

Belajar Hacking Website Dari Nol

Deny Kurniawan

denykurniawan139@gmail.com

<http://www.facebook.com/groups/300042220071174>

Lisensi E-Book :

Copyright © 2013 Network-Security UBL

Seluruh e-book ini di Network-Security UBL dapat di gunakan dan di sebarkan secara bebas untuk tujuan pembelajaran dalam dunia networking. Dengan syarat tidak merubah dan menghapus isi dari atribut penulis dan hak cipta copyright yang di sertakan pada setiap e-book. Tidak di perbolehkan menuliskan ulang, kecuali terdapat izin antara kedua belah pihak

Network-Security UBL

Daftar Isi

Cover.....	1
Daftar Isi.....	2
Pengenalan Hacking.....	3
Pengenalan Software.....	4
1.1 Acunetix.....	4
1.2 John The Ripper.....	4
1.3 Havij 1.15 Pro.....	5
1.4 Admin Finder versi Network Security.....	5
1.5 Active Perl.....	5
1.6 Perl.....	5
Mencari Informasi Target.....	6
Penggunaan Acunetix.....	7
Penggunaan Havij.....	14
Penggunaan Admin Finder.....	17
Penggunaan John The Ripper.....	21
Hacking System.....	24
Penutup.....	26

Pengenalan Hacking

Hacking merupakan sebuah seni yang bisa di bilang mempunyai kedua kekuatan antara white hacking dan black hacking, antara seni berbuat baik dan seni berbuat jahat. Pada dasarnya hacking itu bertujuan untuk menemukan sesuatu kelemahan pada sebuah system atau aplikasi agar kita dapat membongkar source code di dalam system tersebut dan berhasil masuk ke dalam system tersebut. Pada dasarnya kita dapat merubahnya namun kita tidak untuk merusak. Kali ini kita akan mencoba membongkar sebuah keamanan website dengan menggunakan teknik vuln system kelemahan dengan SQL injection.

Belajar hacking website dari nol anda akan di arahkan bagaimana anda yang awalnya tidak tahu tentang dunia hacking. Dengan membaca e-book network security ini anda dalam waktu 1 jam saja mampu menjadi seorang hacker dan mampu melumpuhkan sebuah website dengan menganalisa dan menerobos system kelemahannya.

Banyak kasus hacking yang beredar dan terkenal sampai saat ini salah satunya adalah hacker cina yang berhasil men take over satelit NASA selama kurang dari 15 menit. Selain itu situs-situs besar seperti google, facebook, amazon, ebay juga pernah kebobolan system keamanan mereka.

Keamanan memang merupakan salah satu factor terpenting dalam sebuah system atau aplikasi karena dengan keamanan, system atau aplikasi yang kita buat dapat bertahan lama. Bukan berate system atau aplikasi kita sempurna karena tidak ada sebuah system atau aplikasi yang sempurna 100%. Tujuan dari keamanan adalah memperlama hacker merusak dari system atau aplikasi anda hingga berpuluh-puluh tahun.

Hacking memang memanfaatkan sebuah system misalnya pada jaringan, yang akan kita bahas kali ini adalah hacking website dengan mencari vuln keamanan.

Attacker : Penyerang.

Korban : Sistem yang akan di serang.

Firewall : Sistem pelindung dari website.

Di mana attacker mencoba akan menyerang korban dengan teknik vuln pada sebuah website yang di miliki korban. Dengan memanfaatkan celah firewall website tersebut dan berhasil menerobos sampai halaman admin.

Pengenalan Software

1.1 Acunetix

Acunetix merupakan sebuah program alat scanning website yang sangat populer di dunia hacking. Kemampuannya untuk menscan secara total dari sebuah system dan mendapatkan sebuah informasi secara mendetail. Acunetix ini juga bisa mendeteksi kelemahan pada system aplikasi pada website, seperti vuln pada SQL Blind, SQL Injection, Cross Site Scripting (XSS). Dan dari acunetix ini mampu melihat isi directori dari sebuah website dan bisa di gunakan untuk mencari halaman login website tertentu. Kemampuannya yang begitu lengkap acunetix menjadi salah satu software favorite dari para hacker saat ini. Saat ini acunetix sudah mencapai versi 8 dan dapat di gunakan di windows xp, vista, 7 dan windows 8.

Download : <http://www.4shared.com/rar/nlFJj71b/Acunetix.html>

1.2 John The Ripper

John The Ripper merupakan salah satu alat hack paling populer dan paling lama yang bertahan sampai saat ini. John di gunakan untuk mencrack sebuah password yang sudah di descrypt dari md5 hash, md4, dan password binary lainnya menjadi password login bisaa. Namun untuk menjalankan John anda perlu selalu meng-update source list password directory agar saat mendescrypt password terbantu dengan cepat namun john dapat membaca cepat anatar 1-7 password dalam hitungan menit. Namun jika password tersebut lebih dari 7 karakter dan karakter tersebut terdiri dari beberapa symbol, John akan lama membacannya butuh waktu berjam-jam bahkan berhari-hari.

Download : http://www.4shared.com/zip/uv9GqSx/John_The_Ripper.html

1.3 Havij 1.15 Pro

Havij 1.15 Pro merupakan alat pembaca isi dari daleman suatu database dengan havij kita bisa mendapatkan informasi database baik itu menggunakan sql, oracle, ms access, postgre sql, sybase. Havij sendiri memang tools hacking yang simple dan mudah di gunakan, selain itu di havij mempunyai fitur simpan yang di gunakan untuk penyimpanan dump sql yang kita dapatkan dari proses hacking.

Download : http://www.4shared.com/rar/VNv0xeAv/Havij_115_ProCrack.html

1.4 Admin Finder versi Network Security

Admin finder berfungsi untuk menemukan suatu halaman login dari sebuah website. Admin finder ini telah di modifikasi dan sudah ada tambahan source list halaman login dari sebuah website baik itu menggunakan php, asp, cfm. Tools ini memang cepat dalam melakukan scanning web login pada suatu web.

Download : <http://www.4shared.com/rar/qiOrYXaS/Admin.html>

1.5 Active Perl

Active perl bahasa pemograman yang cukup populer saat ini, bahasa pemograman ini banyak di kembangkan untuk pembuatan tools-tools security dan tools hacking.

Download : <http://www.activestate.com/activeperl/downloads>

1.6 Perl

Perl ini sama seperti active perl hanya saja perl ini untuk menjalankan program-program yang berekstensi .pl seperti adminfinder.pl. Selain itu perl ini anda bisa membuat pemograman yang berbasis pemograman perl.

Download : <http://www.activestate.com/activeperl/downloads>

Mencari Informasi Target

Untuk target yang kita lakukan testing keamanan adalah website salah satu sekolah di Indonesia dengan domain menggunakan .sch.id.

Target sekolah ini di ambil untuk pembelajaran karena lemahnya system keamanan pada website tersebut. Di publikasikan untuk pembelajaran bukan untuk merusak sebuah system.

