eSecurity

Treinamentos em Segurança da Informação

O que temos pra hoje?

Temas de Hoje:

- **SQLMAP Avançado**
  - Buscando Vulnerabilidades no Google
  - Automatização e Alarme
  - Trabalhando com Cookies
  - Trabalhando com RequestFile
  - Trabalhando com Threads

SQLMap avançado

SQLMAP: Buscando no Google

É possível utilizar o SQLMap para fazer buscas no Google através de Dorks e automaticamente efetuar os testes de intrusão para nós.

Utilize a opção –g e acrescente também a opção –gpage

Exemplo:

sqlmap –g “inurl:noticias.php?id=“ –gpage=3 –v 2

Explicação:

-g = Utiliza o Google como site de busca utilizando a dork inurl
-gpage = Seleciona a página do google ao qual quer realizar o ataque, caso não sete essa opção, ele fará na primeira página.
-v = Modo Verbose, ele irá apresentar todo o resultado em tela. Foi setado o nível 2 para trazer mais resultados do que a opção –v tradicional

SQLMAP: Automatização e Alarme

Enquanto você deixa rolar os testes, poderá utilizar a opção --beep para alerta-lo quando encontrar uma vulnerabilidade, enquanto isso, poderá ir jogar um vídeo game ou até mesmo tirar um cochilo.

Mas não se esqueça que deverá ter em seu computador o Speeker funcionando.

Além disso, poderá fazer com que o SQLMAP não te faça perguntas, respondendo de forma padrão qualquer pergunta que ele te faça.

Utilize as opções:
--beep – Alerta sonoro ao encontrar uma vulnerabilidade
--batch – Não te faz perguntas e executa o processo com respostas padronizadas.

SQLMAP: Trabalhando com Cookies

Quando realizamos os testes na mão, muita coisa fica mais difícil, porém, quando trabalhamos com Cookies, o processo manual é mais fácil, afinal, podemos logar em determinadas páginas e testarmos sua segurança durante o tempo de vida do cookie.

Mas, quando estamos usando o SQLMAP, isso fica mais difícil, ou seja, não estamos logados na página, sendo assim, será necessário manipular os cookies para que ele possa automatizar a varredura para você.

Exemplo de uso:

```
sqlmap -u "http://alvo.com/?id=1&Submit=Submit#" --cookie='security=low;
PHPSESSID=rdqa8gsi69qhhadtk32i9igup7'
--dbs
```

SQLMAP: Trabalhando com Request File

O SQLMap trabalha com arquivos de requisições, sendo assim, poderá facilitar a sua vida na hora de realizar um pentest.
O BurpSuite ou outra ferramenta poderá gerar as requisições ao servidor em um arquivo, sendo assim, o SQLMap irá ler este arquivo e fará as devidas configurações para o ataque.

Exemplo de uso:

```
sqlmap -r arquivo.txt --dbs
```

SQLMAP: Trabalhando com Threads

Quando você utilizar o SQLMAP de forma padrão, ele efetua apenas uma requisição a cada ataque. Você pode mudar o número de requisições ao servidor, porém, quanto maior o número de requisições, mais fácil fica a sua identificação e o consumo de link.

É recomendado utilizar esta opção apenas em casos de Pentests autorizados e sem a utilização de um Firewall.

Exemplo de uso:

```
sqlmap –u “http://www.alvo.com/noticias.php?id=1” –dbs --threads=5
```

printf ("\Chega por hoje\n");

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker