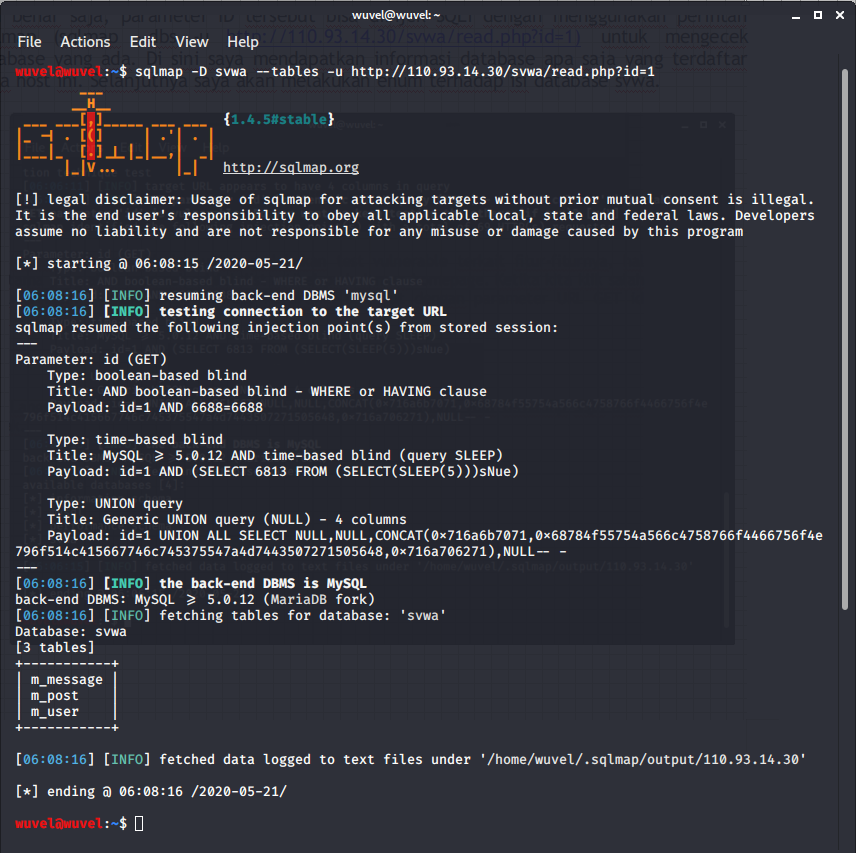
Karena web ini didesign untuk melakukan test vulnerable terkait fitur-fiturnya, hal pertama yang akan saya cek adalah list artikel pada laman homepage. Ketika kita klik salah satu artikelnya, maka akan redirect ke artikel tersebut dengan parameter URL GET id artikelnya.



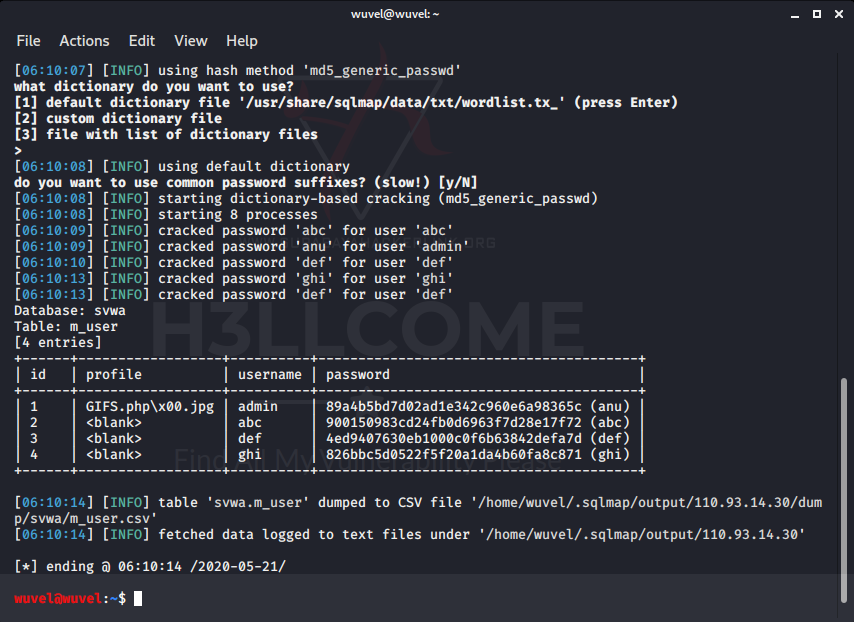
Langsung aja saya pake SQLmap buat nyari apakah memang vuln terhadap SQLi atau tidak. Dan benar saja, parameter ID tersebut bisa diinjek SQLi dengan menggunakan perintah SQLmap (sqlmap --dbs -u <http://110.93.14.30/svwa/read.php?id=1)> untuk mengecek database yang ada. Di sini saya mendapatkan informasi database apa saja yang terdaftar pada host ini. Selanjutnya saya akan melakukan enum terhadap isi database svwa.