Target : <http://smpn18bkl.sch.id>

Untuk scanning gunakan alat : Acunetix

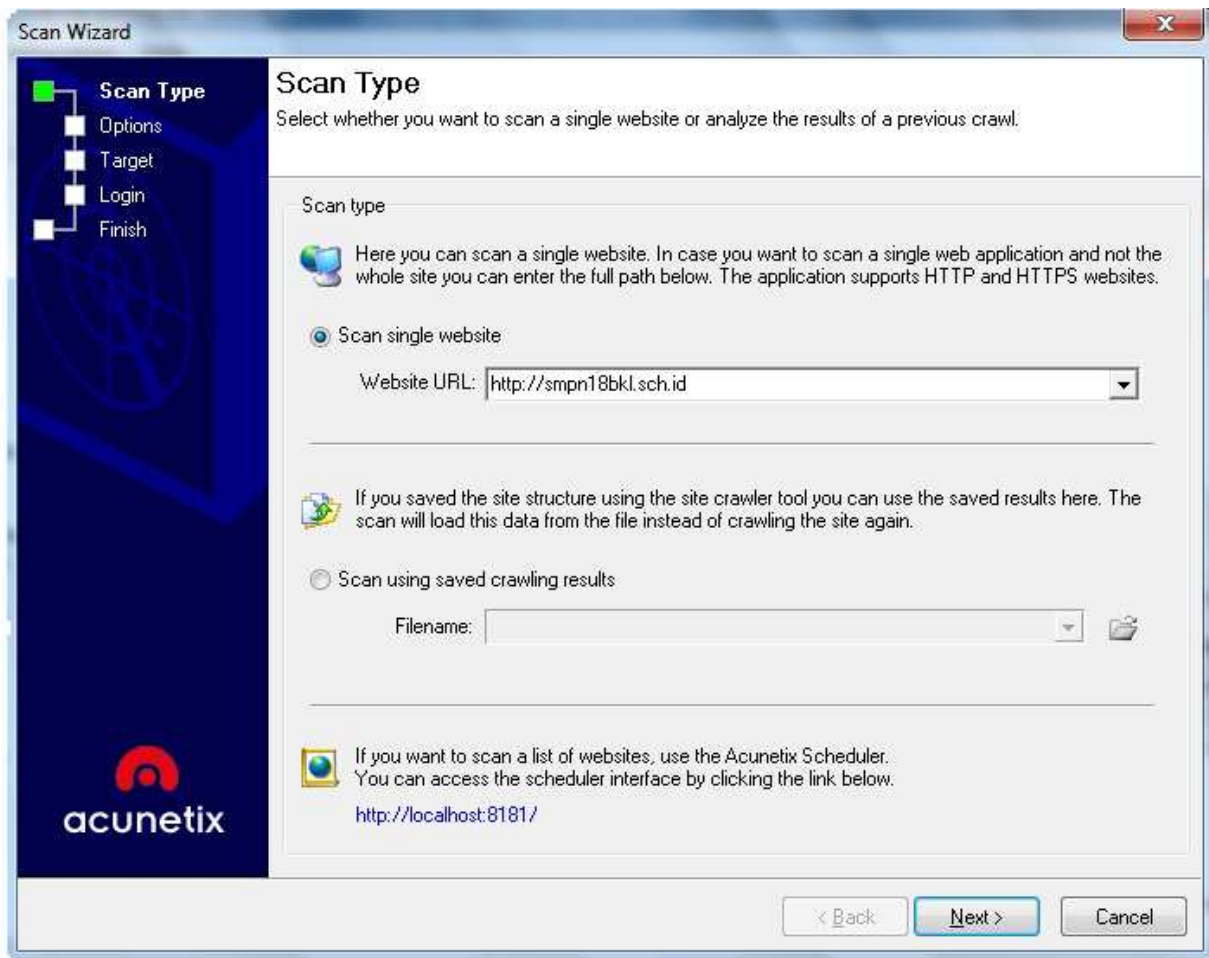
Untuk pengambilan dumping password admin gunakan : Havij

Untuk memecah descrypt md5 password admin menggunakan : John The Ripper

Untuk menemukan halaman login menggunakan : Adminfinder versi Network Security

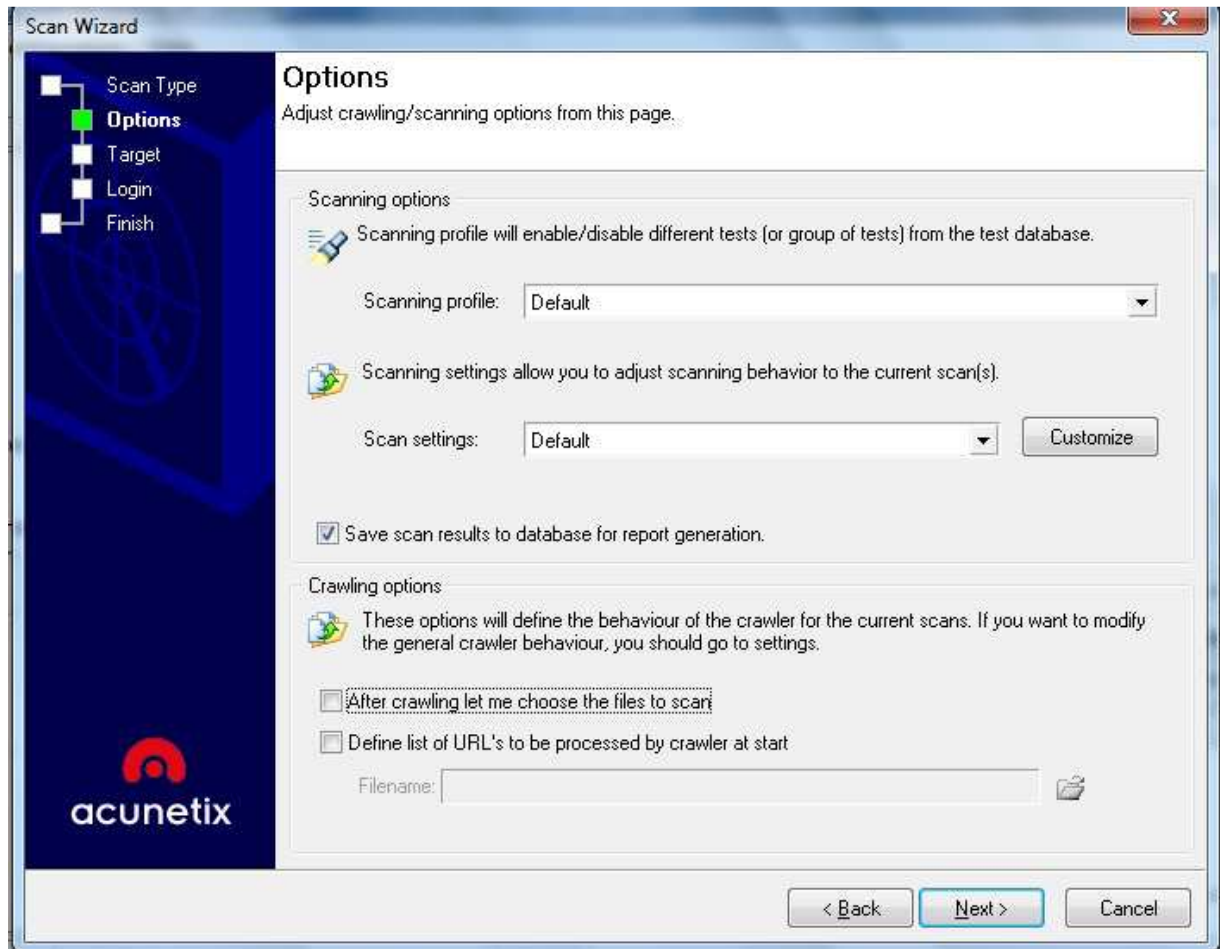
Penggunaan Acunetix

Masuk ke acunetix lalu masukan nama website seperti contoh di bawah ini :



