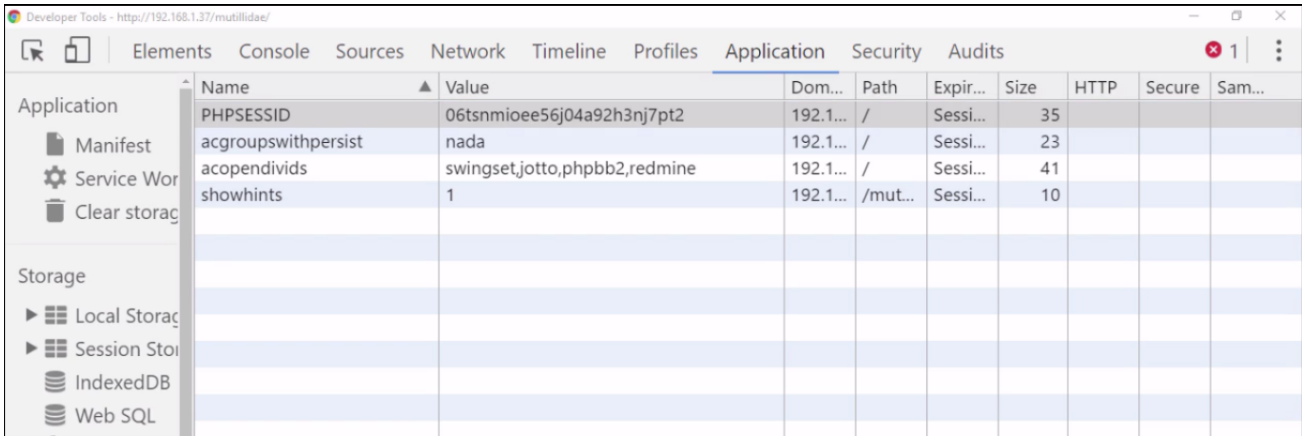
06

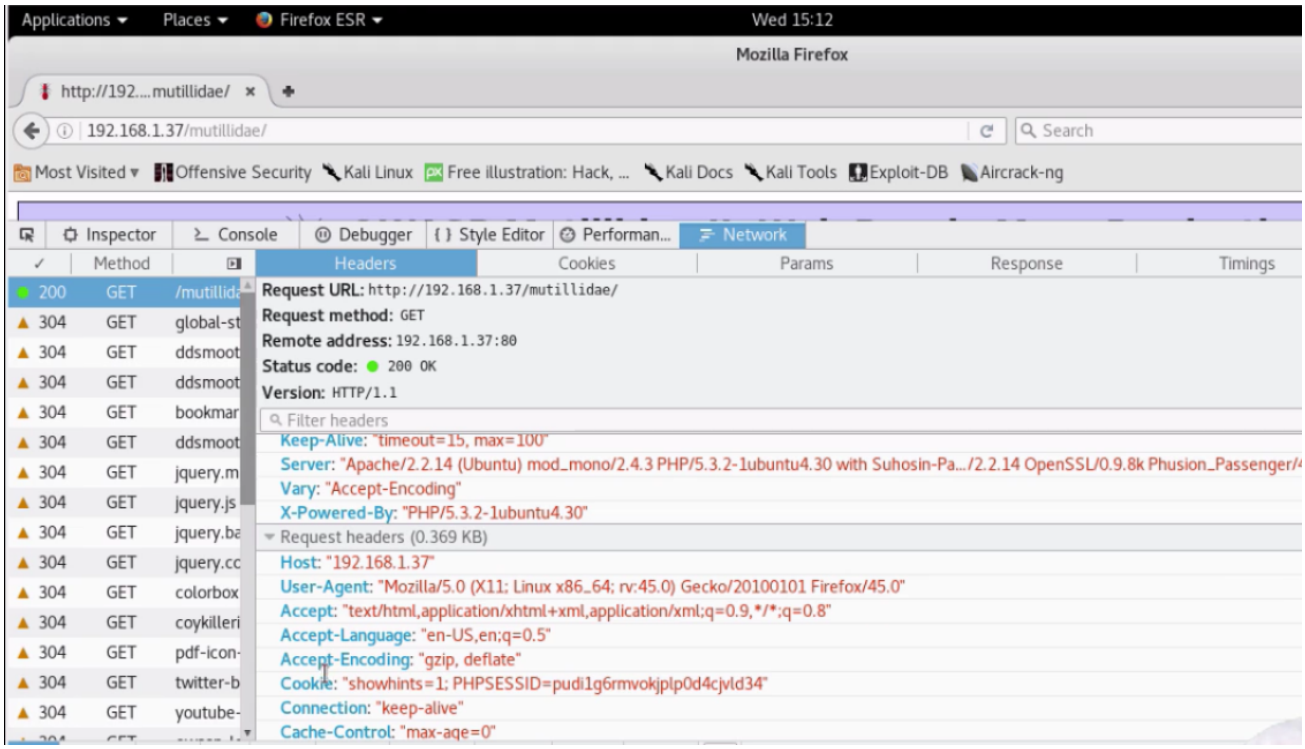
Sequestro de sessão

Transcrição

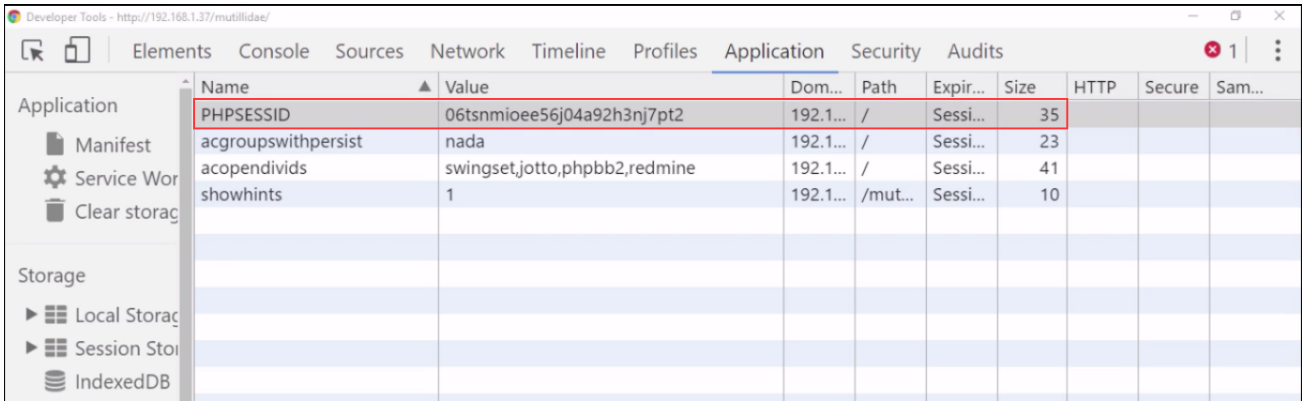
Ao acessar uma URL é feita uma requisição ao servidor e automaticamente é aberta uma sessão, ou seja, um túnel de comunicação. Uma vez que a sessão é aberta é criado um número de identificação, pois o servidor possui uma tabela com chave e valor capaz de identificar o usuário que está enviando a requisição. O complemento da identificação é enviado através de uma resposta, o *Cookie*. Assim, o browser possui um *Cookie* que contem um número de identificação e através dele o servidor identifica quem somos. Resumindo:



Acessando o site do *Multillidae* como hackers verificamos que existe um *Cookie* referente a nosso acesso. Podemos verificar isso clicando com o botão direito do mouse e "Inspect Element(Q) > Network". Apertamos "Reload" para recarregar a página e selecionamos a página *Multillidae* e temos o seguinte:



Podemos verificar, nesse usuário, o item *Cookie* e nele aparece o número de identificação da máquina. Esse número é único, diferente de qualquer outro usuário. Por exemplo, se acessarmos o mesmo site através do *Google Chrome* vamos verificar que o *cookie* possui um número distinto:



Os números são diferenciados pois o próprio servidor identifica que são dois usuários distintos!

Tendo compreendido isso podemos pensar o seguinte: E se o *hacker* conseguisse de alguma maneira ter acesso ao número *cookie* do usuário que acessou pelo *Google Chrome*? E se o hacker inserisse esse número na página do navegador com o intuito de enganar o servidor?

O que aconteceria é que o servidor seria efetivamente enganado, pois entenderia que o hacker é o mesmo usuário referenciado pelo número do **Cookie**, o usuário do **Google Chrome**.

Este fenômeno que acabamos de descrever chama-se **sequestro de sessão**. Vamos efetuar um ataque deste mesmo gênero no próximo vídeo.