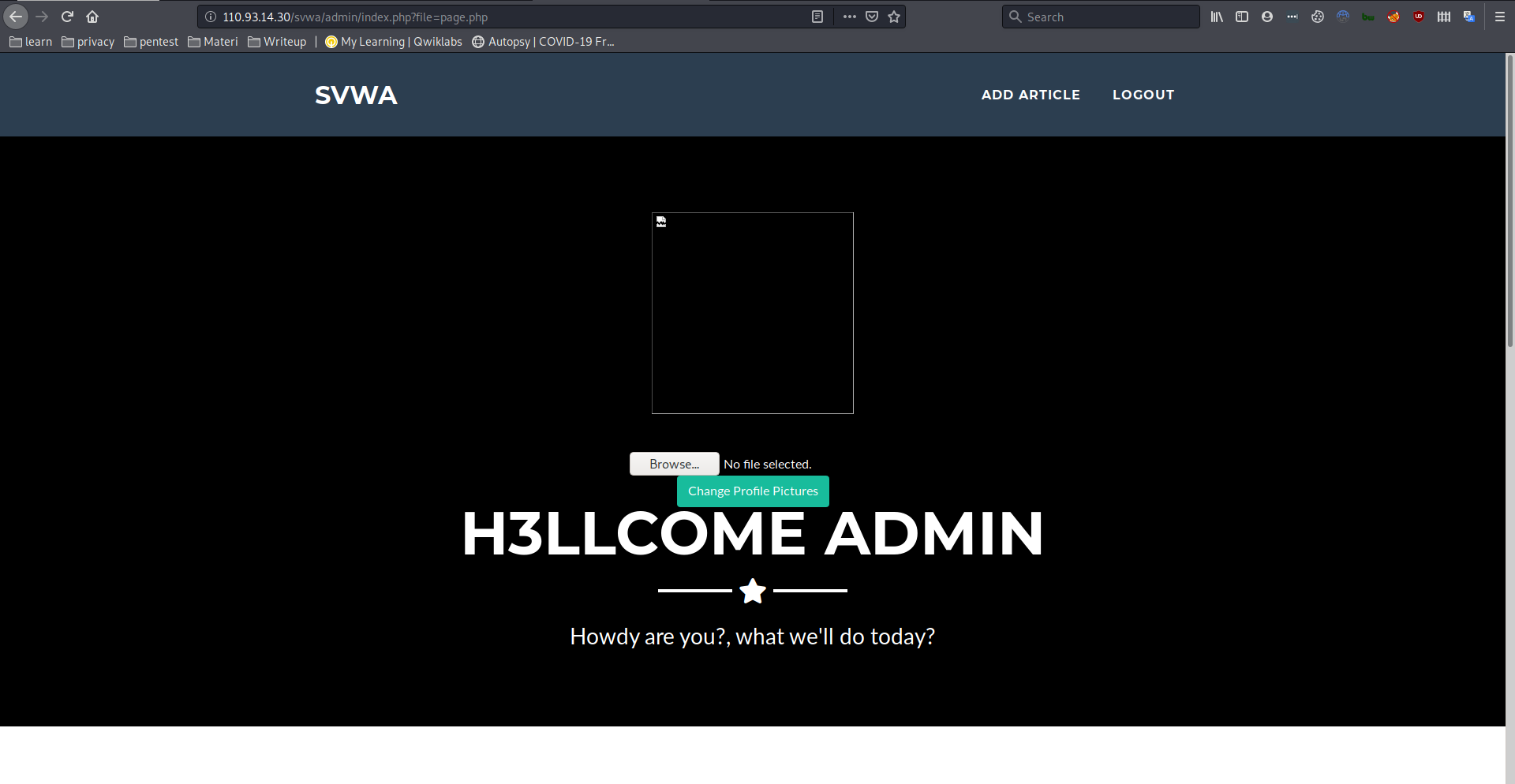
Dari hasil enum tables pada database svwa, saya mendapatkan tabel yang ada yang ada pada db svwa tersebut.



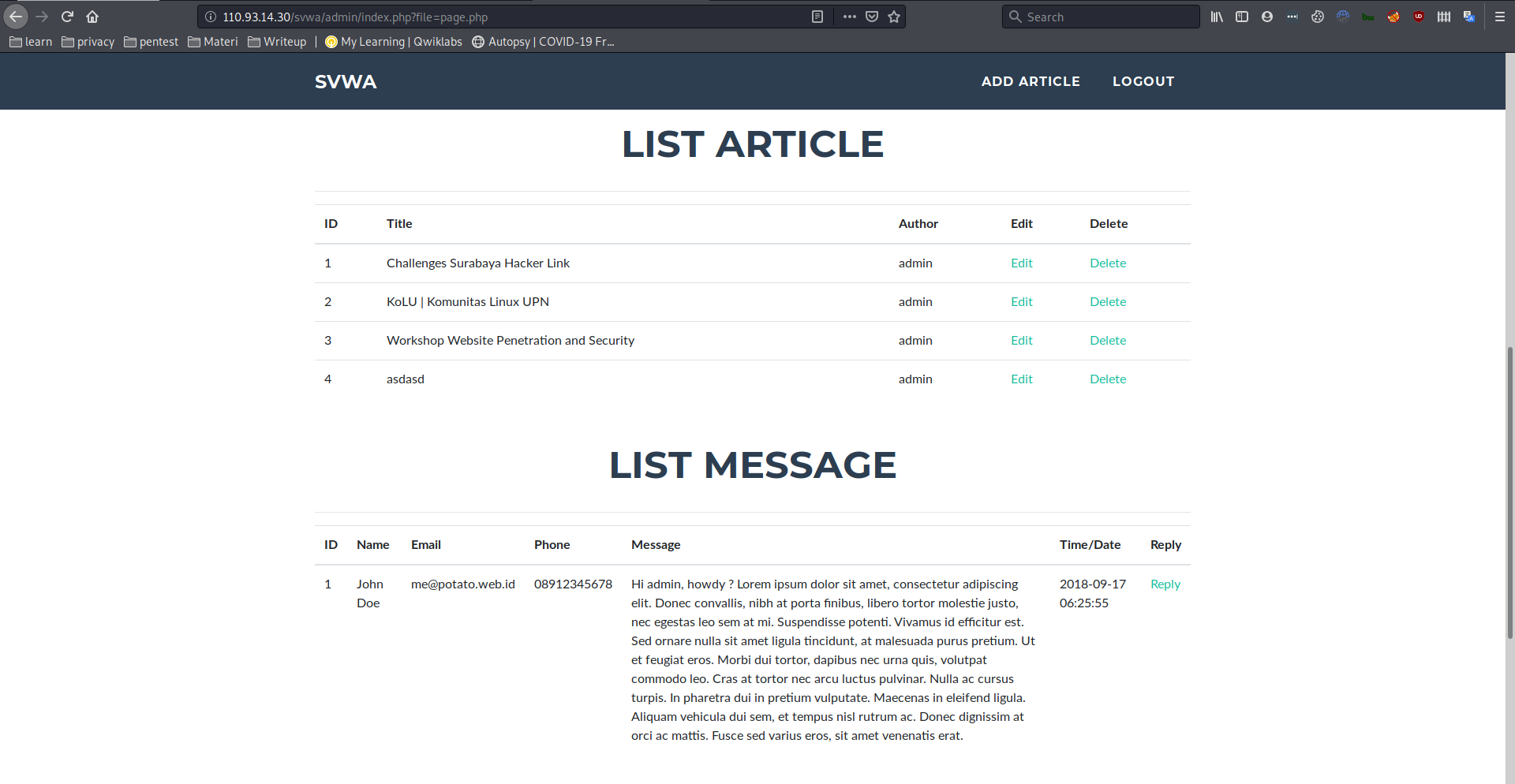
Karena yang menarik adalah tabel m\_user, langsung aja kita cek apa aja isinya pake SQLmap (sqlmap -D svwa -T m\_user --dump -u <http://110.93.14.30/svwa/read.php?id=1)> untuk nge-dump isi dari tabel m\_user.



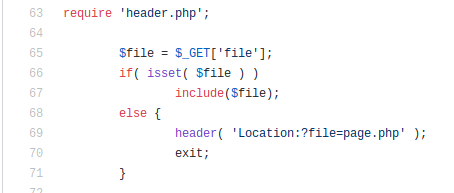
Kita sudah mendapatkan username dan password untuk login ke sistem. Langsung aja kita login ke web pake username: admin dan password: anu.



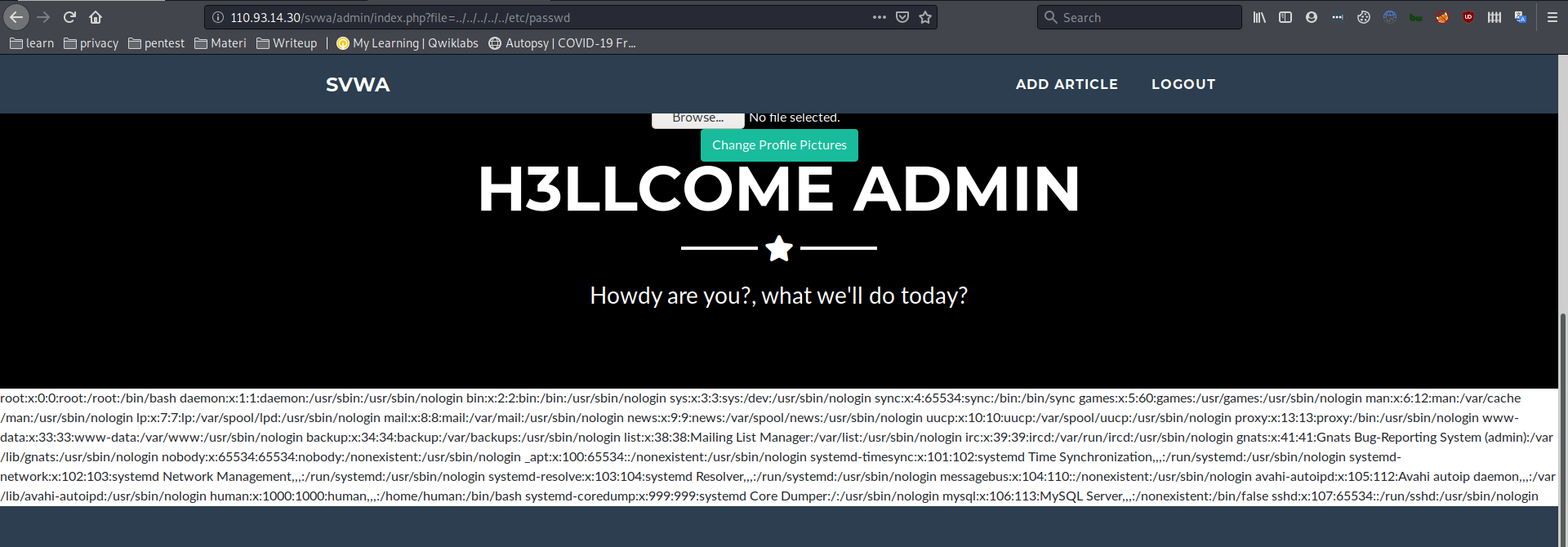
Kita disuguhkan ke laman admin di index.php yang isinya adalah seperti gambar di atas. Kemudian juga terdapat list artikel dan list pesan.



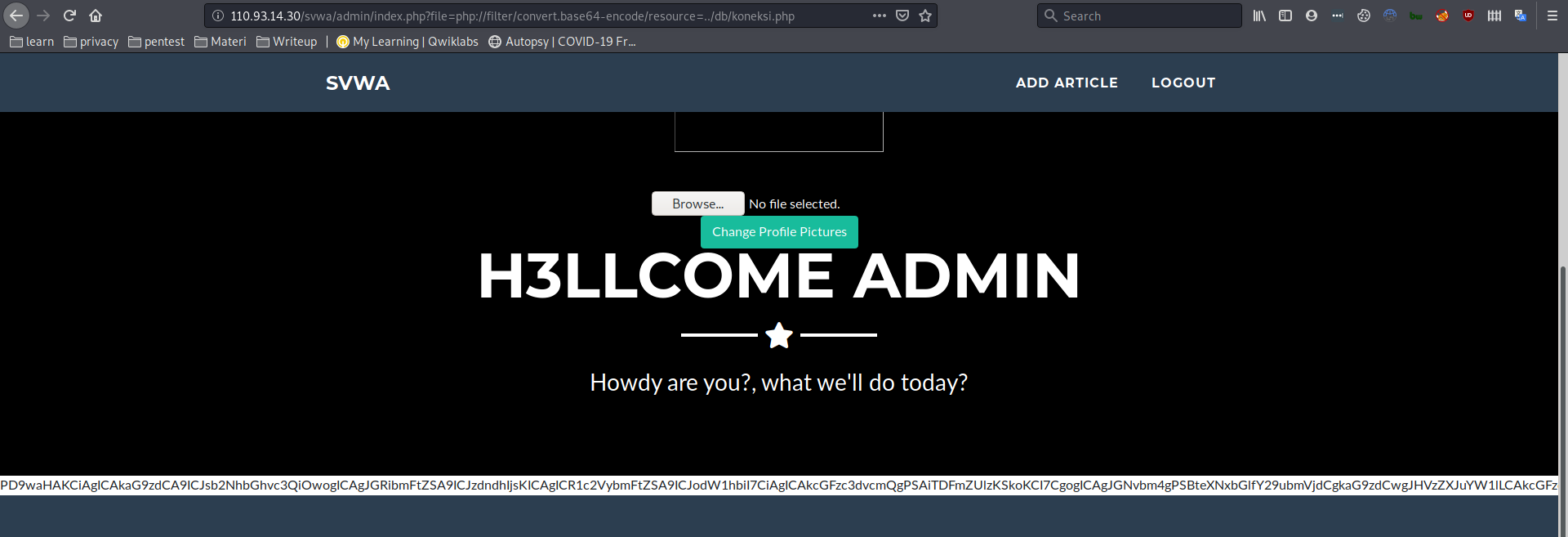
Karena source code yang digunakan sama, saya langsung melihat ke github svwa (https://github.com/laztname/SVWA/blob/master/admin/index.php) untuk melihat beberapa source codenya, khsusunya di index.php admin ini. Di sini saya nemu vuln yang memungkinkan kita untuk melakukan LFI (local file inclusion) pada parameter file di URL.



