****

**Visão**

Com a crescente demanda sobre Tecnologias, percebemos que muitas pessoas apesar de buscarem informações, não possuem fontes que queiram realmente passar o conhecimento da maneira como ela deve ser, livre e com embasamento técnico que permita ser aplicado e utilizado quando necessário, além de serem testados em sua criação, tornando esta informação útil e confiável.

**Missão**

O Laboratório foi criado com a intenção de buscar e disseminar o conhecimento de uma maneira clara e objetiva, de forma gratuita, auxiliando na evolução dos membros e da sociedade na qual estas informações são compartilhadas, buscando o crescimento de todos os envolvidos nesta criação de valores.



Caso você pense que com a leitura dos materiais da How2Security, você irá se tornar um Cracker capaz de invadir sistemas, se você espera encontrar aqui scripts infalíveis para invasão e, a partir deles, sair por aí invadindo computadores, essa não é a leitura indicada. Indicamos, sim a leitura do Código Penal (Lei 2.848/1940), principalmente a Lei Carolina Dickmann (Lei 12.737/2012), nos Artigos 154-A e 154-B.

*154-A Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:*

*Pena – Detenção, de 3 meses a 1 ano, e multa*

Este material é um conjunto de informações compiladas de documentos e ferramentas do Mundo Underground testadas em ambiente de laboratório na nossa intranet. Desta forma, todo conhecimento aqui condensado é tangível, assim como as orientações das contramedidas.

Dessa forma, esperamos ter sido bem claros que, em momento algum, estamos com a pretensão de ensinar a você como se tornar um invasor. Estaremos sim, mostrando muitas das técnicas utilizadas pelos crackers e, em alguns casos, pelos scripts kiddies, para que você, como administrador de redes, seja capaz de identificá-las em tempo hábil para se defender, antes que alguém com desejos menos nobres ô faça por você.

Assim sendo, todo o conteúdo dessa literatura tem apenas o objetivo didático de informar e preparar os administradores de redes dos novos tempos. Em momento algum nos responsabilizamos pelo mau uso desse conhecimento ou por danos causados em seu equipamento ou de terceiros, assim como também não somos responsáveis pelos códigos e ferramentas aqui citados.

Sandro Melo

Adaptado por Wellington Silva aka Well

**0 – Recon Ativo – Visualizando o Código Fonte**

Podemos começar de forma simples nosso garimpo de informações sobre o sistema alvo. Podemos navegar pelo Web Site da organização alvo. Muitas vezes as páginas web de uma organização fornece uma enorme quantidade de informações que podem ajudar o pen-tester. Itens que podem ser do nosso interesse são:

* Endereços da organização;
* Empresas ou entidades relacionadas;
* Notas de fusões e aquisições;
* Números de telefones;
* Normas de privacidade ou segurança que indicam o tipo de mecanismos de segurança em uso;
* Links para outros servidores Web relacionados à organização;
* Endereços de e-mail com o nome do receptor;
* Notas e comentários no código fonte das páginas Web.

Experimente examinar o código-fonte HTML em busca de comentários. Muitos itens não disponíveis à consulta pública são colocados entre as tags ***<!-- ... -->*** de comentário HTML. Outras linguagens também trazem suas tags de comentário.

Para visualizar o código-fonte da página web, utilizando o browser Firefox, clique com o botão direito do mouse e selecione **View Page Source** (Visualizar Fonte da Página).

Devemos pesquisar o código-fonte em busca de dados de entrada, em seguida tente colocar valores possivelmente perigosos de entrada, tais como tags HTML ou JavaScript, e veja se eles são exibidos diretamente no código-fonte sem modificações. Em caso, positivo, este é um sinal de advertência.

Observe a quantidade de informações que são passados via comentários na aplicação.

**1 – Visualizando o Código Fonte HTML de uma Página**

Depois de visualizar a página Web no browser, o próximo passo é visualizar o código fonte.

Recomendo fortemente o uso do Firefox, pois os outros browsers costumam bloquear o ataque inloco dificultando a vida do testador.

Para visualizar o código fonte no navegador basta clicar com o botão direito do mouse na página Web e selecionar View Page Source (Visualizar fonte da página).

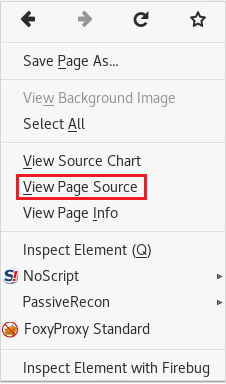


Figura 01 – View Page Source

Outra razão para o uso do Firefox é a sua exibição coloridas das tags e os atributos HTML.



