Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

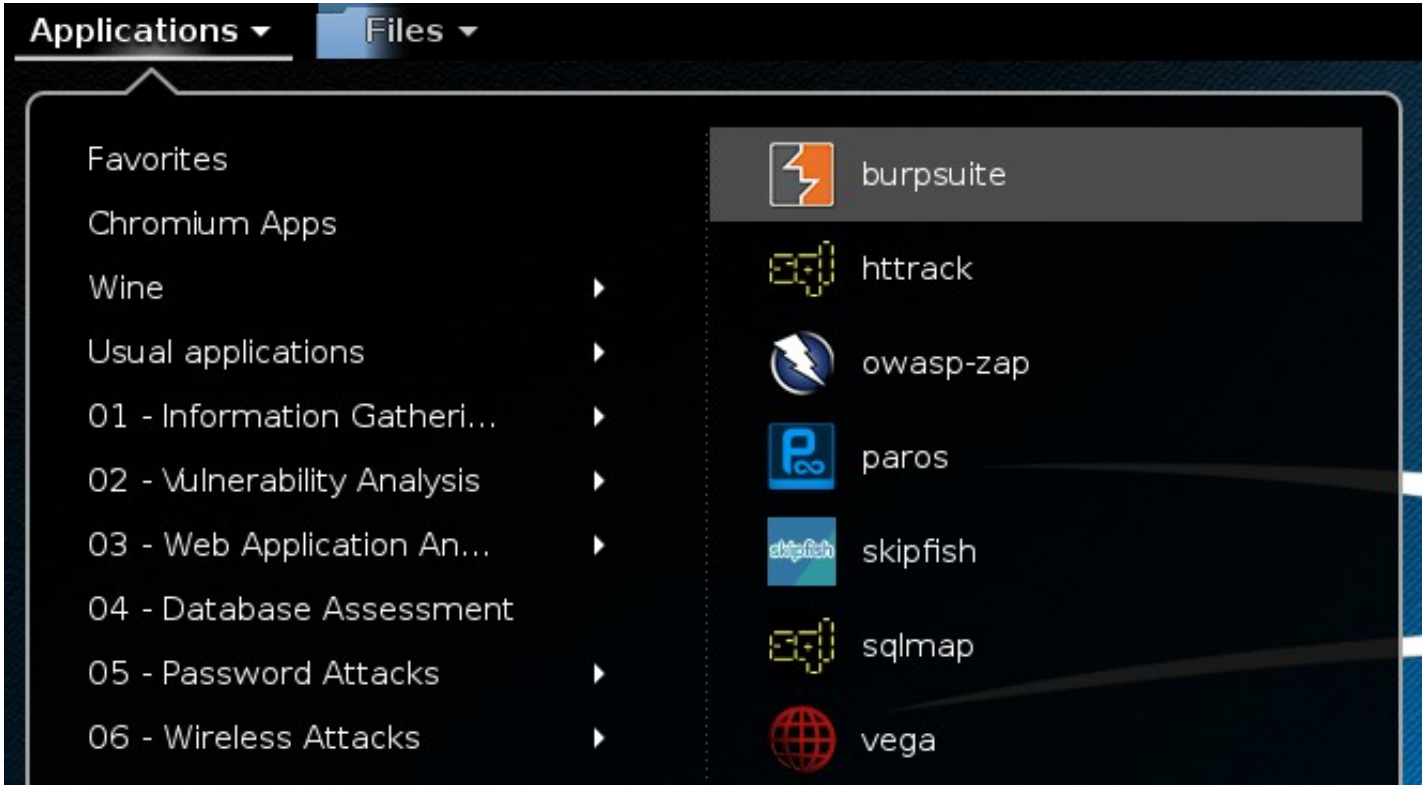
WebSite:http://vmzsolutions.com.br

Burn Suite

Assim como na aula passada, vamos rastrear o site bodgeit usando o Burn Suite, em sua edição free. O Burp é a ferramenta mais utilizada para testes de segurança de aplicativos, pois possui funções semelhantes ao ZAP, com algumas características distintas e uma interface fácil de usar. Burp pode fazer muito mais do que apenas spidering um site.