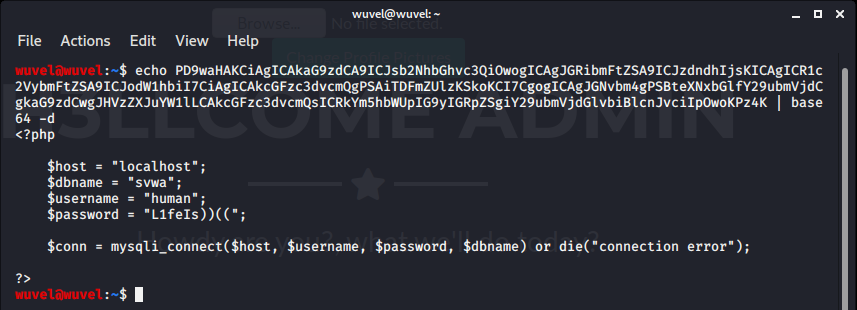
Langsung aja kita coba lfi ke file /etc/passwd buat ngetest apakah bisa apa engga.



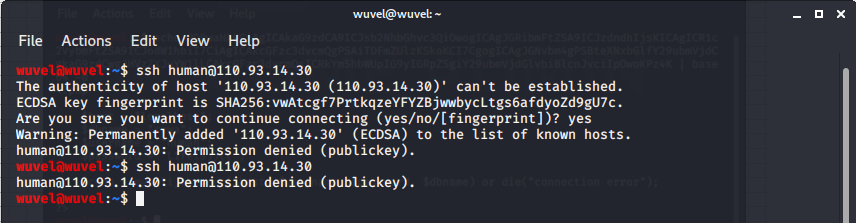
Nah bisa! Langsung aja kita pake php filter buat dapetin source code dari svwa ini yang mungkin menarik. Saya mendapatkan file yang cukup menarik pada repo svwa di github, yaitu file koneksi.php pada direktori db yang berisi username dan password db ini. Mungkin kita bisa menemukan sesuatu di sana. Dengan menggunakan payload (http://110.93.14.30/svwa/admin/index.php?file=php://filter/convert.base64-encode/resource=../db/koneksi.php).



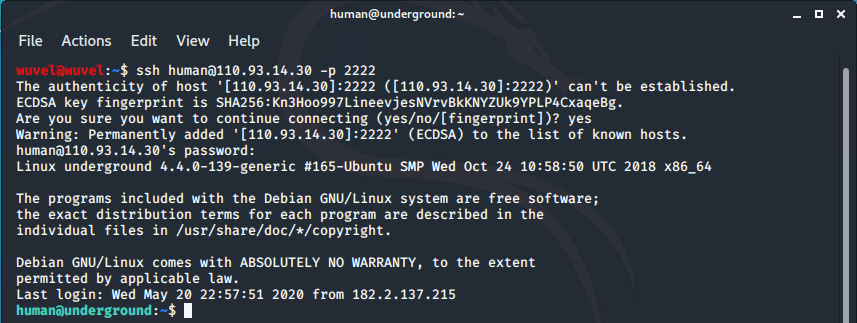
Filter masuk, kita dapet source code koneksi.php dalam bentuk base64. Kita decode dulu untuk lihat source codenya.



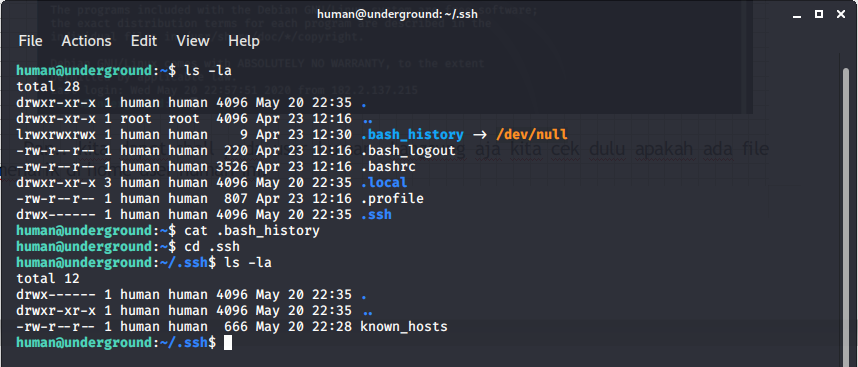
Saya mendapatkan username dan password seperti di atas. Melihat hasil enum kita pake nmap pertama kali, terlihat bahwa host memiliki port terbuka pada service ssh, mungkin kita bisa pake data ini buat masuk ke user human. Langsung aja kita cek.



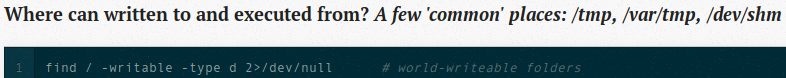
Access denied. Coba kita cek SSH di port 2222. Yang di atas ini menggunakan port SSH default (port 22).



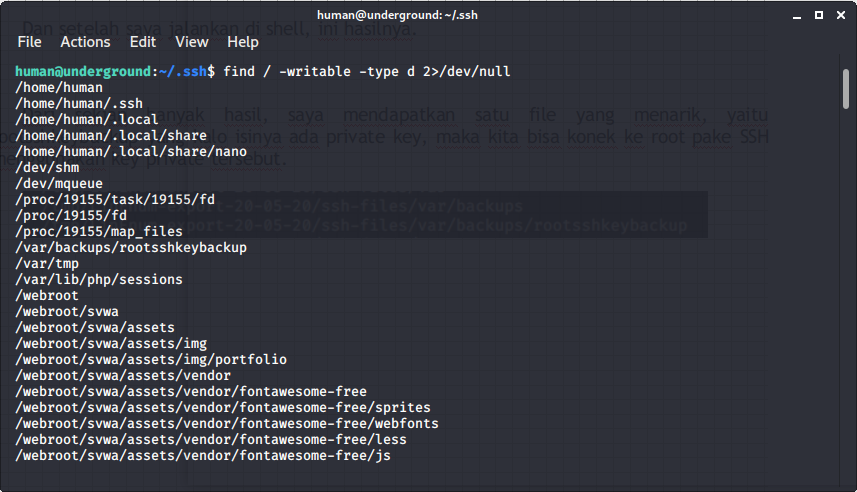
Dan.. kita dapet shell pada user human. Langsung aja kita cek dulu apakah ada file menarik di home user human ini.



Sepertinya ga ada. Sekarang tugas kita menaikan privilege menggunakan priv esc. Setelah saya cari-cari, ada satu blog yang ngebahas tentang priv esc di linux (https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/). Saya make perintah di gambar bawah ini buat ngecek file-file/direktori yang bisa kita write dan execute pada permissionnya.



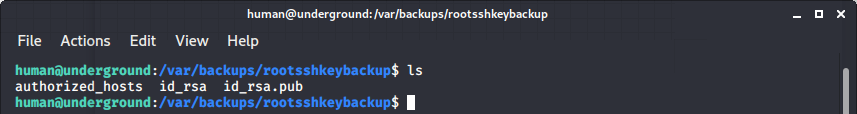
Dan setelah saya jalankan di shell, ini hasilnya.



