****

**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 – Spider Crawling em WebSites**

O WebScarab é uma ferramenta bem parecida com o Burp Suite e sua maior função é a manipulação dos dados enviado e recebido do servidor Web e o Spider Crawling.

**1 – Sipdering com WebScarab**

Para fazermos o Web Spidering:

1. Configure seu browser para usar o WebScarab como proxy local;
2. Navegue normalmente pela aplicação, acesse todos os links/URLs. Submeta todos os dados de todos os Forms HTML. Faça a navegação com o JavaScript habilitado e desabilitado, assim como, com o Cookie habilitado e desabilitado para analisar o comportamento da aplicação web. Utilize várias configurações de browser (User-Agent) para ver se é habilitado outras funções.
3. Reavalie o sitemap gerado pelo proxy/spider para identificar pontos que você deixou passar e refaça os testes, este é um processo que você deve fazer várias vezes.
4. Oportunamente, enumere o que você já achou e descarte os pontos que não temos interesse ou é irrelevante.

Vamos abrir o WebScarab e configurar o proxy do Browser para passar pelo WebScarab.

Com o Firefox aberto, clique em **Menu🡪Preferences🡪Advanced** em **Connection** clique no botão **Settings**.

Em **Connection Settings**, selecione **Manual proxy configuration**. Em **HTTP Proxy** digite o endereço do proxy, que no nosso caso o WebScarab está configurado para ouvir em **127.0.0.1** na porta **8008/TCP**. Após isso, selecione o checkbox **Use this proxy server for all protocols** e clique em **OK**.

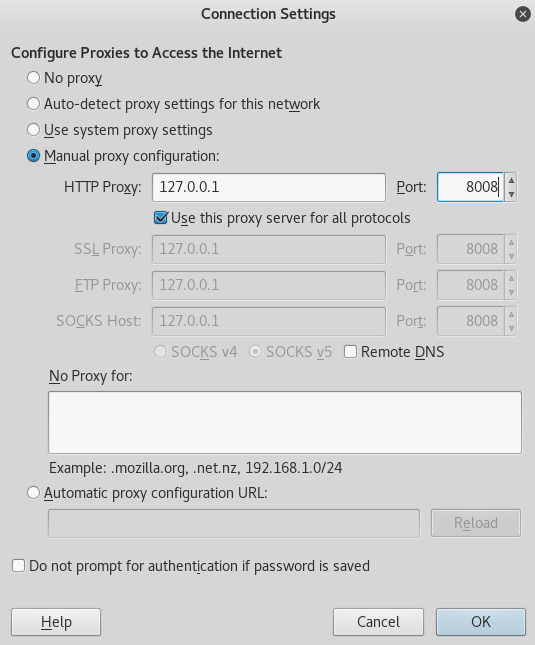
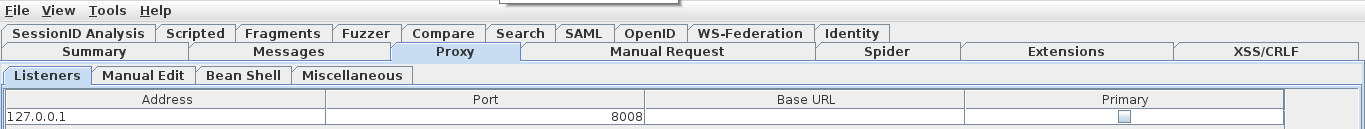


Figura 01 – Configurando o Browser para Proxiar Pelo WebScarab

Agora vá para o WebScarab, clique na aba **Proxy** e certifique-se que o WebScarab está configurado para escutar no endereço de loopback e na porta **8008/TCP**, para isso, clique na sub-aba **Listeners**. Caso não esteja configure ele para trabalhar com essas opções. Com o proxy configurado podemos navegar pelo WebSite para fazermos o spider, para visualizar nosso spider clique na aba Spider.



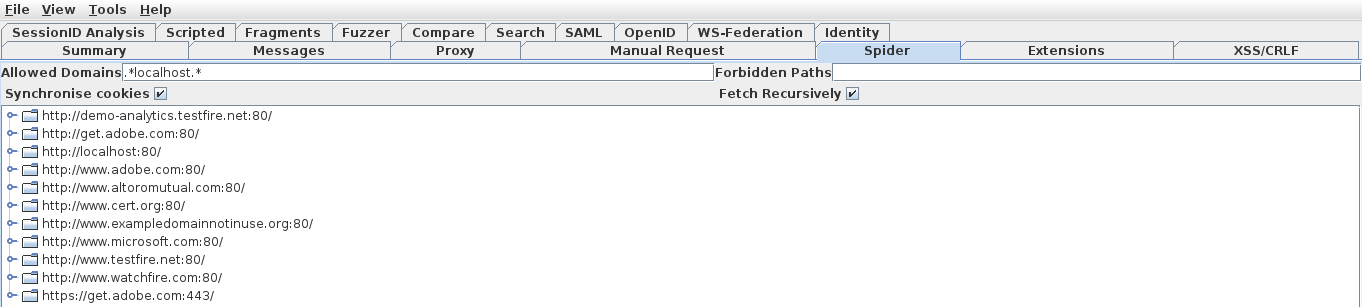


Figura 02 – WebScarab

Na aba **Proxy** e sub-aba **Miscellaneous** selecione os checkbox **Reveal hidden filds in HTML pages**, **Inject know cookies into requests** e **Get cookie from responses**.

