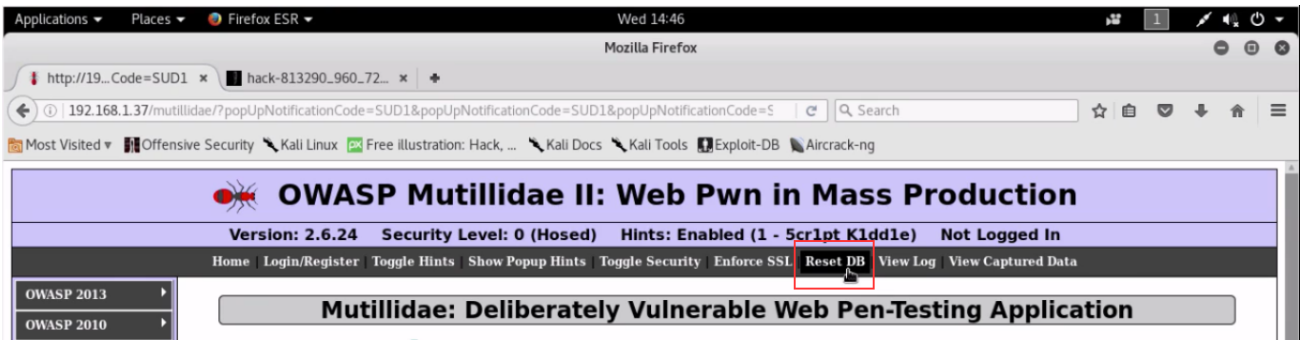
03

Código XSS

Transcrição

Na aula anterior descobrimos que o sistema é vulnerável para *javascript*, então, vamos explorar isso!

Ao retornar a página do Multillidae clicamos na opção que aparece no menu, a "Reset DB":

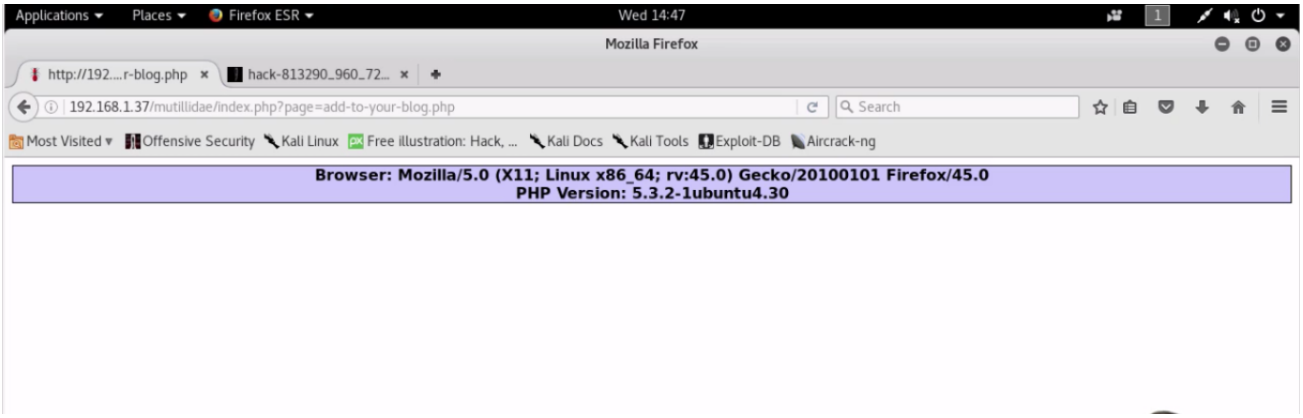


Dessa maneira, o site retorna para suas configurações iniciais, isto é, sem a mensagem do *pop up* inserida pelo hacker. Acessando o Blog em "OWASP 2O13 > A3 - Cross Site Scripting(XSS) > Persistent(Second Order) > Add to your blog" e podemos verificar que ele está normal.

No papel de hacker, nosso desejo é assustar a vítima, portanto, passaremos um script que envie para o usuário uma página em branco! Para fazer isso acrescentamos o seguinte `script`:

```
<script>
document.body.innerHTML="";
</script>
```

Assim, estamos passando a informação de que o `body` é `""`, ou seja, em branco! Feita essa inserção podemos clicar em "Save Blog Entry" e teremos o seguinte:



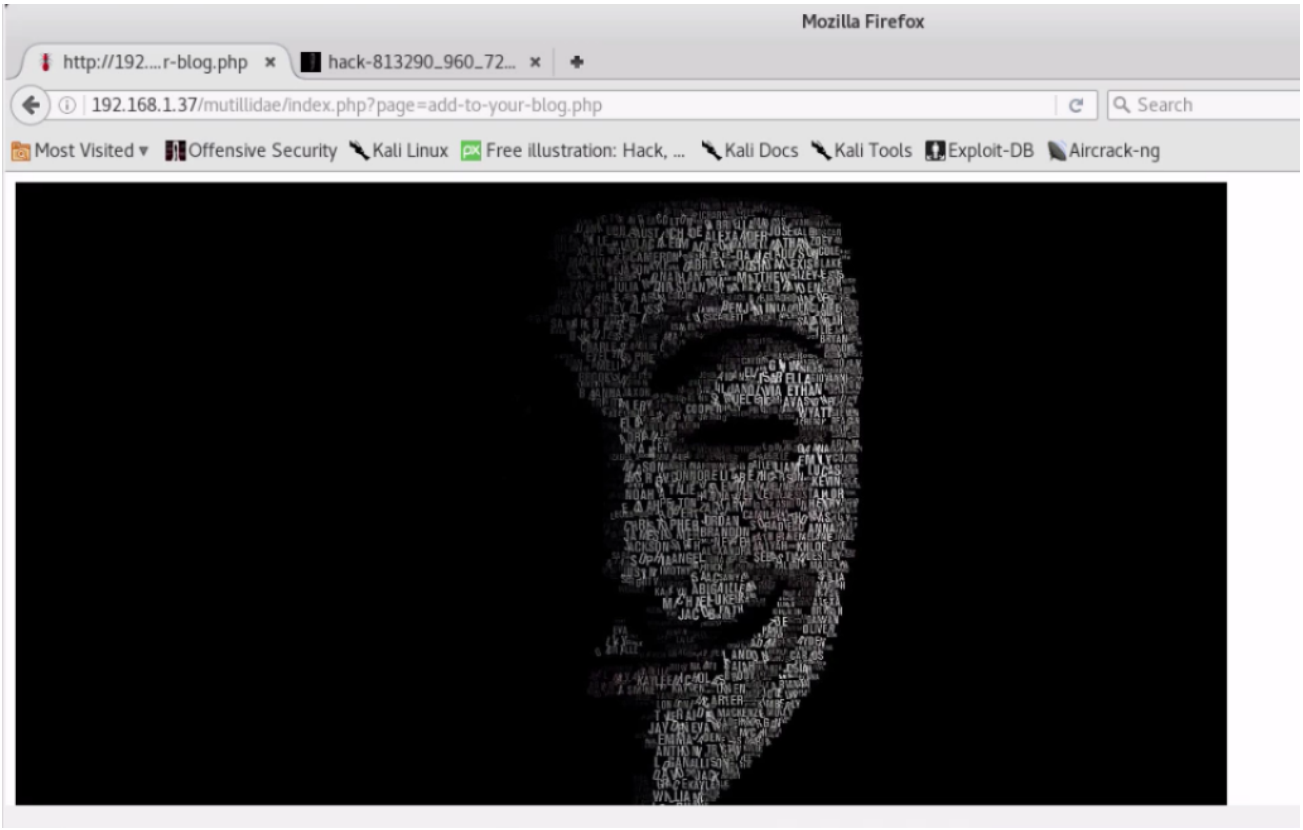
Vamos minimizar a tela do hacker e acessar o site como usuário e ao entrar no Blog encontramos a mensagem em branco da imagem acima!

Podemos, ainda, dar um passo a mais! Vamos fingir que somos do *Anonymus*! Assim, vamos inserir na tela em branco uma imagem referente ao grupo. Para fazer isso voltamos na máquina do hacker e acessamos o site do Multillidae e nele clicamos mais uma vez na aba *Reset DB* para zerar as configurações.

Vamos inserir um código na caixa de comentários, um `script` , como queremos que a tela siga em branco escrevemos `document.body.innerHTML=""` . Também é nossa vontade inserir uma imagem, assim, acrescentamos `var imagem=new Image()` e abaixo disso colocamos o endereço da imagem, `imagem.src="endereço da imagem"` . Finalizamos isso dizendo que a imagem deve permanecer na página, portanto, `document.body.appendChild(imagem)` e fechamos o `script` . Teremos o seguinte:

```
<script>
document.body.innerHTML="";
var imagem=new Image();
imagem.src="https://cd.pixabay.com/photo/2015/06/18/01/46/hack-813290_960_720.jpg";
document.body.appendChild(imagem);
</script>
```

Ao inserir esse código e clicando no "Save Blog Entry" teremos a imagem aparecendo na tela:



Entrando no site como usuário verificamos que ele também visualizará a imagem!