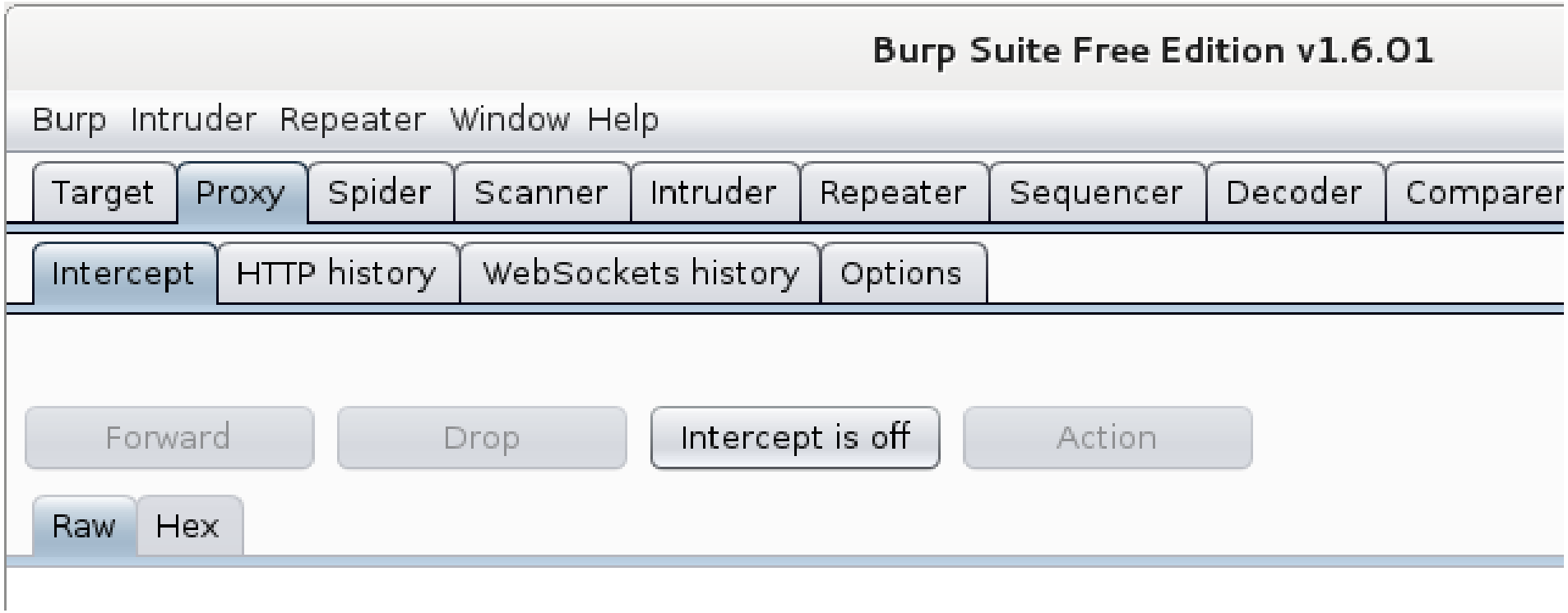
Burn Suite

Vamos abrir o Burn Suite no Kali Linux, ou pode digitar pelo terminal a palavra # burpsuite



Em seguida, configure o navegador para usá-lo como um proxy através da porta 8080, como fizemos anteriormente com o ZAP. O proxy do Burp é configurado por padrão para interceptar todas as solicitações. Precisamos desativá-lo para navegar sem interrupções. Vá para a guia **Proxy** e clique no botão I**ntercept is on**; Ele será alterado para I**ntercept is off**, como mostrado:

Burn Suite


Burp Suite Free Edition v1.6.01
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is off
Action
Raw Hex

Agora, abra no seu navagador o boggeit:

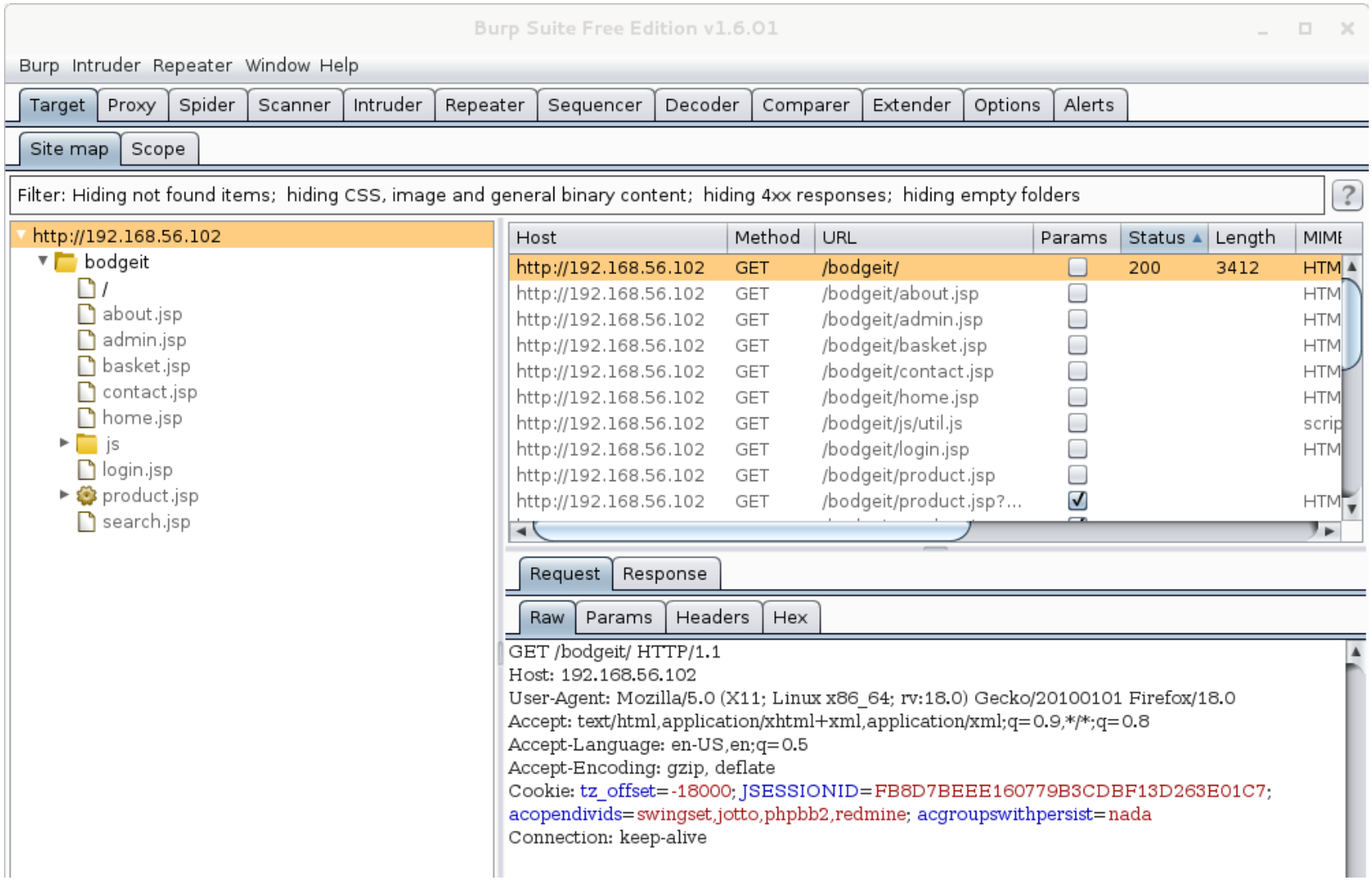
http://192.168.1.163/bodgeit/

Na janela do Burp, quando vamos para a guia Target,

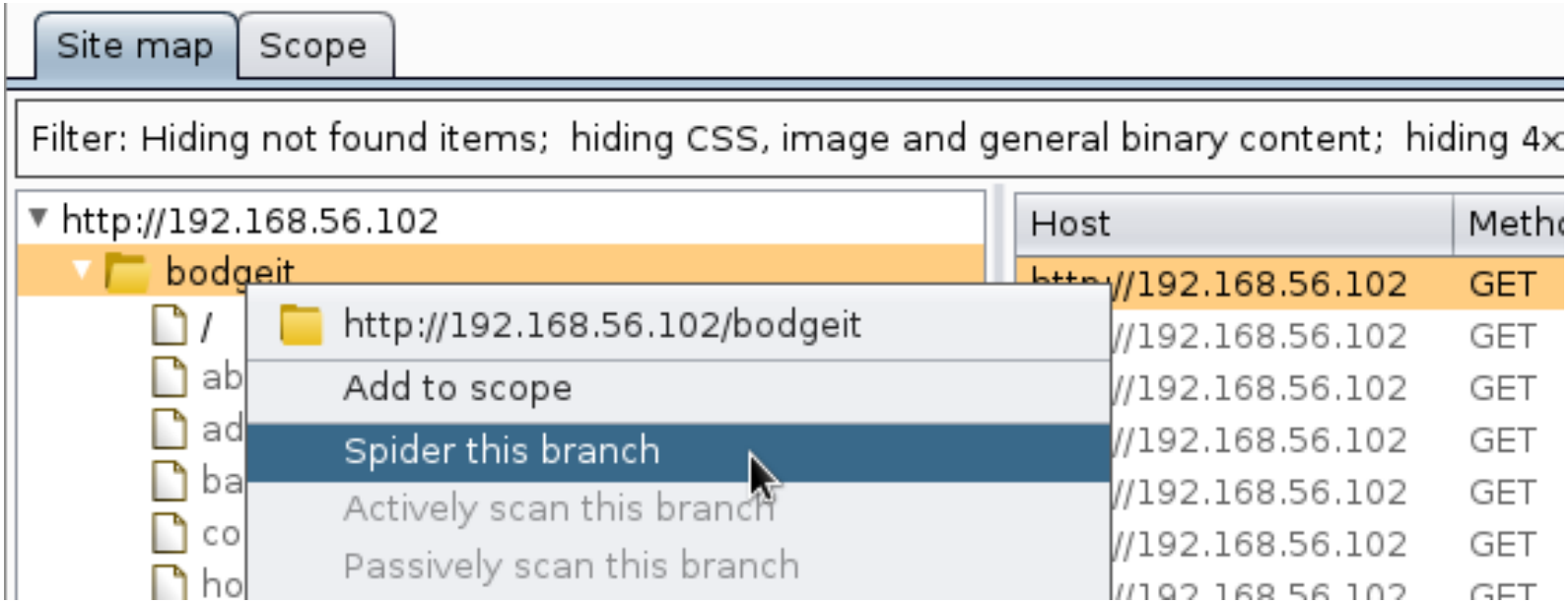
veremos que ele tem a informações dos sites que estamos

navegando e as solicitações feitas pelo navegador:

Burn Suite


Burp Suite Free Edition v1.6.01
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://192.168.56.102
bodgeit
/
about.jsp
admin.jsp
basket.jsp
contact.jsp
home.jsp
js
login.jsp
product.jsp
search.jsp
Host Method URL Params Status Length MIME
http://192.168.56.102 GET /bodgeit/ 200 3412 HTM
http://192.168.56.102 GET /bodgeit/about.jsp HTM
http://192.168.56.102 GET /bodgeit/admin.jsp HTM
http://192.168.56.102 GET /bodgeit/basket.jsp HTM
http://192.168.56.102 GET /bodgeit/contact.jsp HTM
http://192.168.56.102 GET /bodgeit/home.jsp HTM
http://192.168.56.102 GET /bodgeit/js/util.js scrip
http://192.168.56.102 GET /bodgeit/login.jsp HTM
http://192.168.56.102 GET /bodgeit/product.jsp
http://192.168.56.102 GET /bodgeit/product.jsp?... HTM
Request Response
Raw Params Headers Hex
GET /bodgeit/ HTTP/1.1
Host: 192.168.56.102
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: tz_offset=-18000; JSESSIONID=FB8D7BEEE160779B3CDBF13D263E01C7;
acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Connection: keep-alive