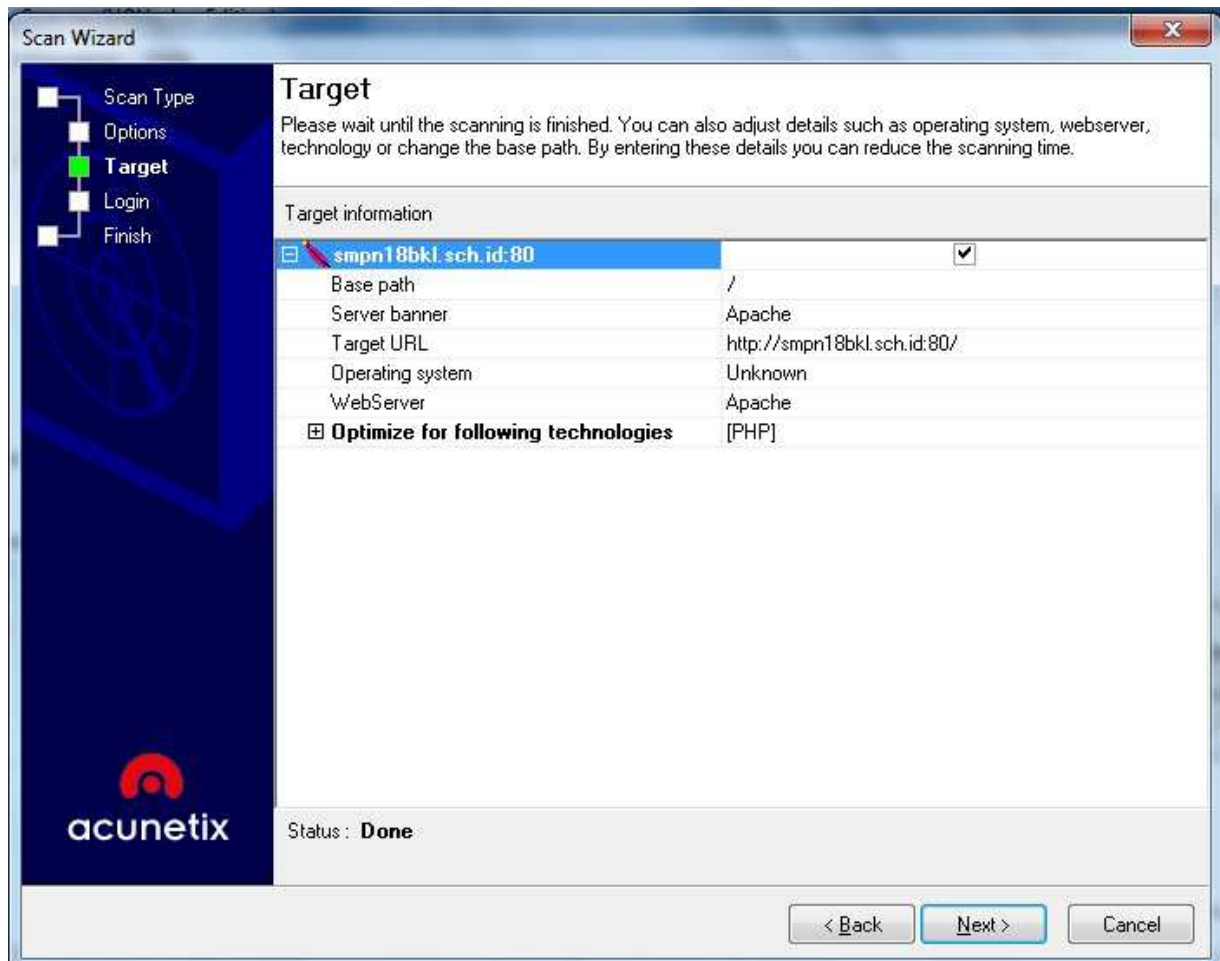
Masukan nama websitenya pada kolom website url, seperti gambar di atas dan lalu selanjutnya pilih tombol next.

Selanjutnya akan tampil gambar seperti di bawah ini :



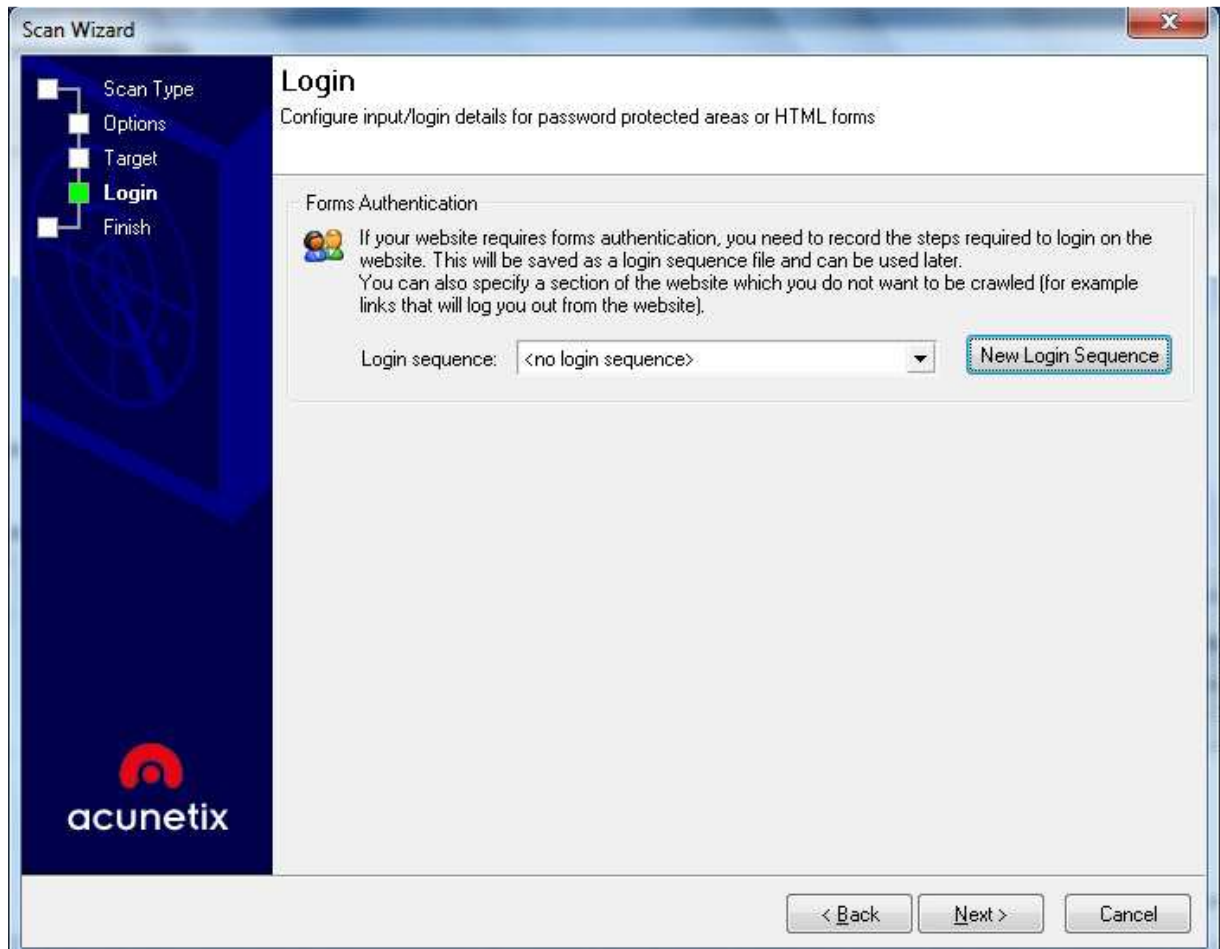
Biarkan saja defaultnya seperti itu, lalu klik tombol next.

Selanjutnya adalah informasi target korban seperti server, operating system, web server, pemograman technologies yang di gunakan oleh korban akan terekam di sini :



Lalu klik tombol next.

