Roteiro sobre a ferramenta Burp Suite

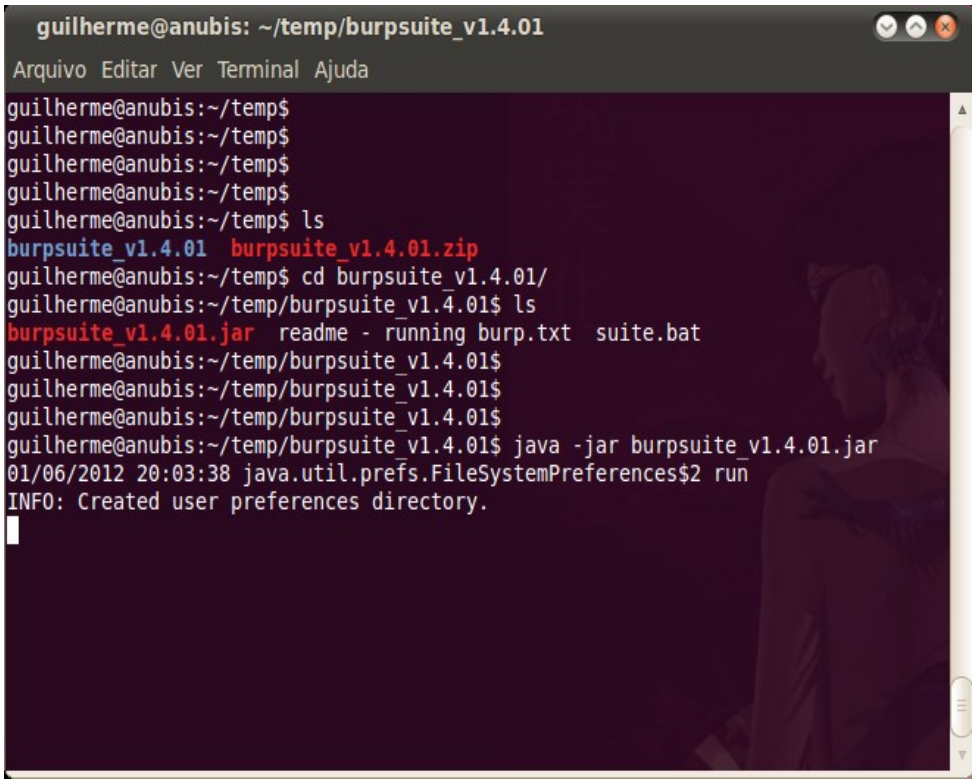
Ferramenta comercial para análise de segurança em aplicações WEB. Desenvolvida na linguagem JAVA, ou seja, pode ser utilizada em vários sistemas operacionais.

Instalação / Utilização:

No site do projeto é disponibilizada uma versão Freeware, com funcionalidades limitadas da ferramenta.

Feio o download, basta descompacta-la em um diretório qualquer, logo em seguida executar:

$ java -jar burpsuite_v1.4.01.jar



Os módulos (funcionalidades):

Proxy – é um servidor proxy HTTP/S que atua como interceptando as informações entre o navegador e a aplicação a qual se deseja testar. Facilitando tarefas de inspeção e alteração das mensagens trocadas em ambas direções.

Spider – é um agente especializado em enumerar o conteúdo das aplicações e funcionalidades.

Scanner – é uma ferramenta avançada disponível somente na versão comercial para descoberta de vulnerabilidades potenciais em aplicações web.

Intruder – é uma ferramenta configurável, para a realização de ataques especializados as aplicações.

Repeater – é uma ferramenta para a manipulação manual de requisições feitas ao servidor, possibilitando analisar a resposta de cada requisição.

Sequencer – É uma ferramenta para análise da qualidade das variações que ocorrem nas sessoẽs das aplicações, ou outros dados importantes que são imprevisíveis.

Decoder – Uma ferramenta para traduzir manualmente ou de forma inteligente os dados das aplicações.

