Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

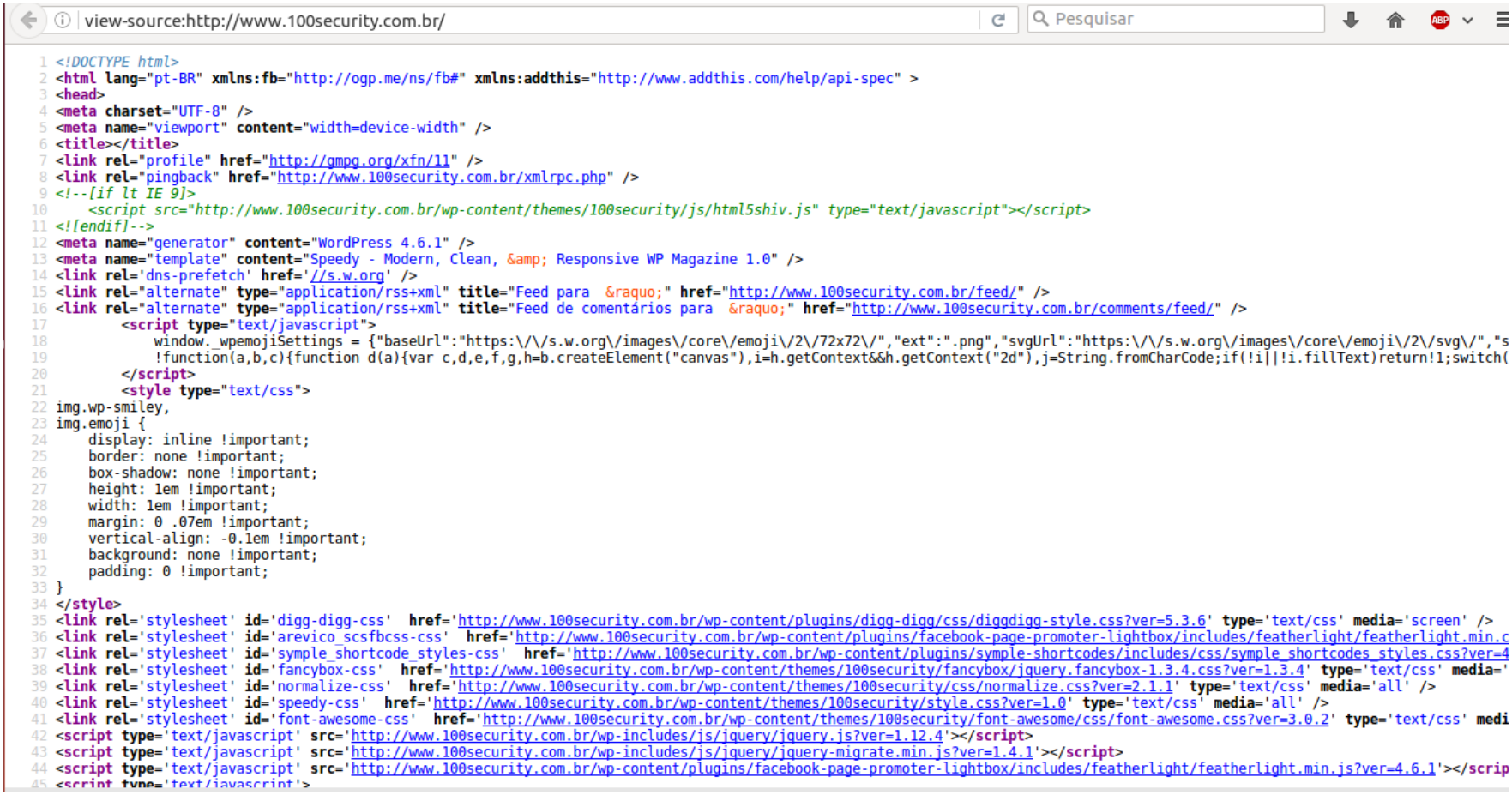
WebSite:http://vmzsolutions.com.br

Nessa aula, vamos explorar um pouco mais de aplicações WEB.