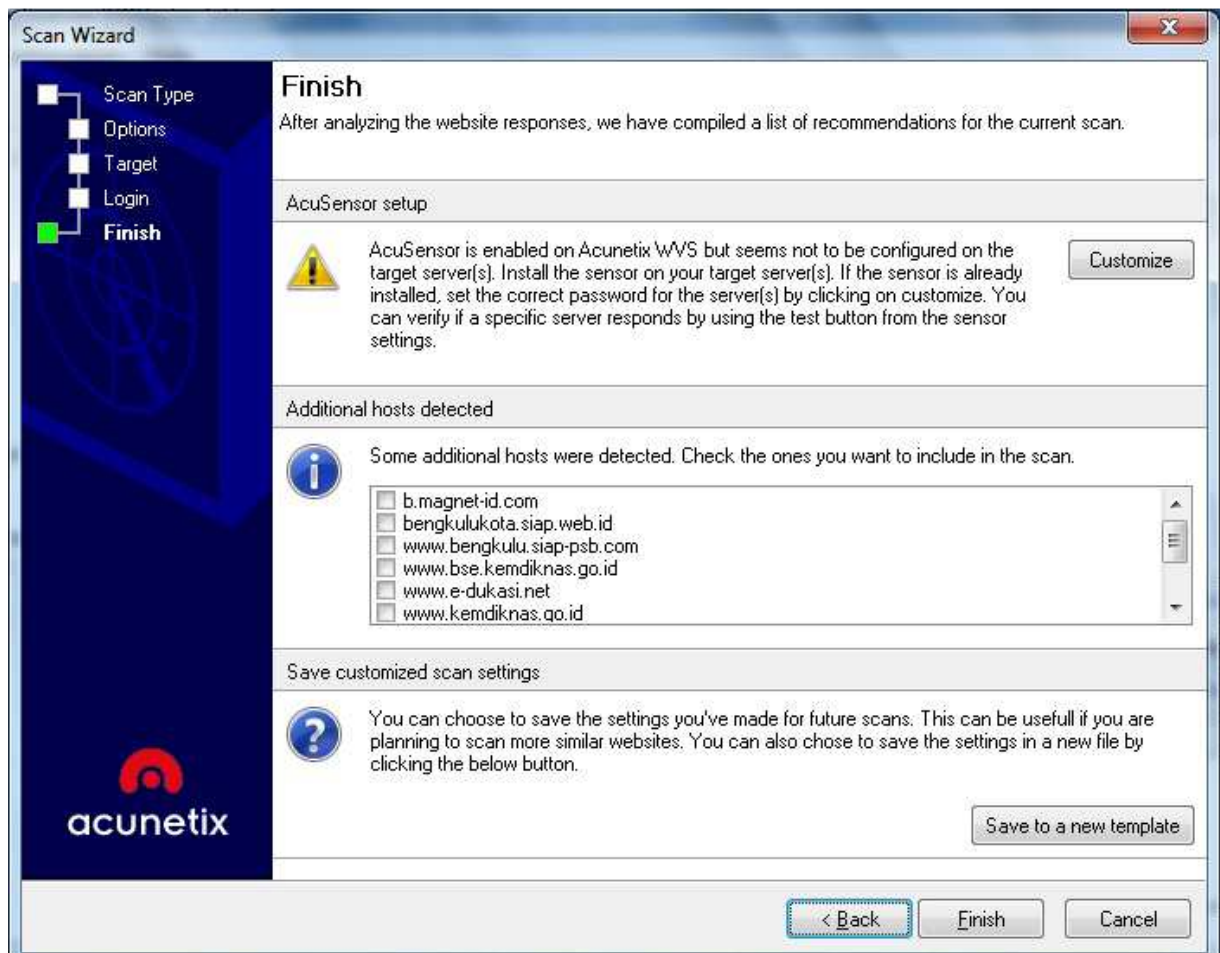
Tampilan selanjutnya adalah informasi login biarkan saja default seperti bawaan :



Lalu pilih tombol next.

Jika sudah akan muncul tampilan finish dan siap melakukan scanning di acunetix dan biarkan acunetix men-scan website korban hingga selesai.

Untuk additional host detected biarkan saja, bila ada subdomain dari web utama misalnya <http://a.smpn18bkl.sch.id> bisa anda centang, terhubung dari website korban tidak mempunyai sub domain anda biarkan saja.



Selanjutnya pilih tombol finish.

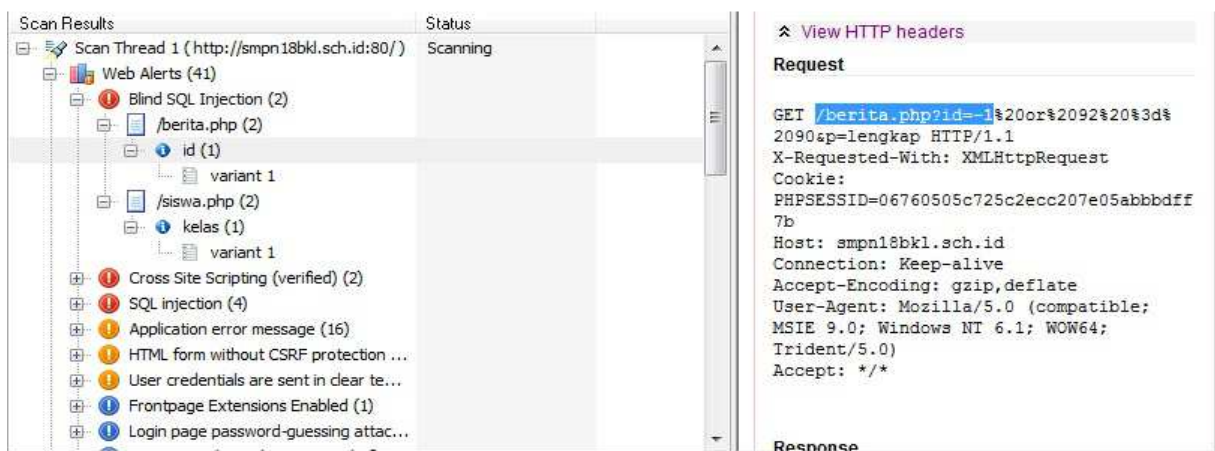
Selanjutnya dari data korban kita menangkap adanya sebuah vuln blind sql yang dapat kita serang kita menemukan

[http://smpn18bkl.sch.id/berita.php?p=lengkap&id=1'](http://smpn18bkl.sch.id/berita.php?p=lengkap&id=1)

Tampak gambar



Kita dapatkan dari hasil scanner menggunakan acunetix



Pada awalnya yang mempunyai blind sql injection adalah pada website

<http://smpn18bkl.sch.id/berita.php?id=-1>

Lihat seperti pada gambar di atas.

(*) Catatan : Bagi anda yang menemukan web lain yang bertuliskan **"You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near"** berate website tersebut bisa di dump dengan havij.

Dari hasil scanning di atas dapat di simpulkan bahwa website tersebut mempunyai banyak celah untuk di trobos systemnya termasuk dengan sql injection dan juga xss.

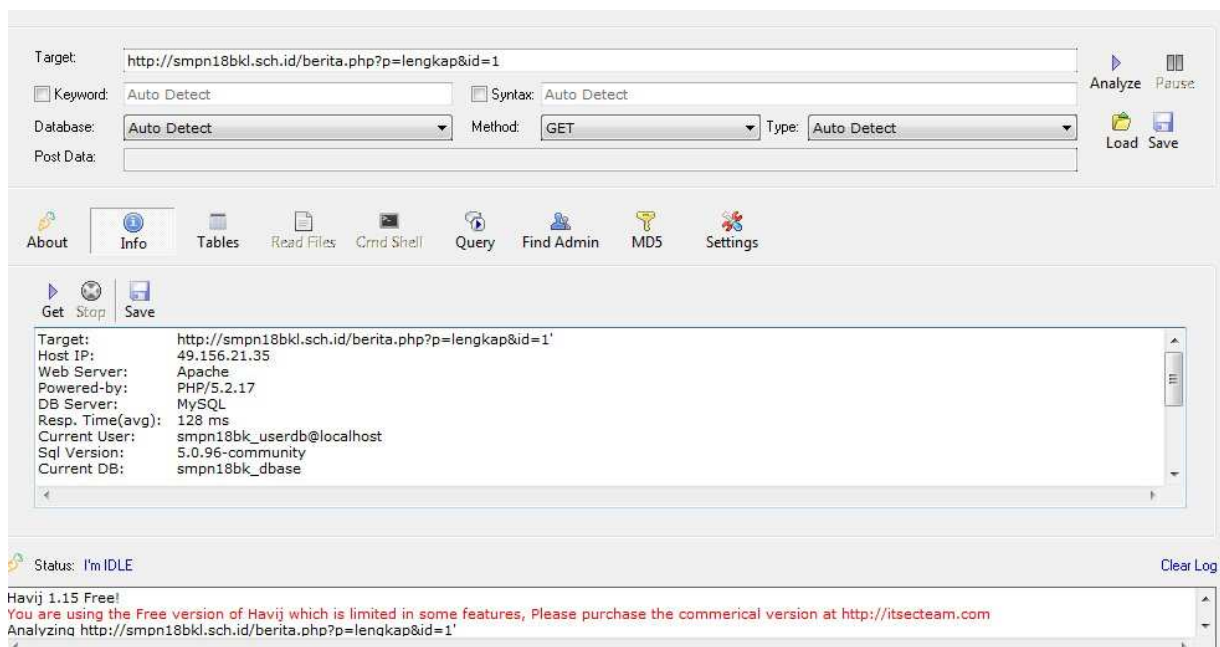
Penggunaan Havij

Masuk ke havij gunakan alamat yang kita serang tadi bisa menggunakan

<http://smpn18bkl.sch.id/berita.php?id=-1> atau yang telah saya trobos lebih dalam lagi

<http://smpn18bkl.sch.id/berita.php?p=lengkap&id=1'>

hilangkan tanda – untuk yang pertama dan ‘ untuk yang kedua dan tampak seperti di gambar untuk sql injection menggunakan havij



Lalu setelah memasukkan web url klik analyze tunggu sampai selesai.

Setelah selesai anda buka menu info dan klik get dan tunggu hingga selesai, jika selesai maka informasi yang kita dapatkan adalah

Target: http://smpn18bkl.sch.id/berita.php?p=lengkap&id=1'

Host IP: 49.156.21.35

Web Server: Apache

Powered-by: PHP/5.2.17

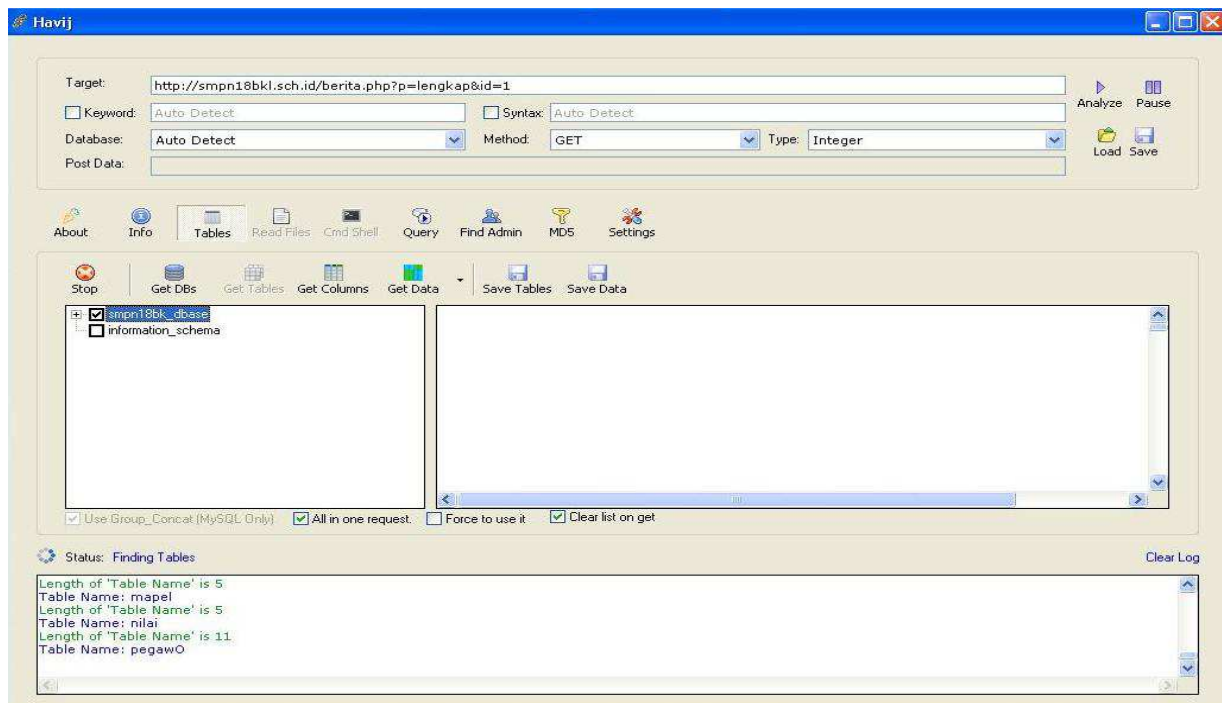
DB Server: MySQL

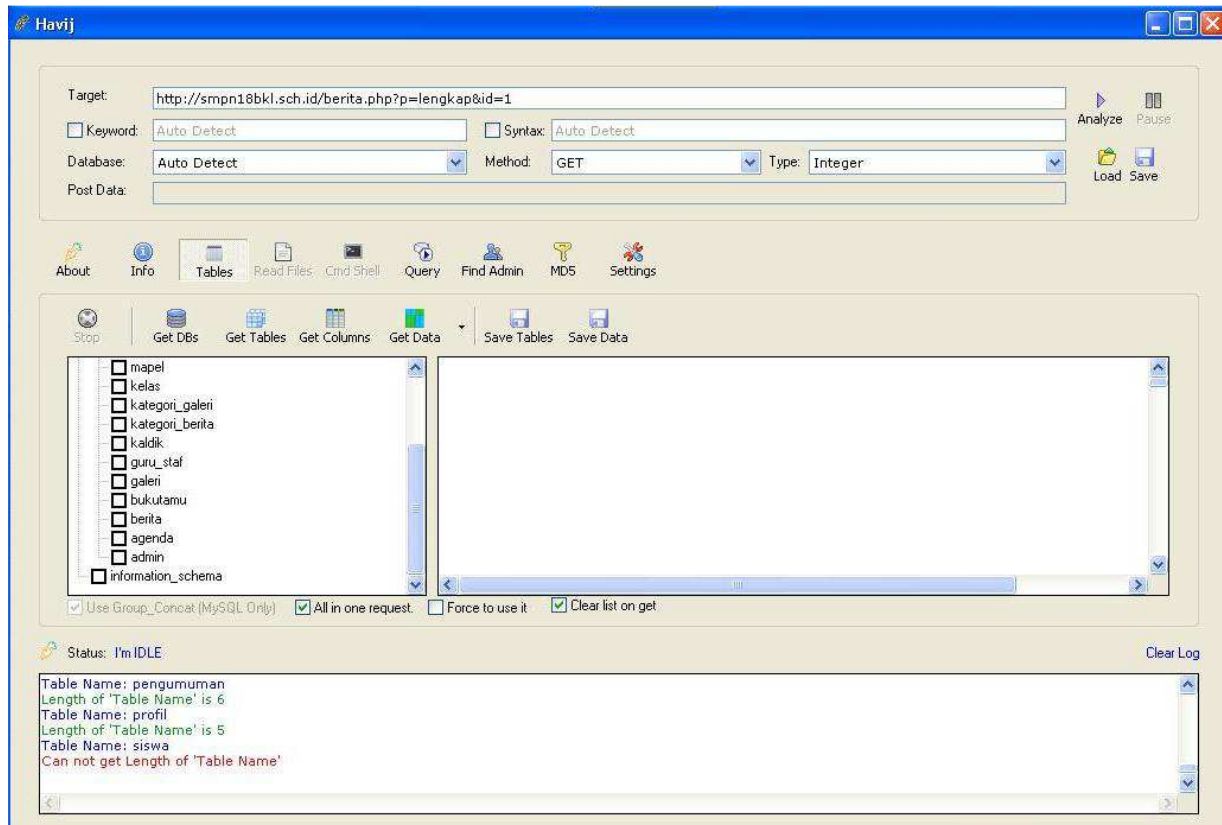
Resp. Time(avg): 128 ms

Current User: smpn18bk_userdb@localhost
Sql Version: 5.0.96-community
Current DB: smpn18bk_dbase
System User: smpn18bk_userdb@localhost
Host Name: pasai.magnethost.asia
Installation dir: /
DB User: 'smpn18bk_userdb'@'localhost'
Data Bases: information_schema
smpn18bk_dbase
Data Bases: information_schema
smpn18bk_dbase

Selanjutnya adalah klik tables untuk mendapatkan informasi dari database smpn18bk_dbase

Pertama-tama adalah klik **get dbs** untuk mendapatkan nama database, selanjutnya adalah Untuk mencari tables anda centang table smpn18bk_base klik **get tables** setelah itu maka akan muncul tables lebih detail lihat gambar.