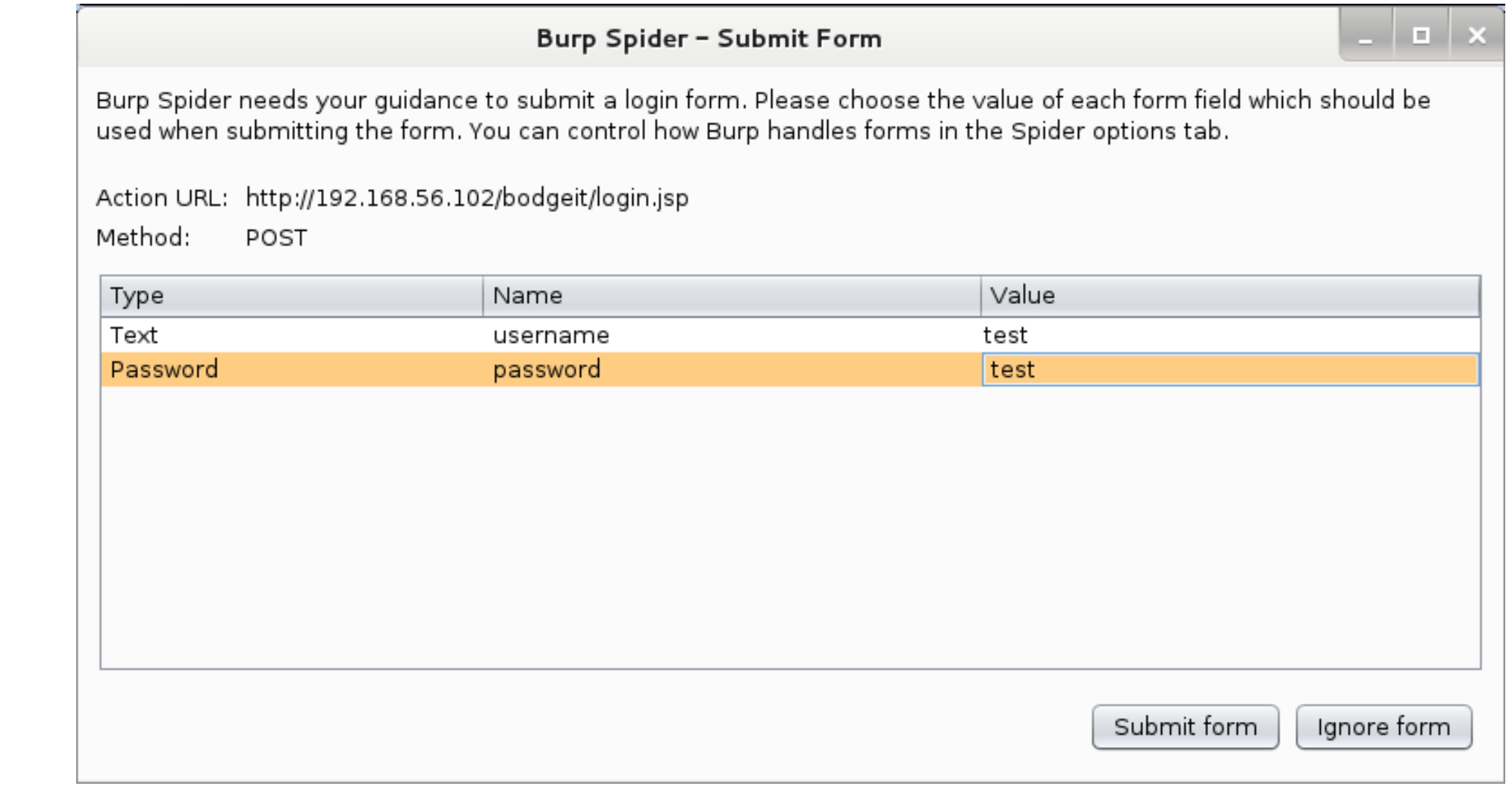
Agora, para ativar o **Spider**, clique com o botão direito do mouse na pasta bodgeit e selecione **Spider this branch**.



O Burp perguntará se queremos adicionar o item ao escopo, clicamos em **Yes**. Por padrão, o spider de Burp rastreia apenas os itens correspondentes aos padrões definidos na guia **Scope** dentro da guia **Target**.

Depois disso, o spider vai começar. Quando ele detecta um formulário de login, ele pedirá as credenciais de login. Podemos ignorá-lo e o spider vai continuar ou podemos enviar alguns valores de teste e o Spider vai preencher esses valores para o formulário. Vamos preencher os campos nome de usuário e senha com a palavra test, em seguida, clique em **Submit form**:

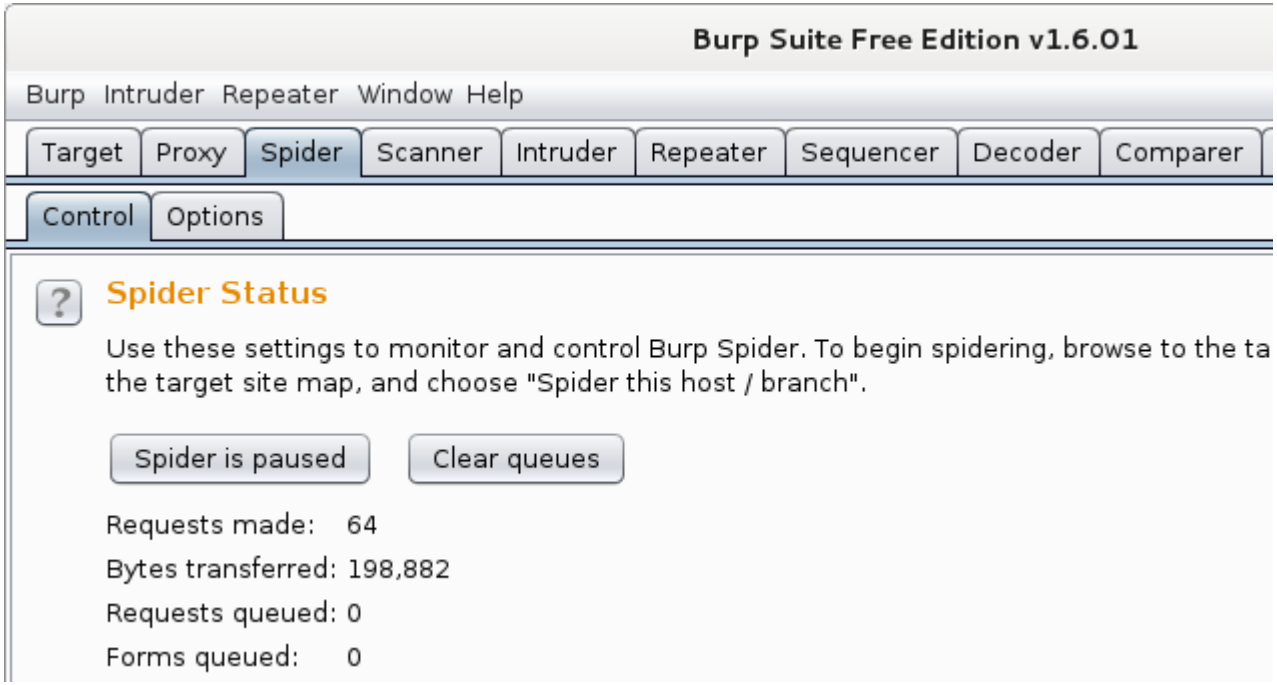
Burn Suite


Burp Spider – Submit Form
Burp Spider needs your guidance to submit a login form. Please choose the value of each form field which should be used when submitting the form. You can control how Burp handles forms in the Spider options tab.
Action URL: http://192.168.56.102/bodgeit/login.jsp
Method: POST
Type
Name
Value
Text
username
test
Password
password
test
Submit form
Ignore form

Em seguida, será pedido para preencher o nome de utilizador e a senha para a página de registo. Ignoraremos este formulário clicando em **Ignore form**.

