17

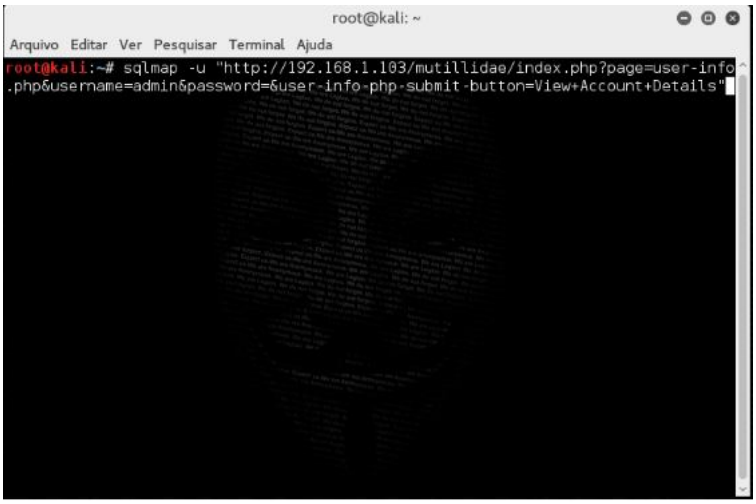
Mãos à obra: Sqlmap

Clique na aba:

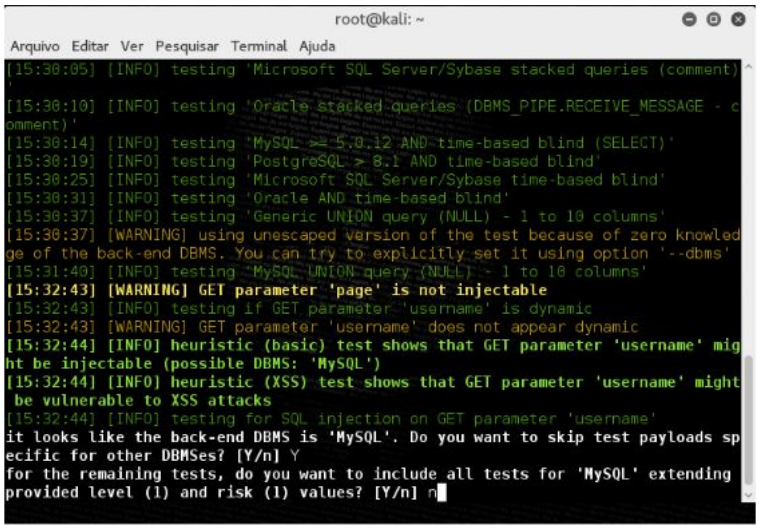
OWASP 2013 -> A1 - Injection (SQL) -> SQLi Extract Data -> User Info (SQL).

Insira nos campos de username e password um valor qualquer, veja que o *form* dessa página está utilizando a requisição GET e os parâmetros aparecem na URL.

Copie esta url e vá até o terminal e digite: sqlmap -u [url]



Caso o programa encontre um banco e peça para pular os testes para os demais, confirme digitando Y e em seguida se perguntar se queremos incluir todos os testes para MySQL dizemos que não, digitamos n.



Ele mostrou qual o banco de dados (MySQL, Oracle, PostgreSQL) a aplicação está usando?

Obs importante: Se o sqlmap perder conexão e não retomar os testes, assista o vídeo *SQLMAP - Informações adicionais* e faça a mesma configuração que eu fiz. Uma vez terminado esse teste, volte as configurações como estavam no início do vídeo (Placa em modo Bridge), pois os outros exercícios nesse curso vão precisar dessa configuração. A configuração mostrada nesse vídeo *Sqlmap_info_adicional,* só vai funcionar se o Kali Linux e o servidor estiverem instalados no mesmo computador.

NÃO USE O SQLMAP em sites que estão na Internet