10

Mãos à obra: Sequestro de sessão - Burp Suite

Uma vez que sequestramos a sessão de nossa pobre vítima, vá até o browser de seu computador e clique no botão **Login/Register** para se logar no sistema como administrador. O usuário e senha são admin e admin.

Posteriormente, vá até o Kali Linux e configure novamente o browser para que a requisição seja passada ao Burp Suite:

Clicar no ícone

-> Preferences -> Advanced -> Network -> Settings -> Manual Proxy Configuration -> IP: 127.0.0.1 -> Porta: 8080

Abra o Burp Suite, vá até a aba *Target->Scope* e adicone a url que será interceptada pelo Burp Suite: *http:// [ip do servidor]*. Posteriormente vá na aba *Proxy -> Intercept* e pressione o botão **Intercept is On**, para que fique **Intercept is off**. Dessa forma, estamos interrompendo a interceptação momentaneamente.

No Kali Linux, vá até a página da mutillidae, clique no botão **Login/Register** e clique no link *Please register here*. Faça o registro com seu nome e senha de preferência. Posteriormente, clique novamente no botão **Login/Register** e faça o login com o usuário e senha que foram criados. Perceba que somos redirecionados para o link: *http:// [ip do servidor]/mutillidae/index.php*

No Kali Linux, clique no botão **Logout** e volte ao Burp Suite, iremos realizar a interceptação para que possamos assim usar a sessão que sequestramos. Vá até a aba *Proxy ->Intercept* e clique no botão **Intercept is Off** para que fique **Intercept is On.**

Volte para o browser do hacker e coloque a url *http:// [ip do servidor]/mutillidae/index.php* e pressione ENTER. O Burp Suite interceptou a requisição.

Vá até o Burp Suite e veja a requisição interceptada. No parâmetro PHPSESSID troque a sessão pelo da vítima (do terminal). Pressione o botão **Forward**.

Volte ao browser do Kali Linux.Qual o resultado?