Hasil keseluruhan isi database :

siswa

profil

pengumuman

pegawai_str

nilai

mapel

kelas

kategori_galeri

kategori_berita

kaldik

guru_staf

galeri

bukutamu

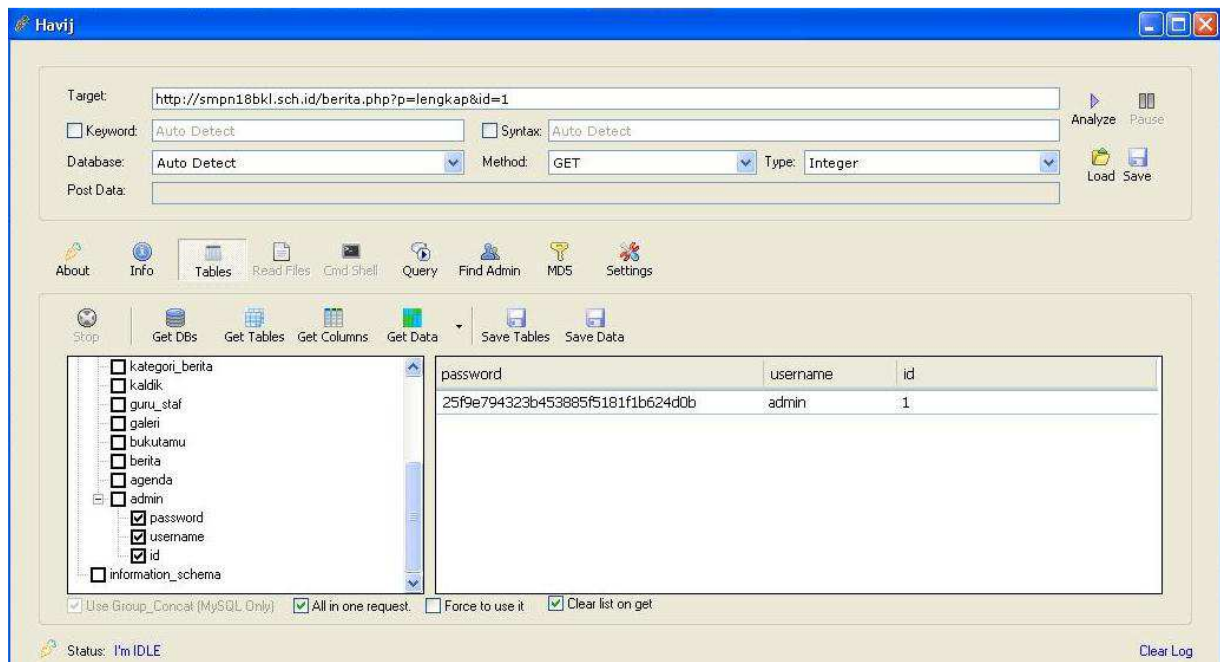
berita

agenda

admin

Setelah itu kita centang tables admin lalu klik get **coloums** untuk mendapatkan username, password, id dan setelah itu akan muncul password dalam bentuk md5, username, id centang semua dan klik **get data**.

Hasil dari gambar dump tables admin tersebut dari havij



Dan dapat hasil sebagai berikut

Username : admin

Password dalam bentuk md5 : 25f9e794323b453885f5181f1b624d0b

Penggunaan Admin Finder

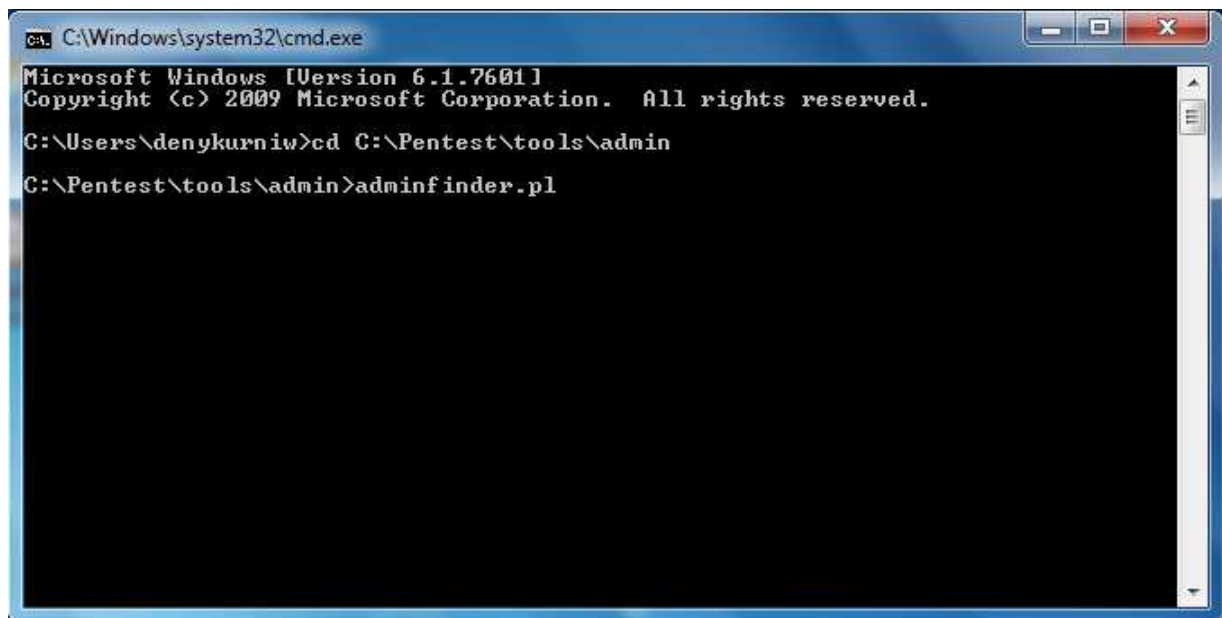
Selanjutnya adalah bagaimana kita bisa menemukan halaman login website tersebut, kita bisa menggunakan admin finder atau pun dari acunetix di atas sudah bisa melihat halaman login. Namun untuk lebih mengetahui admin finder ini anda bisa mencobanya.

Sebagai tutorial saya menaruh admin finder di directori

C:\Pentest\tools\admin

Adminfinder.pl

Lalu buka cmd dengan perintah berikut dan pastikan perl anda sudah terinstall dengan baik. Dan lihat gambar di bawah ini untuk penggunaan.

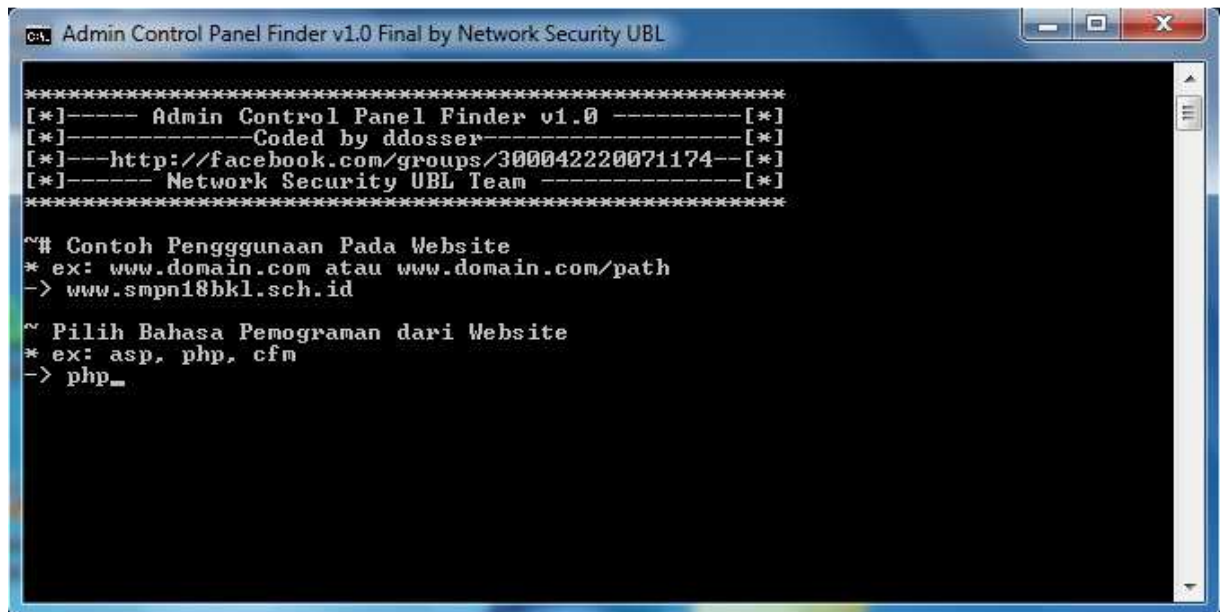


```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\denykurniw>cd C:\Pentest\tools\admin
C:\Pentest\tools\admin>adminfinder.pl
```

Setelah adminfinder.pl tekan enter dan akan muncul perintah seperti di bawah ini, itu merupakan adminfinder.pl yang siap anda gunakan untuk mencari halaman login.

