eSecurity

Treinamentos em Segurança da Informação

O que temos pra hoje?

Temas de Hoje:

- **SQLMAP Avançado**
  - Alternando entre técnicas
  - Trabalhando com Formulários
  - Respostas pré definidas
  - POST Methods
  - Trabalhando com SQLQUERY
  - Checando a existência de WAF

SQLMap avançado

SQLMAP: Alternando entre técnicas

Existem 5 tipos de técnicas que podemos utilizar para realizar uma invasão por SQLi, o SQLMAP usa por padrão todas as 5, porém, você pode selecionar cada uma separadamente com a opção **--technique**.

- **Boolean-based blind**
  - com base nas mudanças de página, os dados são inferidos, caractere por caractere
- **Error based**
  - usa os erros que são exibidos para extrair dados
- **Union query-based**
  - mudanças de consultas SQL para extrair dados
- **Stacked queries**
  - ponto e vírgula são usados para injetar várias declarações sobre a consulta SQL
- **Time-based blind**
  - com base no tempo, os dados são inferidos, char por caractere

Exemplo de uso:

sqlmap –u ‘alvo.com/index.php?noticia=1’ --tecnique=SU

Você irá preencher apenas as iniciais das técnicas, sendo assim, todas juntas equivale a opção BEUST

SQLMAP: Trabalhando com Forms

Muitas vezes nos deparamos com sites que possuem vulnerabilidades em formulários, sendo assim, páginas que possuem formulários extensos, possuem uma maior probabilidade de sofrerem injeção SQL.

Para trabalhar com formulários, usa-se a opção --forms

Exemplo de uso:
sqlmap –u “alvo.com/cadastro.php” --forms --dbs

SQLMAP: Respostas pré-definidas

Falamos na aula passada sobre a opção --batch, que dá as respostas automáticas às perguntas do SQLMAP, porém, temos também que nos atentar, que, nem todas as respostas são positivas ou seguem o padrão sugerido pelo sistema.

Podemos também dizer quais sãos respostas de nossa preferência com a opção --answers.

Exemplo de uso:

sqlmap –u “alvo.com/cadastro.php” --answers=“quit=N,follow=N” --dbs

SQLMAP: POST Methods

Já sabemos que podemos trabalhar com 2 tipos de requisições no SQLMAP, o método padrão é GET, porém, caso precisemos usar o método POST, devemos utilizar algumas sintaxes adicionais como o --data e o -p.

Exemplo de uso:

sqlmap –u “alvo.com/cadastro.php” --data=“login=admin&senha=teste” –p login

A opção --data refere-se ao formulário que será explorado, porém, acompanhado da opção –p irá dizer ao SQLMAP qual é o campo que possui a vulnerabilidade.

SQLMAP: Trabalhando com SQL Query

Query é o processo de extração de informações de um banco de dados e sua apresentação em forma adequada ao uso.
Pode utilizar diversas Querys para facilitar nossa vida no processo de um pentest.

O principal objetivo da utilização da query no SQLMAP é a alteração ou adição de conteúdo em algum banco de dados.

Exemplos de uso:

```
sqlmap –u “alvo.com/teste.php?id=1” --sql-query "SELECT @@datadir“
sqlmap –u “alvo.com/teste.php?id=1” --sql-query "select now();“
sqlmap –u “alvo.com/teste.php?id=1” --sql-query="select * from reminder"
```

SQLMAP: Checando a existência de WAF

WAF vem de Wep Application Firewall, que é o cara mais chato para o atacante efetuar um ByPass, ou seja, é ele que prejudica o atacante na hora de efetuar uma invasão.
O SQLMAP possui um parâmetro para checar a existência dos principais WAFs, antes de você começar a realizar os testes de intrusão.

Para usar esta opção, adiciona ao SQLMAP a sintaxe: --check-waf

Exemplo de uso:
sqlmap –u “alvo.com/news.php?id=1” --check-waf

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