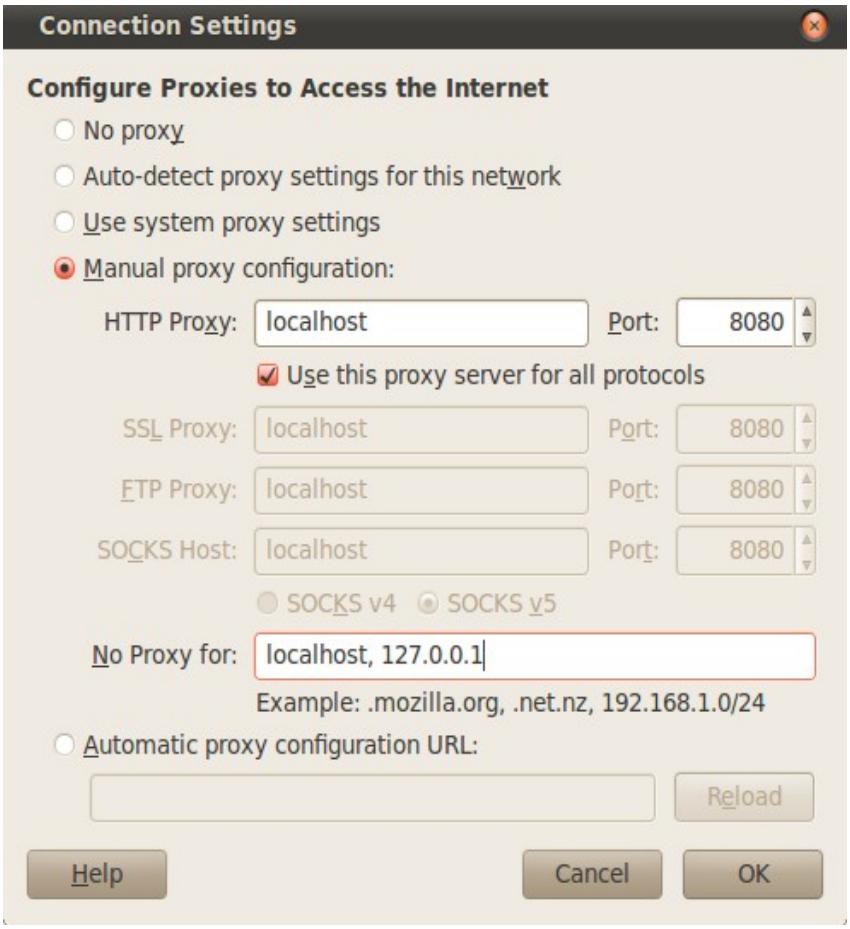
Comparer – Um utilitário para a visualização de dois streams de dados, normalmente relacionados a requisições e respostas.

Documentação:

http://portswigger.net/burp/help/
http://forum.portswigger.net/
http://blog.portswigger.net/

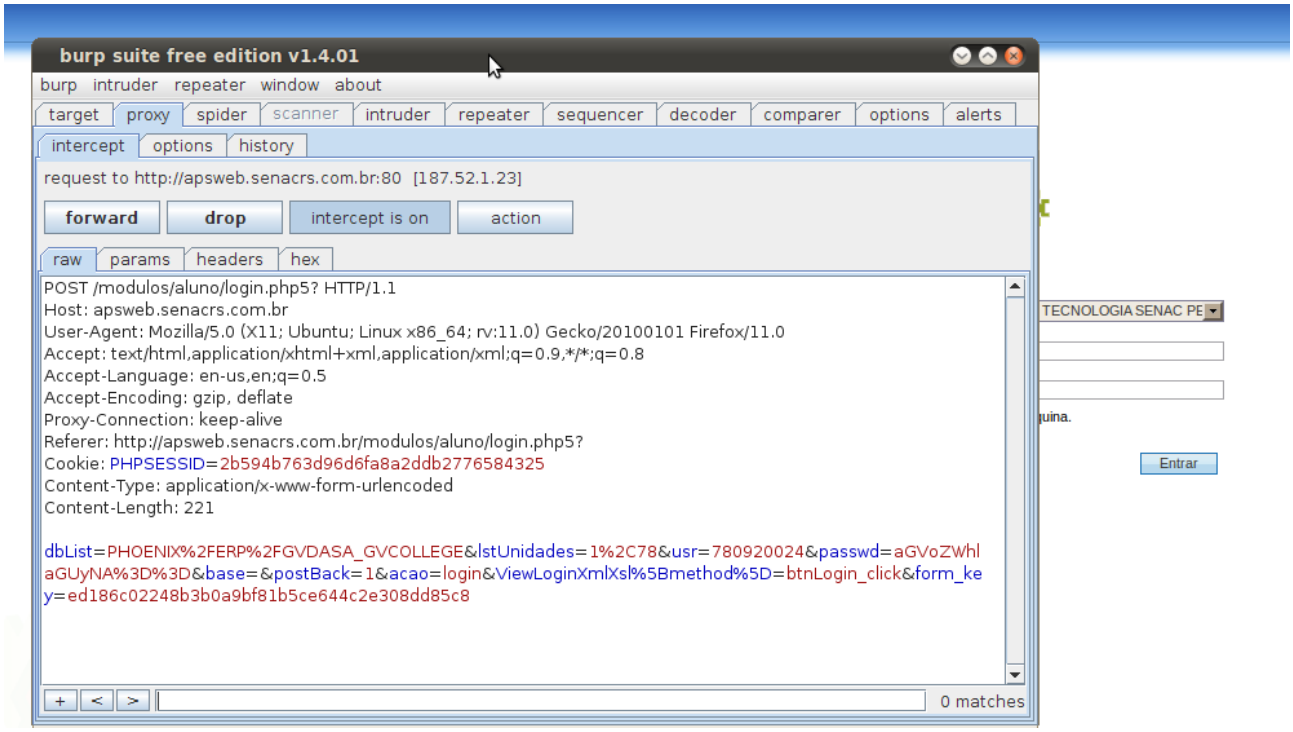
Roteiro:

Assim que a ferramenta é executada, uma porta local no sistema operacional é aberta (padrão 8080) possibilitando utilizar a funcionalidade de proxy. Sendo assim, configuramos o browser para que passe pelo Burp Suite:

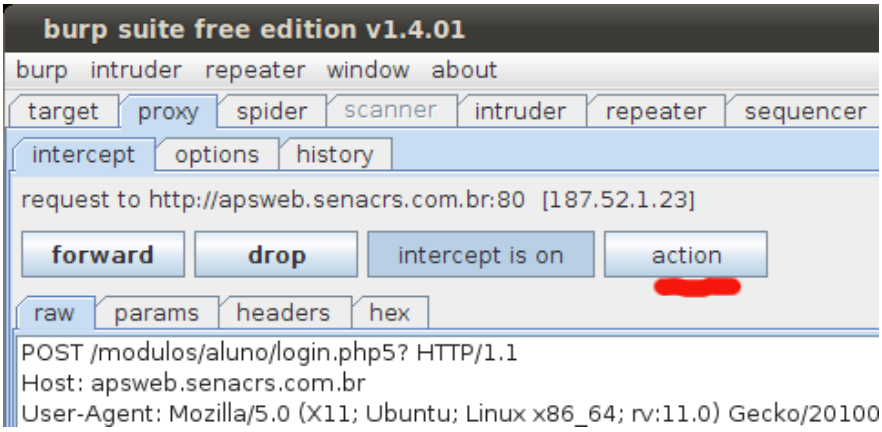


Realizando um ataque de força bruta contra uma aplicação WEB:

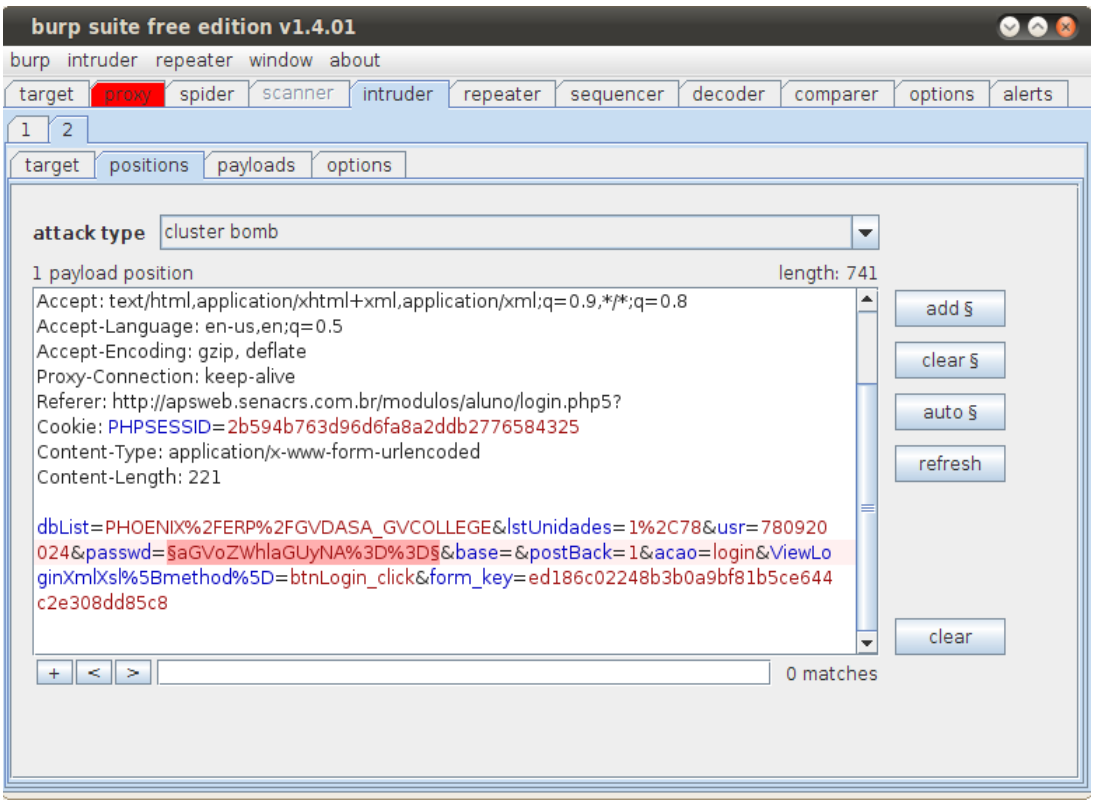
Com o Burp Suite ativado, navegue até o site: www.senacrs.com.br/aluno note que desde a primeira requisição é controlada pelo Proxy. Na tela do proxy avance (Forward) até que fique posicionado a tela de autenticação do portal e logo em seguida simule uma autenticação e não avance a requisição.