(*) nb : untuk tempat file adminfinder anda bisa merubahnya sesuai dengan keinginan anda pastikan berada dalam disk C



```
C:\> Admin Control Panel Finder v1.0 Final by Network Security UBL

*****
[*]----- Admin Control Panel Finder v1.0 -----[*]
[*]-----Coded by ddosser-----[*]
[*]---http://facebook.com/groups/300042220071174---[*]
[*]----- Network Security UBL Team -----[*]
*****

~# Contoh Penggunaan Pada Website
* ex: www.domain.com atau www.domain.com/path
-> www.smpn18bkl.sch.id

~ Pilih Bahasa Pemograman dari Website
* ex: asp, php, cfm
-> php_
```

Setelah itu masukan nama website target www.smpn18bkl.sch.id dan tekan enter setelah itu ketik php dan tekan enter. Selanjutnya tools ini akan mencari halaman admin secara otomatis.



```
C:\> Admin Control Panel Finder v1.0 Final by Network Security UBL

*****
[*]----- Admin Control Panel Finder v1.0 -----[*]
[*]-----Coded by ddosser-----[*]
[*]---http://facebook.com/groups/300042220071174---[*]
[*]----- Network Security UBL Team -----[*]
*****

~# Contoh Penggunaan Pada Website
* ex: www.domain.com atau www.domain.com/path
-> www.smpn18bkl.sch.id

~ Pilih Bahasa Pemograman dari Website
* ex: asp, php, cfm
-> php

->Target Website: http://www.smpn18bkl.sch.id/
->Bahasa Pemograman Yang di Cunakan: php
->Mencari Halaman Admin Silahkan Tunggu.....
```

Carilah yang found berate itulah halaman login website dari target.

Lihat gambar selanjutnya untuk melihat found login dari website target.

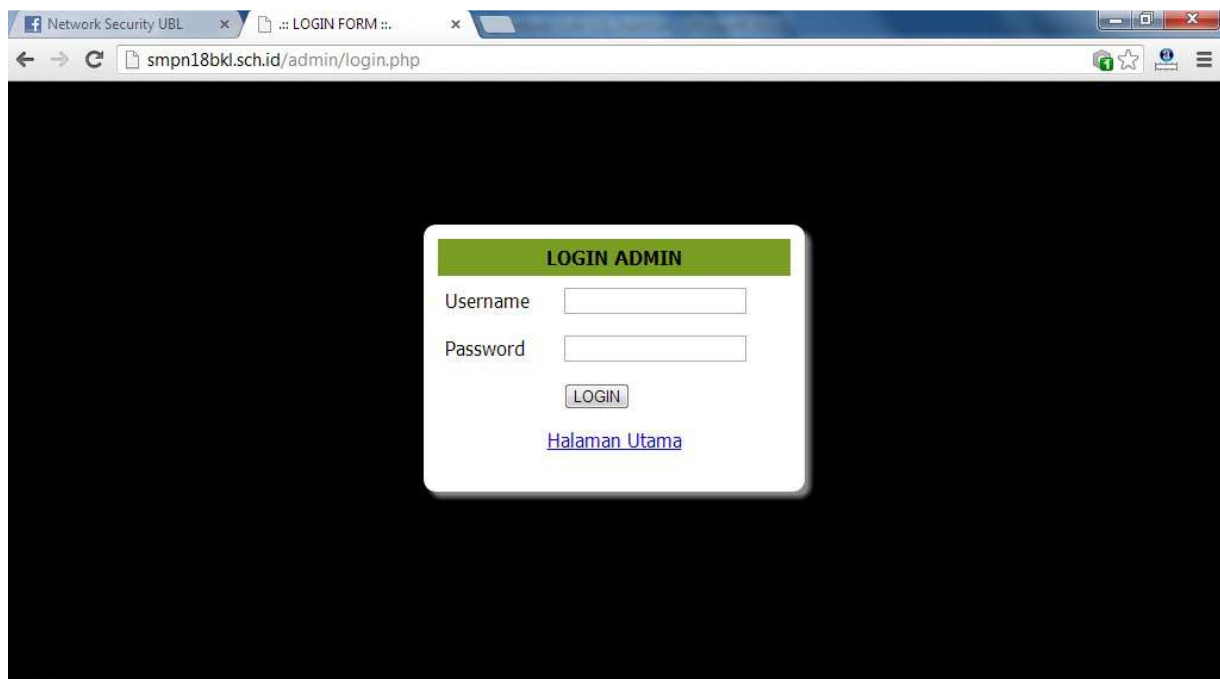
```
[+] Found -> http://www.smpn18bkl.sch.id/cpanel
[-] Not Found <- http://www.smpn18bkl.sch.id/log/admin/
[-] Not Found <- http://www.smpn18bkl.sch.id/log/administrator/
[-] Not Found <- http://www.smpn18bkl.sch.id/log/moderator/
[+] Found -> http://www.smpn18bkl.sch.id/admin/

[+] Found -> http://www.smpn18bkl.sch.id/admin/index.php

[+] Found -> http://www.smpn18bkl.sch.id/admin/login.php
```

Itulah halaman found dari admin

Saya membuka dengan alamat <http://smpn18bkl.sch.id/admin/login.php> maka akan terbuka menu login dari website tersebut.



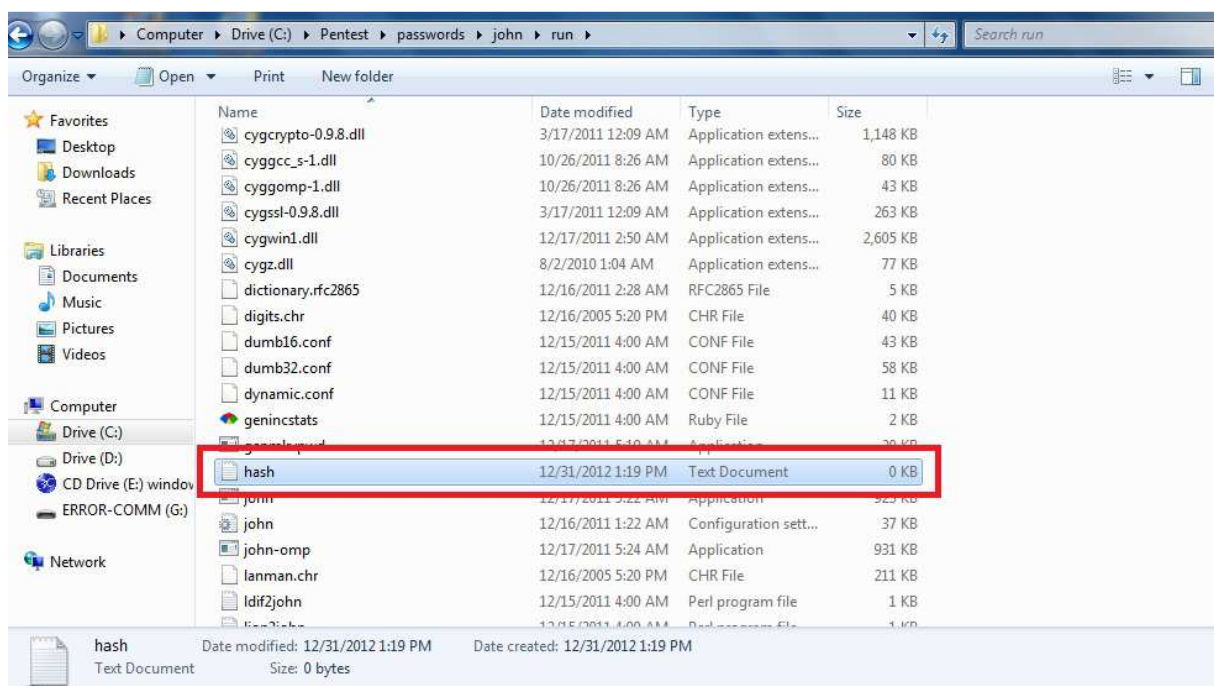
Selanjutnya adalah crack password md5 dengan john the ripper.

Penggunaan John The Ripper

Selanjutnya adalah penggunaan john the ripper di mana kita sudah dapatkan password dari md5 dari vuln sql injection yang berhasil di baca dengan software havij yakni

25f9e794323b453885f5181f1b624d0b sebelum kita memulai aksi penggunaan john the ripper pastikan kita membuat sebuah file .txt pada folder john semua akan di bahas pada gambar-gambar di bawah ini.

Pertama-tama masuk ke folder *john* dan masuk ke direktori *run* lalu buat file bernama *hash.txt* (*) bn bisa di ubah dengan nama file lainnya.



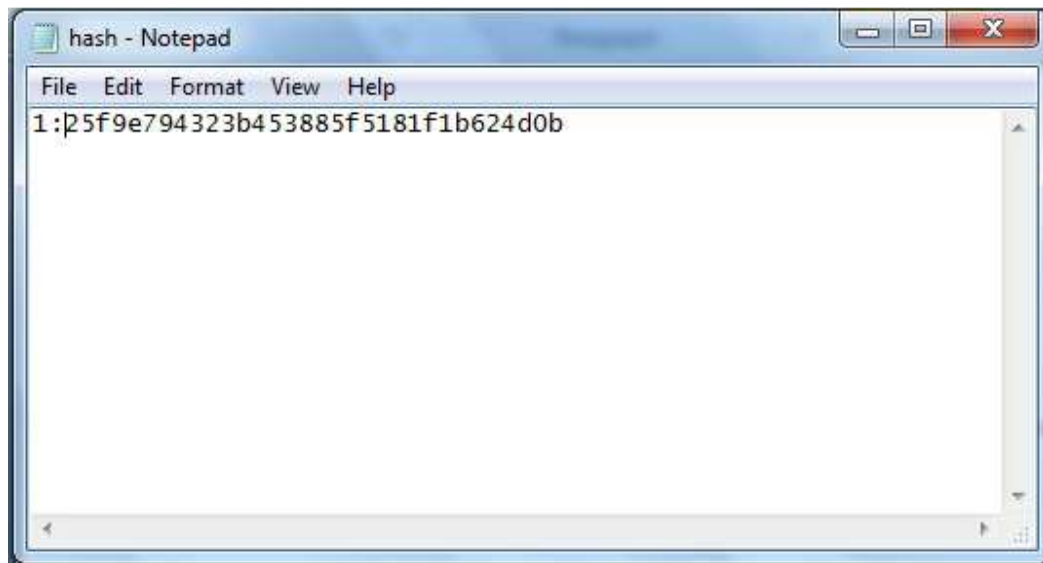
Selanjutnya isi file tersebut dengan md5 hash yang kita dapatkan dari havij sebelumnya tambahkan 1: pada awal. Jika banyak password pada saat dumping kita bisa menggunakan 2: 3: dan seterusnya contoh:

1: 25f9e794323b453885f5181f1b624d0b

2: 25f9e794323b453885f5181f1b624d0a

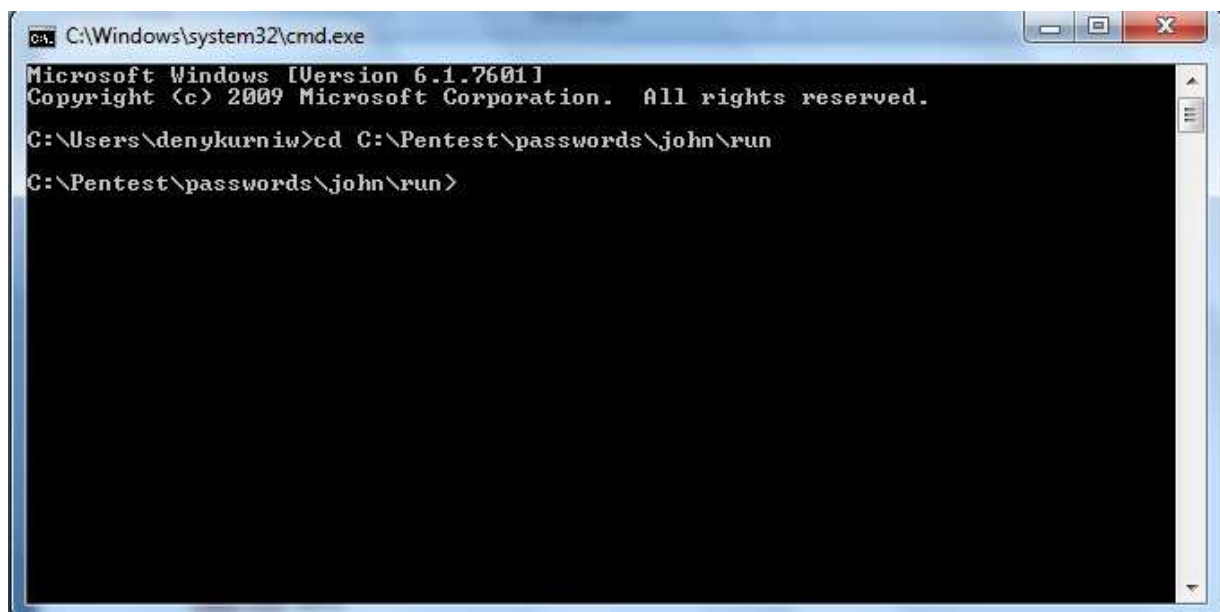
3: 25f9e794323b453885f5181f1b624d0c

Lihat di gambar berikut :



Lalu kita save.


Selanjutnya buka command prompt (cmd)



Cd C:\Pentest\passwords\john\run itu adalah folder directori yang saya taruh untuk menempatkan john. Yakni di folder C:\Pentest\passwords

Selanjutnya dalah jalankan john dengan perintah

John -format=raw-md5 hash.txt lihat gambar lebih detail



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\denykurniw>cd C:\Pentest\passwords\john\run
C:\Pentest\passwords\john\run>john --format=raw-md5 hash.txt
Loaded 1 password hash (Raw MD5 [SSE2i 10x4x31])
123456789 (1)
guesses: 1 time: 0:00:00:00 DONE (Mon Jan 7 21:39:39 2013) c/s: 7486 trying:
123456 - boomer
Use the "--show" option to display all of the cracked passwords reliably
C:\Pentest\passwords\john\run>_
```

Yang bertanda merah adalah password login asli sebelum di md5 yakni 123456789

Berate dapat kita simpulkan login dari website target adalah :

Username : admin

Password : 123456789

Hacking System

Selanjutnya dalam hacking system kita dapat melihat isi dalam dari website korban, ingat jangan untuk di ubah sekali lagi kita hanya untuk memperingati kelemahan pada website korban bukan untuk merusak !!!

Lihat gambar, kita login dengan username dan password tadi yang sudah kita crack dengan john the ripper.



Maka akan terlihat dengan jelas halaman login dari isi website tersebut. Jika anda setelah login



KELOLA BUKU TAMU		
1	Mantap..., kembangkan lagi dan update informasi tentang sekolah.... Salam kangen kepada bapak ibu guru sekalian... Semoga SMP 18 tambah maju dan sukses selalu..... manjadi SMP terbaik di kota Bengkulu...	Hapus
2	SMP Negeri 18 is the best	Hapus
3	1	Hapus
4	1	Hapus
5	1	Hapus
6	1	Hapus
7	1	Hapus
8	1	Hapus
9	1	Hapus
10	1	Hapus

Terpampang dengan jelas gambar di atas halaman menu admin dari website. Anda bisa memperigati admin tersebut dengan meninggalkan jejak dan ingat sekali lagi tutorial ini bukan untuk merusak system 😊

Penutup

Demikian tutorial yang kami buat, semoga dapat bermanfaat dan memberikan pelajaran terhadap system keamanan website yang kita buat. Salaman network security.

Spesial Thankyou buat anak-anak network security

Ungke Wyethman

Roy Fauzan

Beni Anwar

Iga Wienh Kaol Gathzo

Ariez Coelz

Pak Camat (Pak RT)

Muhammad Yusuf Maulana Ratmaja

Katon

Dan rekan-rekan dari blue_code Network Security yang tidak bisa di sebutkan satu-satu tanpa mengurangi rasa hormati kami ke kalian :)

08-Januari-2013