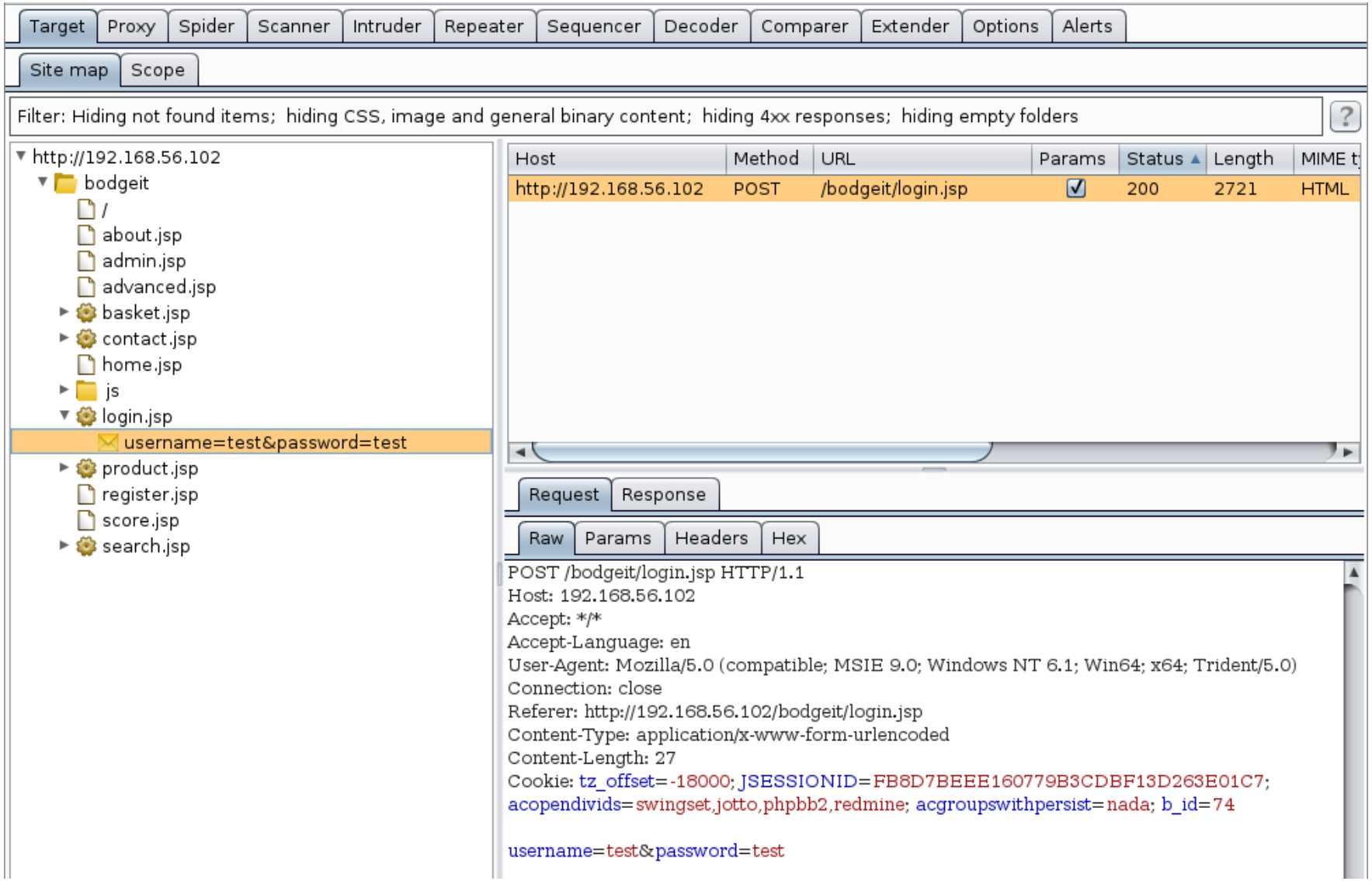
Podemos verificar o status na guia **Spider**. Podemos também pará-lo clicando no botão **Spider is running**.

Vamos pará-lo agora, como mostrado:



Podemos verificar os resultados que o spider está gerando na aba **Site map**, dentro do **Target**. Vejamos o pedido de login preenchido anteriormente:

Burn Suite


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Options
Alerts
Site map
Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://192.168.56.102
bodgeit
/
about.jsp
admin.jsp
advanced.jsp
basket.jsp
contact.jsp
home.jsp
js
login.jsp
username=test&password=test
product.jsp
register.jsp
score.jsp
search.jsp
Host
Method
URL
Params
Status
Length
MIME t
http://192.168.56.102
POST
/bodgeit/login.jsp
200
2721
HTML
Request
Response
Raw
Params
Headers
Hex
POST /bodgeit/login.jsp HTTP/1.1
Host: 192.168.56.102
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Referer: http://192.168.56.102/bodgeit/login.jsp
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Cookie: tz_offset=-18000; JSESSIONID=FB8D7BEEE160779B3CDBF13D263E01C7;
acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; b_id=74
username=test&password=test

O **Burp spider** segue a mesma metodologia que as outras **spiders**, mas funciona de uma forma ligeiramente diferente. Podemos tê-lo em execução enquanto navegamos pelo site e ele adicionará os links que seguimos (que correspondem à definição do escopo) à fila de rastreamento.

Assim como no **ZAP**, podemos usar os resultados de rastreamento do Burp para executar qualquer operação; Podemos executar qualquer pedido, como o scanning (se tivermos a versão paga), repetir, comparar, fuzz, visualizar no navegador, e assim por diante.