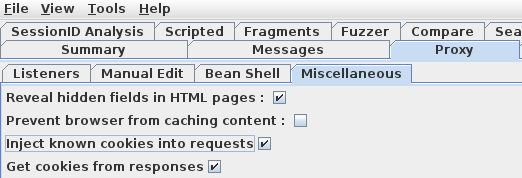


Figura 03 – Configurando o Proxy no WebScarab

Para interceptar as requisições e respostas basta clicarmos na aba **Proxy** e depois clique na sub-aba **Manual Edit** e selecionar o checkbox **Intercept request** e **Intercept Response**.

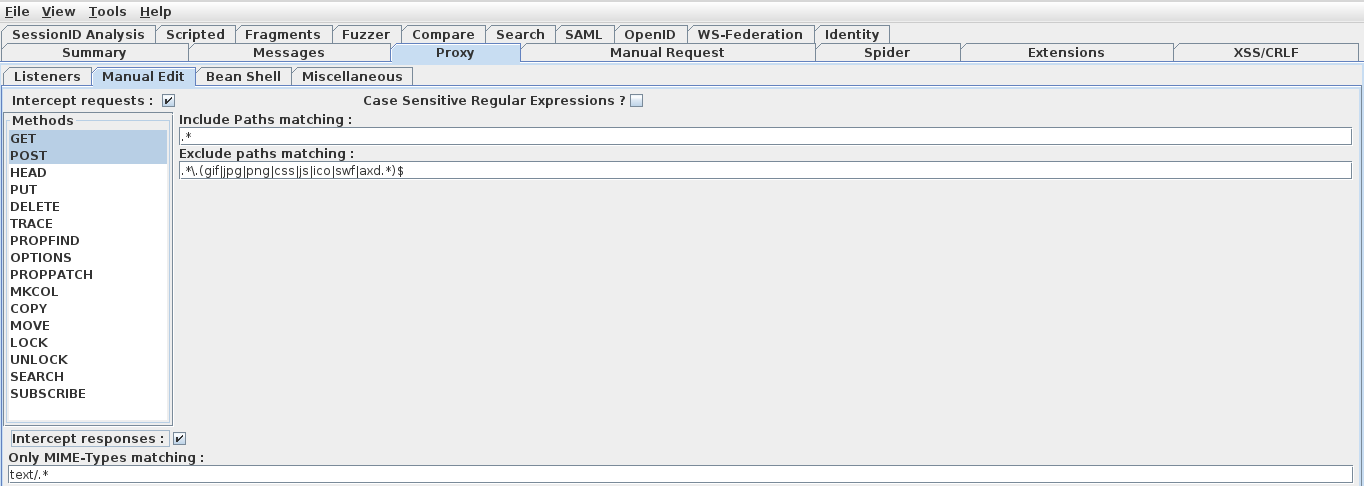


Figura 04 – Intercept Request e Response

Clique duas vezes em qualquer solicitação e você verá todos os detalhes relativos à solicitação dessa página Web.

O WebScarab mostra na própria página os valores de campos ocultos em texto puro, como podemos ver na figura abaixo, facilitando a visualização por parte do testador.

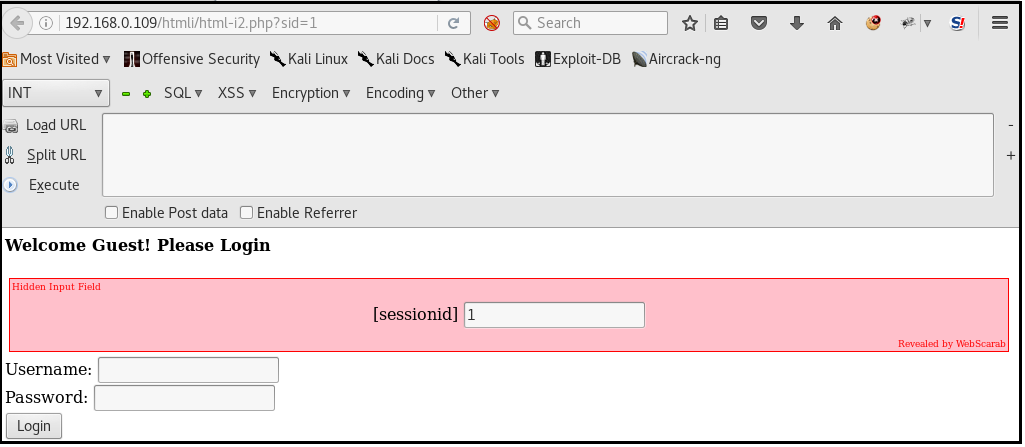


Figura 05 – Campos Ocultos no Formulário

**2 – 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; WALTHER, Ben – Web Segura Guia de Testes e Soluções – Rio de Janeiro – 2009, Alta Books.