Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Usando o WPScan

Nessa aula, vamos usar o WPScan para achar as possíveis vulnerabilidade em sites que usam o WordPress. Primeiro passo é achar onde está o *wpscan.rb* em seu Kali Linux. Use o comando locate para isso.

```
# locate wpscan.rb
```

Usando o WPScan

Depois dentro diretório do app, sempre antes que você for usar o WPScan, atualize o seu banco de dados com o comando:

```
# ruby ./wpscan.rb --update
```

Usando o WPScan

Os commandos no WPScan sempre começam com a linguagem

ruby wpscan.rb seguido da URL do seu alvo.

```
# ruby wpscan.rb --url http://seusitealvo.com.br
```

Usando o WPScan

A ação de adicionar o argumento --enumerate vp checa se há alguma vulnerabilidades nos *plugins* de sites WordPress. Essa ação, pode demorar.

ruby wpscan.rb --url http://seusitealvo.com.br --enumerate vp

```
[+] Enumerating installed plugins (only ones with known vulnerabilities) ...
  Time: 00:15:52 <=================                          > (560 / 1417) 39.52%  ETA: 00:24:18
```

Usando o WPScan

Ao colocar a opção --enumerate vt ao comando, você checará se o seu site WordPress contém temas vulneráveis.

```
# ruby wpscan.rb --url http://seusitealvo.com.br --enumerate vt
```

Usando o WPScan

Para descobrir os logins de usuário do seu site, utilize o argumento --enumerate u no final do comando.

```
# ruby wpscan.rb --url http://seusitealvo.com.br --enumerate u
```