

Pentest com Kali Linux





Instrutor: Vitor Mazuco

<http://facebook.com/vitormazuco>

Email: vitor.mazuco@gmail.com

WebSite: <http://vmzsolutions.com.br>



Ao analisar os resultados do spider e testar possíveis entradas para formulários, pode ser útil enviar versões diferentes da mesma solicitação alterando os valores específicos.



O nosso primeiro passo é ir para a guia **Target** e, em seguida, ver a solicitação que o spider fez para a página de login (**`http://192.168.1.163/bodgeit/login.jsp`**), aquela que diz `username = test & password = test`.



Burn Repeater

Clique com o botão direito do mouse na solicitação e, no menu, selecione **Send to Repeater**, conforme mostrado:

Burn Repeater

The screenshot displays the Burp Suite Free Edition v1.6.01 interface. The main window shows the 'Repeater' tab, which is used for sending and managing HTTP requests. The left sidebar shows a site map for the target 'http://192.168.56.102', with a folder named 'bodgeit' containing various files like 'about.jsp', 'admin.jsp', 'advanced.jsp', 'basket.jsp', 'contact.jsp', 'home.jsp', 'js', 'login.jsp', 'product.jsp', 'register.jsp', 'score.jsp', and 'search.jsp'. The 'login.jsp' file is selected, and its corresponding request is highlighted in the main table. The table has columns for Host, Method, URL, Params, Status, Length, and MIME type. The selected request is a POST to '/bodgeit/login.jsp' with a status of 200 and a length of 2721. A context menu is open over the selected request, showing various actions such as 'Remove from scope', 'Spider from here', 'Do an active scan', 'Do a passive scan', 'Send to Intruder', 'Send to Repeater' (highlighted), 'Send to Sequencer', 'Send to Comparer (request)', 'Send to Comparer (response)', 'Show response in browser', 'Request in browser', 'Engagement tools [Pro version only]', 'Compare site maps', 'Delete item', 'Copy URL', 'Copy as curl command', 'Copy links', and 'Save item'. The 'Send to Repeater' option is highlighted with a mouse cursor. The bottom right corner shows a search bar with '0 matches'.

Burp Suite Free Edition v1.6.01

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

Host	Method	URL	Params	Status	Length	MIME type
http://192.168.56.102	POST	/bodgeit/login.jsp	<input checked="" type="checkbox"/>	200	2721	HTML

Context menu options:

- POST: username=test&password=test
- Remove from scope
- Spider from here
- Do an active scan
- Do a passive scan
- Send to Intruder (Ctrl+I)
- Send to Repeater (Ctrl+R)**
- Send to Sequencer
- Send to Comparer (request)
- Send to Comparer (response)
- Show response in browser
- Request in browser
- Engagement tools [Pro version only]
- Compare site maps
- Delete item
- Copy URL
- Copy as curl command
- Copy links
- Save item

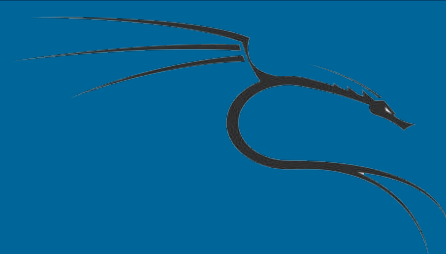
0 matches



Burn Repeater

Agora, passamos para a guia **Repeater**. Clique em **Go** para exibir a resposta do servidor no lado direito:

Burn Repeater



Burp Suite Free Edition v1.6.01

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

1 x 2 x ...

Go Cancel < >

Target: http://192.168.56.102

Request

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=FD47021A589E3B022358A67C67F6F66F; b_id=2
username=test&password=test
```

Response

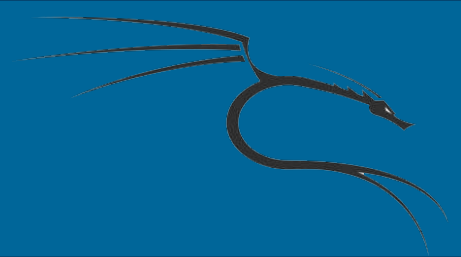
Raw Headers Hex HTML Render

```
<tr>
<td align="left" valign="top" width="25%">
<a href="product.jsp?typeid=6">Doodahs</a><br/>
<a href="product.jsp?typeid=5">Gizmos</a><br/>
<a href="product.jsp?typeid=3">Thingamajigs</a><br/>
<a href="product.jsp?typeid=2">Thingies</a><br/>
<a href="product.jsp?typeid=7">Whatchamacallits</a><br/>
<a href="product.jsp?typeid=4">Whatsits</a><br/>
<a href="product.jsp?typeid=1">Widgets</a><br/>

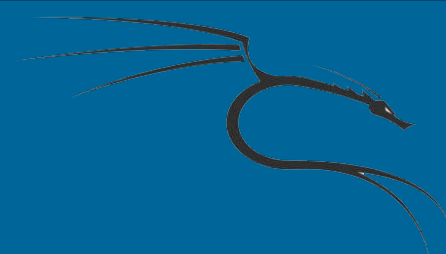
<br/><br/><br/><br/><br/><br/><br/><br/><br/><br/><br/><br/><br/>
</td>
<td valign="top" width="70%">

<p style="color:red">You supplied an invalid name or password.</p>

<h3>Login</h3>
Please enter your credentials: <br/><br/>
<form method="POST">
```



Na seção **Request** podemos ver a solicitação em bruto feito para o servidor. A primeira linha mostra o método utilizado: POST, o URL solicitado e o protocolo: HTTP 1.1. As próximas linhas até o Cookie :, são os parâmetros de cabeçalho; Depois deles temos uma quebra de linha e, em seguida, os parâmetros POST com os valores que introduzimos no formulário.



Na seção **response** temos algumas guias: **Raw**, **Headers**, **Hex**, **HTML** e **Render**. Estes mostram as mesmas informações de resposta em diferentes formatos. Vamos clicar em **Render** para visualizar a página, como será visto no navegador:

Burn Repeater



Target: <http://192.168.56.102>  

Response

Raw Headers Hex HTML Render

The BodgeIt Store

We bodge it, so you dont have to!

Guest user

[Home](#) [About Us](#) [Contact Us](#) [Login](#) [Your Basket](#) [Search](#)

[Doodahs](#)
[Gizmos](#)
[Thingamajigs](#)
[Thingies](#)
[Whatchamacallits](#)
[Whatsits](#)
[Widgets](#)

Login

Please enter your credentials:

Username:

Password:

If you dont have an account with us then please [Register](#) now for a free account.



Podemos modificar qualquer informação no lado da solicitação. Clique em **Go** novamente e verifique a nova resposta. Para fins de teste, vamos substituir o valor da senha por um apóstrofo (') e então enviar a solicitação:

Burn Repeater





Go Cancel < ▾ > ▾

Request

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: 24
Cookie: tz_offset=18000;
JSESSIONID=FD47021A589E3B022358A67C67F6F66F; b_id=2

username=test&password='

Target: http://192.168.56.102  

Response

Raw Headers Hex HTML Render

HTTP/1.1 200 OK
Date: Mon, 13 Jul 2015 17:24:02 GMT
Server: Apache-Coyote/1.1
Content-Type: text/html
Content-Length: 2543
Via: 1.1 127.0.1.1
Vary: Accept-Encoding
Connection: close

System error.

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2//EN">
<html>
<head>
<title>The BodgeIt Store</title>



Como pode ser visto, nós provocamos um erro de sistema alterando o valor de uma variável de entrada. **Isso pode indicar uma vulnerabilidade no aplicativo.**