Vamos testar o NMAP

nmap -sS -O www.100security.com.br

Podemos ver o código fonte de uma página, e assim nos revelar algumas informações interessantes.




```
<!DOCTYPE html>
<html lang="pt-BR" xmlns:fb="http://ogp.me/ns/fb#" xmlns:addthis="http://www.addthis.com/help/api-spec" >
<head>
<meta charset="UTF-8" />
<meta name="viewport" content="width=device-width" />
<title></title>
<link rel="profile" href="http://gmpg.org/xfn/11" />
<link rel="pingback" href="http://www.100security.com.br/xmlrpc.php" />
<!--[if lt IE 9]>
    <script src="http://www.100security.com.br/wp-content/themes/100security/js/html5shiv.js" type="text/javascript"></script>
<![endif]-->
<meta name="generator" content="WordPress 4.6.1" />
<meta name="template" content="Speedy - Modern, Clean, &amp;amp; Responsive WP Magazine 1.0" />
<link rel='dns-prefetch' href='//s.w.org' />
<link rel="alternate" type="application/rss+xml" title="Feed para  &amp;raquo;" href="http://www.100security.com.br/feed/" />
<link rel="alternate" type="application/rss+xml" title="Feed de comentários para  &amp;raquo;" href="http://www.100security.com.br/comments/feed/" />
        <script type="text/javascript">
            window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/2\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/images\/core\/emoji\/2\/svg\/","s
            !function(a,b,c){function d(a){var c,d,e,f,g,h=b.createElement("canvas"),i=h.getContext&&h.getContext("2d"),j=String.fromCharCode;if(!i||!i.fillText)return!1;switch(
        </script>
        <style type="text/css">
img.wp-smiley,
img.emoji {
    display: inline !important;
    border: none !important;
    box-shadow: none !important;
    height: 1em !important;
    width: 1em !important;
    margin: 0 .07em !important;
    vertical-align: -0.1em !important;
    background: none !important;
    padding: 0 !important;
}
</style>
<link rel='stylesheet' id='digg-digg-css'  href='http://www.100security.com.br/wp-content/plugins/digg-digg/css/diggdigg-style.css?ver=5.3.6' type='text/css' media='screen' />
<link rel='stylesheet' id='arevico_scsfbcss-css'  href='http://www.100security.com.br/wp-content/plugins/facebook-page-promoter-lightbox/includes/featherlight/featherlight.min.c
<link rel='stylesheet' id='symple_shortcode_styles-css'  href='http://www.100security.com.br/wp-content/plugins/symple-shortcodes/includes/css/symple_shortcodes_styles.css?ver=4
<link rel='stylesheet' id='fancybox-css'  href='http://www.100security.com.br/wp-content/themes/100security/fancybox/jquery.fancybox-1.3.4.css?ver=1.3.4' type='text/css' media='
<link rel='stylesheet' id='normalize-css'  href='http://www.100security.com.br/wp-content/themes/100security/css/normalize.css?ver=2.1.1' type='text/css' media='all' />
<link rel='stylesheet' id='speedy-css'  href='http://www.100security.com.br/wp-content/themes/100security/style.css?ver=1.0' type='text/css' media='all' />
<link rel='stylesheet' id='font-awesome-css'  href='http://www.100security.com.br/wp-content/themes/100security/font-awesome/css/font-awesome.css?ver=3.0.2' type='text/css' medi
<script type='text/javascript' src='http://www.100security.com.br/wp-includes/js/jquery/jquery.js?ver=1.12.4'></script>
<script type='text/javascript' src='http://www.100security.com.br/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1'></script>
<script type='text/javascript' src='http://www.100security.com.br/wp-content/plugins/facebook-page-promoter-lightbox/includes/featherlight/featherlight.min.js?ver=4.6.1'></scrip
<script type='text/javascript'>
```

Tem a ferramenta curl, que também consegue pegar algumas informações legais de sites, banco de dados, linguagem de programação, versão, etc:

```
# curl -vv 100security.com.br -o /dev/null
```

Com o curl, você pode filtrar algumas partes do seu código-fonte de seu site alvo de forma mais rápida:

```
# curl -s http://www.100security.com.br | grep "generator" | grep "meta name"
```