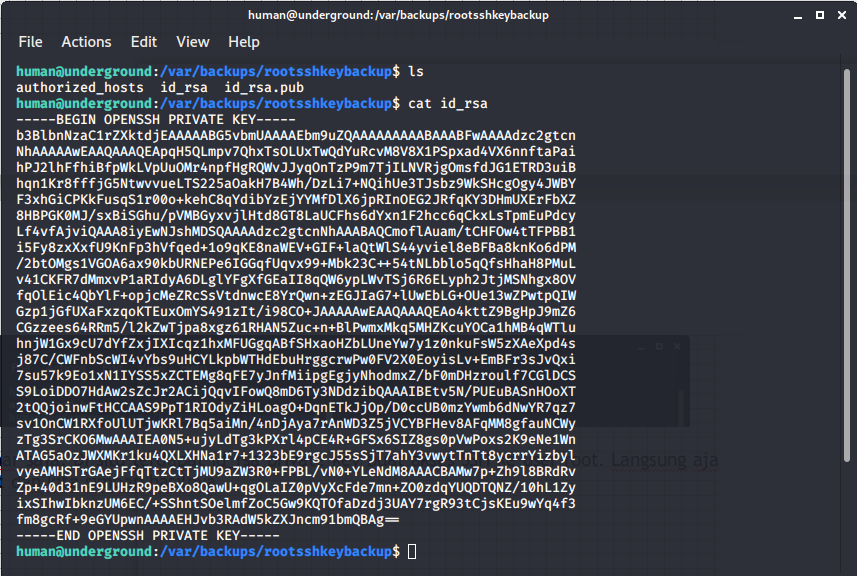
Dari sekian banyak hasil, saya mendapatkan satu direktori yang menarik, yaitu rootsshkeybackup yang kalo isinya ada private key, maka kita bisa konek ke root pake SSH menggunakan key private tersebut.



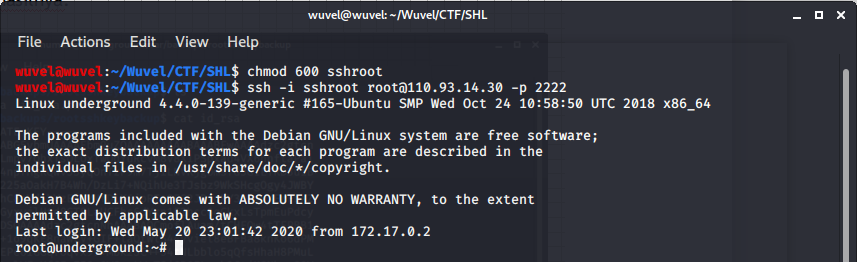
Langsung aja kita cek direktori tersebut.



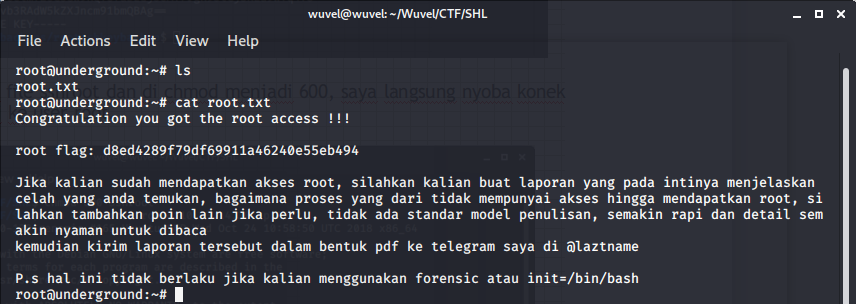
Benar saja. Di situ terdapat id\_rsa private key buat akses SSH ke user root. Langsung aja kita cat dan kita simpan hasilnya.



Setelah disimpan jadi file sshroot dan di chmod menjadi 600, saya langsung nyoba konek SSH pake private key tadi ke user root.



Dan.. kita dapet shell user root. Langsung aja kita liat isinya dan nampilin file root.txt yang menjadi goal pada challenge ini.



Nice! Challenge yang bagus menurut ku. Root flagnya adalah **d8ed4289f79df69911a46240e55eb494**.