Figura 02 – Código Fonte

Acessar o fonte HTML pode nos ajudar com ponto de referência para comparação. As vulnerabilidades da Web mais comuns envolvem fornecer dados de entrada maliciosos para o seu aplicativo Web no intuito de alterar o fonte HTML. Ao testarmos essas vulnerabilidades, a forma mais fácil de verificar se o teste foi aprovado ou não é a verificação do código fonte com relações às alterações maliciosas.

Tente colocar valores possivelmente perigosos como dados de entrada, tais como tags HTML ou JavaScript, e veja se eles são exibidos diretamente na fonte sem modificação. Em caso positivo, este é um sinal de advertência.

**2 – Visualizando o Código Fonte HTML com View Source Chart**

Plataformas mais novas com estruturas de tags gerada automaticamente baseadas em modelos tendem a criar códigos fonte complexos, inibindo a análise manual. Podemos usar uma ferramenta chamada View Sorce Chart, para lidar com essa complexidade.

Para visualizar o código fonte no navegador com o View Source Chart, basta clicar com o botão direito do mouse na página Web e selecionar **View Page Chart**.

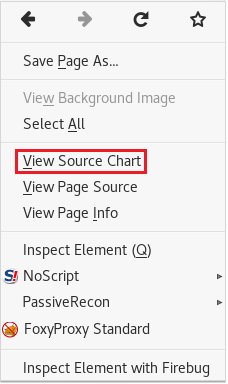


Figura 03 – View Source Chart

Para procurar um determinado trecho de um texto basta clicar CTRL+F e digitar o texto.



Figura 04 – View Source Chart

Para filtrar e excluir porções do site no quadro-fonte, clique na tag HTML na parte superior daquela porção. Outras pesquisas não vão encontrar o texto naquela área.

Muitas vezes ao visualizar o fonte de uma página, serão vistos elementos do frame. Esses frames incluem outra página HTML, ocultada do visualizador de código fonte. Com o View Source Chart, é possível visualizar o HTML de um frame clicando com o botão esquerdo do mouse dentro do frame, antes de clicar com o botão direito do mouse para selecionar View Source Chart. A manipulação de frames gera ataques de XSS. Se vulnerável, ele permite que o atacante crie um frame que engloba toda a página, substituindo o conteúdo real pelo conteúdo malicioso.

Outro conteúdo a ser procurado são os campos ocultos dentro de um formulário. Eles podem ser encontrados pela palavra **hidden**. Esses campos podem ser facilmente manipulados como veremos.

**3 – Referências Bibliográficas**

**[1]** MUNIZ, JOSEPH and LAKHANI, AAMIR – Web Penetration Testing with Kali Linux, 2013, Birmingham – Mumbai, Packet Publishing.

**[2]** GRAVES, KIMBERLY – CEH – Official Ethical Hacker Review Guide, Indianapolis - Indiana, 2007, Wiley Publishing Inc.

**[3]** STUTTARD, DAFYDD and PINTO, MARCUS – The Web Application Hacker’s Handbook, Indianapolis - Indiana, 2º Edition, Wiley Publishing Inc.

**[4]** SCAMBRAY, JOEL, McCLURE, STUART and KURTZ, GEORGE – Hackers Expostos Segredos e Soluções para a Segurança de Redes, São Paulo, 2001, MAKRON Books Ltda.

**[5]** LONG, JOHNNY - GOOGLE HACKING - Para Teste de Invasão [tradução Sérgio Pereira Couto] 2005, DIGERATI (BOOKS).

**[6]** MELO, Sandro – Estudo de Técnicas para Exploração de Vulnerabilidades em Redes TCP/IP, 2º Ed, Rio de Janeiro, 2006, Editora Alta Books Ltda.

**[7]** AHARONI, Mati; Offensive Security Lab Exercises - Curso de Pen-Test oferecido pela Offensive Security, 2007.

**[8]** SCAMBRAY, Joel; LIU, Vicent; SIMA, Caleb - Hacking Exposed Web Application: Web Application Security Secrets And Solutions – 3ª Edition, New York – 2011, McGraw-Hill.

**[9]** DHANJANI, Nitesh; RIOS, Billy; HARDIN, Brett - Hacking A Próxima Geração – Rio de Janeiro – 2011, Alta Books.

**[10]** HOPE, Paco e WALTER, Ben – Web Segura – Guia de Testes e Soluções, 2009, Rio de Janeiro, Alta Books.