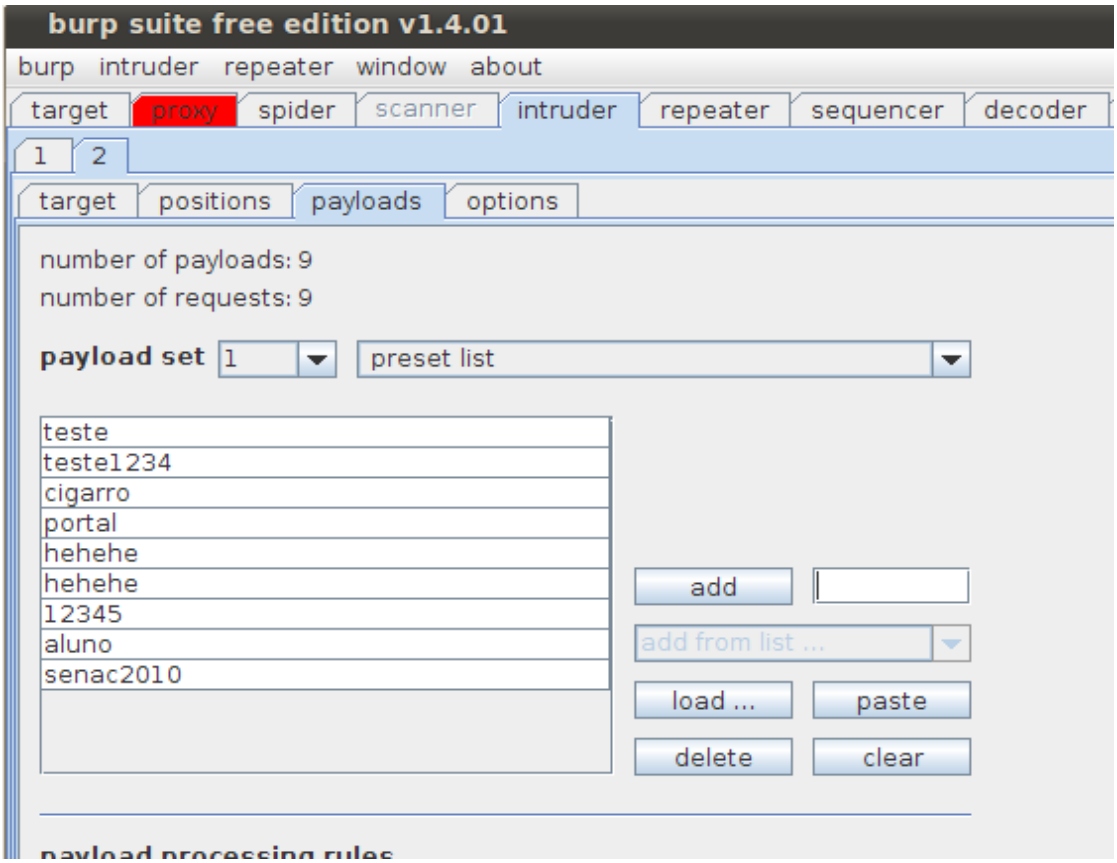
Clique em “Action” e em seguida “Send to Intruder”



Na aba “positions” da ferramenta *Intruder*, desmarque todas as opções clicando em “Clear”. Selecione o valor após a notação **password=** e clique em “Add”. Feito isto troque o tipo de ataque para “cluster bomb”.



Agora vá para a aba “payloads”. Escolha “preset list” e carregue em “load” uma lista de senhas. Na barra do Burp clique em *Intruder* e “start attack” para começar o ataque de quebra de senhas.



Conclusão:

Esta foi uma breve demonstração de como inicar um ataque de quebra de senhas baseado em dicionário de palavas no Burp Suite. Certamente existem técnicas mais avançadas a serem testadas posteriormente.